KINNAIRD COLLEGE FOR WOMEN

ADAPTATION OF XAI-FML METHODOLOGY FOR EFFICIENT AND SECURE E-HEALTHCARE SYSTEM

RABIA ABID
F18MPCS009

DEPARTMENT OF COMPUTER SCIENCE
KINNAIRD COLLEGE FOR WOMEN
LAHORE, PAKISTAN
2022

ADAPTATION OF XAI-FML METHODOLOGY FOR EFFICIENT AND SECURE E-HEALTHCARE SYSTEM

A THESIS SUBMITTED TO
KINNAIRD COLLEGE FOR WOMEN
IN FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF

MASTER OF PHILOSOPHY
IN
COMPUTER SCIENCE

BY

RABIA ABID
F18MPCS009

DEPARTMENT OF COMPUTER SCIENCE
KINNAIRD COLLEGE FOR WOMEN, LAHORE
2022

KINNAIRD COLLEGE FOR WOMEN

RESEARCH COMPLETION CERTIFICATE

It is certified that Ms. Rabia Abid of MPhil (session 2018 – 2020), Department of Computer Sciences has carried out research work entitled "Adaptation of XAI-FML methodology for Efficient and Secure e-Healthcare Systems" under my supervision.

It is assured that research work is original and has not yet been published anywhere else. All changes suggested by examiners during defense are incorporated in this final copy.

Signatures of Internal Supervisor
Dr. Muhammad Rizwan
Lecturer
Kinnaird College for Women
Lahore, Pakistan

Signatures of External Supervisor

Signatures of Head of Department
Ms. Jaweria Manzoor
Assistant Professor
Kinnaird College for Women
Lahore, Pakistan

Dated

KINNAIRD COLLEGE FOR WOMEN

ANTI-PLAGIARISM DECLARATION

I certify that this is my own research work. The work has not, in whole or in part, been presented elsewhere for assessment. Where material has been used from other sources, it has been properly acknowledged. The similarity index of the research report is **4%**. If this statement is untrue and I am found guilty of plagiarism, the punitive actions against me should be taken as per Kinnaird Anti Plagiarism Policy.

Rabia Abid
F18MPCS009
M.Phill in CS
Signature:

Signature of Internal Supervisor

Signature of HOD

ACKNOWLEDGMENT

I am really thankful to my supervisor at Kinnard college for women, Dr. Muhammad Rizwan whose expertise is invaluable in formulating the research questions and methodology. Her continuous support, sagacious advice and keen intuitive criticism pushed me to sharpen my thinking and brought my work to a higher level.

Secondly, I would like to thank Ms. Jaweria Manzoor, H.O.D (Department of Computer Sciences), who always extended her helping hands towards my problems and provided with every facility to undergo this research. Last but not least, I would like to thank my beloved parents, who bore my study expenses as well as my mood swings whenever I went through extreme pressure for meeting deadlines to complete this thesis. Without constant support from all of these people, I would not have been making through.

ABSTRACT

Artificial Intelligence (AI) has been applicable in many sector (like educations, healthcare, businesses, government bodies, etc) to lessen the human effort and to create an ease. All AI based systems have decision support systems (DSS) to help human in all high-pitch and low-pitch situation. As a support system many machines learning (ML) based algorithms helps to make accurate decision according to situation, increase accuracy rate in data classification and enhance the performance of systems. Explainable AI (XAI) has advance feature to enhanced the decision-making feature and improve the rule base technique by using more advance ML and deep learning (DL) based algorithms. In this research we chose e-healthcare systems for efficient decision making and data classification, where quite massive data like patients' health record (PHR), hospitals confidential information, administrative data, research data, physicians' details, and many other. In this research work, we identify the existing gaps in traditional AI and ML based algorithms for efficient e-healthcare systems and trying to overcome it by using XAI and advance ML based algorithm Federated Machine Learning (FML). FML is a new and advance technology which helps to maintain privacy for PHR and handle large amount of medical data effectively. In this context, XAI along with FML increase the efficiency and improve the security also of the e-healthcare systems. The performed experiment shows the efficient system performance by implementing federated averaging algorithm on open source FL platform. The evaluating graphs shows the accuracy rate by taking epochs size 5, batch size 16 and no. of clients 5, which shows higher accuracy rate with (19, $10^{-}4$). To conclude our research, we discuss the future work with still existing some gaps in e-healthcare system like security, price, efficiency, performance evaluation and many other.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
AE	Auto-Encode (term used in artificial intelligence)
AHN	An-isotropic Hybrid Network
ANN	Artificial Neural Networks
ASD	Autism Spectrum Disorder
CAM	Computer Aided Manufacturer
CBR	Case based Reasoning
CFG	Context Free Grammar
CMGE	Counter-factual Multi-granularity Graph Supporting Facts Extraction
CycleGAN	Cycle Generative Adversarial Network
CNN	Convolutional Neural Networks
C-P LOHAM	Cherry Pick Low Overhead Aggregation Model
DARPA	Defense Advanced Research Projects Agency
DDQ-Net	Double Deep Q Network
DNN	Deep Neural Network
DMLA	Distributed Machine Learning Algorithms
DL	Deep Learning
EDNN	Explainable Deep Neural Network
EC	Efficient Communication
EHR	Electronic Health Record
FCN	Fully Convolutional Network
FIS	Fuzzy Inference SYstem
FML	Federated Machine Learning
FMLA	Federated Machine Learning Algorithms
GAN	Generative Adversarial Network
GBM	Glinoblastoma Multi-fome
GSInquire	Graphical Interface Inquire
HC	Health Condition
IoHT	Internet of Health Things
KNN	K-Nearest Networks

LIME	Local Interpret-able Model Agnostic Explanation
LNN	Logistic Neural Network
LR	Linear Regression
LRP	Layer-wise Relevance Propagation
LSTM	Long-Short Term Memory Model
NN	Neural Networks
ML	Machine Learning
MLA	Machine Learning Algorithms
MLP	Mulit-layer Perceptron
MRI	Magnetic Resonance Imaging
PD	Parkinson Disease
PDP	Partial Dependence Plot
PHR	Patients' Health Record
SGD	Stochastic Gradient Descent
SHAP	Shaplay Additive Explanation
SVM	Support Vector Machine
VInet	Visually Interpret Network
VGG16	Visual Geometry Group 16
VBP	Value Based Purchasing
XAI	Explainable Artificial Intelligence

CHAPTER I

INTRODUCTION

1.1 Artificial Intelligence (AI)

Artificial Intelligence (AI) is considered a branch of Computer Science Engineering, which deals with the study of programming [1], computer intelligence systems and intelligent creations. It refers to intelligent computing concepts as human intelligence works [2, 3], where humans are bound due to some biological processes, AI free from it. Either it about human, animals or machines, AI is about all those studies which helps the world to face problems and find appropriate solution for them intelligently. AI used to solve problems, error, defects in the already existing systems. If we look into living lifestyle, AI provides an ease in daily living as well. AI researchers are working to provide an easy method to help human, to reduce their effort and perform all task by using AI based intelligent systems, which helps in problem solving and provide efficient decision-making method [4, 5]. AI is an effective evolution which achieved processing methodologies by using advance computational techniques. AI is not typically bound to provide simple generic pattern for problem solving [6], it helps to provide most possible combination to get accurate results and doesn't stick to particular human intelligence. In modern time, evolution of AI is considered as an amazing intelligence in this era.

AI has been made to lessen human effort and processed large amount data, which human unable to process efficiently. A programmed and intelligent systems have been designed to made computation, decision, and increase accuracy rate, by reducing time consumption and complexity. According to many studies, AI based systems are more efficient. Due to advancement and implementation of AI in real world [7], it becomes applicable in all sectors as shown in figure 1.1.

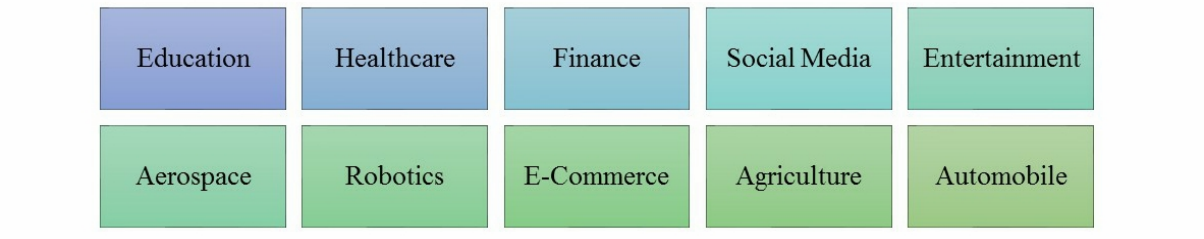


Figure 1.1: Applications of Artificial Intelligence (AI)

AI works by managing large data and perform fast processing, higher accuracy algorithm, easy detection methodology and allows feature to extract at great extent. AI considered as a broader field including theories [8], methodologies [9], technologies as well as machine learning algorithms which helps in efficient decision making and fast data processing. Here figure 1.2. shows the AI based architecture which helps in decision making processing and solving complex problems.

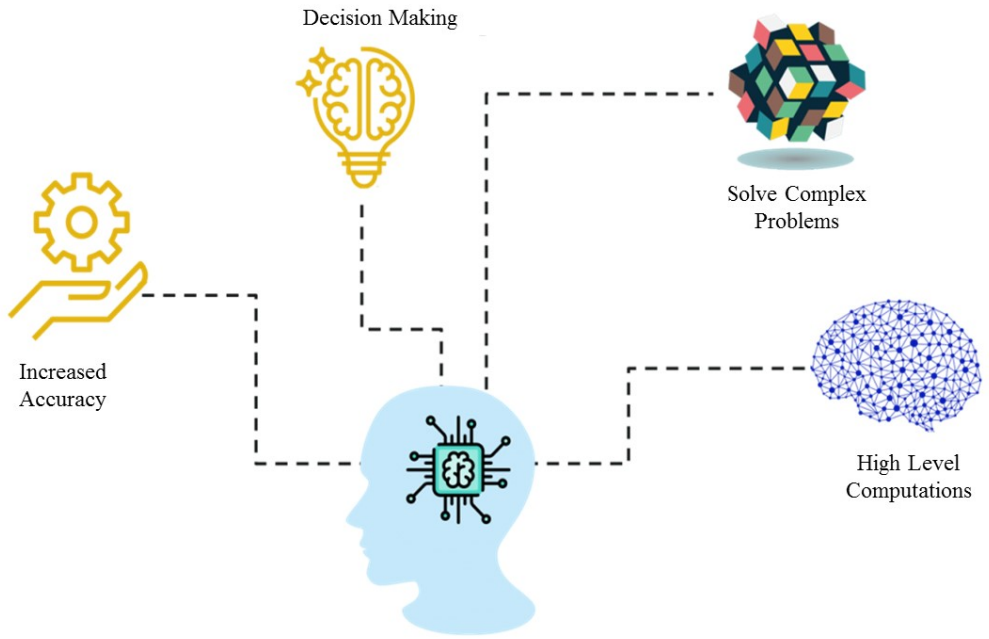


Figure 1.2: Concept of Artificial Intelligence (AI)

In easy terms, AI is the capability to compete with cognitive process (human intelligence), also AI is the name of adaptability of human like activities[10]. AI performs task with higher accuracy rate, efficiency, productivity of entire system. Many AI researchers are working to implement AI based system in practical fields to input values and get adequate results in return. Apart form all this, AI has been implemented in many fields like healthcare [11], gaming [12], speech recognition [13], voice conversion, automotive [14], finance, aerospace [15], government bodies, vision systems, defence and many other. To design AI based expert systems, many practice is acquire to justify its end users. Installing AI devices to get identifiable result for complex task by using algorithms in computer and implement it. According to technology and algorithmic behaviour AI has been categories into following branches, present in the figure 3. The figure represents the taxonomy of AI branches and its sub-branches on the basis data classification[16]. Let's acquire the major categories of AI and its information.

In this research work, we mainly focus on healthcare industry. AI has great impact on

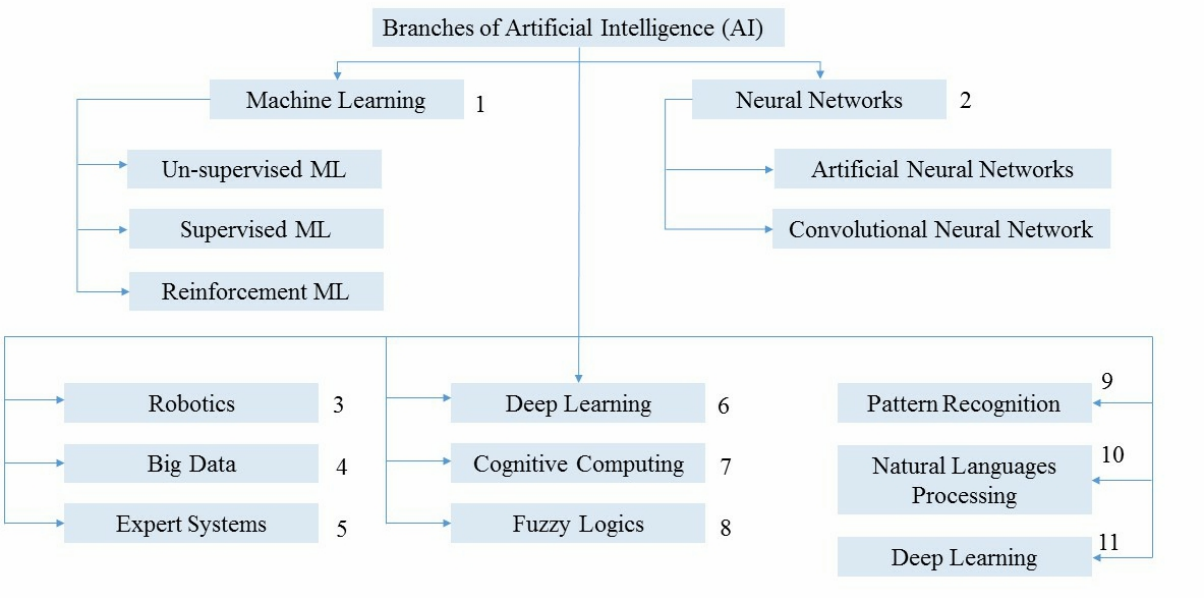


Figure 1.3: Taxonomy of Artificial Intelligence (AI) and its branches

healthcare sector by its advance and intelligent inventions. With the help of AI and strong machine learning (ML) based algorithms more tools for clinic sector becomes available to produce better result and performance. It helps to improve the diagnosis, researches, data handling providing privacy and security to patients' sensitive information. Amongst all sector where we can implement AI technique, healthcare [17] considers more sensitive and important because human life related to it. According to many recent researches, AI and ML algorithms helps in efficient and quick decision making, solve complex medical issues, maintain privacy in patient health record (PHR) [18], maintain privacy and secrecy through advance cryptographic and data classification algorithms. On the same time, most of the algorithm are too complex which can be explained to human easily, such type of algorithms named as 'Black Box Algorithms'[19]. According to some researches AI is much more efficient for healthcare sector like for diagnosis, clinics, emergency rooms, medical research centres, for physician, Administration, database centres, operation theatres, pathology department, laboratories, palliative care centres, and many more. Now many algorithms have been designed in radiology sector to detect and treat tumours. Though, AI made many advancements in medical field, it takes many decades to replace human. The process AI adaptation in e-healthcare system [20] illustrated through the following table 1.

In today's world AI provide many advantages to human in all sector either it is education, healthcare, businesses, government, military, aerospace, smart cities, or many other. It has many disadvantages like due to rapid development in AI, every individual losing its private

Table 1.1: Application of AI in Diagnosis and Prediction

	Diagnosis and case identification	**Prediction**
Analysis of Waveform	Obstetrics – fatal heart rate monitoring	Cardiovascular Risk
	Neurology – diagnosis of Alzheimer's disease	Survival of Breast Cancer
Analysis of Image	Pathology – detection of lymph node in breast cancer (metastases)	Colorectal cancer
	Dermatology – identification of tumours, fungal infection and skin cancer	Non-small cell lung cancer
	Ophthalmology – detection of diabetes and grading of macular degeneration	Admit in hospital due to heart disease
	Cardiology – identification of coronary syndrome, heart failure status	Utilization of primary care
	Radiology – mammography and X-ray to diagnosis of pneumonia	Sepsis in ICU, emergency department
Analysis of E-health Record	Prediction of central-line infections and mortality, detection of sepsis in the emergency, diagnosis of breast cancer, Heart-attack identification and patient phenotype analysis from ICU data, Extraction of autopsy report form death record of patients	Treatment of Social Anxiety

space and no secrecy element left in our daily life. As AI advances it becoming more dangerous and making human being lazy at it makes human lazier and tension free. In the figure 1.4. We try to illustrate some basic advantages and disadvantage of AI in today's world scenario.

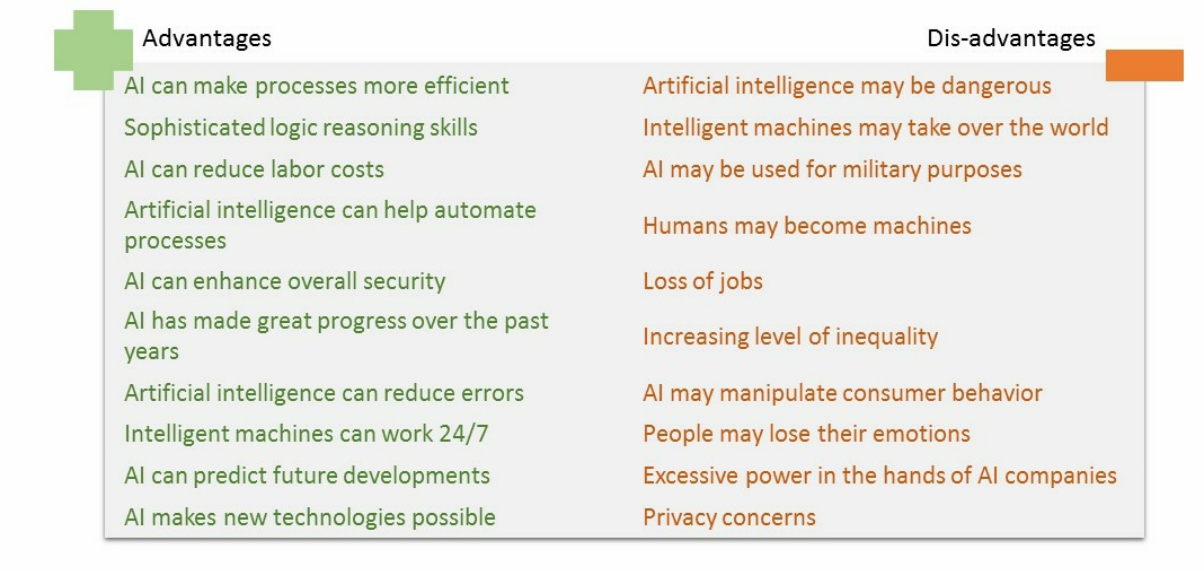


Figure 1.4: Advantages and Disadvantages of AI in today's world

1.2 Gaps in AI

Healthcare is a sensitive sector, where large amount of data or information needs to be handled. Though AI makes remarkable advancement in healthcare specially in radiology and clinical trials. But the main question which rises in researchers mind are:

- How can we handle massive amount of medical data?
- How medical or PHR can be secure and maintain secrecy?
- How PHR can classify with higher accuracy rate and reduce management cost?

In todays' healthcare systems, there are many challenges [21] like classification of medical data, handling errors and injuries, data availability, changes in professional working, sensitive patient information, privacy policy, rules and regulations, effective decision power, higher accuracy rate, authentication and authorizations, and legal provisions. All AI based research centers are working to make AI more advance and user friendly, especially which are easy to understand for human. In any sudden situation expertise doesn't require to cope with situation. By keeping in mind all the challenges and issue in existing or traditional AI technology and advanced version of AI has been developed, named as Explainability Artificial Intelligence (XAI).

1.3 Explainable Artificial Intelligence (XAI)

Explainable AI is an advance methodology which helps every single human to understand the solution by adaptation of ML and AI techniques. Basically, XAI is a contrast of 'Black Box', which is used in ML [22]. In this situation, programmer or designer of the system unable to elaborate why AI based system to some specific decision. On the other hand XAI, helps to provide most possible solutions to easy understandable. Here, the figure 1.5, shows why explianability becomes the foundation of AI.

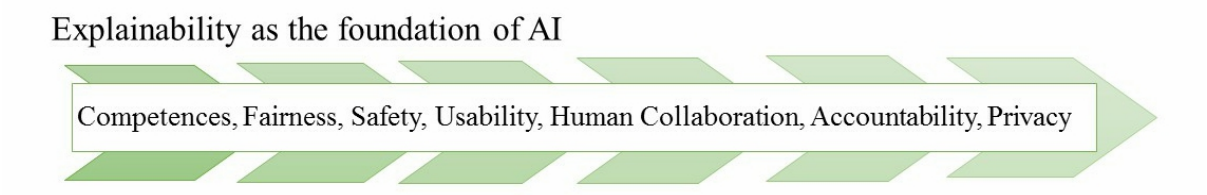


Figure 1.5: Explainability in AI

There some basic and important reason why we choose XAI in our research as a decision making tool. It helps to improve the decision readability for human beings. It helps to just justify the decision which system made and XAI justify the decision made by system. In today's' world, the basic debate about AI is how it can be explainable and how its system or model design for the proper working. The part where XAI technique is implemented, its core design is shown in figure 1.6, as an integral part, which attached to the system with higher accuracy and better decision making power. In XAI some popular methodologies has been proposed: [23] better data understanding (visually showing different features), better model understanding (visually neural net activation), better understanding of human psychology (adding human behaviour detection model in system). Though, DARPA [1] has been designed their systems based on XAI algorithms for better future of AI and ML systems. Why we need explainable system? this is the question , which should be answer at the time of system designing. In our research work we choose XAI based model for better decision because e-healthcare is a sensitive and human life dependent system. The proper diagnosis and its treatment is first and foremost obligation in medical sector for practitioner and physicians as well.

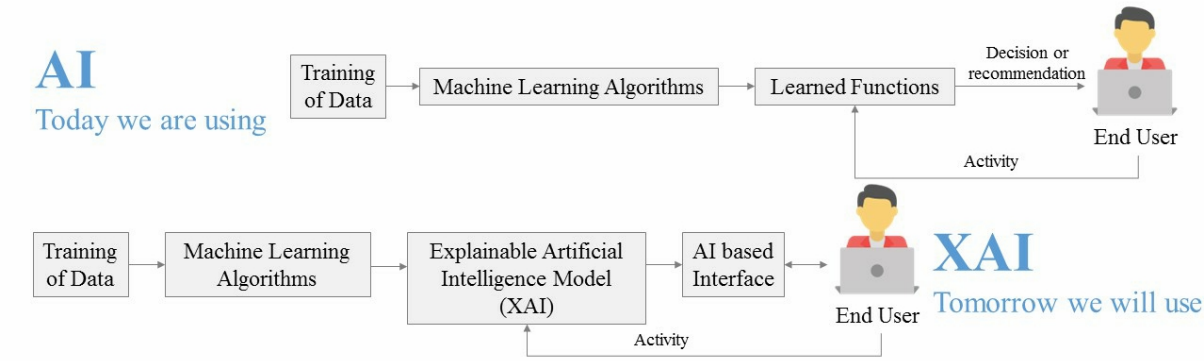


Figure 1.6: Now and Tomorrow: AI and XAI based model

According to author in study [24], explained the ability of decision making in AI, which can be easily understandable by human, in a broader term that how every single connected users interact and understand the decision making applications. Every client have their own different perspective and view point about the term explain-ability. In the field of research every scientist and researchers much interested about the explainability model and its algorithm, medical physicians concerned about the efficient diagnosis and clinical decision. Another term which is closely related to the concept of explainability is 'interpretation'. Explainability related to the

[1] https://sites.cc.gatech.edu/ alanwags/DLAI2016/(Gunning)%20IJCAI-16%20DLAI%20WS.pdf

prediction by interpretability in every case scenario [25], whereas interpretability is rendition of learning model during training process. Futher on, there are 2 methods used for decision making: Intrinsic and post-hoc. In **intrinsic method** the decision is made without the interference of any additional data or source of information. In intrinsic method following techniques has been used: linear regression, k-nearest, bayesian model, DT, rule based learning model. According to the hierarchy, DL is a subset of ML, ML is a subset of AI and XAI lie within the umbrella of AI and its has intrinsic methodology named as ML. Here figure 1.7, illustrate the relationship between AI, XAI, ML, DL, and FML.

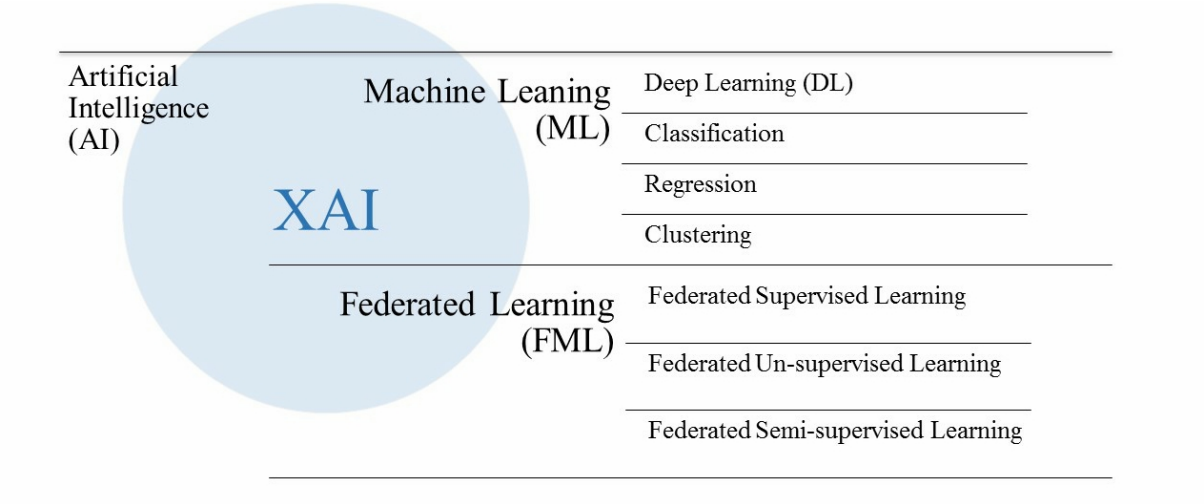


Figure 1.7: Relationship between AI,ML, XAI, and FML

In post-hoc method, includes multiple other techniques for classification and data handling: Shapley Additive Explanation (SHAP) [26], Principle Component analysis (PCA) [27], Class activation mapping (CAM) [28] and gradient weighted class for activation (GRAD_CAM) [29]. According to the authors in studies, **post-hoc** methodology categorised into further sub classes: attention mechanism, text explanation, dimension reduction, explanation by examples, restricted NNA (neural network architecture), feature extraction, explanation by simplification and lastly local explanations. The taxonomy of XAI based branches are shown in figure 1.8. For the practical evaluation of XAI based systems still not exist, only theoretical based approaches has been used to deploy XAI in near future with proper physical integration.

1.4 Machine Learning (ML)

Machine Learning is a branch of AI, and making many wonderful advancements in every field. As, everyone looking for AI in everything, there is a fast emerging trend to adopt AI based

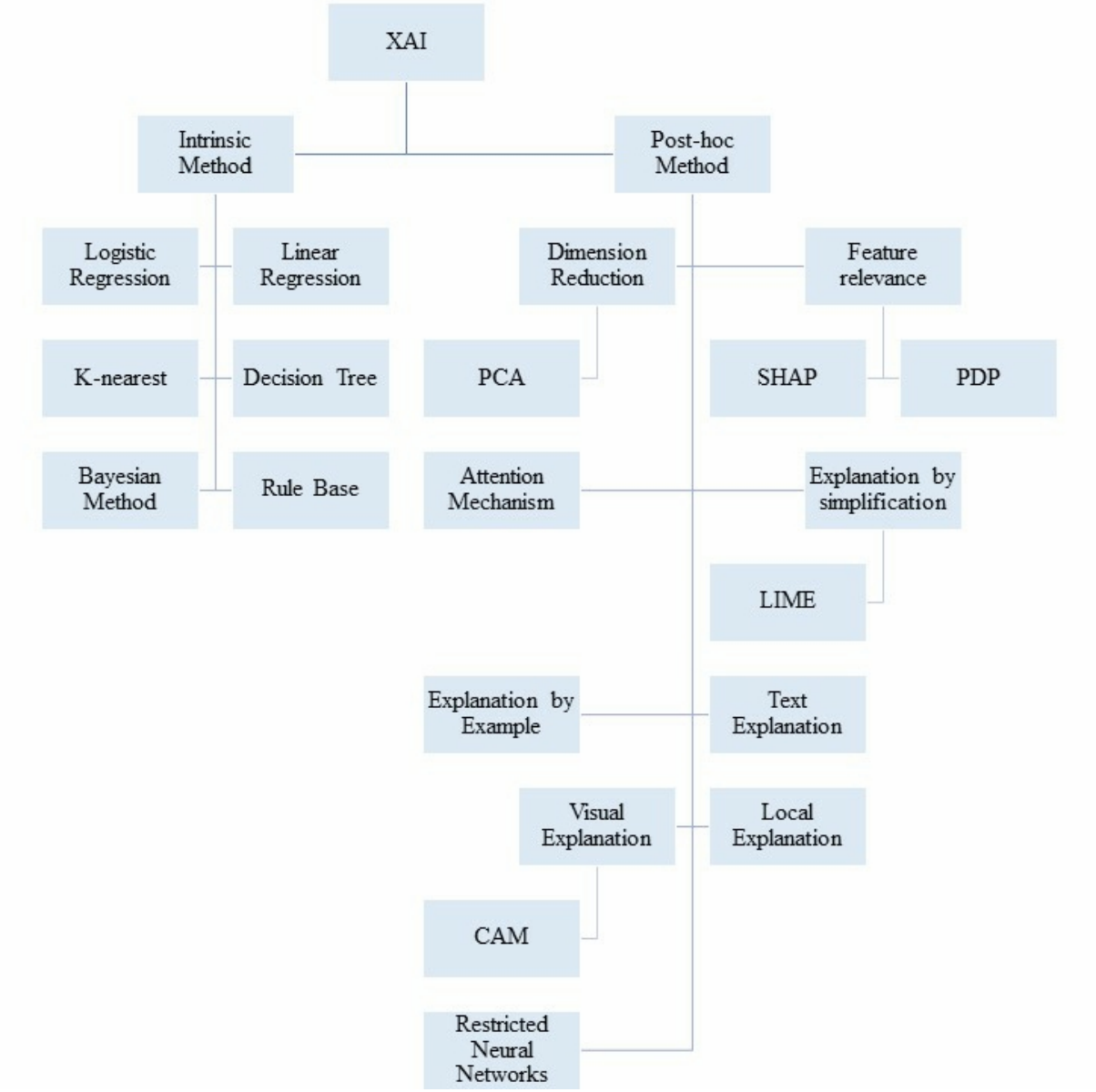


Figure 1.8: Taxonomy of XAI methods: Intrinsic and Post-hoc methodologies

large, complex and high speed systems [30]. As time passes more pressure has been loaded on AI invention to produce more powerful and innovative systems or model to compete today's' world. The main focus is on the integrated circuit which helps to computer architecture and AI based application more strong[31]. Conventionally, human experts designed computer architecture or system, where a lot of expertise and ML knowledge required. Although, these design contain many problems like optimisation, scalability, specially in complex systems. So, to overcome such issue, computer design and system architecture adopted automated and advance methodologies to recreate a strong relationship between MLA and designs. Since few decades, architecture of ML [32] keep updating and optimised the performance of ML models.

Here the figure 1.9, shows the general workflow of MLA. Machine learning algorithms runs

on the raw datasets of any selected department (like healthcare record, sign-in record, images or numerical values to predict any thing and many other). The input dataset processed to get attributes of the data (means features which work with MLA). When feature extracted, class labels categories into three: training, validating and testing of datasets. In training phases, some specific portion of dataset selected for training purpose and create classifier model. Then, validation phase, work on the performance of trained dataset (validation can be many type like cross validation etc.). and then remaining dataset sent for testing phase, which test the performance of system and calculate the final outcome and generate output.

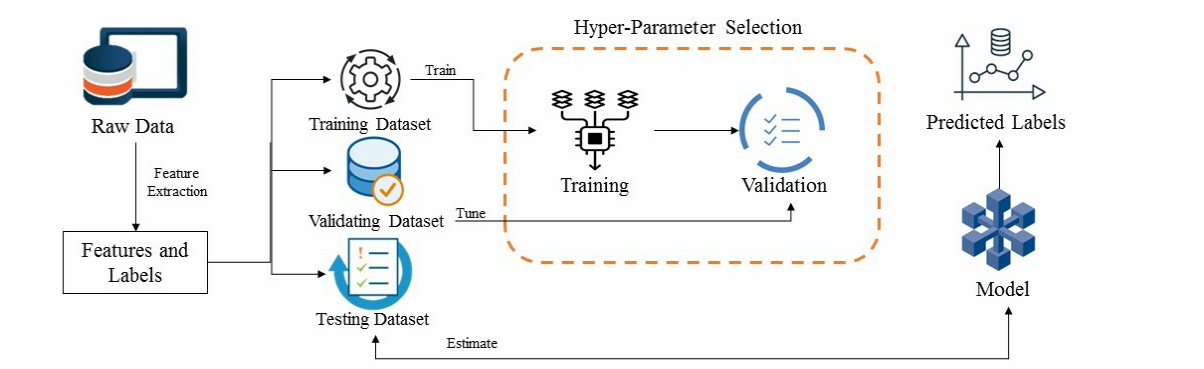


Figure 1.9: Architecture of Machine Learning (ML)

During the last few decades, machine learning (ML) and artificial intelligence (AI) has been made huge progress. In ML algorithms, data or datasets has been trained or test to get accuracy rate and to predict better outcome [33]. Machine learning algorithms (MLA) has been applicable in almost all fields: healthcare, military, business, education, social media, government bodies, security, privacy, and many more. All areas where application of MLA evolved, a large number of problems has been solved. The combination of AI and ML has been made healthcare industry more effective, efficient, and improves its performance, whether its diagnosis, treatment, clinical appointments, laboratories or any other issue [34]. As the main concern of our research work is to implement better algorithms and framework of AI and ML in healthcare industry, so take it from healthcare, medical and patients perspective. Machine learning (ML) is a branch of artificial intelligence (AI), where combination of both algorithms create a predictive power in data management [35]. Mostly, ML deals in the statistical data of computers and used statistics based methodologies specially to work in medical industry. MLA has been categorised on the basis of data type and further classified into four main branches: supervised, un-supervised, reinforcement and recommended systems. The detail taxonomy of ML, its branches and its sub-branches has been presented in the figure 1.9.

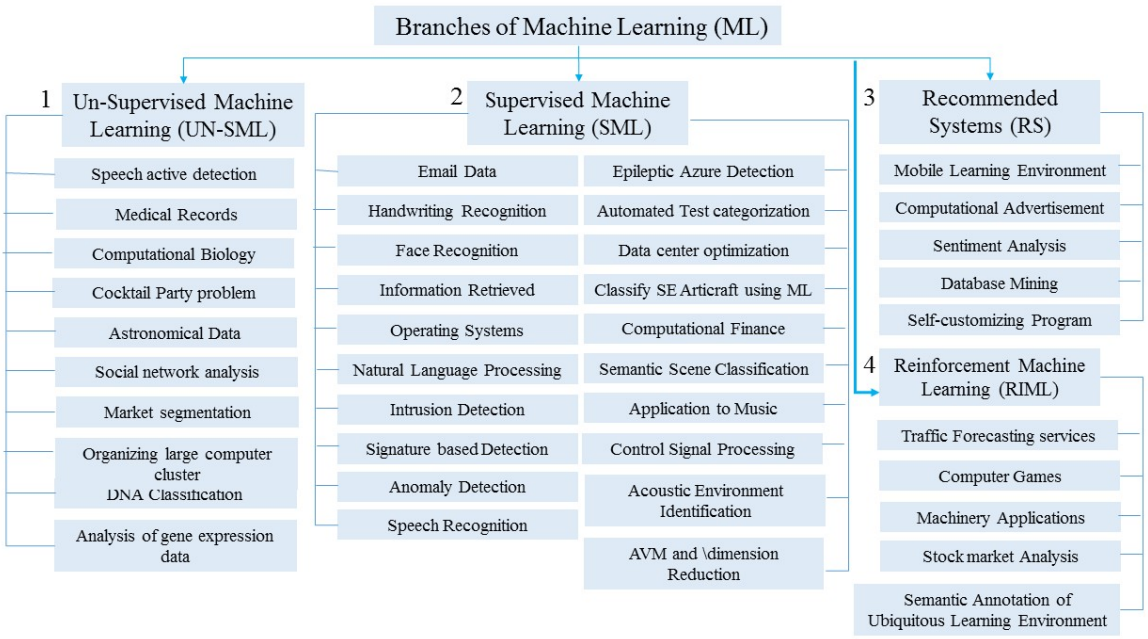


Figure 1.10: Taxonomy of Machine Leaning (ML) and its branches

In healthcare industry, an effective management of public and private healthcare, is an important data processing task. Every healthcare organization divide its management [36] into main categories: screening /diagnosis (which depends on the data classification of previous case history, detection and plans) and monitoring/ treatment (which depends on planning, recovery and future outcomes). MLA has potential to improve decision making by testing and training of its raw data, which leave strong impact on patients and healthcare systems too. As the technology advances, researchers works on ML domain to improve the expert systems performance. Many ML learning algorithms has been proposed to deal with type of data [37] (data types maybe: statistical, images, voices, sensors, document, and many other). All algorithms has been designed to overcome the flaw of previous algorithm, as the technology advances the data learning model has been proposed (like SVM,CNN, ANN, KNN, linear regression, decision tree and many other). Though machine learning has made remarkable inventions and working in the medical but side by side its has advantages as well as dis-advantages [38]. The figure 1.11 represents the main pros and cons of ML on the basis of system efficiency, performance ,security and data classification.

Figure 1.11: Advantages and Disadvantages of ML in today's world

1.5 Gaps in ML

Though ML has made remarkable advance in many fields, but when we talk about healthcare industry where sensitive information or data involved. It requires more security and high data handling methodologies [18, 39]. Where every single connected device to main server is secure and manages PHR with satisfactory outcome. The main question which arises are:

- How can large amount of data handle efficiently on local and global servers?
- How patients sensitive information be secured to every single connected device?
- Is adopted algorithms provide low battery consumption, take less time and improve systems performance?

Since last many yearns, machine learning (ML) has been advance data processing on a wide scope. The traditional or classical architecture of ML has been modified time to time to adapt according emerging technologies. The changing trends make ML design challenging [40], main of them are: **data handling, privacy /security, data sharing, data training at central server or main server and many others**. To overcome such challenges, Federated machine learning algorithms (FMLA) has been introduced which make data handling more easier and training process as [41]. In FML, data trained at local servers in-spite of main or central server, which helps to provide more security to data and cloud. Distributed machine learning algorithms (DMLA) handle many and different datasets, the main challenges id can it be handle at larger scale, which is the biggest limitation of traditional machine learning algorithms [42, 43]. Therefore, to cope with such situation, a new advancement has been made in the field of AI is the Federated Machine Learning algorithms (FMLA). In our research we are trying to implement FMLA in healthcare industry [44] to handle large amount of data at

wider scale and provide more security to data and healthcare systems are local level instead of global or main server.

1.6 Federated Machine Learning (FML)

Now-a-days, Federated Machine Learning (FML) consider as better solution for XAI, which enhance the performance and efficiency of healthcare systems [45]. It helps to manage PHR more efficiently on main cloud or global servers, with less chances of security threats during uploading/downloading and data accessing. As far as security and data handling concerns it helps to increase the accuracy rate [46]. It help to handle multiple risks like data handling, login credentials, data sharing, securing connected devices [47]. In healthcare industry still av lot of changes needs to be done, which FMLA tries to overcome some how. The main departments in healthcare industry(pathology, laboratories, emergency unit [48], operation theaters, radiology, neurology, medical record centers, clinics, oncology, research centers and many other) can be improved by implementing FMLA.

Federated machine learning (FML) is basically a distributed machine learning technology. The basic concept of FML is: training of ML based models with distributed nodes and local system [49] data under federated learning. FML is basically a global model which maintain large amount of data and maintain its model by handling them. FML model assigned to resolve many ML problems with higher accuracy rate and efficiently. The figure 1.12 represent the general architecture of FML algorithms and its working. Data from multiple nodes or sources come to a single system. According to FMLA, every single node handle data against same identity and work according to that data sharing strategy. In this hierarchy, three main components are connected to each other: users, federated model, and data sources. By studying the

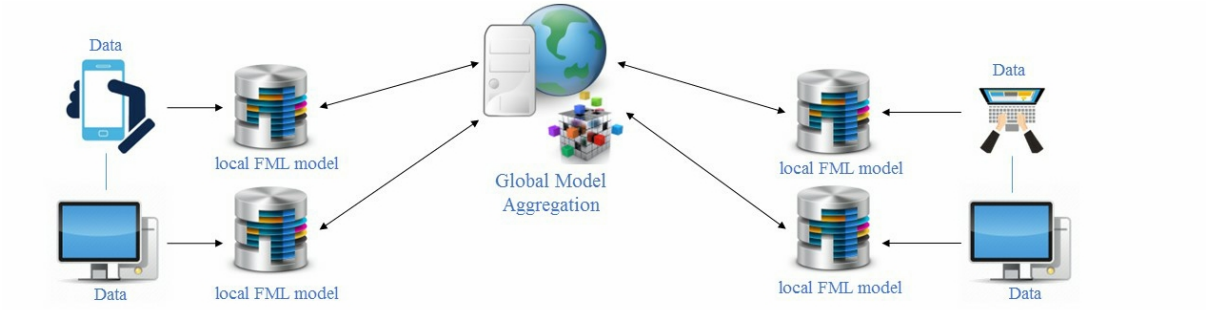


Figure 1.12: General Architecture of Federated Machine Learning Algorithm (FMLA)

background of FML applications, we can categories the application of FMLA in further 4 parts:

privacy, data distribution, communication framework, and models. The categorized dimension contain some basic factors in existing FML and in consideration. These can be used to design the taxonomy and architecture of FML as shown in figure 1.13.

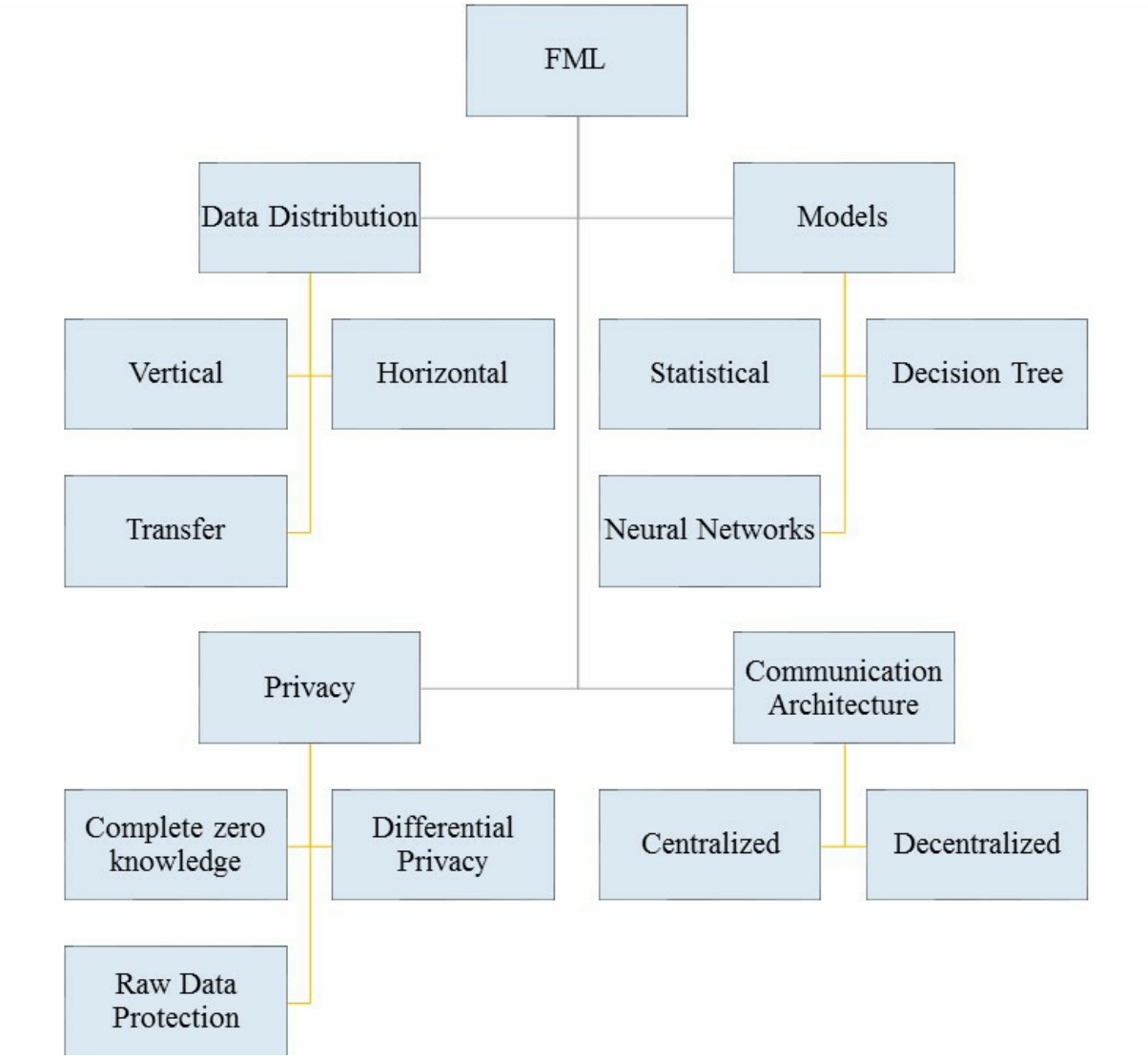


Figure 1.13: Taxonomy of FML Applications

In traditional ML and FML the properties for selecting datasets are different for each other. In ML every single connected systems the processing power is equal while in FML the most of the time data come from un-identified source, which vary in quality and diversity, that is due to multiple hardware specifications and devices or nodes for training process. On the basis of data distribution FML categorised into three types: Vertical, Horizontal and transfer federated Learning.

In FML networking architecture, it categorized in centralized and decentralized networks. (1) In Centralized networking model, all connected nodes or clients updates their model model

at initial stage before sending to the global model. At main central server these updated model has been aggregated to communicates back to its own client. Just for an example, in hospitals all single systems updates their model at initial stage and then send it to main server room for aggregation or updation. The centralized architecture contains more risk due to the malicious attacks and eavesdroppers. It required high rate of processing power and more bandwidth to communicate efficiently. (2) In Decentralized networking model, no independent model learning procedure includes, just connected clients update model and receives the aggregated update to their local systems. A cryptographic algorithms has been used to make the process secure and maintain privacy in data aggregation. In our research work, we choose FMLA for data classification model, security model and for better system performance.

In healthcare sector, most of the hospitals are using AI methodology to work efficiently and effectively. In existing AI based healthcare system contains challenges like data classification, injuries and errors, data availability, bias and inequality, professional realignment, sensitive data, privacy regulations, term and policies and many more. Modern health systems require cooperation among research institutes, hospitals, and federal agencies. Moreover, in a pandemic like situation, collaborative research among countries is vital but not at the expense of privacy. FML makes the cooperation possible because it can ensure privacy. In a federation of healthcare, there is probably no central server. So, another challenging part is the design of a decentralised FLS, which should also be robust against malefactors. In this manner, XAI and FML considered as an efficient and effective technology. To overcome the above mention issues and challenges, XAI and Federated machine learning has been studied and discussed. It will help us to provide better version of secure, protected and efficient healthcare system

1.7 Scope and Limitations

The scope and limitations of our proposed model are as follows:

1. Our proposed model can easily helps to increase the efficiency of the e-healthcare system.
2. Our proposed model can reduce the error detection rte and increase the accuracy rate with high density.
3. Our proposed model can boost the speed of data evaluation in training and testing phase with less time consumption.

4. Our proposed model tries to overcome the shortcoming of the previous researches.

5. The only limitation in our proposed model it can hardly identify the irregular access of the e-healthcare systems.

CHAPTER II

LITERATURE REVIEW

In e-healthcare system, the smart technology has been adopted to facilitate the patients and make an ease in diagnosis and better treatment procedure. Now-a-days, AI, ML, DL and FML makes an advance changes in healthcare and become main element of systems, to check and to treat patients. So, the main task for researcher and programmer is to implement these techniques in e-healthcare physically. The following table 2.1 represents the AI techniques and their application in e-healthcare systems [50].

Table 2.1: Application of e-healthcare and its their purpose

Ref.	**Applications**	**Purposes**
[51]	Detecting and Analysing Diseases	One of the critical uses of machines is to diagnose disease correctly
[52]	Medicine manufacturing	At initial stage identify medicine, prescribe by using machine with high-low dose and then design for forecasting
[53]	Special medicine for Specific disease	machine which recommend medicine according to patient's condition and its adverse or positive effects
[54]	e-Health record	large, private, secure and encouraging platform by using advance machine to handle it efficiently
[55]	Medical Research centers	It depends on machine which make advance medical research on the basis of medical history of patients by taking permission from the concerned person
[56]	Data over-sourcing	The advance machines are required to handle over flow of medical records, in-going and out-going medical data
[57]	Advance disease prediction	Machine and advance learning systems to predict the condition of patients before it getting worse or getting cure
[58]	Image processing	Intelligence machinery to diagnose the stage of disease to meet the borders, and expanding the explore by diagnosing from different clinical image data

2.1 Artificial Intelligence (AI) to Explainable Artificial Intelligence (XAI)

In 2004, the first ever explainable artificial intelligence (XAI) system has been designed [59]. The general and main purpose of XAI is to make AI based systems more easy to understand and close to human understanding model. Though, XAI has no proper definition, which shows clarity in term of its terminology. Few word from this concepts are: transparency of systems, interpret-ability and most important among them explainability. All of these have different meaning in its term [60, 61]. The term 'interpret-ability' refers that how a model can be interpreted and understood, it can also be used in the context of explainability. While transparency shows that how the model show its working without any flaw. It includes training procedure, analysing distribution of training data, codes, explaining features of data and algorithmic clarity that how the model keep working. Among them all explainability have main reason, it helps in decision making [62]. Therefore in our research work we mainly focus on 'explainability. or 'explainable artificial intelligence (XAI)'. The table 2.2 shows the latest work of XAI by following the concept of explainability.

Table 2.2: Adaptation of XAI model in latest studies (Literature Table)

Ref.	**Years**	**XAI Adaptability Method**
[63]	2022	A Book: On XAI models having interpret-ability, transparent and agnostic methodologies
[64]	2021	A detail survey on XAI, with codes and referencing toolkit
[65]	2021	A taxonomy of XAI based survey which shows some examples and extensive future directions
[66]	2020	Using table mapping properties in extensive surveys
[67]	2021	The XAI systems for designing and survey on metrics
[68]	2021	Detail taxonomy of XAI metrics with methods
[69]	2020	Extensive collection of XAI and responsible AI
[70]	2020	XAI: Introduction, variety of examples and standard methodology
[71]	2020	A review and taxonomy: local/global explainability by using back-propagation and perturbation methodologies
[72]	2019	Vast collection of variant XAI concepts, examples and metrics
[73]	2018	An extensive survey based on XAI technology having literature of around 381 research papers
[74]	2018	A detailed survey on XAI methodology containing references for special issue surveys

In e-healthcare industry, AI plays a magnificent role by using machine learning algorithms and deep learning techniques to diagnose and for treatment. The medical experts has been

transcend, by using DL to get higher accuracy rate. Though, the black-box nature of DL model, limitize the explainability and deployment models in e-healthcare. Though, many researchers come forward with the concept that traditional AI based model helps to increase accuracy but the concept of explainability left behind, which is not right AI model. In successful AI based model higher rate of accuracy and explainability comes together, and then the concept of XAI has been created to deal with both of them specially in e-healthcare industry. In medical domain before the practical implementation of AI model, it should be understandable for the correct diagnosis. Therefore, the motivation behind the concept of XAI is 'explainability'. In this research, we review some of the research papers, where XAI has been used for diagnoses and treatment of diagnosed diseases. The table 2.4 show the detail comparison of the latest research, where AI based algorithms has been used in medical research, which motivated us to do research on XAI with advance ML algorithms for the betterment of e-healthcare industry.

Table 2.3: XAI based Healthcare Application for Diagnosis and Prediction

Ref.	**Years**	**Detection**	**AI Algorithms**	**XAI Algorithm**	**Methodology**
[75]	2021	Allergy	KNN, SVM, C	condition-prediction	Rule based
[76]	2021	breast cancer	clustering	adaptive reduction dimension	reduction
[77]	2021	spine	SVM, binary random forest	LIME agnostic explanation	simplification
[78]	2021	Alzheimer	2-layer with random forest	SHAP, using fuzzy inference features	rule based
[79]	2021	hepatitis	linear regression, K-nearest, SVM, random forest	Partial Dependence Plot (PDP)	simplification
[80]	2021	chronic wounds	CNN model	LIME	simplification
[81]	2021	Fenestral otosclerosis	CNN model, Logical Neural Network (LNN)	Deep visualization representation	visual explanation
[82]	2021	Lymphedema	multi-granularity-graph (CMGE) model	Graph neural network	neural network architecture
[83]	2020	clinical	entity aware CNN	Bayesian networks	Bayesian model
[84]	2020	Glioblastoma multi-fome (GBM)	VGG16	LIME explanation	simplification

After the detail survey of all recent researches, it is examined that ML and DL algorithms consider as an optimising answer for XAI based medical applications or systems. There are no

Table 2.4: XAI based Healthcare Application for Diagnosis and Prediction

Ref.	Years	Detection	AI Algorithms	XAI Algorithm	Methodology
[85]	2020	Pulmonary	CNN	VInet, LRP, VBP	visual explanation
[86]	2020	Alzheimer	Naive Bayes, Grammatical Evolution	CFG	rule based
[87]	2020	lung cancer	NN, random forest	LIME, Natural language processing	simplification, text explanation
[88]	2020	brain injury	k-means, clustering, Gaussian	clustering	feature extraction
[89]	2020	Covid-19, chest x-ray	CNN model	GSInquire	Restricted NNA
[90]	2020	Colorectal cancer	CNN	explainable cumulative FIS	visual explanation
[91]	2020	Thyroid	Neural Networks	CAM	Visual Explanation
[92]	2020	Psychiatric disorder	DNN, White matter	EDNN	Visual explanation
[93]	2020	Parkinson disease (PD)	CNN	LIME explanation	simplification
[94]	2020	Surgery	XGBoost validation	SHAP	feature resemblance
[95]	2020	surgery	SVM	Virtual assistance	feature resemblance
[96]	2019	Hospital discharge information	Linear Reg., Random forest, MLP	LR, LIME	Simplification
[97]	2019	breast cancer	KNN, distance-weighted KNN	CBR	explanation through example
[98]	2019	Alzheimer	Random forest, SVM,Decision tree	SHIMR	rule based
[99]	2019	Surgery	FCN	CAM	Visual explanation
[100]	2019	Laparoscopy	CNN	Map's activation	Visual Explanation
[101]	2019	Surgery	CNN	Saliency Map, Image extraction	Explanation through example

currently that enhance scheme available, which helps in all healthcare domain at once. Most of the time its totally depends on the size of data, type of data and some other factor. To solve such problem, in our research work we trying to adopt advance machine learning model to handle large data, make system's performance better and also along with improve the security element.

2.2 Machine Learning (ML) to Federated Machine Learning (FML)

Recent studies on federated machine learning (FML) [102] and its implementation in e-healthcare classify FL into two types: Data Classification and Data segmentation. Which is presented in table with proper categorization of recent researches. **Classification:** In healthcare industry, data classification is the main task to handle with. In MLA, many approaches has been used to to classify data and manage them in multiple classes. Whereas in FML there are few data classification types used in e-healthcare: diagnosing cancer, Covid prediction, emotion detection, autism disorder detection, alol types of tumor detection, chronic disease detection, patient hospital record handling, and many other.

Cancer diagnosis: According to many recent studies it has been observed that FML has been deployed to diagnose cancer for ML application for diagnostic. Like, in [103] author proposed a CNN based data classifier model to detect benign or malign stage of thyroid. HE used 8457 images of ultrasound to perform experiment and apply FMLA for getting higher accuracy rate with 97%. Similarly, the author in research [104] proposed MLP model with FML implementation to diagnose lung cancer and classify the data by using advance algorithm. The proposed technique enhance the rate of accuracy 92.8% for diagnosing cancer. According to [105], the author used raw medical data based on multiple images, without violating the rules and privacy of FMLA. The image translation use CycleGAN model and achieved higher accuracy rate 99% by using 8 nodes data for training and apply ROC-curve diagram to represent it.

Covid-19 diagnosis: For detecting Covid-19 positive or negative by examining images data(collected from various medical centers), helps to crate a model by keeping security of the data. By adapting such methodology many e-healthcare record center enhanced the performance of framework. Like, In [106] author performed experiment by using FMLA to diagnose Covid-19 by using images data and classify them. The proposed result showed that SGD and GAN framework optimized the accuracy rate with 98.03% and detect less loss rate as compared to MLA. Similarly, in [48] author used FMLA to train dataset of different hospital. For training dataset has been collected form one hospital of one country (China) and for validating collected dataset from other hospital of other country(Germany). This research proposed to detect the anomalies from the medical record of almost 132 patients and classify them to achieve accuracy rate of 83.12%. According to research [107], the author proposed a FML based model to diag-

nose Covid-19 by using images data of X-ray and CT-scan. The author proposed CNN based model to detect Covid-19 positive or negative. After performing experimentation to classify data, the accuracy rate was 95.27%. Likewise, in [108] author proposed an FML based algorithm to detect the side effects of Covid-19 (diagnosed Pneumonia). It generates a data training model by considering the privacy rule of FML. To overcome the challenges of Covid-19, GAN based framework deployed to compare the performance of simple FML and GAN based FML with accuracy rate of 94.11%.

Activity and Emotion diagnosis: In the field of data security and system efficiency, IoHT along with FML is an advanced solution for the privacy of medical record and designing a model to detect emotions and activities of human being. Likewise, according to research [109], the author proposed a framework where DNN has been used to detect activities of human being like : walk, sitting, looking, standing etc. Then author proposed a research where CNN model has been used with transfer FML to train and achieve accuracy rate 99.4%. According to [110], author used FML for cloud infrastructure to maintain privacy of the database servers and monitoring the smart applications during Covid-19 pandemic. An AE based model has been proposed to divide the healthcare connected devices into 5 different layers. The proposed framework achieved 95.14% accuracy rate after performing the experiment. Then, in research [111] author used FML to detect facial expression and voice signal of patients in healthcare sector. A dataset based on facial expression has been used and FMLA deployed and AE based framework model for secure data classification. After performing the experimentation the 88% accuracy has been achieved.

Mortality diagnose: In e-healthcare systems, FML plays a remarkable participation to diagnose the mortality of patients, by using predictive model which helps the physicians to treat patients. According to research [112], the author used FMLA to detect the severity level of patient's condition and calculate the medicine dosage, and time duration of staying in ICU. Then AE model has been used to categorise the patients into multiple communities on the basis of IDs and non-IDs patient. On the basis of this division the trained trained to calculate the accuracy of performed data classification. The performed experiment achieved accuracy with 69.13&. According to [113] the author mentioned in study that FML algorithms helps to diagnose the heart rate of patients and predict the future. For this model SVM classifier has been used along with FML framework environment. The proposed model achieved 77.47% accuracy rate after experimentation. In [114], the author proposed a MLP and FML based

model to diagnose the mortality of the patients in hospitals. The author performed experiment and compare the results of FML model and centralised model and get 97.7% accuracy rate. According to author in [115], the study stated that FML and MLD based model has been used to detect the mortality of Covid-19 patients in e0healthcare systems. The proposed model showed that it maintain the privacy of patient record as well as increase the level accuracy with 82.9%rate.

Other domains diagnose: Other than mentioned areas of healthcare, FML also helps to diagnose many other disease and classify them with high level accuracy rate. According to author in [116] studied that distributed FML along with NN model will collect data from all IoT based connected nodes in healthcare. An D-FML helps to diagnose sepsis disease and provide most possible suggests to cure them. Also, in [117] author proposed a FL framework to diagnose ASD for MRI analysis.

Segmentation: of medical images or image based records is an essential part in diagnosis. It is a process to select a area of interest through which medical diagnosis performed. Medical image based record collected in many forms like: MRI, CT-scan, X-rays and others. There are many researches where FL has been choose to performed operation on medical image data for segmentation (for brain tumor [118], Covid-19 detection [119, 120], cancer diagnoses [121] etc.).

Table 2.5: Summary of FML models in e-Healthcare systems

	Domain	**Data Type**	**Algorithm**
Classification	ASD or HC	f-MRI	CNN
	Cancer (Prostate, Thyroid, Lung cancer)	MRI, Ultra-sound, radon data	GAN, CNN, MLP
	COVID-19	X-ray	CNN
	Human activity	Wearable device	LSTM
	Emotions	Sensing device	CNN
	Patient's Admission detail	EHR	SVM
	Mortality	Palliative care	MLP
	Sepsis disease	EHR	DDQ-Net
Segmentation	Brain-tumor	MRI	U-Net
	COVID-19	3D Chest scan	3D U-Net
	Cancer	MRI	3D AHN

2.3 Data Aggregation

In FML, local model has been aggregated at global server in an important step to secure and train the data. After aggregation a learning model has been generated by considering the local parameters of every single connected note by using FML processing. To enhance the security and accuracy rate global and local parameters has been combined to get results. According to many studies, data aggregation helps to enhance the security by classifying before combining parameters globally, and imply an algorithm which helps to increase the accuracy rate. According to [122], the author classify local data models by using concept of uncertainty, it will train only local data model instead of global models to get higher accuracy by using aggregation algorithms. Then, by checking the local model quality by sending data to global model for aggregation, which defines the threshold property of model. The proposed approach helps to increase the accuracy rate after training. Similarly, according to [123],the proposed a matrices model which quantifies the data from every single model and aggregate them. This methodology helps to reduce network need and increase rate of accuracy.

According to [124], perform the evaluation on metric which shows improvement on global model by using parameters of learning model. The data aggregation model will perform aggregation only on those model which have higher accuracy rate. Similarly, in [125] propose a scheme where model will check those number of clients who contribute in training process globally. Local nodes will work only if the global model accuracy rate guaranteed. Along with it, all those local model which consume more time in training process discarded. Then, in [126], author proposed a methodology where labelled and un-labelled dataset is available for training . Connected nodes will employ the FML model to get pseudo-code of un-labelled global FML model. By using the data aggregation methodology many other researches uses, evaluate and proposed an optimised version of FML aggregator. According to another study [127], used attentive framework to select parameters for global training model to classify them. In outcome the gradient descent model perform the aggregation on global model. Then in [128],the author examine the divergence issue, which occurs during aggregation process in FML and increase time consumption and lessen the accuracy of model. An optimised solution has been proposed in this research that among all connected nodes increase the entropy of activation.

CHAPTER III
PROPOSED METHODOLOGY

3.1 Problem Statement

Though AI and ML has been considered as a remarkable invention of computer sciences, still contains challenges and issues now-a-days. In healthcare sector, most of the hospitals are using AI methodology to work efficiently and effectively. In existing AI based healthcare system contains challenges like data classification, injuries and errors, data availability, bias and inequality, professional realignment, sensitive data, privacy regulations, term and policies and many more.

Modern health systems require cooperation among research institutes, hospitals, and federal agencies. Moreover, in a pandemic like situation, collaborative research among countries is vital but not at the expense of privacy. FML makes the cooperation possible because it can ensure privacy. In a federation of healthcare, there is probably no central server. So, another challenging part is the design of a decentralised FLS, which should also be robust against malefactors. In this manner, XAI and FML considered as an efficient and effective technology. To overcome the above mention issues and challenges, XAI and Federated machine learning has been studied and discussed. It will help us to provide better version of secure, protected and efficient healthcare system.

3.2 Research Questions

The proposed research is predicated on the following research question:

- What are the gaps in existing XAI and ML approaches?
- Why healthcare systems need efficient and secure system?
- What algorithm improves the performance beyond ML?
- What data security framework and algorithm required to make efficient decision?

3.3 Research Objectives

Based on the problem statement, the present research aims to supply the approaches that can increase accuracy rate in data classification and security algorithm by using the XAI interface and FML model to make healthcare system more efficient. During this research, most characteristics will be:

- To enhance the efficiency and secure the data aggregation model by using FML
- Increase the performance of e-healthcare systems without decreasing the accuracy rate.
- To enhance the decision making system more strong and accurate.

The main objective of this research work is to enhance the performance of e-healthcare systems by using XAI based framework and implementing FMLA for data training and testing. The propose framework mainly emphasize on the better data training and testing with higher accuracy, lowest error rate and security of cloud by using data aggregation theorem in FMLA. And for testing and training our proposed federated learning algorithm we use Google Collaborator for performance evaluation which show the accuracy rate, time consumption, and number of epochs rounds.

3.4 Research Contribution

This thesis research discusses the following:

- We researched about the application of AI and ML in healthcare industry, on the basis of existing work we identify some gaps in existing models.
- We identify most possible solutions of AI and ML in healthcare industry for better and efficient decision making process.
- We proposed a XAI based decision making flow chart, which helps the physicians in accurate decision making.
- We proposed a FML based model training flowchart of single connected node for data aggregation.

- We proposed an optimised data aggregation algorithm for efficient and secure data training on global servers.
- We perform computational proof of security by using Diffie-Hellman problem to enhance the security of system.
- We perform experiments on MNIST dataset using open source framework to show the working of FML secure aggregation algorithm.
- We perform 4 experiments in our research to compare our results with already existing FML and ML architectures.
- Finally, we conclude our thesis our with future directions and challenges of FML and XAI.

The main Idea of this research work is to adopt two more efficient methodologies to make e-healthcare systems more efficient and secure. The impact of FML and XAI is quite huge in e-healthcare systems. In our proposed model, the system will work more efficiently by passing from training phase, which helps to make decision more efficiently. The model for prediction make lower latency in the architecture. In e-healthcare systems, becomes more efficient and secure in the context of patients, doctors, pharmacists, researchers, and laboratory. And most important amongst all data privacy and security enhancement. Federated machine learning (FML) is an advance form of machine learning which helps to improve the performance of the system. FML allows multiple XAI based systems to share data with higher security model. In the training phase, it train every single connected node to train its data locally and then transfer trained data model to main central server for data aggregation, to get final aggregated or processed data, which becomes available to every connected system afterward. This process complete its as much as required iteration to complete the processing. The figure 3.1. Shows the architecture of XAI-FML in healthcare sector.

In Healthcare system, XAI-FML plays a significant role to enhance the performance, decision-making power, critical analysis of human life. Medical information contains personal information, which includes name, gender, age, and address, physical health, reports, and the leakage of these information may cause serious risks to patients. Though the data of patient is stored on cloud servers, and attackers can launch various security attacks, such as data confidentiality, privacy, and integrity attacks, which will pose a serious threat to patients. Many organizations or companies collect personal privacy or sensitive data on the Internet, which means that

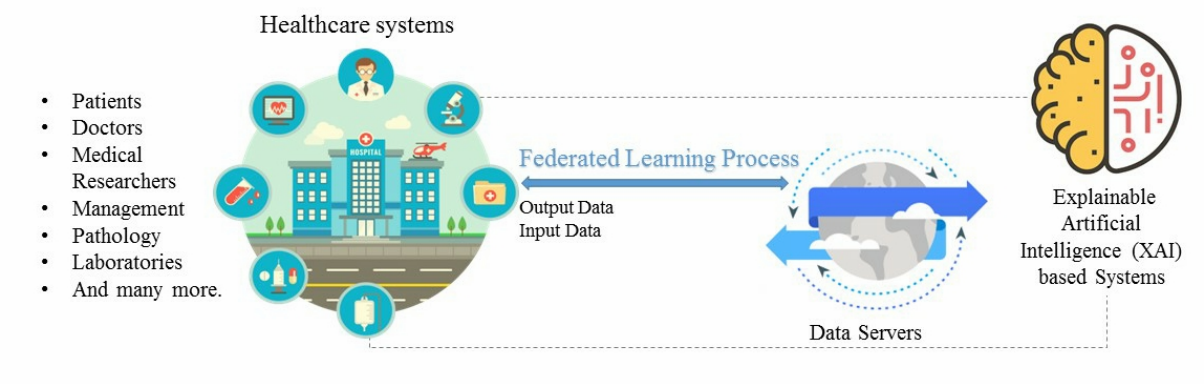


Figure 3.1: Proposed Architecture of XAI-FML

personal information of sensitive data must be protected, and the individual has the right of management to access data or information for himself or herself. The figure 3.2. Shows the flow chart of XAI-FML based healthcare system where input data sent from various sectors of hospital like doctors, receptions, laboratories, management, clinical staff etc. The data then forward to the FML based Model for processing of the raw input data. After processing data transfer to the testing module and then executing phase. After testing if data is not according to defined example it repeats its iteration otherwise forwarded next. And then data transfer to cloud data storage centre in the final formed. And then final output generated and accessible to all sector by following the security algorithms. The main purpose of selecting FML technology for data classification and security because its perform its internal functionality on every single node in spite of whole architecture. After processing it transfer final processed data to central server.

3.5 Working of XAI Model

There are few surveys explore the effects of explainability and artificial intelligence in medical industry [129]. XAI mainly implemented to diagnose and in surgery. The generic application of XAI in diagnose can be easily understood through the figure 3.3. The figure adopt intrinsic and post-hoc XAI, which enable AI based examining tool to examine PHR and provide efficient decision making procedure to physicians. While in post-hoc XAI methodology the concept of black box has been used for medical diagnose and give final decision. The explanation provided to physicians based on the decision of black box.

Since few years, the need and importance of XAI has been required in few sectors like , medical, education, and industrial work. Due to the complex nature of work, decision making

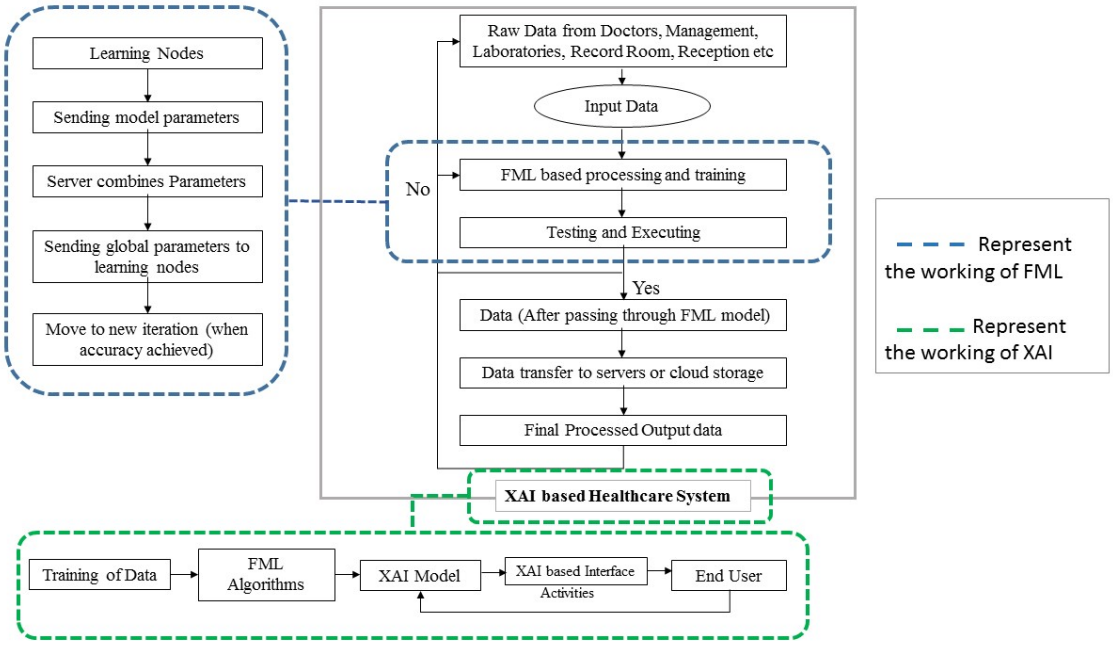


Figure 3.2: Proposed Flow-chart of XAI-FML based e-healthcare system

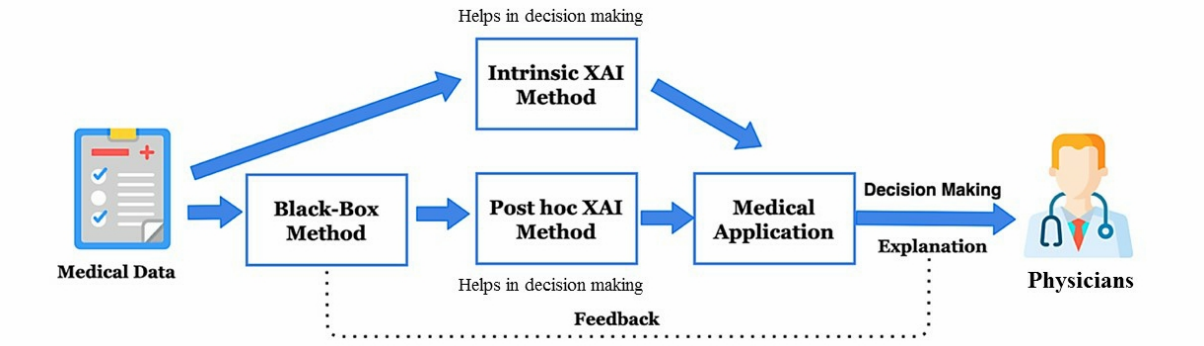


Figure 3.3: Application XAI using intrinsic and post-hoc method to make decision in diagnoses

and efficient systems are need of hours to interpret hard and difficult models with ease. Though, black box model have threatening nature, to implements it in healthcare sector will cause risk in diagnosis applications. It will also give unjustified and unreliable decision to physicians in diagnosis decision. Many studies try to overcome this issue in healthcare industry. Therefore, in the field of healthcare, the DL model which are AI based used for medical applications. Hence, it needed to design XAI based healthcare model which helps to overcome the issue of DL and black box. Though, many surveys and researches uses DL in medical applications, it is time to shift to XAI based application to provide more ease to physician to make efficient decision in diagnosis and surgeries as well. It will surely help and motivates medical researchers to deploy XAI model in medical applications and systems.

In this research work, we use XAI intelligent system and its model to make the healthcare

systems more efficient and secure. How XAI is embedded in our research scenario, here we demonstrate the working of XAI model which we show in figure 3.2. It is based on some step are as follows:

- **e-Healthcare Systems:** Every healthcare systems contain sensitive and private information or data of its patients or hospital. For every diagnose and analysis a AI based decision making model has been used, which helps to predict the chances of risks in disease or in diagnoses.
- **Predictions:** Then the PHR is used for prediction by XAI based decision making model, which get explanation.
- **Explain-ability:** The obtain explanation analysed by the practitioner or consultant. Then, the practitioner will validate the result which is generated by XAI based model to get transparency.
- **Correct Prediction:** If prediction becomes correct, then medical knowledge helped to get recommendations.
- **Wrong Prediction:** If unfortunately prediction become wrong, then concept of contradiction has been used between medical knowledge and concept of explainability, and suggest improvement in XAI model for correct future prediction or result.

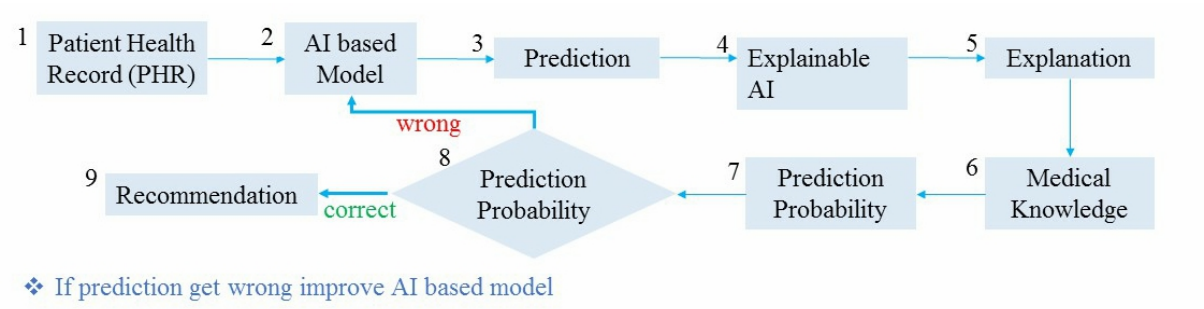


Figure 3.4: Proposed XAI decision making flow chart

The figure 3.4, illustrate the flowchart of the XAI based decision making flow chart, which can helps in medical section for expert and accurate prediction. Here, an example which can better explain the working of this proposed flowchart. Suppose, a patient with higher blood pressure comes to diagnose, consultant will examine and send the diagnosed report to the physician, report will be based on the input parameters like pulse rate, body temperature. An XAI

based model predicts the severity level of the blood pressure and generate alarm according to diagnose. The report send for final analysis, if the medical knowledge and XAI model prediction will be same then the diagnose will be correct and doctor prescribed medicine. In a case if prediction gets wrong and the result of medical knowledge and doctor are different then the next round will be generated till the AI model improves it working and generate correct decision.

3.6 Working of FML Model

In our thesis research work, we select e-healthcare industry to make systems efficient and secure, where every connected node becomes more efficient and secure by using FML algorithm. FML algorithms is based on three steps, Data training on local models, uploading trained data model to central server for data aggregation to cloud and then again data available to all connected nodes for further validation and testing phase. In this scenario, XAI helps to system to become more efficient and easy to understand for all clients or users. FML helps the clients to train data globally with breaching the privacy of the systems and data. In healthcare industry, patients personal health record is the main sensitive data which needs to be focused. In this research we mainly focus to secure PHR through FML and make healthcare systems efficient by using explainability (XAI).

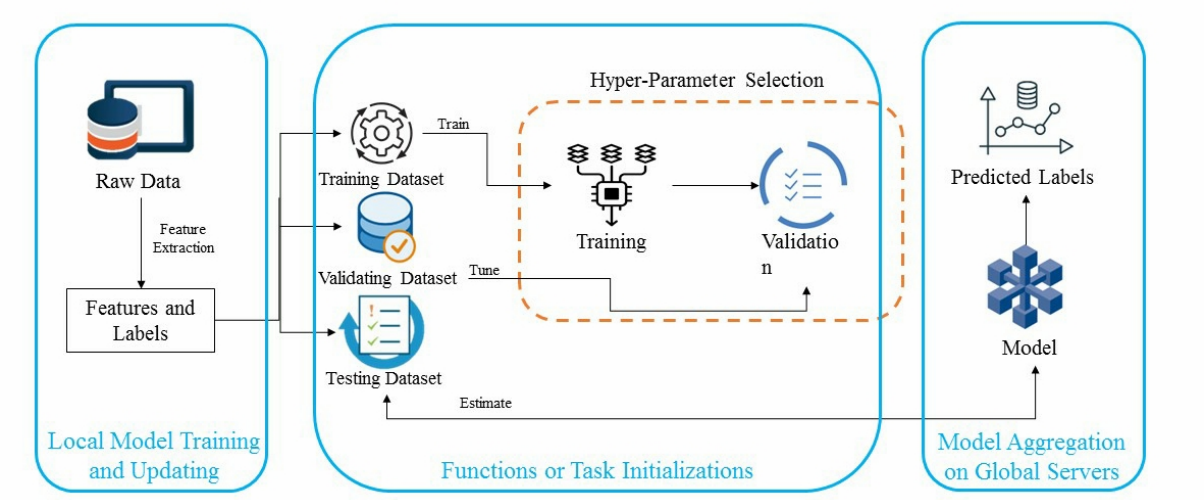


Figure 3.5: Proposed Architecture of FML

The technique for preserving privacy illustrated in the figure 3.5, which is based on three steps:

- **Work Initialization:**

  At a single time thousand of multiple devices or nodes are connected to the central or main servers and performing the training steps. Then data training servers specify the training process and set parameters of data. After performing training all the trained model send its data to the main central server for further proceedings.

- **Local Model Training:**

  One the basis of main server model, all the connected nodes train their models locally to update the selected parameters by global server. The main purpose of this step is to identify the parameters which minimize the loss function and then updated parameters sent back to the main servers. By following all these steps the flow chart of a single node data training and aggregation is represented in the figure 3.6.

- **Globally Data Aggregation:**

  When central servers receives all the parameter collected from local model or connected nodes, the main server update them and sent them back to their recipient devices to avoid data loss.

Then finally step two and three keep repeating until it reached the correct rate of accuracy with minimum loss detection. Here FMLA face some challenges during parameter updating and model training which are as: **Non-ID data:** All the data which has been sent to server with unknown and random ids, which cause big chance of privacy breaching. There may be chance of misplacement of data occurs and every connected node collect data on the basis of its connected environment. **No. of clients:** Learning models evaluate the data on the basis of connected devices or nodes and that data which is important. In this scenario, the number of connected nodes is big challenge as the connection lost and devices lost the connectivity, the data sent after training back to nodes with tendencies is big challenge. **Server's Parameter:** After increasing the work-load of large numbers of connected nodes effects the process of communication and central server aggregation. So, through server's parameter it is important to resolve by using FML. It helps to minimize the number of epochs round of communication. It reduce the cost of systems.But the main issue is, it needed more efficient and secure system to handle the data (while uploading and downloading the data), for data efficient distribution and training of data. **Connected battery and memory space:** All the connected device (working according to architecture of FML) have limited battery consumption and effects the memory

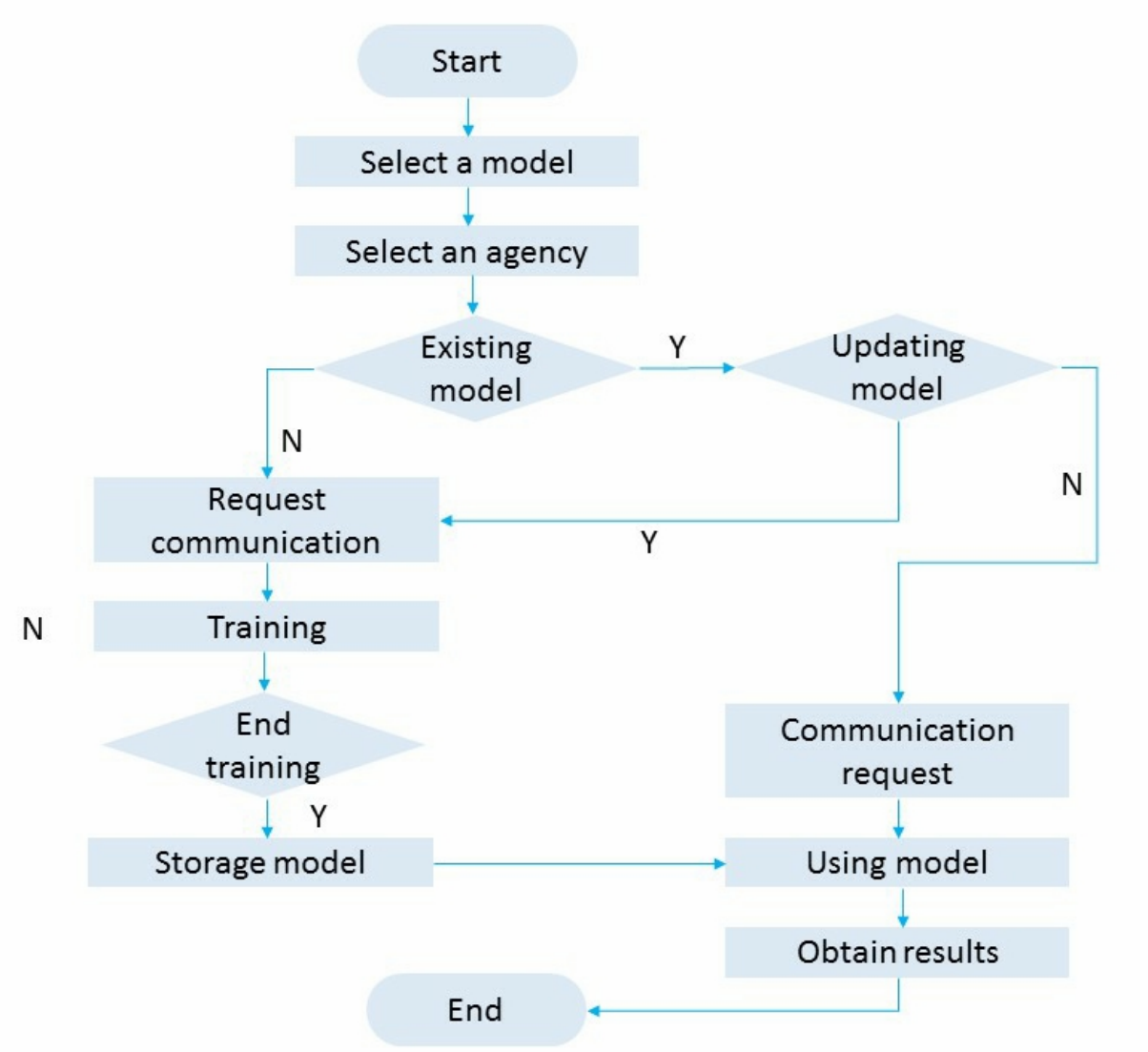


Figure 3.6: Proposed flowchart of client model training and aggregation by using FML architecture

space of local as well as globally. Though, SGD (Stochastic Gradient descent) model is used to train each iteration, working also with many DL based algorithms which effects the cost of systems badly. In order to recover these elements an efficient model has been designed.

Our proposed system is designed to make secure and efficient aggregator, which is beyond large size cryptographic techniques. At the same time, our proposed system accept third node (if they are trusted or not) on the basis of secure aggregator which set-up its keys. In many security algorithm at the end secret key revealed before them, that exploits the confidentiality of the systems, and also expose the secret key of drop-out client during process of aggregation. Our model helps to keep the secret key of drop-out devices and restrict the device to join in upcoming round of aggregation till new key adding them. In our proposed approach we use cherry pick low overhead aggregation model (C-P LOHAM), which is other than lightweight

and hashing cryptographic algorithm. Our proposed model helps to increase the efficiency and security of system. It will not trust third party and reveal secret key to them, which drop-out due to low battery consumption. On this basis of this, our crafting design for FML and secure data aggregator of every single model.

3.7 Efficient and Secure Data Aggregation Protocol

Now, here we represents the protocol for secure data aggregation model and its algorithm with mathematical working. For the cryptographic calculation we use fractional values as practical. The vector-value shows that updated value should be in the form of integers. We adopt common-scaling-factor technique, because large scaling values (sv) helps to scale fractional-value (fv) in integers. Specifically, fv and sv is given, we get integer values as fv as $\overline{fv} = b.fc.sv.c$. The approximation of fv converted into $\overline{fv}/sv$. After applying such things to our context, we scaling down the data aggregation model. In this calculation, it is to be sure that scaling function will not compromise the result and its quality. the space for scaling integer is ($2^{32} or 2^{64}$). Our proposed security algorithm 1 as been show as follow:

The steps which we compute in every single model are: **Initialization:** Suppose in our system, there are X no. of clients and every client has unique index of integer $i \epsilon [1.X]$. In this step every single node or connected device create its key by its-self, which later share to main server as public-key. Let, C be cycle of prime numbers P, along with generator G. Also, $A : \{0,1\}* \rightarrow ZP$ is the mapping of hashing cryptographic step of measuring string length in the form of integers ZP. Every client C_i creates a private key $PR\_ki = xi \epsilon ZP$ and public key $PU\_ki = G^{xi} \epsilon G$ to the main or central server. Then every C_i get public key other party and calculates $X\_k_{i,j} = A(PU\_ki)^{xi}$, here i, j ϵ X and j $\neq$ i. **FML Security:** Here we discuss about the security of aggregation process of just 1 epoch round. The main server select the η fraction of clients. Here we donated selected no. of clients with X_s. The set X_s and global model vector G_w sent to selected client. every selected client $X_k (k \epsilon X_s)$, here training process executed and global model generates $G_{w(k)}$. The masked updated model is created on the basis of blinding factor. Specifically, In vector model $G_{w(k)}$, every element of model regenerates blinding factor and produce B_k

The main idea for security of aggregation model over masked aggregator model is, if on client of third party forged the input value and add randomness to its, then other client remove that randomness from its value. Afterward, that randomness removed when summation of

Algorithm 1 Working of Secure Aggregator (FML)

Initialization:
for every client X **do**
$PR_i = x_i \epsilon ZP$
$PU_i = G^{xi} \epsilon G$
Upload PU_i to main server
for every $j \epsilon X, j \neq i$ **do**
download PU_i from main server
calculate $CK_i = A((PU_j)^{xi})$
end for
end for
Execution of Server:
Initialization of G^0
for each round t = 1,2,3,.... **do**
Fraction of client and create set τ^t
for for every client C_k in τ^t **do**
$G_k^{'t} \leftarrow$ client updation (G^{t-1}, τ)
end for
$G^{'} \leftarrow \Sigma_{k \epsilon \tau} G_k^{'t} modm$
$G^{'} \leftarrow \frac{1}{|\tau^t|} . G^{'}$
end for
(Updating at Client side ($G^t - 1\tau^t$):)
G $\leftarrow G^t - 1$
Cut dataset DS_k into batches β
for every epoch E from 1 to e **do**
for every batch β in β **do**
G G - $\eta . \bigtriangledown$ sv (G;β)
end for
end for
G_k^t G
Create vector B_k^t (blinding factor)
$B_k^t(n) = \Sigma_{n \epsilon \tau, n} (-1)^{k>n} A(CK_{k,n} || b || t)$
Calculate $G_k^{'t} \leftarrow G_k^t + B_k^t modm$
return $G_k^{'t}$ to the main central server

clients duplicated input formed. In particular, every $B_K(n)$ for nth-element in G_k generated as equation 3.1:

$$B_k(n) = \Sigma n \epsilon \tau, n \neq \tau^{(-1)^{k>n}} A(CK_i, ||b||t) \tag{3.1}$$

where $(-1)^{k>n} = -1$ if k>n and 1, otherwise 't' is counter. It can be calculate by the total of every blinding factor$\Sigma_{k \epsilon \tau} B_k(n)$ is 0 and τ is calculate when the X_s is formed.

From the above , mentioned G_k updated model where every element consider to base on

message m (where $m = 2^3 2$), every client X_s build a factor B_k and calculate as equation 3.2:

$$G_k^{'} = G_k + B_k mod m \tag{3.2}$$

here modulus operation is used to calculate the performed operation. After receiving the updates of masked model, the main or central server computes equation 3.3 and get equation 3.4 as:

$$\Sigma_{k \epsilon \tau} G_k^{'} mod m = \Sigma_{k \epsilon \tau} (G_k + B_k) mod m \tag{3.3}$$

$$\Sigma_{k \epsilon \tau} G_k mod mas \Sigma_{k \epsilon \tau^{B_k=0}} \tag{3.4}$$

CHAPTER IV
RESULTS & DISCUSSION

In this section, we perform practical proofs and shows experiment results. Then represents a comparison graph which shows the performance of Traditional FML, our proposed approach and comparison of FML and ML techniques (helps to show better performance.

4.1 Computational Proof of Security: Proposed Secure FML Algorithm

To prove the efficiency and security enhancement of our proposed model and algorithm, we choose Diffie-Helman problem, its working along with theorem as:

Definition: A cyclic group CG of order of prime number P with generator G. The CDH is consider as hard problem if, for polynomial time probability of algorithm ABC and value a & b calculated from ZP: $Pr[ABC(CG; P; G; G^a; G^b) = G^{ab}]$ is neglected.

Theorem: The hardness of CDH problem, our proposed system guarantees that main central server learns the secure aggregate model updates, without considered that client model update or not. Here is a case scenario, that if both sides (client or main server) update model at the same time collision occurs, now client model will keep the updated version (if it is true client).

Proof of Security: Every values which updates in client model CK, will keep the masked value and generate the key by using blinding factor $CK_{key,n} : A((G^{x_n})^{x_k ey})$. By using this we show that main central server is unaware from the client's secret key $CK_{key,n}$. In our system we proposed that main server can access only public key G^{x_i} of every client X, according to the setup of system. According to the CDH problem it is hard to prove that $G^a and G^b is equal to G^{ab}$. Therefore, on the basis of available public key $G^{x_k} and G^{x_n}$, the main server is not allowed to inter-fare in client's secret key $CK_{key,n} = A((G^{x_n})^{x_k})$, Then, we check the cause of collision where single node collide with the main server at the time of updation. At this point every single connected node or client share its private data to the main server. Now, here is the time when no data loss, and we give a proof of security. The real node or client is represented by C_i. Suppose set-of-client is denoted by ε in the aggregation round t and real client is denoted by ε_r and set of all those client who collide with main server is denoted by ε_{sc}. Just for revising

the data which we sent to real client C_i is represented in equation 4.1for thee n-th element off $G_{w(i)}$:

$$G_{w(i)}(n) + r_i(n) = G_{w(i)}(n) + \Sigma_{n\in\varepsilon,n\neq i}(-1)^{i>n}A(CK_{i,n}||b||t) \tag{4.1}$$

Then, ε_r and ε_{sc}, $\Sigma_{n\in\varepsilon,n\neq i}(-1)^{i>n}A(CK_{i,n}||b||t)$ can be split into two part as presented in equations 4.2 and in 4.3 ;

$$\Sigma_{n\in\varepsilon,n\neq i}(-1)^{i>n}A(CK_{i,n}||b||t) \tag{4.2}$$

$$\Sigma_{n\in\varepsilon_{sc}}(-1)^{i>n}A(CK_{i,n}||b||t) \tag{4.3}$$

So, the data which main hosting server get is represented as 4.4:

$$G_{w(i)} + \Sigma_{n\in\varepsilon,n\neq i}(-1)^{i>n}A(CK_{i,n}||b||t) + \Sigma_{n\in\varepsilon_{sc}}(-1)^{i>n}A(CK_{i,n}||b||t) \tag{4.4}$$

As ε_{sc} wjich collide with the main servers, now able to expose to the main server its part: $\Sigma_{n\in\varepsilon_{sc}}(-1)^{i>n}A(CK_{i,n}||b||t)$. By getting the collision from ε_{sc} then main server will get 4.5 :

$$G_{w(i)} + \Sigma_{n\in\varepsilon,n\neq i}(-1)^{i>n}A(CK_{i,n}||b||t) \tag{4.5}$$

After performing all the calculation, it can be concluded that real client's C_i updated model secure the data, as the honest collaboration created between all other real clients C_r. Now, the masked model and real client can be easily detected by the main server. This complete process helps to finish the proof of security.

4.2 Experiment: Interface and System Specification

For the practical implementation and result an open source collaborator has been used. It helps to implement ML and FML based algorithms by using different datasets for many tasks like data classification, image diagnoses, data maintaining and many others. This framework has been developed to facilitate open research and experimentation with Federated Learning (FL and FC) and other machine learning techniques, an approach to machine learning where a shared global model is trained across many participating clients that keep their training data locally. The following table 4.1 shows the system specification.

Table 4.1: System Specification for Experiment

Processor	Intel(R) Core(TM) i3-3110M CPU @ 2.40GHz
Memory Installed (RAM)	8.00 GB (7.89 GB usable)
System Type	64-bit Operating System, x64-based processor

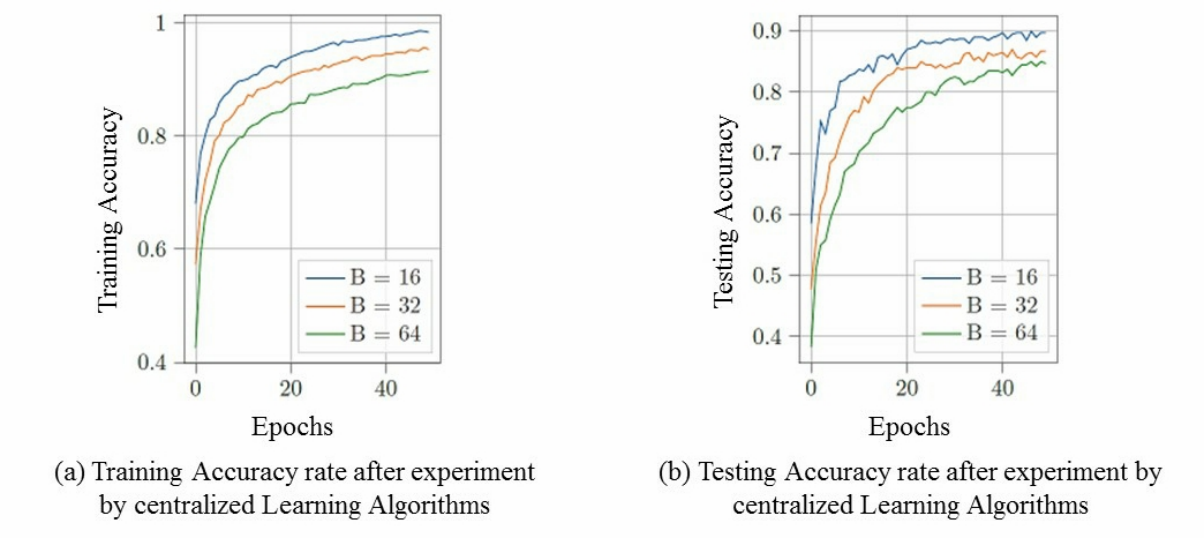
4.3 MNIST: Dataset

The dataset MNIST [1] contains data in the form of images. This dataset consider as an important data for the practical experimental in the field of ML and AI. Basically, it helps to compare and analyse the performance of ML algorithms. The MNIST dataset contains 60,000 images as a sample and have around 10,000 images for testing phase. Therefore, due to low computational space and power, in our experiment we use 500 of images and keep 20% for testing and remaining for training. The data contain all images of grey-scale vision with 28x28 (0-255 values) dimensions and having variant classes. By using the MNIST dataset following experiments has been performed to evaluate the performance. Firstly, it has been conducted on ML algorithms as a baseline. It will helps to make efficient comparison with the proposed approach. Then, proposed FML algorithms has been used for experiment and then lastly, the concept of explainability has been measured.

4.4 Experiment 1: With ML or Centralised learning Algorithms

The purpose of experiment 1 is to evaluate the architecture and performance of ML or centralised learning algorithms. And later on, the results used for comparison. In results the rate of calculated accuracy and after testing and training can be seen in the figures 4.1 and 4.2. The number of epochs and batch size (BS) value keep the same for further validation. By taking less BS the computational power is higher for training and testing phase. After passing from 20 epochs, and having BS=16 the training accuracy rate is 95% and testing accuracy is 90% with little bit overfitting. This result will be used for next comparison in experiment. The figure 4.3 shows the confusion matrix of the performed model.

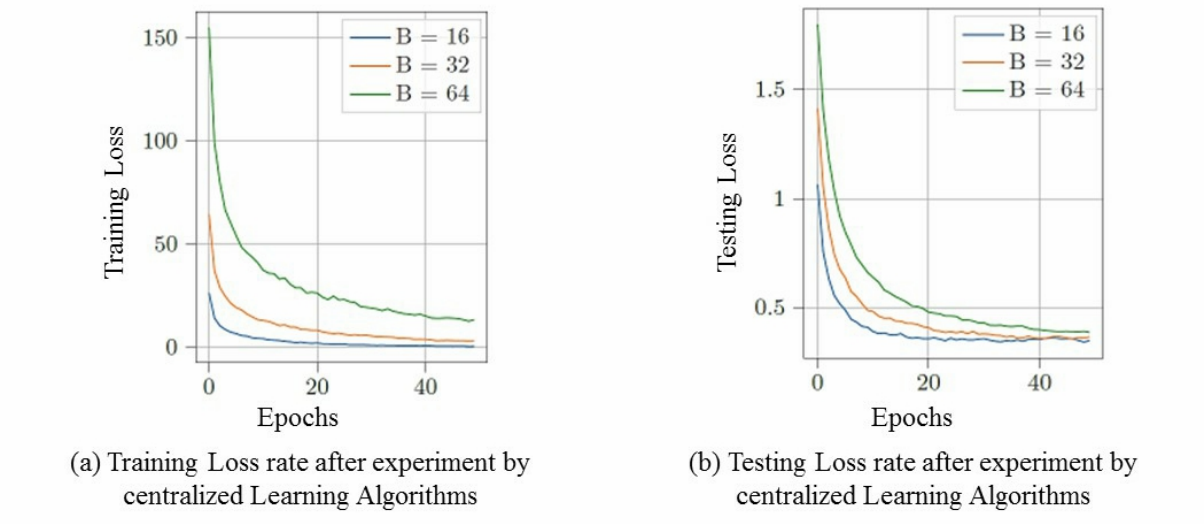
[1] https://github.com/gargarchit/Federated-Learning-on-MNIST



(a) Training Accuracy rate after experiment by centralized Learning Algorithms

(b) Testing Accuracy rate after experiment by centralized Learning Algorithms

Figure 4.1: Training Testing Accuracy rate by using Centralised Learning Algorithms where batch-size vary and having epochs=20



(a) Training Loss rate after experiment by centralized Learning Algorithms

(b) Testing Loss rate after experiment by centralized Learning Algorithms

Figure 4.2: Training & Texting Loss rate by using Centralised Learning Algorithms where batch-size vary and having epochs=20

4.5 Experiment 2: With Local Differential Model

The purpose of experiment is to calculate the rate of accuracy that how LDM effects the accuracy rate and data loss rate vs. effects of FML in large or small data distribution. In results, the training and testing accuracy rate in presented in figure 4.4 and 4.5, based on multiple epochs, where as no. of clients X= 5 and BS=16. And matrix of performed experiment represented in figure. And lastly, privacy $\in$ presented in figure 4.6. It can be easily seen that green and purple color lines show the worse output by using private differential method. At this point we can change by epochs and BS variations. By taking large epoch size FMLA stops working.

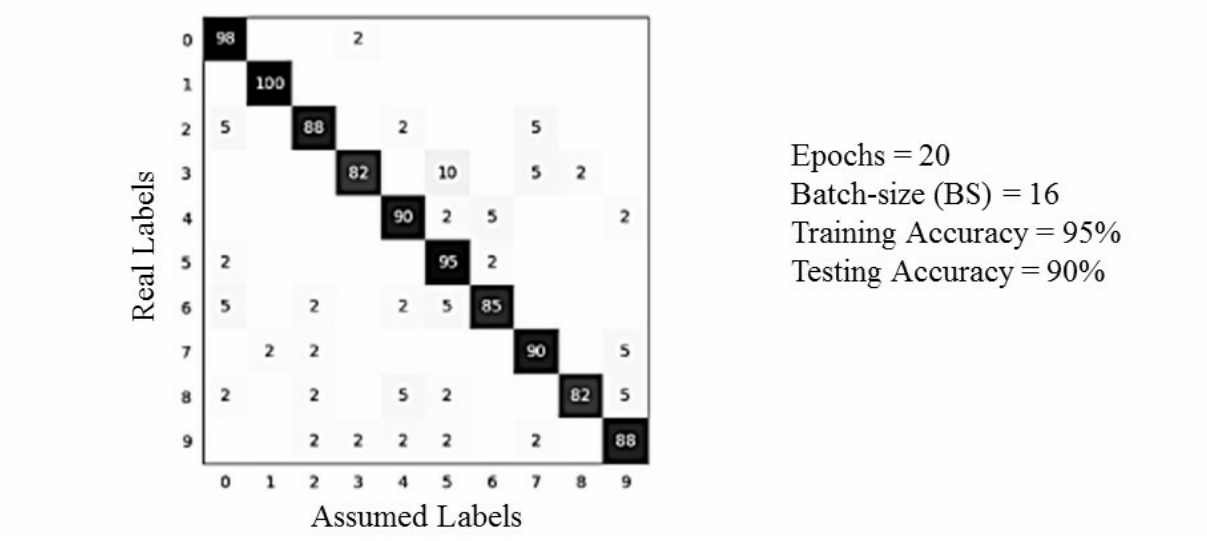
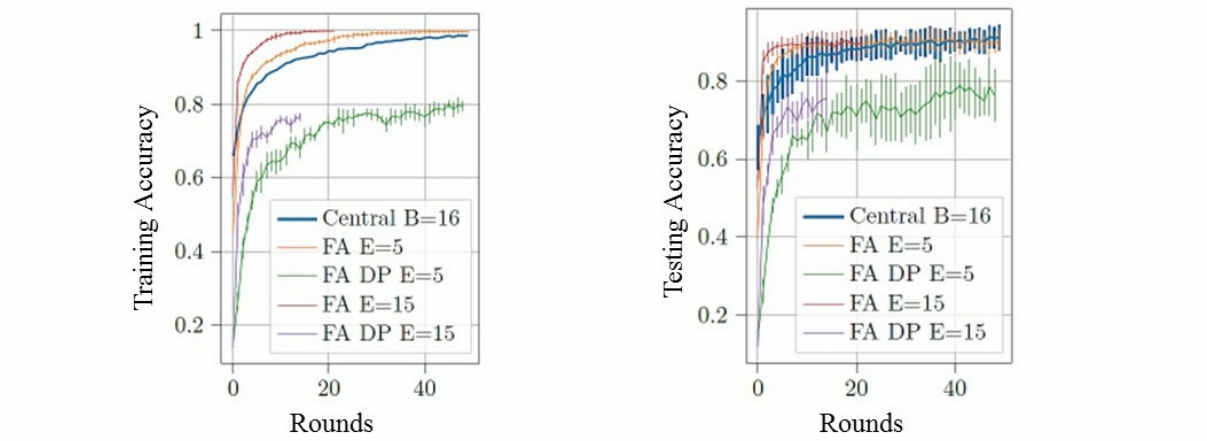


Figure 4.3: Diagram of Confusion Matrix: Training=95% & Texting=90% by using Centralised Learning Algorithms where batch-size=20 vary and having epochs=20

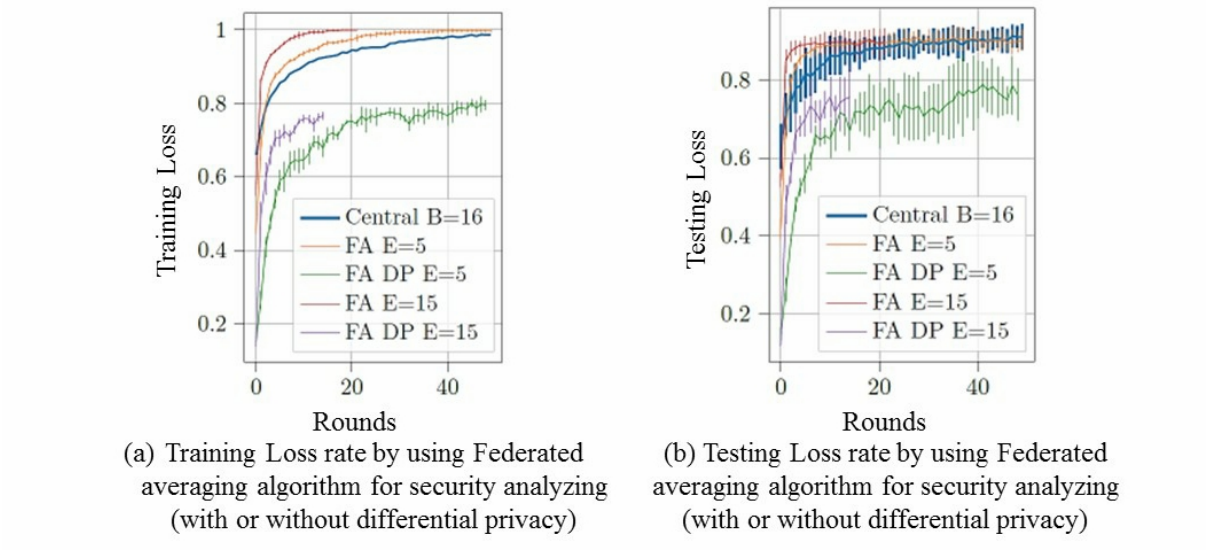
Basically, it seems alright because on local model too number number of clients X are difficult to handle which cause loss of clients at the time of aggregation of model at main central server. Lastly, It seems the cost for the deploying LDM increases as number of samples increase. Which also proves that as BS and epochs size increase the rate of accuracy in higher security also increases.



(a) Training Accuracy rate by using Federated averaging algorithm for security analyzing (with or without differential privacy)

(b) Testing Accuracy rate by using Federated averaging algorithm for security analyzing (with or without differential privacy)

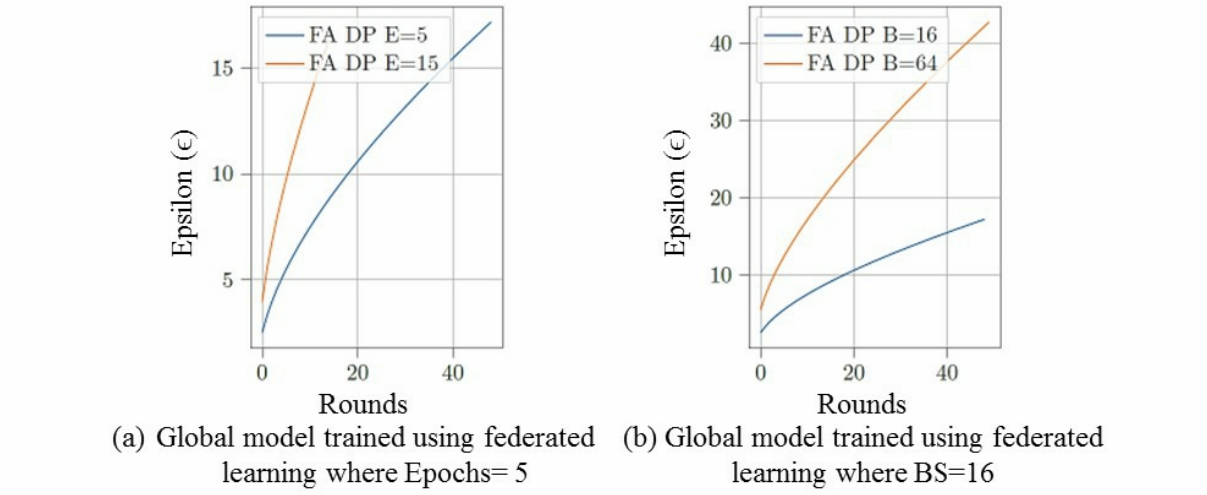
Figure 4.4: Training & Testing Accuracy rate by using proposed federated averaging algorithm at global level where BS=16 and no. of client X=5



(a) Training Loss rate by using Federated averaging algorithm for security analyzing (with or without differential privacy)

(b) Testing Loss rate by using Federated averaging algorithm for security analyzing (with or without differential privacy)

Figure 4.5: Training & Testing Loss rate by using proposed federated averaging algorithm at global level where BS=16 and no. of client X=5



(a) Global model trained using federated learning where Epochs= 5

(b) Global model trained using federated learning where BS=16

Figure 4.6: Privacy cost (Epsilon ∈) by using proposed federated averaging algorithm at global level where BS=16, no. of epochs=5 (which is fixed) and no. of client X=5

4.6 Experiment 3: Calculating Time Consumption

The purpose is to make comparison between traditional FMLA and our proposed FMLA working and execution time. As in result parameters set as default value like epochs=5, BS=16 and X=5. These parameters helps to remove redundancies from the results. The comparison between proposed algorithm and traditional federated learning algorithm has been shown in table 4.2, by using different and multiple number of epochs, rounds, clients, batch sizes. The time consumption has been computed by using standard deviation formula on almost 5 rounds.

Table 4.2: Computation time of traditional FML and proposed FML by having different epochs, clients and batch-size

Algorithm	**epoch=5**	**epoch=10**	**epoch=15**
Federated Averaging	37.23 ± 1.75	68.42 ± 0.89	99.58 ± 1.17
Federated Averaging (Differential privacy)	195.21 ± 0.59	375.28 ± 4.10	554.04 ± 0.95
Increasing rate	x5.11	x5.47	x5.58
Algorithm	**BS=16**	**BS=32**	**BS=64**
Federated Averaging		22.93 ± 0.23	17.49 ± 0.13
Federated Averaging (Differential privacy)		148.37 ± 1.41	134.89 ± 0.45
Increasing rate	x5.11	x6.20	x7.46
Algorithm	**client=3**	**client=5**	**client=10**
Federated Averaging		33.54 ± 0.45	38.58 ± 0.46
Federated Averaging (Differential privacy)		207.51 ± 1.97	260.327 ± 1.78
Increasing rate	x5.11	x5.48	x6.70

4.7 Experiment 4: Explainability in FML

The purpose of our experiment is to show that concept of explainability with the collaboration of FMLA significantly brings a bring change in performance and efficiency of systems. A SHOP plotting model is a traditional model helps to train data by following the concept of explainability. The figure 4.7, helps to illustrate the plot where DP and FML averaging models has been implemented. Here we can see that images are more clear and easy to understand. It is all due to feature of neural networks (MLP). The vision of (a) where proposed FML used show more crisp and understand image rather that (b) where data trained using centralised learning and (c) where model of FML with DP has been trained.

4.8 Comparison with State-of-Art

In our thesis research,it has been discussed that our proposed approach and security algorithm on MNIST dataset achieves higher accuracy rate with (19, $10^{-}4$), where best parameter used to provide better performance. Our performance has been compared with the research work of Michael Quach [121], where accuracy rate on differential privacy achieved (17, 10^{5}). In our research work, algorithms proves the higher accuracy and less time consumption. And in the context of explainability, proof of security has been discussed with computational analysis.

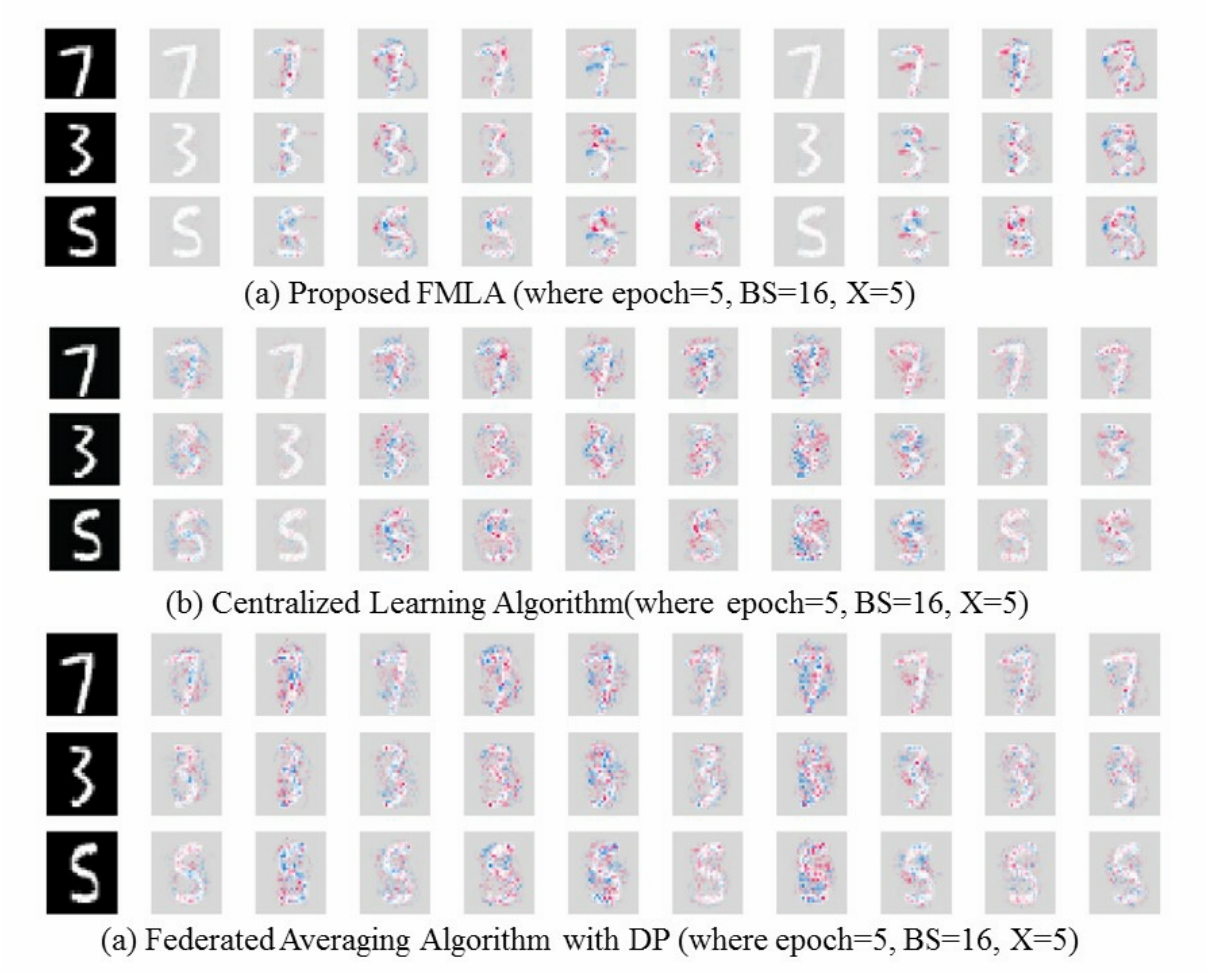


Figure 4.7: SHAP plotting model for image training where (a) shows Proposed FMLA model (b) Centralised learning algorithm (CLA) and (c) FML with DP has been trained by using MNIST dataset collected from Github

CHAPTER V

FUTURE WORK AND CONCLUSION

FUTURE WORK

Since few years, many ways has been proposed to measure and evaluate the performance of XAI, but no proper platform has been proposed, which show practical implementation. Therefore, there are no proper channel to show the working of XAI and non-XAI model [59]. Some of the measures which have been taken are just theoretical, from user and view point (for just user satisfaction). It can only be measured by subjective discussion and clarity. Now the question arises: Does just theoretical explanation fulfill the need of advance XAI system? So, the answer: it is still under processing as a future work. Currently, the concept of XAI can be easily explained through models, frameworks, flowcharts, which helps little bit to evaluate the flow of XAI based model.

Issues and Challenges for XAI

For the effective collaboration of XAI and ML has some common and essential issues and challenges listed as:

- **Computer vs. Users:**
  Can XAI explain system or knowledge to users particularly? How can we XAI explain to end users to collaborate with system and respond back as feedback?

- **Interpretation vs. Accuracy:**
  A major thread and problem for XAI is the interpret-ability, its limitations and challenges. Interpret-ability needs adjustment to get higher rate of accuracy by maintaining balance between interpret-ability, tracking and accuracy rate.

- **Competencies vs. Decision:**
  A team of highly qualified experts needed to make system understandable. So, its important to make competent AI systems for end users. And the thing is, how competency is measure and helped in decision making?

- **Confidentiality:**

  In XAI, the Decision making algorithm consider as confidential trading secret. So, it was quite difficult to find training, testing and validation updating to set functional goal. In case, if code or programmer unable to come or rectify the code its hard to overcome the shortcoming of algorithm.

- **Injustice:**

  In XAI, the system should follow the legal privacy policy and moral code of the algorithms. It must maintain the clarification.

- **Privacy or Security:**

  Similarly, Privacy and security is the key element of any decision making system. In XAI, security algorithms are essential to implement as according to described literature review, it is hard to perform practical implementation ion it.

- **Complexity:**

  Most o the time, XAI based algorithms are complex in nature. And XAI have many alternative ways to create algorithms.

- **Practical Implementation:**

  As XAI is an advance invention in the field of AI. It is quite hard to implement XAI practical, because no proper framework or interface is available for implementation. Till now its all about theoretical discussion.

Issues and Challenges for FML

Now, Federated Machine Learning Algorithms (FMLA) is new and advanced technology. SO, it also contain some issues and challenges as well. Some of the main challenges of FML, which needs to addressed in future are as:

- **Efficient Communication:**

  In FML, efficient communication (EC) is an important factor while developing model or system. It (EC) is essential because in FML scenario multiple and large number of devices or nodes are connected to each other for communication. Due to over burden, the whole system will become slower, because every single connected node train their

data and sent to cloud or main server for data aggregation. There are two types of recommendation overcome this issue.

1. shortening the communication rounds in numbers, and
2. reducing the size of data file in every round of epochs.

- **Heterogeneity (of Systems):**

  In FML based systems the power of computation, storage space and communications skills with devices differ from each other significantly. Due heterogeneity of the system, sometimes few device dropout due to low connectivity power in training process and create unreliability in the systems, which mainly cause fault tolerance in the systems.Therefore, FMLA must be designed in a way that:

  1. decrease the limit of connected nodes or enlarge the network functionality by using advance algorithms,
  2. hardware manage or resolve fault tolerance, and
  3. having robustness in lost devices in a network.

- **Statistical (Heterogeneity):**

  By using FMLA, devices connected to main server by containing anonymous identity in the network. The data which train and sent to main server may vary from every device to device or node to node. And the framed structured create relationship between devices and connection host which is used for association. It crate trouble in data modeling, testing and evaluation of the systems.

- **Privacy concern:**

  Due to privacy and security concern, FMLA allows the node to keep raw data on the local host. SO, in the step of data training at local host my breach the privacy of the data and reveal the information to irrelevant user or the main central server without passing from training step. Recently few privacy preserving methods has been used in FMLA: secure multipart computation (SMC) or differential privacy (DP). Recently, ML based privacy preserving methodologies or strategies has been used to enhance system performance and efficiency: homomorphic encryption (HE) for data encryption, and for security multiparty computation and safe functioning. Though currently, FML used ML techniques to deal with the privacy element but it should work on its own framework by using FML model and enhance the system efficiency more effectively.

CONCLUSION

In this thesis research, we use concept of explainability in AI and federated machine learning algorithm, for the efficiency and security of healthcare systems. We have documented and implemented optimised federated machine learning averaging model to optimised the performance of the system. For result comparison two more concept has been used to present the performance: Centralized learning algorithms and federated learning with differential privacy. The proposed algorithm has been evaluated on the MNIST dataset. We proposed an efficient e-healthcare framework, and detail model with flow-chart of whole healthcare system. For practical experimentation and better results and analysis, we use google collaborator and FML algorithm to test and train the dataset of PHR collected from Github website. The final results show the efficient system performance by implementing federated averaging algorithm on open source FL platform. The evaluating graphs shows the accuracy rate by taking epochs size 5, batch size 16 and no. of clients 5, which shows higher accuracy rate with ((19, $10^{-}4$). Finally, it shows the state of art and accuracy comparison with different research values.

REFERENCES

[1] Rupali Kamble and Deepali Shah. Applications of artificial intelligence in human life. *International Journal of Research–Granthaalayah*, 6(6):178–188, 2018.

[2] RITURAJ MAHATO. Artificial intelligence, what is it? *"Keep your dreams alive. Understand to achieve anything requires faith and belief in yourself, vision, hard work, determination, and dedication. Remember all things are possible for those who believe"*., page 197.

[3] S SANJANA. Artificial intelligence a super power. *"Keep your dreams alive. Understand to achieve anything requires faith and belief in yourself, vision, hard work, determination, and dedication. Remember all things are possible for those who believe"*., page 21.

[4] Ransome Epie Bawack, Samuel Fosso Wamba, and Kevin Daniel Andre Carillo. A framework for understanding artificial intelligence research: insights from practice. *Journal of Enterprise Information Management*, 2021.

[5] Marina Johnson, Abdullah Albizri, Antoine Harfouche, and Samuel Fosso-Wamba. Integrating human knowledge into artificial intelligence for complex and ill-structured problems: Informed artificial intelligence. *International Journal of Information Management*, 64:102479, 2022.

[6] Shivam Gupta, Sachin Modgil, Samadrita Bhattacharyya, and Indranil Bose. Artificial intelligence for decision support systems in the field of operations research: Review and future scope of research. *Annals of Operations Research*, pages 1–60, 2021.

[7] Jiamin Yin, Kee Yuan Ngiam, and Hock Hai Teo. Role of artificial intelligence applications in real-life clinical practice: systematic review. *Journal of medical Internet research*, 23(4):e25759, 2021.

[8] Iqbal H Sarker. Machine learning: Algorithms, real-world applications and research directions. *SN Computer Science*, 2(3):1–21, 2021.

[9] Iqbal H Sarker. Data science and analytics: an overview from data-driven smart computing, decision-making and applications perspective. *SN Computer Science*, 2(5):1–22, 2021.

[10] J Korteling, G van de Boer-Visschedijk, R Blankendaal, Rudy Boonekamp, and Aletta Eikelboom. Human-versus artificial intelligence. *Frontiers in artificial intelligence*, 4, 2021.

[11] Federico Cabitza, Davide Ciucci, Gabriella Pasi, and Marco Viviani. Responsible ai in healthcare. *arXiv preprint arXiv:2203.03616*, 2022.

[12] Rajat Gera and Priyanka Chadha. Narrative review of game ai 2000 onwards and future research directions. *Handbook of Research on Innovative Management Using AI in Industry 5.0*, pages 192–203, 2022.

[13] Chih-Hung Chen, Chorng-Shiuh Koong, and Chien Liao. Influences of integrating dynamic assessment into a speech recognition learning design to support students' english speaking skills, learning anxiety and cognitive load. *Educational Technology & Society*, 25(1):1–14, 2022.

[14] André Sagodi, Christian Engel, Johannes Schniertshauer, and Benjamin Van Giffen. Becoming certain about the uncertain: How ai changes proof-of-concept activities in manufacturing–insights from a global automotive leader. In *Proceedings of the 55th Hawaii International Conference on System Sciences*, 2022.

[15] Rabia Abid, Bakhtawar Aslam, Sadaf Shakeel, Fahad Ahmad, and Muhammad Rizwan. Implementation of high dimensional-qkd using bb84 protocol in the security of aerospace industry. In *2019 International Conference on Innovative Computing (ICIC)*, pages 1–11. IEEE, 2019.

[16] Sofia Samoili, Montserrat Lopez Cobo, Emilia Gomez, Giuditta De Prato, Fernando Martinez-Plumed, and Blagoj Delipetrev. Ai watch. defining artificial intelligence. towards an operational definition and taxonomy of artificial intelligence. 2020.

[17] S Menaga and J Paruvathavardhini. Ai in healthcare. *Smart Systems for Industrial Applications*, pages 115–140, 2022.

[18] Rabia Abid, Bakhtawar Aslam, Muhammad Rizwan, Fahad Ahmad, and Mian Usman Sattar. Block-chain-security advancement in medical sector for sharing medical records. In *2019 International Conference on Innovative Computing (ICIC)*, pages 1–9. IEEE, 2019.

[19] Jerzy Respondek. Matrix black box algorithms–a survey. *Bulletin of the Polish Academy of Sciences: Technical Sciences*, pages e140535–e140535.

[20] Yang Xiong, Yangchang Zhang, Fuxun Zhang, Changjing Wu, Feng Qin, and Jiuhong Yuan. Applications of artificial intelligence in the diagnosis and prediction of erectile dysfunction: a narrative review. *International journal of impotence research*, pages 1–8, 2022.

[21] Massimo Regona, Tan Yigitcanlar, Bo Xia, and Rita Yi Man Li. Opportunities and adoption challenges of ai in the construction industry: A prisma review. *Journal of Open Innovation: Technology, Market, and Complexity*, 8(1):45, 2022.

[22] Tim Miller, Robert Hoffman, Ofra Amir, and Andreas Holzinger. Special issue on explainable artificial intelligence (xai), 2022.

[23] Cecilia Zanni-Merk and Anne Jeannin-Girardon. Towards the joint use of symbolic and connectionist approaches for explainable artificial intelligence. In *Advances in Selected Artificial Intelligence Areas*, pages 271–286. Springer, 2022.

[24] Finale Doshi-Velez and Been Kim. Towards a rigorous science of interpretable machine learning. *arXiv preprint arXiv:1702.08608*, 2017.

[25] Mi-Young Kim, Shahin Atakishiyev, Housam Khalifa Bashier Babiker, Nawshad Farruque, Randy Goebel, Osmar R Zaïane, Mohammad-Hossein Motallebi, Juliano Rabelo, Talat Syed, Hengshuai Yao, et al. A multi-component framework for the analysis and design of explainable artificial intelligence. *Machine Learning and Knowledge Extraction*, 3(4):900–921, 2021.

[26] Scott M Lundberg and Su-In Lee. A unified approach to interpreting model predictions. *Advances in neural information processing systems*, 30, 2017.

[27] Zhe Fan, Xing Hu, Wen-Ming Chen, Da-Wei Zhang, and Xin Ma. A deep learning based 2-dimensional hip pressure signals analysis method for sitting posture recognition. *Biomedical Signal Processing and Control*, 73:103432, 2022.

[28] Bolei Zhou, Aditya Khosla, Agata Lapedriza, Aude Oliva, and Antonio Torralba. Learning deep features for discriminative localization. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 2921–2929, 2016.

[29] Ramprasaath R Selvaraju, Michael Cogswell, Abhishek Das, Ramakrishna Vedantam, Devi Parikh, and Dhruv Batra. Grad-cam: Visual explanations from deep networks via gradient-based localization. In *Proceedings of the IEEE international conference on computer vision*, pages 618–626, 2017.

[30] Yanjie Li and He Mao. Study on machine learning applications in ideological and political education under the background of big data. *Scientific Programming*, 2022, 2022.

[31] Zhiqin Wang, Ying Du, Kejun Wei, Kaifeng Han, Xiaoyan Xu, Guiming Wei, Wen Tong, Peiying Zhu, Jianglei Ma, Jun Wang, et al. Vision, application scenarios, and key technology trends for 6g mobile communications. *Science China Information Sciences*, 65(5):1–27, 2022.

[32] Shamik Kundu, Kanad Basu, Mehdi Sadi, Twisha Titirsha, Shihao Song, Anup Das, and Ujjwal Guin. Special session: Reliability analysis for ml/ai hardware. *arXiv preprint arXiv:2103.12166*, 2021.

[33] Jobeda Jamal Khanam and Simon Y Foo. A comparison of machine learning algorithms for diabetes prediction. *ICT Express*, 7(4):432–439, 2021.

[34] Christian Tchito Tchapga, Thomas Attia Mih, Aurelle Tchagna Kouanou, Theophile Fozin Fonzin, Platini Kuetche Fogang, Brice Anicet Mezatio, and Daniel Tchiotsop. Biomedical image classification in a big data architecture using machine learning algorithms. *Journal of Healthcare Engineering*, 2021, 2021.

[35] Sudhakar Sengan, R Vidya Sagar, R Ramesh, Osamah Ibrahim Khalaf, and R Dhanapal. The optimization of reconfigured real-time datasets for improving classification performance of machine learning algorithms. *Mathematics in Engineering, Science & Aerospace (MESA)*, 12(1), 2021.

[36] Akshit Garg, Vijay Vignesh Venkataramani, Akshaya Karthikeyan, and U Priyakumar. Modern ai/ml methods for healthcare: Opportunities and challenges. In *International Conference on Distributed Computing and Internet Technology*, pages 3–25. Springer, 2022.

[37] Ahmedbahaaaldin Ibrahem Ahmed Osman, Ali Najah Ahmed, Yuk Feng Huang, Pavitra Kumar, Ahmed H Birima, Mohsen Sherif, Ahmed Sefelnasr, Abdel Azim Ebraheemand, and Ahmed El-Shafie. Past, present and perspective methodology for groundwater modeling-based machine learning approaches. *Archives of Computational Methods in Engineering*, pages 1–17, 2022.

[38] Zarlish Ashfaq, Rafia Mumtaz, Abdur Rafay, Syed Mohammad Hassan Zaidi, Hadia Saleem, Sadaf Mumtaz, Adnan Shahid, Eli De Poorter, and Ingrid Moerman. Embedded ai-based digi-healthcare. *Applied Sciences*, 12(1):519, 2022.

[39] Rahma Mukta, Hye-young Paik, Qinghua Lu, and Salil S Kanhere. A survey of data minimisation techniques in blockchain-based healthcare. *Computer Networks*, page 108766, 2022.

[40] Jorge Munoz-Gama, Niels Martin, Carlos Fernandez-Llatas, Owen A Johnson, Marcos Sepúlveda, Emmanuel Helm, Victor Galvez-Yanjari, Eric Rojas, Antonio Martinez-Millana, Davide Aloini, et al. Process mining for healthcare: Characteristics and challenges. *Journal of Biomedical Informatics*, 127:103994, 2022.

[41] Chaoyang He, Songze Li, Jinhyun So, Xiao Zeng, Mi Zhang, Hongyi Wang, Xiaoyang Wang, Praneeth Vepakomma, Abhishek Singh, Hang Qiu, et al. Fedml: A research library and benchmark for federated machine learning. *arXiv preprint arXiv:2007.13518*, 2020.

[42] Tiffany Tuor, Shiqiang Wang, Theodoras Salonidis, Bong Jun Ko, and Kin K Leung. Demo abstract: Distributed machine learning at resource-limited edge nodes. In *IEEE INFOCOM 2018-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 1–2. IEEE, 2018.

[43] Joost Verbraeken, Matthijs Wolting, Jonathan Katzy, Jeroen Kloppenburg, Tim Verbelen, and Jan S Rellermeyer. A survey on distributed machine learning. *ACM Computing Surveys (CSUR)*, 53(2):1–33, 2020.

[44] Fadila Zerka, Samir Barakat, Sean Walsh, Marta Bogowicz, Ralph TH Leijenaar, Arthur Jochems, Benjamin Miraglio, David Townend, and Philippe Lambin. Systematic review of privacy-preserving distributed machine learning from federated databases in health care. *JCO clinical cancer informatics*, 4:184–200, 2020.

[45] Dianbo Liu, Dmitriy Dligach, and Timothy Miller. Two-stage federated phenotyping and patient representation learning. In *Proceedings of the conference. Association for Computational Linguistics. Meeting*, volume 2019, page 283. NIH Public Access, 2019.

[46] Ahmet Ali SÜZEN and Mehmet Ali ŞİMŞEK. A novel approach to machine learning application to protection privacy data in healthcare: Federated learning. *Namık Kemal Tıp Dergisi*, 8(1):22–30, 2020.

[47] Satyabrata Aich, Nday Kabulo Sinai, Saurabh Kumar, Mohammed Ali, Yu Ran Choi, Moon-IL Joo, and Hee-Cheol Kim. Protecting personal healthcare record using blockchain & federated learning technologies. In *2022 24th International Conference on Advanced Communication Technology (ICACT)*, pages 109–112. IEEE, 2022.

[48] Qi Dou, Tiffany Y So, Meirui Jiang, Quande Liu, Varut Vardhanabhuti, Georgios Kaissis, Zeju Li, Weixin Si, Heather HC Lee, Kevin Yu, et al. Federated deep learning for detecting covid-19 lung abnormalities in ct: a privacy-preserving multinational validation study. *NPJ digital medicine*, 4(1):1–11, 2021.

[49] Yufeng Zhan, Peng Li, Zhihao Qu, Deze Zeng, and Song Guo. A learning-based incentive mechanism for federated learning. *IEEE Internet of Things Journal*, 7(7):6360–6368, 2020.

[50] Md Manjurul Ahsan and Zahed Siddique. Machine learning-based heart disease diagnosis: A systematic literature review. *Artificial Intelligence in Medicine*, page 102289, 2022.

[51] Matthew Oyeleye, Tianhua Chen, Sofya Titarenko, and Grigoris Antoniou. A predictive analysis of heart rates using machine learning techniques. *International Journal of Environmental Research and Public Health*, 19(4):2417, 2022.

[52] Daniel A Domingo-Lopez, Giulia Lattanzi, Lucien HJ Schreiber, Eimear J Wallace, Robert Wylie, Janice O'Sullivan, Eimear B Dolan, and Garry P Duffy. Medical devices,

smart drug delivery, wearables and technology for the treatment of diabetes mellitus. *Advanced Drug Delivery Reviews*, page 114280, 2022.

[53] Kyoung Hwa Lee, Jae June Dong, Subin Kim, Dayeong Kim, Jong Hoon Hyun, Myeong-Hun Chae, Byeong Soo Lee, and Young Goo Song. Prediction of bacteremia based on 12-year medical data using a machine learning approach: Effect of medical data by extraction time. *Diagnostics*, 12(1):102, 2022.

[54] G Umashankar, P Abinaya, J Premkumar, T Sudhakar, and S Krishnakumar. Evolution of electronic health records. *The Internet of Medical Things (IoMT) Healthcare Transformation*, pages 143–160, 2022.

[55] Steven Lin. A clinician's guide to artificial intelligence (ai): Why and how primary care should lead the health care ai revolution. *The Journal of the American Board of Family Medicine*, 35(1):175–184, 2022.

[56] Pijush Kanti Dutta Pramanik, Saurabh Pal, and Moutan Mukhopadhyay. Healthcare big data: A comprehensive overview. *Research Anthology on Big Data Analytics, Architectures, and Applications*, pages 119–147, 2022.

[57] Michael F Gensheimer, Sonya Aggarwal, Kathryn RK Benson, Justin N Carter, A Solomon Henry, Douglas J Wood, Scott G Soltys, Steven Hancock, Erqi Pollom, Nigam H Shah, et al. Automated model versus treating physician for predicting survival time of patients with metastatic cancer. *Journal of the American Medical Informatics Association*, 28(6):1108–1116, 2021.

[58] Arpit Kumar Sharma, Amita Nandal, Arvind Dhaka, and Rahul Dixit. Medical image classification techniques and analysis using deep learning networks: A review. *Health Informatics: A Computational Perspective in Healthcare*, pages 233–258, 2021.

[59] David Gunning, Mark Stefik, Jaesik Choi, Timothy Miller, Simone Stumpf, and Guang-Zhong Yang. Xai—explainable artificial intelligence. *Science Robotics*, 4(37):eaay7120, 2019.

[60] Filip Karlo Došilović, Mario Brčić, and Nikica Hlupić. Explainable artificial intelligence: A survey. In *2018 41st International convention on information and communi-*

cation technology, electronics and microelectronics (MIPRO), pages 0210–0215. IEEE, 2018.

[61] Christine M Cutillo, Karlie R Sharma, Luca Foschini, Shinjini Kundu, Maxine Mackintosh, and Kenneth D Mandl. Machine intelligence in healthcare—perspectives on trustworthiness, explainability, usability, and transparency. *NPJ digital medicine*, 3(1):1–5, 2020.

[62] Prerna Juneja and Tanushree Mitra. Algorithmic nudge to make better choices: Evaluating effectiveness of xai frameworks to reveal biases in algorithmic decision making to users. *arXiv preprint arXiv:2202.02479*, 2022.

[63] Andreas Holzinger, Anna Saranti, Christoph Molnar, Przemyslaw Biecek, and Wojciech Samek. Explainable ai methods-a brief overview. In *International Workshop on Extending Explainable AI Beyond Deep Models and Classifiers*, pages 13–38. Springer, 2022.

[64] Gesina Schwalbe and Bettina Finzel. Xai method properties: A (meta-) study. *arXiv preprint arXiv:2105.07190*, 2021.

[65] Sheikh Rabiul Islam, William Eberle, Sheikh Khaled Ghafoor, and Mohiuddin Ahmed. Explainable artificial intelligence approaches: A survey. *arXiv preprint arXiv:2101.09429*, 2021.

[66] Giulia Vilone and Luca Longo. Notions of explainability and evaluation approaches for explainable artificial intelligence. *Information Fusion*, 76:89–106, 2021.

[67] Sayantan Polley, Atin Janki, Marcus Thiel, Juliane Hoebel-Mueller, and Andreas Nuernberger. Exdocs: Evidence based explainable document search. In *ACM SIGIR Workshop on Causality in Search and Recommendation*, 2021.

[68] Jianlong Zhou, Amir H Gandomi, Fang Chen, and Andreas Holzinger. Evaluating the quality of machine learning explanations: A survey on methods and metrics. *Electronics*, 10(5):593, 2021.

[69] Julie Gerlings, Arisa Shollo, and Ioanna Constantiou. Reviewing the need for explainable artificial intelligence (xai). *arXiv preprint arXiv:2012.01007*, 2020.

[70] Marina Danilevsky, Kun Qian, Ranit Aharonov, Yannis Katsis, Ban Kawas, and Prithviraj Sen. A survey of the state of explainable ai for natural language processing. *arXiv preprint arXiv:2010.00711*, 2020.

[71] Q Vera Liao, Daniel Gruen, and Sarah Miller. Questioning the ai: informing design practices for explainable ai user experiences. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–15, 2020.

[72] Diogo V Carvalho, Eduardo M Pereira, and Jaime S Cardoso. Machine learning interpretability: A survey on methods and metrics. *Electronics*, 8(8):832, 2019.

[73] Amina Adadi and Mohammed Berrada. Peeking inside the black-box: a survey on explainable artificial intelligence (xai). *IEEE access*, 6:52138–52160, 2018.

[74] Leilani H Gilpin, David Bau, Ben Z Yuan, Ayesha Bajwa, Michael Specter, and Lalana Kagal. Explaining explanations: An overview of interpretability of machine learning. In *2018 IEEE 5th International Conference on data science and advanced analytics (DSAA)*, pages 80–89. IEEE, 2018.

[75] Ramisetty Kavya, Jabez Christopher, Subhrakanta Panda, and Y Bakthasingh Lazarus. Machine learning and xai approaches for allergy diagnosis. *Biomedical Signal Processing and Control*, 69:102681, 2021.

[76] Nicola Amoroso, Domenico Pomarico, Annarita Fanizzi, Vittorio Didonna, Francesco Giotta, Daniele La Forgia, Agnese Latorre, Alfonso Monaco, Ester Pantaleo, Nicole Petruzzellis, et al. A roadmap towards breast cancer therapies supported by explainable artificial intelligence. *Applied Sciences*, 11(11):4881, 2021.

[77] Carlo Dindorf, Jürgen Konradi, Claudia Wolf, Bertram Taetz, Gabriele Bleser, Janine Huthwelker, Friederike Werthmann, Eva Bartaguiz, Johanna Kniepert, Philipp Drees, et al. Classification and automated interpretation of spinal posture data using a pathology-independent classifier and explainable artificial intelligence (xai). *Sensors*, 21(18):6323, 2021.

[78] Shaker El-Sappagh, Jose M Alonso, SM Islam, Ahmad M Sultan, and Kyung Sup Kwak. A multilayer multimodal detection and prediction model based on explainable artificial intelligence for alzheimer's disease. *Scientific reports*, 11(1):1–26, 2021.

[79] Junfeng Peng, Kaiqiang Zou, Mi Zhou, Yi Teng, Xiongyong Zhu, Feifei Zhang, and Jun Xu. An explainable artificial intelligence framework for the deterioration risk prediction of hepatitis patients. *Journal of Medical Systems*, 45(5):1–9, 2021.

[80] Salih Sarp, Murat Kuzlu, Emmanuel Wilson, Umit Cali, and Ozgur Guler. The enlightening role of explainable artificial intelligence in chronic wound classification. *Electronics*, 10(12):1406, 2021.

[81] Weimin Tan, Pengfei Guan, Lingjie Wu, Hedan Chen, Jichun Li, Yu Ling, Ting Fan, Yunfeng Wang, Jian Li, and Bo Yan. The use of explainable artificial intelligence to explore types of fenestral otosclerosis misdiagnosed when using temporal bone high-resolution computed tomography. *Annals of Translational Medicine*, 9(12), 2021.

[82] Haoran Wu, Wei Chen, Shuang Xu, and Bo Xu. Counterfactual supporting facts extraction for explainable medical record based diagnosis with graph network. In *Proceedings of the 2021 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies*, pages 1942–1955, 2021.

[83] Jun Chen, Xiaoya Dai, Quan Yuan, Chao Lu, and Haifeng Huang. Towards interpretable clinical diagnosis with bayesian network ensembles stacked on entity-aware cnns. In *Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics*, pages 3143–3153, 2020.

[84] Matteo Rucco, Giovanna Viticchi, and Lorenzo Falsetti. Towards personalized diagnosis of glioblastoma in fluid-attenuated inversion recovery (flair) by topological interpretable machine learning. *Mathematics*, 8(5):770, 2020.

[85] Donghao Gu, Yaowei Li, Feng Jiang, Zhaojing Wen, Shaohui Liu, Wuzhen Shi, Guangming Lu, and Changsheng Zhou. Vinet: A visually interpretable image diagnosis network. *IEEE Transactions on Multimedia*, 22(7):1720–1729, 2020.

[86] Jean-Philippe Kröll, Simon B Eickhoff, Felix Hoffstaedter, and Kaustubh R Patil. Evolving complex yet interpretable representations: application to alzheimer's diagnosis and prognosis. In *2020 IEEE Congress on Evolutionary Computation (CEC)*, pages 1–8. IEEE, 2020.

[87] Anna Meldo, Lev Utkin, Maxim Kovalev, and Ernest Kasimov. The natural language explanation algorithms for the lung cancer computer-aided diagnosis system. *Artificial Intelligence in Medicine*, 108:101952, 2020.

[88] Dacosta Yeboah, Louis Steinmeister, Daniel B Hier, Bassam Hadi, Donald C Wunsch, Gayla R Olbricht, and Tayo Obafemi-Ajayi. An explainable and statistically validated ensemble clustering model applied to the identification of traumatic brain injury subgroups. *IEEE Access*, 8:180690–180705, 2020.

[89] Linda Wang, Zhong Qiu Lin, and Alexander Wong. Covid-net: A tailored deep convolutional neural network design for detection of covid-19 cases from chest x-ray images. *Scientific Reports*, 10(1):1–12, 2020.

[90] Patrik Sabol, Peter Sinčák, Pitoyo Hartono, Pavel Kočan, Zuzana Benetinová, Alžbeta Blichárová, L'udmila Verbóová, Erika Štammová, Antónia Sabolová-Fabianová, and Anna Jašková. Explainable classifier for improving the accountability in decision-making for colorectal cancer diagnosis from histopathological images. *Journal of biomedical informatics*, 109:103523, 2020.

[91] Xi Wei, Jialin Zhu, Haozhi Zhang, Hongyan Gao, Ruiguo Yu, Zhiqiang Liu, Xiangqian Zheng, Ming Gao, and Sheng Zhang. Visual interpretability in computer-assisted diagnosis of thyroid nodules using ultrasound images. *Medical science monitor: international medical journal of experimental and clinical research*, 26:e927007–1, 2020.

[92] Yu-Wei Chang, Shih-Jen Tsai, Yung-Fu Wu, and Albert C Yang. Development of an al-based web diagnostic system for phenotyping psychiatric disorders. *Frontiers in Psychiatry*, page 1060, 2020.

[93] Pavan Rajkumar Magesh, Richard Delwin Myloth, and Rijo Jackson Tom. An explainable machine learning model for early detection of parkinson's disease using lime on datscan imagery. *Computers in Biology and Medicine*, 126:104041, 2020.

[94] Tae Keun Yoo, Ik Hee Ryu, Hannuy Choi, Jin Kuk Kim, In Sik Lee, Jung Sub Kim, Geunyoung Lee, and Tyler Hyungtaek Rim. Explainable machine learning approach as a tool to understand factors used to select the refractive surgery technique on the expert level. *Translational vision science & technology*, 9(2):8–8, 2020.

[95] Nykan Mirchi, Vincent Bissonnette, Recai Yilmaz, Nicole Ledwos, Alexander Winkler-Schwartz, and Rolando F Del Maestro. The virtual operative assistant: An explainable artificial intelligence tool for simulation-based training in surgery and medicine. *PloS one*, 15(2):e0229596, 2020.

[96] Jin Cho, Alnour Alharin, Zhen Hu, Nancy Fell, and Mina Sartipi. Predicting post-stroke hospital discharge disposition using interpretable machine learning approaches. In *2019 IEEE International Conference on Big Data (Big Data)*, pages 4817–4822. IEEE, 2019.

[97] Jean-Baptiste Lamy, Boomadevi Sekar, Gilles Guezennec, Jacques Bouaud, and Brigitte Séroussi. Explainable artificial intelligence for breast cancer: A visual case-based reasoning approach. *Artificial intelligence in medicine*, 94:42–53, 2019.

[98] Diptesh Das, Junichi Ito, Tadashi Kadowaki, and Koji Tsuda. An interpretable machine learning model for diagnosis of alzheimer's disease. *PeerJ*, 7:e6543, 2019.

[99] Hassan Ismail Fawaz, Germain Forestier, Jonathan Weber, Lhassane Idoumghar, and Pierre-Alain Muller. Accurate and interpretable evaluation of surgical skills from kinematic data using fully convolutional neural networks. *International journal of computer assisted radiology and surgery*, 14(9):1611–1617, 2019.

[100] Sabrina Kletz, Klaus Schoeffmann, and Heinrich Husslein. Learning the representation of instrument images in laparoscopy videos. *Healthcare Technology Letters*, 6(6):197–203, 2019.

[101] Deepak Roy Chittajallu, Bo Dong, Paul Tunison, Roddy Collins, Katerina Wells, James Fleshman, Ganesh Sankaranarayanan, Steven Schwaitzberg, Lora Cavuoto, and Andinet Enquobahrie. Xai-cbir: Explainable ai system for content based retrieval of video frames from minimally invasive surgery videos. In *2019 IEEE 16th International Symposium on Biomedical Imaging (ISBI 2019)*, pages 66–69. IEEE, 2019.

[102] Khan Muhammad, Salman Khan, Javier Del Ser, and Victor Hugo C De Albuquerque. Deep learning for multigrade brain tumor classification in smart healthcare systems: A prospective survey. *IEEE Transactions on Neural Networks and Learning Systems*, 32(2):507–522, 2020.

[103] Viraaji Mothukuri, Reza M Parizi, Seyedamin Pouriyeh, Yan Huang, Ali Dehghantanha, and Gautam Srivastava. A survey on security and privacy of federated learning. *Future Generation Computer Systems*, 115:619–640, 2021.

[104] Suraj Rajendran, Jihad S Obeid, Hamidullah Binol, Kristie Foley, Wei Zhang, Philip Austin, Joey Brakefield, Metin N Gurcan, and Umit Topaloglu. Cloud-based federated learning implementation across medical centers. *JCO Clinical Cancer Informatics*, 5:1–11, 2021.

[105] Zengqiang Yan, Jeffry Wicaksana, Zhiwei Wang, Xin Yang, and Kwang-Ting Cheng. Variation-aware federated learning with multi-source decentralized medical image data. *IEEE Journal of Biomedical and Health Informatics*, 25(7):2615–2628, 2020.

[106] Mustafa Abdul Salam, Sanaa Taha, and Mohamed Ramadan. Covid-19 detection using federated machine learning. *PLoS One*, 16(6):e0252573, 2021.

[107] Ines Feki, Sourour Ammar, Yousri Kessentini, and Khan Muhammad. Federated learning for covid-19 screening from chest x-ray images. *Applied Soft Computing*, 106:107330, 2021.

[108] Longling Zhang, Bochen Shen, Ahmed Barnawi, Shan Xi, Neeraj Kumar, and Yi Wu. Feddpgan: federated differentially private generative adversarial networks framework for the detection of covid-19 pneumonia. *Information Systems Frontiers*, 23(6):1403–1415, 2021.

[109] Yiqiang Chen, Xin Qin, Jindong Wang, Chaohui Yu, and Wen Gao. Fedhealth: A federated transfer learning framework for wearable healthcare. *IEEE Intelligent Systems*, 35(4):83–93, 2020.

[110] Qiong Wu, Xu Chen, Zhi Zhou, and Junshan Zhang. Fedhome: Cloud-edge based personalized federated learning for in-home health monitoring. *IEEE Transactions on Mobile Computing*, 2020.

[111] Prateek Chhikara, Prabhjot Singh, Rajkumar Tekchandani, Neeraj Kumar, and Mohsen Guizani. Federated learning meets human emotions: A decentralized framework for human–computer interaction for iot applications. *IEEE Internet of Things Journal*, 8(8):6949–6962, 2020.

[112] Li Huang, Andrew L Shea, Huining Qian, Aditya Masurkar, Hao Deng, and Dianbo Liu. Patient clustering improves efficiency of federated machine learning to predict mortality and hospital stay time using distributed electronic medical records. *Journal of biomedical informatics*, 99:103291, 2019.

[113] Theodora S Brisimi, Ruidi Chen, Theofanie Mela, Alex Olshevsky, Ioannis Ch Paschalidis, and Wei Shi. Federated learning of predictive models from federated electronic health records. *International journal of medical informatics*, 112:59–67, 2018.

[114] Rulin Shao, Hongyu He, Ziwei Chen, Hui Liu, Dianbo Liu, et al. Stochastic channel-based federated learning with neural network pruning for medical data privacy preservation: model development and experimental validation. *JMIR Formative Research*, 4(12):e17265, 2020.

[115] Akhil Vaid, Suraj K Jaladanki, Jie Xu, Shelly Teng, Arvind Kumar, Samuel Lee, Sulaiman Somani, Ishan Paranjpe, Jessica K De Freitas, Tingyi Wanyan, et al. Federated learning of electronic health records to improve mortality prediction in hospitalized patients with covid-19: Machine learning approach. *JMIR medical informatics*, 9(1):e24207, 2021.

[116] Zeyue Xue, Pan Zhou, Zichuan Xu, Xiumin Wang, Yulai Xie, Xiaofeng Ding, and Shiping Wen. A resource-constrained and privacy-preserving edge-computing-enabled clinical decision system: A federated reinforcement learning approach. *IEEE Internet of Things Journal*, 8(11):9122–9138, 2021.

[117] Xiaoxiao Li, Yufeng Gu, Nicha Dvornek, Lawrence H Staib, Pamela Ventola, and James S Duncan. Multi-site fmri analysis using privacy-preserving federated learning and domain adaptation: Abide results. *Medical Image Analysis*, 65:101765, 2020.

[118] Ece Isik-Polat, Gorkem Polat, Altan Kocyigit, and Alptekin Temizel. Evaluation and analysis of different aggregation and hyperparameter selection methods for federated brain tumor segmentation. *arXiv preprint arXiv:2202.08261*, 2022.

[119] Antonios Georgiadis, Varun Babbar, Fran Silavong, Sean Moran, and Rob Otter. St-fl: style transfer preprocessing in federated learning for covid-19 segmentation. In *Medical Imaging 2022: Imaging Informatics for Healthcare, Research, and Applications*, volume 12037, pages 13–27. SPIE, 2022.

[120] Pengfei Guo, Dong Yang, Ali Hatamizadeh, An Xu, Ziyue Xu, Wenqi Li, Can Zhao, Daguang Xu, Stephanie Harmon, Evrim Turkbey, et al. Auto-fedrl: Federated hyperparameter optimization for multi-institutional medical image segmentation. *arXiv preprint arXiv:2203.06338*, 2022.

[121] B Camajori Tedeschini, STEFANO Savazzi, ROMAN Stoklasa, LUCA Barbieri, IOANNIS Stathopoulos, MONICA Nicoli, and LUIGI Serio. Decentralized federated learning for healthcare networks: A case study on tumor segmentation. *IEEE Access*, 2022.

[122] Trung Kien Dang, Xiang Lan, Jianshu Weng, and Mengling Feng. Federated learning for electronic health records. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 2022.

[123] Xingjian Cao, Zonghang Li, Hongfang Yu, and Gang Sun. Cofed: Cross-silo heterogeneous federated multi-task learning via co-training. *arXiv preprint arXiv:2202.08603*, 2022.

[124] Hanxiao Chen, Hongwei Li, Guowen Xu, Yun Zhang, and Xizhao Luo. Achieving privacy-preserving federated learning with irrelevant updates over e-health applications. In *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, pages 1–6. IEEE, 2020.

[125] Weishan Zhang, Tao Zhou, Qinghua Lu, Xiao Wang, Chunsheng Zhu, Haoyun Sun, Zhipeng Wang, Sin Kit Lo, and Fei-Yue Wang. Dynamic-fusion-based federated learning for covid-19 detection. *IEEE Internet of Things Journal*, 8(21):15884–15891, 2021.

[126] Dong Yang, Ziyue Xu, Wenqi Li, Andriy Myronenko, Holger R Roth, Stephanie Harmon, Sheng Xu, Baris Turkbey, Evrim Turkbey, Xiaosong Wang, et al. Federated semi-supervised learning for covid region segmentation in chest ct using multi-national data from china, italy, japan. *Medical image analysis*, 70:101992, 2021.

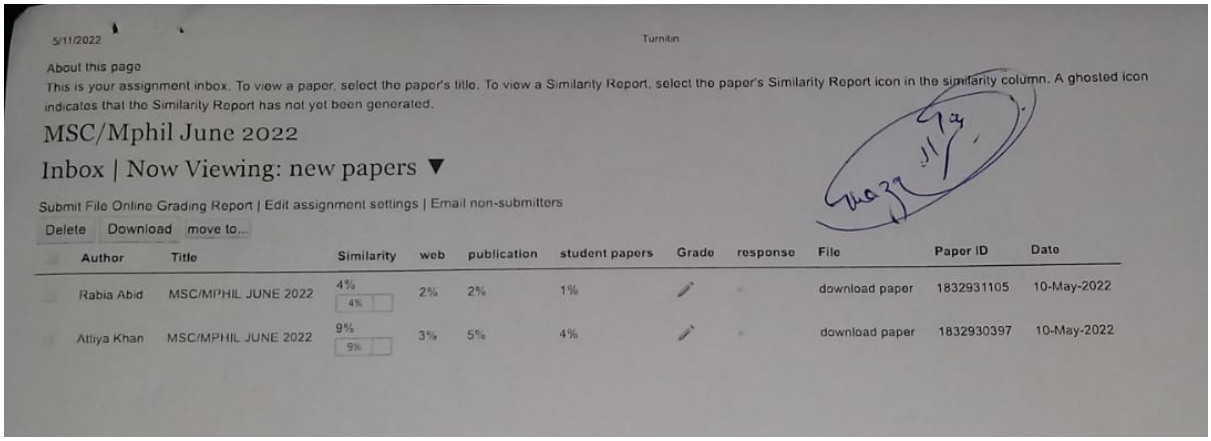
[127] Jing Jiang, Shaoxiong Ji, and Guodong Long. Decentralized knowledge acquisition for mobile internet applications. *World Wide Web*, 23(5):2653–2669, 2020.

[128] Wei Chen, Kartikeya Bhardwaj, and Radu Marculescu. Fedmax: mitigating activation divergence for accurate and communication-efficient federated learning. In *Joint Euro-*

pean Conference on Machine Learning and Knowledge Discovery in Databases, pages 348–363. Springer, 2020.

[129] Erico Tjoa and Cuntai Guan. A survey on explainable artificial intelligence (xai): Toward medical xai. *IEEE transactions on neural networks and learning systems*, 32(11):4793–4813, 2020.

PLAGIARISM REPORT



5/11/2022 Turnitin

About this page

This is your assignment inbox. To view a paper, select the paper's title. To view a Similarity Report, select the paper's Similarity Report icon in the similarity column. A ghosted icon indicates that the Similarity Report has not yet been generated.

MSC/Mphil June 2022

Inbox | Now Viewing: new papers ▼

Submit File Online Grading Report | Edit assignment settings | Email non-submitters

Delete Download move to...

Author	Title	Similarity	web	publication	student papers	Grade	response	File	Paper ID	Date
Rabia Abid	MSC/MPHIL JUNE 2022	4% 4%	2%	2%	1%			download paper	1832931105	10-May-2022
Atiiya Khan	MSC/MPHIL JUNE 2022	9% 9%	3%	5%	4%			download paper	1832930397	10-May-2022