Computers, Materials & Continua

Tech Science Press

DOI: xxx
Type: xxx

Adaptation of Federated Explainable Artificial Intelligence for Efficient and Secure E-Healthcare Systems

Rabia Abid[1], Muhammad Rizwan[2, *] Abdulatif Alabdulatif[3], Abdullah Alnajim[4] Meznah Alamro[5] and Mourade Azrour[6]

[1]Department of Computer Science, Kinnaird College for Women, Lahore, Pakistan
[2]College of Science and Engineering, University of Derby, Derby DE221GB, United Kingdom
[3]Department of Computer Science, College of Computer, Qassim University, Buraydah, 51452, Saudi Arabia
[4]Department of Information Technology, College of Computer, Qassim University, Buraydah, 51452, Saudi Arabia
[5]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh, 84428, Saudi Arabia
[6]STI Laboratory, IDMS team, Faculty of Sciences and Techniques, Moulay Ismail University of Meknès, Morocco

[*]Corresponding Author: Abdullah Alnajim . Email: najim@qu.edu.sa
Received: XX Month 202X; Accepted: XX Month 202X

Abstract: Explainable Artificial Intelligence (XAI) has an advanced feature to enhance the decision-making feature and improve the rule-based technique by using more advanced Machine Learning (ML) and Deep Learning (DL) based algorithms. In this paper, we chose e-healthcare systems for efficient decision-making and data classification, especially in data security, data handling, diagnostics, laboratories, and decision-making. Federated Machine Learning (FML) is a new and advanced technology that helps to maintain privacy for Personal Health Records (PHR) and handle a large amount of medical data effectively. In this context, XAI, along with FML, increases efficiency and improves the security of e-healthcare systems. The experiments show efficient system performance by implementing a federated averaging algorithm on an open-source Federated Learning (FL) platform. The experimental evaluation demonstrates the accuracy rate by taking epochs size 5, batch size 16, and the number of clients 5, which shows a higher accuracy rate (19, 104). We conclude the paper by discussing the existing gaps and future work in an e-healthcare system.

Keywords: Artificial Intelligence; Data privacy; Federated Machine Learning; Healthcare system; Security

1 Introduction

Explainable AI is an advanced methodology that helps every human understand the solution by adapting ML and AI techniques. Explainability becomes the foundation of AI due to competencies, fairness, safety, usability, human, collaboration, accountability, privacy, and many others. XAI helps to improve the decision readability of human beings. In XAI, some popular methodologies have been proposed for a better data understanding (visually showing different features), a better model understanding (visual neural net activation), and a better understanding of human psychology (adding a human behavior detection model in the system) [1]. However, DARPA has designed its systems based on XAI algorithms for a better future for AI and ML systems. Why do we need an explainable system? This question must be addressed during system design. In this paper, we choose an XAI-based model for better decisions because e-healthcare is a sensitive and human-life-dependent system. Proper diagnosis and treatment are the first and foremost obligations in the medical sector for both practitioners and physicians. Explainability Artificial Intelligence (XAI) is developed to enhance traditional AI technology as illustrated in Figure 1.

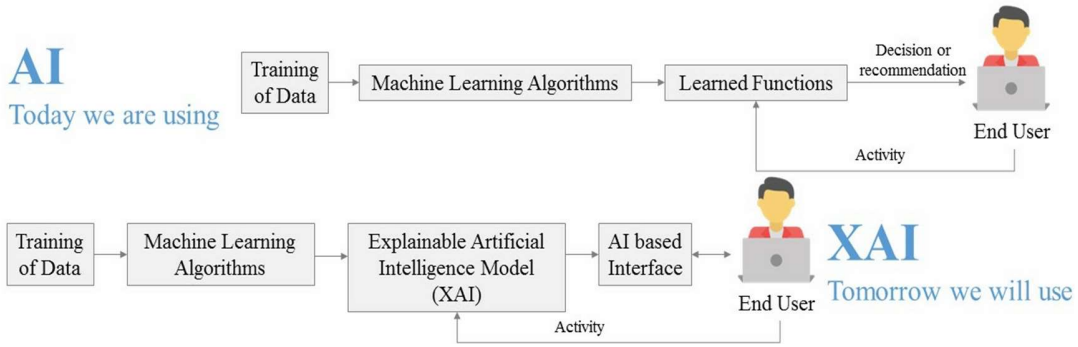


Figure 1: Now and Tomorrow: AI and XAI-based model.

Healthcare is a sensitive sector where a large amount of data or information needs to be handled. AI makes remarkable advancements in healthcare, especially in radiology and clinical trials. Nevertheless, the main questions which arise in researchers' minds are:

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

In today's healthcare systems, there are many challenges [2] like the classification of medical data, handling errors and injuries, data availability, changes in professional working, sensitive patient information, privacy policy, rules and regulations, adequate decision power, higher accuracy rate, authentication and authorizations, and legal provisions. The author in [3] explained the ability of AI decision-making that humans can follow and comprehend. In broader terms, it shows that connected users interact and understand decision-making applications. Another term that is closely related to the concept of explainability is known as "interpretation". However, these two words should be used with caution. Explainability, on the one hand, is related to the prediction by interpretability in every case scenario [4], whereas, on the other hand, interpretability is a rendition of the learning model during the training process.

The main concern of our research work is to implement better algorithms and frameworks of AI and ML in the healthcare industry, so take it from healthcare, medical, and patient perspectives. Machine learning (ML) is a branch of artificial intelligence (AI) where a combination of both algorithms creates

predictive power in data management [5]. ML in the medical industry mainly handles statistical data computing and is used in statistics-based methodologies. According to the hierarchy, Deep Learning (DL) is a subset of ML, ML is a subset of AI, and XAI lies within the umbrella of AI and has an intrinsic methodology named ML. Practical public and private healthcare management is an essential data-processing task in the healthcare industry. Every healthcare organization divides its management [6] 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 the potential to improve decision-making by testing and training its raw data, which leaves a substantial impact on patients and healthcare systems too. Many ML learning algorithms have been proposed to deal with the data type [7] (data types may be statistical, images, voices, sensors, documents, and many others). However, ML has made a remarkable advance in many fields in the healthcare industry where sensitive information or data is involved. It requires more security and high data handling methodologies [8-9], where every connected device to the central server is secure and manages PHR satisfactorily.

ML-based algorithms have many challenges [10], mainly data handling, privacy, security, data sharing, data training at the central server or main server, and many others. To overcome such challenges, Federated Machine Learning Algorithms (FMLA) have been introduced to better handle data and training processes as in [11]. In our research, we are trying to implement Federated Machine Learning Algorithms in the healthcare industry [12] to handle a large amount of data at a broader scale and provide more security to data. In addition, we treat healthcare systems at the local level instead of the global or central server. Federated machine learning (FML) is a distributed machine learning technology. The basic concept of FML is training ML-based models with distributed nodes and local system [13] data under federated learning. FML is a global model that maintains a large amount of data and maintains its model by handling them. FML model was assigned to resolve many ML problems with higher accuracy and efficiency [14]. Based on data distribution, FML is categorized into three types: Vertical, Horizontal, and transfer federated learning. Figure 2. shows the general architecture of FML algorithms and their working. Data from multiple nodes or sources come to a single system. According to FMLA, every node handles data against the same identity and works according to that data-sharing strategy. This hierarchy connects three main components: users, federated model, and data sources.

Figure 2: General Architecture of Federated Machine Learning Algorithms.

Many hospitals use AI methodology to work efficiently and effectively in the healthcare sector. Existing AI-based healthcare systems contain challenges like data classification, injuries and errors, data availability, bias and inequality, professional realignment, sensitive data, privacy regulations, terms, and policies, and many more. Collaboration between federal agencies, hospitals, and research institutions is necessary for modern health systems. Furthermore, international cooperation in research is essential in a pandemic-like scenario, but not at the price of privacy. Cooperation is made feasible by FML since it can protect privacy. There is no central server in a federation of healthcare providers. Therefore, designing a decentralized FLS, which

must also be resistant to malefactors, is another difficult task. In this manner, XAI and FML are considered efficient and effective technology. XAI and Federated machine learning have been studied and discussed to overcome the above mentioned issues and challenges. It will help us to provide a better version of a secure, protected, and efficient healthcare system.

The scope and limitations of the suggested model can contribute to improving the e-healthcare system's efficiency. The model can reduce the error detection rate and increase the accuracy rate with high density. Moreover, it can boost the speed of data evaluation in the training and testing phase with less time consumption. The developed model tries to overcome the shortcomings of previous research. This research's main objective is to enhance e-healthcare systems' performance by using XAI based framework and implementing FMLA for data training and testing. The proposed framework mainly emphasizes better data training and testing with higher accuracy, the lowest error rate, and the security of the cloud by using the data aggregation theorem in FMLA. Moreover, for testing and training our proposed federated learning algorithm, we use Google Collaborator for performance evaluation which shows the accuracy rate, time consumption, and the number of epoch's rounds.

In this research, Explainable Artificial Intelligence (XAI) and Federated Machine Learning Algorithms (FMLA) have been discussed to maintain patient health record security and efficiency. In section 2, detailed literature review has been discussed on the adaptability of the explainable Artificial Intelligence. In section 3, proposed model and in section 4, the results and discussions of proposed model along with experimental analysis has been discussed in detail. In the end, papers concluded existing gaps and future work in the e-healthcare systems.

1.1 Problem Statement

Exploring block chain-based structures is spurred by the growing security issues related to password protection and important communications. Although IoT devices in messaging applications provide useful features, there are serious security risks associated with their centralized communication networks. All IoT devices in smart homes are connected to the router, which may lead to security flaws. Malicious software, such as backdoors, may infect PCs as well and allow unauthorized users to access and manage networks. The proliferation of Internet of Things (IoT) devices increases the risk of package delivery problems, message hacking, and receiver delays. Furthermore, there is an extra chance of unwanted access to the sender's or recipient's data due to message-based assaults.

1.2 Contributions

The contributions can be summarized as follows:

- Develop an XAI-FML-based decision-making model that can help physicians in accurate decision-making.
- Develop an FML-based model training model of a single connected node for data aggregation. It is an optimized data aggregation algorithm for efficient and secure data training on global servers.
- Conduct computational proof of security using the Diffie-Hellman problem to enhance the system's security.

2. Literature Review

In the e-healthcare system, innovative technology has been adopted to facilitate the patients and make easy diagnoses and better treatment procedures. Nowadays, AI, ML, DL, and FML have made progressive healthcare changes and have become the central element of systems to check and treat patients. So, the main task of the researcher and programmer is to implement these techniques in e-healthcare physically.

In 2004, the first-ever explainable artificial intelligence (XAI) system was designed [15]. XAI's general and primary purpose is to make AI-based systems easier to understand and close to the human understanding model. However, XAI has no proper definition, which shows clarity in terms of its terminology. A few words from these concepts are transparency of systems, interpretability, and most importantly, explainability. All of these have different meanings in their terms [16-17]. The term 'interpretability' refers to how a model can be interpreted and understood. It can also be used in the context of explainability. At the same time, transparency shows how the model works without any flaws. It includes training procedures, analyzing training data and code distribution, explaining data features, and algorithmic clarity on how the model keeps working. Among them, all explainability has its main reason; it helps in decision-making [18]. Therefore, our research work mainly focuses on 'explainability'. or 'explainable artificial intelligence (XAI)'. Table 1 shows the related work of XAI which follows the concept of explainability.

Table 1: Adaptation of XAI model in latest studies.

Ref	Year	XAI Adaptability Method
[19]	2020	A Book: On XAI models having interpretability, transparent and agnostic methodologies.
[20]	2023	A detailed survey on XAI, with codes and referencing toolkit.
[21]	2023	A taxonomy of XAI based survey which shows some examples and extensive future directions.
[22]	2021	The XAI systems for designing and survey on metrics.
[23]	2023	Detailed taxonomy of XAI metrics with methods.
[24]	2021	Extensive collection of XAI and responsible AI.
[25]	2021	XAI: Introduction, variety of examples and standard methodology.

In the e-healthcare industry, AI plays a magnificent role by using machine learning algorithms and deep learning techniques to diagnose and treat patients. The medical experts have been transcending by using DL to get a higher accuracy rate. However, the black-box nature of the DL model limits the explainability and deployment models in e-healthcare. Though many researchers have come forward with the concept that the traditional AI-based model helps to increase accuracy, the concept of explainability needs to be revised, which is not the right AI model. Healthcare systems need several very specific AI algorithms, tailored to solve certain challenges, to be able to handle a disease X event better than they did during COVID-19. In the case of a Disease X incident, the suggested structure would lessen supply chain and production risk and complexity. Machine Learning is a branch of AI, and making many wonderful advancements in every field. As everyone is looking for AI in everything, there is a fast emerging trend to adopt AI based large,

complex and high speed systems [26]. As time passes more pressure has been put on AI inventions to produce more powerful and innovative systems or models to compete in today's world. The main focus is on the integrated circuit which helps to make computer architecture and AI based applications stronger [27]. In a successful AI-based model, the higher rate of accuracy and explainability come together, and then the concept of XAI has been created to deal with both, especially in the e-healthcare industry. In the medical domain, before the practical implementation of the 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 diagnosis and treatment of diagnosed diseases.

Federated Machine Learning (FML) is considered a better solution for XAI, enhancing healthcare systems' performance and efficiency [28]. Regarding security and data handling, it helps to increase the accuracy rate. It helps to handle multiple risks like data handling, login credentials, and data sharing, and securing connected devices. This work [29] built a unique ADRU-SCM model for BT segmentation and classification. Initially, WF-based pre-processing is used in the proposed ADRU-SCM technique to remove any noise. The BT classification process may be carried out using the ADRU-SCM model. In the future, deep instance segmentation models based on metaheuristics will be used to improve the ADRU-SCM approach's performance. The author [30] suggests a method that uses information fusion and a residual network in Federated Learning (FL) to merge various magnification factors of histopathology images. FL is used to enable the development of a global model while protecting patient privacy. The combination of AI and ML has made the healthcare industry more effective, efficient, and improves its performance, whether its diagnosis, treatment, clinical appointments, laboratories or any other issue [31]. In the healthcare industry, many changes still need to be made, which FMLA tries to overcome. The main departments in the healthcare industry (pathology, laboratories, emergency unit, operation theaters, radiology, neurology, medical record centers, clinics, oncology, research centers, and many others) can be improved by implementing FMLA.

In todays' healthcare systems, there are many challenges 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 advanced and user friendly, especially which are easy to understand for humans. The changing trends make ML design challenging, 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) have been introduced which make data handling more easy and a training process. In FML, data is trained at local servers' in-spite of the 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 are handling at larger scale, which is the biggest limitation of traditional machine learning algorithms. Therefore, to cope with such a 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 the healthcare industry.

3. Proposed model

The impact of FML and XAI is quite huge in e-healthcare systems. In the proposed model, the

system will work more efficiently by passing from the training phase, which helps to make a decision more efficiently. The prediction model makes lower latency in the architecture. E-healthcare systems have become more efficient and secure in the context of patients, doctors, pharmacists, researchers, and laboratories. And most important among all data privacy and security enhancement. Federated machine learning (FML) is an advanced form of machine learning which helps improve the system's performance. FML allows multiple XAI-based systems to share data with a higher security model.

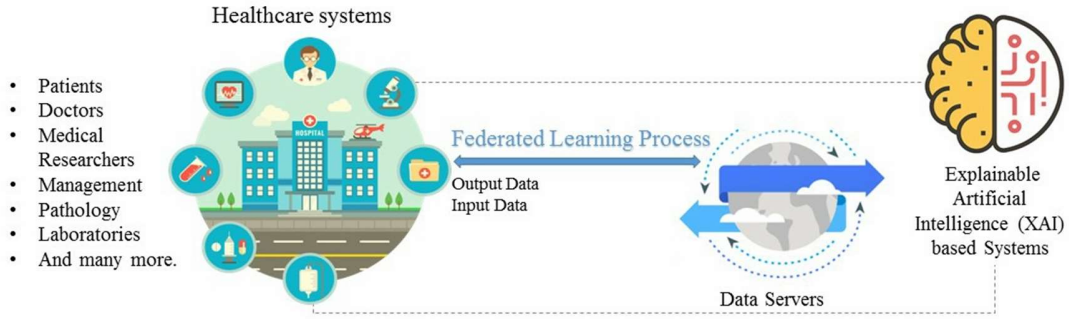


Figure 3: An overview of the proposed Architecture of XAI-FML.

In the training phase, it trains every connected node to train its data locally. Then, it transfers the trained data model to the main central server for data aggregation to get the final aggregated or processed data, which becomes available to every connected system afterward. This process completes as much as required iteration to complete the processing. Figure 3 shows the architecture of XAI-FML in the healthcare sector. In the Healthcare system, XAI-FML plays a significant role in enhancing performance, decision-making power, and critical analysis of human life. Medical records contain personal data about patients, such as name, gender, age, and residence, as well as physical and medical reports. If this data is leaked, patients might be put in grave danger. Healthcare companies gather sensitive information and personal privacy online. As a result, sensitive information and personal privacy must be secured, and each person has the right to access information and data for themselves.

The flow chart of the XAI-FML-based healthcare system, which receives input data from many healthcare sectors, is shown in Figure 4. The working of XAI-FML based model is based on two modules, where XAI based architecture contains FML algorithms for data processing and security. Every single connected node uploads data and passes it to the FML module where data process and train using FML algorithm. Then, it passes for testing and executing and transfers it for data aggregation on the cloud server. Finally, the output is executed.

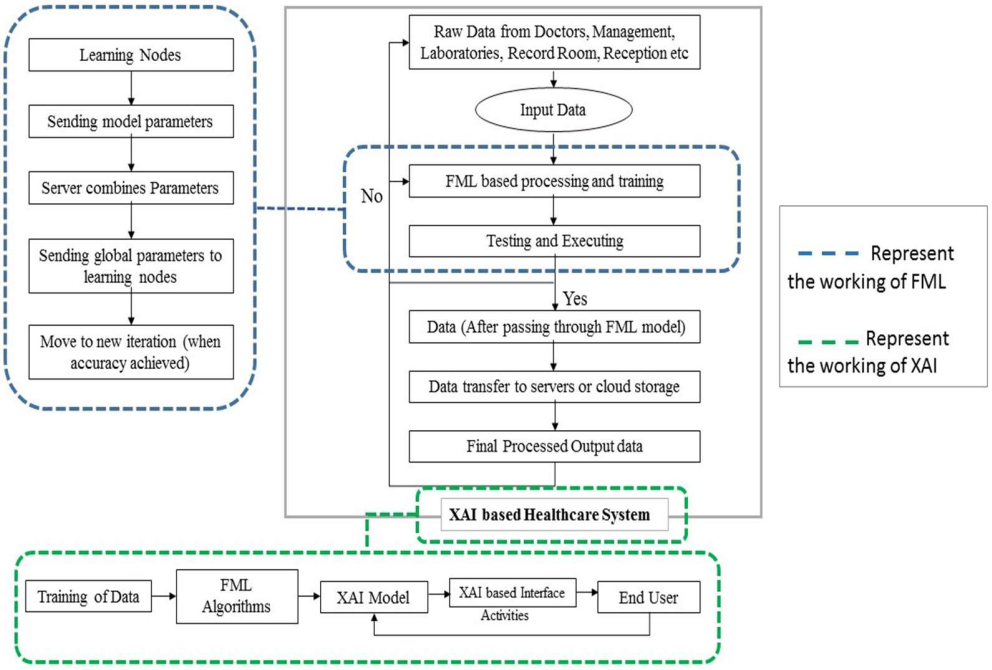


Figure 4: Flowchart of XAI-FML based e-healthcare system.

In the developed model, XAI is mainly implemented to diagnose and in surgery. The generic application of XAI in diagnosis can be easily understood through Figure 5. The figure adopts intrinsic and post hoc XAI, which enable AI-based examining tools to examine PHR and provide efficient decision-making procedures to physicians.

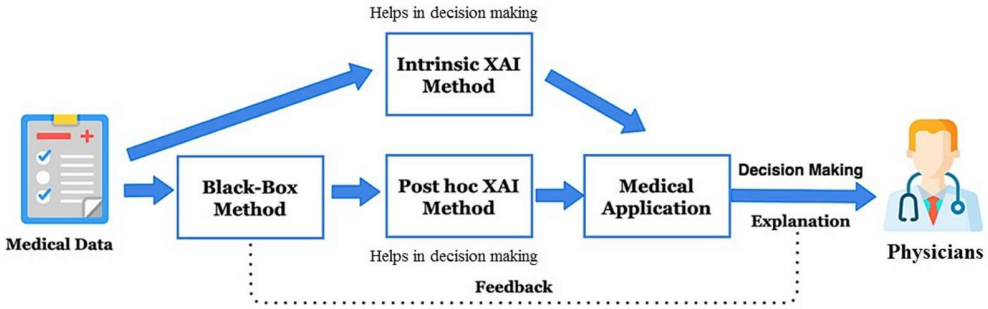


Figure 5: Application XAI using an intrinsic and post-hoc method to decide diagnoses.

For a few years, the need for and importance of XAI have been required in a few sectors like medical, education, and industrial work. Due to the complex nature of work, decision-making, and efficient systems need hours to interpret complex models easily. Although the black box model is threatening, implementing it in the healthcare sector will cause risk in diagnosis applications. It will also give an unjustified and unreliable decision for physicians in diagnosis decisions. Many studies have tried to overcome this issue in the healthcare industry. Therefore, in healthcare, the DL model is AI-based and used for medical applications. Hence, it needed to design an XAI based healthcare model which helps to overcome the issue of DL and a black box. Though many surveys

and research use DL in medical applications, it is time to shift to XAI-based applications to provide more ease to a physician to make efficient decisions in diagnosis and surgeries. It will surely help and motivate medical researchers to deploy the XAI model in medical applications and systems.

We use the XAI intelligent system and its model to make healthcare systems more efficient and secure. How XAI is embedded in our research scenario, here we demonstrate the working of the XAI model, which we show in Figure 3.2. It is based on some steps as follows:

- **E-Healthcare Systems:** Every healthcare system contains sensitive and private information or data of its patients or hospital. For every diagnosis and analysis, an AI-based decision-making model has been used, which helps to predict the chances of risks in disease or diagnoses.
- **Predictions:** Then the PHR is used for prediction by the XAI-based decision-making model, which gets an explanation.
- **Explainability:** The obtained explanation is analyzed by the practitioner or consultant. Then, the practitioner will validate the result, which is generated by the XAI based model, to get transparency.
- **Correct Prediction:** If the prediction becomes correct, medical knowledge helps get recommendations.
- **Wrong Prediction:** If, unfortunately, the prediction becomes wrong, then a contradiction has been used between medical knowledge and the concept of explainability and suggests improvement in the XAI model for correct future prediction or result.

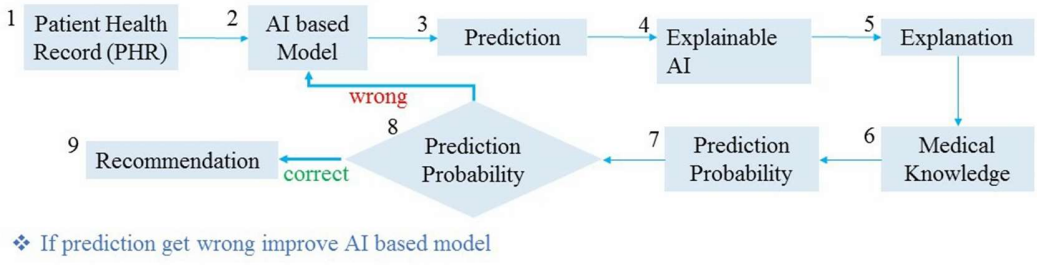


Figure 6: The flowchart of proposed XAI decision-making.

Figure 6 illustrates the flowchart of the XAI-based decision-making flow chart, which can help in the medical section for expert and accurate prediction. Here is an example that can better explain the workings of this proposed flowchart. Suppose a patient with higher blood pressure comes to be diagnosed, and the consultant will examine and send the diagnosis report to the physician. The report will be based on the input parameters like pulse rate and body temperature. An XAI-based model predicts the severity level of the blood pressure and generates an alarm according to diagnosis. The report is sent for final analysis; if the medical knowledge and XAI model prediction are the same, then the diagnosis and the doctor-prescribed medicine will be correct. Suppose the prediction gets wrong and the result of medical knowledge and doctor differs. In that case, the next round will be generated until the AI model improves working and makes the correct decision. We

select the e-healthcare industry to make systems efficient and secure, where every connected node becomes more efficient and secure using the FML algorithm. FML algorithms are based on three steps: data training on local models, uploading trained data models to a central server for data aggregation to the cloud, and then again, data available to all connected nodes for further validation and testing phase. In this scenario, XAI helps the system become more efficient and easily understood by all clients or users. FML helps clients train data globally without breaching the systems and data privacy. In the healthcare industry, a patient's health record is the primary sensitive data that needs to be focused on. This research mainly focuses on securing PHR through FML and making healthcare systems efficient using explainability (XAI).

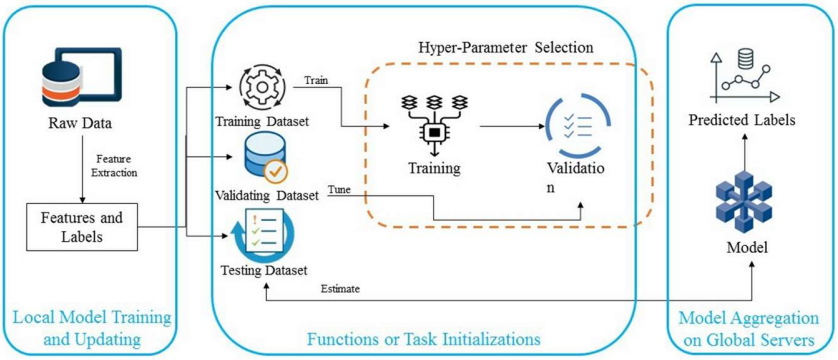


Figure 7: The architecture of developed FML.

The preserving privacy technique is illustrated in Figure 7, which is based on three steps:

- **Work Initialization:** At a single time, thousands of multiple devices or nodes are connected to the central servers and performing the training steps. The data training servers specify the training process and set parameters of data. After training, all the trained models send their data to the main central server for further proceedings.

- **Local Model Training:** the connected nodes train their models locally to update the selected parameters by the global server. The main purpose of this step is to identify the parameters that minimize the loss function and then update the parameters sent back to the main servers. Following all these steps, the flow chart of a single node data training and aggregation is represented in Figure 8.

- **Globally Data Aggregation:** When central servers receive all the parameters collected from the local model or connected nodes, the main server updates them. It sends them back to their recipient devices to avoid data loss.

FML networking architecture is categorized into centralized and decentralized networks. (1) In the centralized networking model, all connected nodes or clients update their model initially before sending it to the global model. This updated model has been aggregated to communicate to their client at the main central server. For example, in hospitals, all single systems update their model at the initial stage and then send it to the main server room for aggregation or updating.

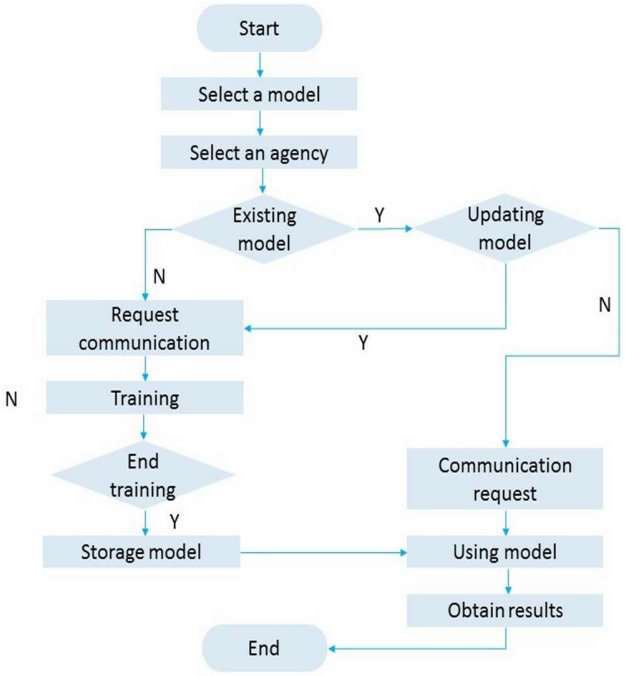


Figure 8: The client model training and aggregation by using FML architecture.

The centralized architecture contains more risk due to malicious attacks and eavesdroppers. It required a high rate of processing power and more bandwidth to communicate efficiently. (2) In the 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 algorithm has been used to secure the process and maintain data aggregation privacy. We chose FMLA for the data classification and security models and better system performance.

Then finally, steps two and three keep repeating until they reach the correct accuracy rate with minimum loss detection. Here FMLA faces some challenges during parameter updating and model training which are as **Non-ID data**: All the data has been sent to the server with unknown and random IDs, which causes a big chance of privacy breach. There may be a chance of misplacement of data occurring, and every connected node collects data based on its connected environment. **No. of clients:** Learning models evaluate the data based on connected devices or nodes, and that data is important. In this scenario, the number of connected nodes is a big challenge as the connection is lost and devices lose connectivity. The data sent after training back to nodes with tendencies is a big challenge. **Server's Parameter:** Increasing the workload of large numbers of connected nodes affects the process of communication and central server aggregation. So, through the server's parameter, it is important to resolve by using FML. It helps to minimize the number of epochs round of communication. It reduces the cost of systems. However, the main issue is that it needed a 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 devices (working according to the architecture of FML) have limited battery

consumption and affect the memory space locally and globally. Although the SGD (Stochastic Gradient descent) model is used to train each iteration, it also works with many DL-based algorithms; it badly affects the cost of systems. To recover these elements, an efficient model has been designed.

The proposed model is designed to make a secure and efficient aggregator beyond large-size cryptographic techniques. At the same time, our proposed system accepts the third node (if they are trusted) based on a secure aggregator that sets up its keys. In many security algorithms, in the end, the secret key is revealed before them, which exploits the confidentiality of the systems. It also exposes the secret key of the drop-out client during the aggregation process. Our model helps keep the secret key of drop-out devices and restricts the device from joining in an upcoming round of aggregation until a new key is created. In our proposed approach, we use a cherry-picking low overhead aggregation model (C-P LOHAM), other than a lightweight and hashing cryptographic algorithm. Our proposed model helps to increase the efficiency and security of the system. It will not trust the third party and reveal a secret key to them, which drops out due to low battery consumption. On the basis of this, our crafting design for FML and secure data aggregator of every single model.

4. Results and Discussion

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 maintenance, and many others. In order to promote open research and experimentation with Federated Learning (FL) and other machine learning approaches, a paradigm has been established. It is a machine learning technique in which several participating clients that store their training data locally build a common global model. The system specification is displayed in Table 2.

Table 2: System specification.

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

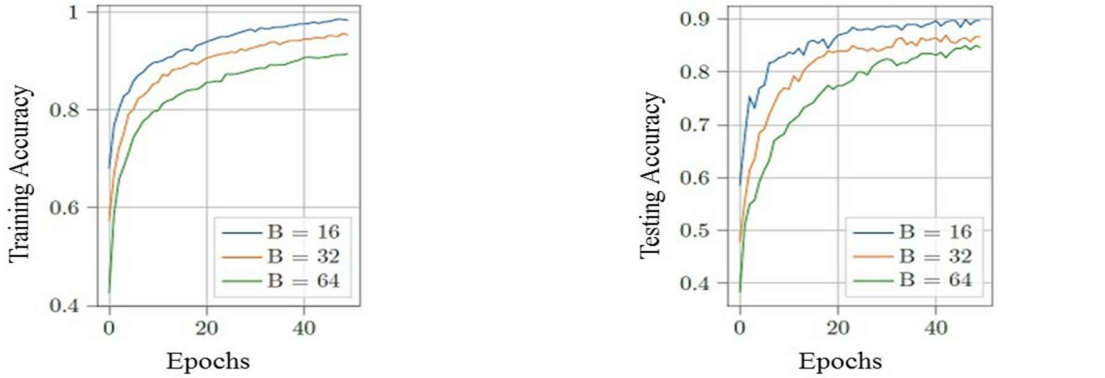
4.1 Dataset

The MNIST dataset contains data in the form of images. The primary purpose of selecting the MNIST dataset is because its images are of greyscale instead of colored images. As in medical diagnostic centers, all results of X-rays, MRI, CT-scan, and other tests are filmed in grayscale format. It helps to compare and analyze the performance of FML algorithms. The MNIST dataset contains 60,000 images as a sample and has around 10,000 images for the testing phase. Therefore, due to insufficient computational space and power, we use 500 in our experiment images and keep 20% for testing and the remaining for training. The data contain all images of grayscale vision with dimensions of 28x28 (0-255 values) and variant classes. By using the MNIST dataset following experiments have been performed to evaluate the performance. Firstly, it has been conducted on ML algorithms as a baseline. It will help to make an efficient comparison with the

proposed approach. Then, proposed FML algorithms were used for the experiment, and then lastly, the concept of explainability was measured.

4.1 Experiment 1: With ML or Centralized learning algorithms

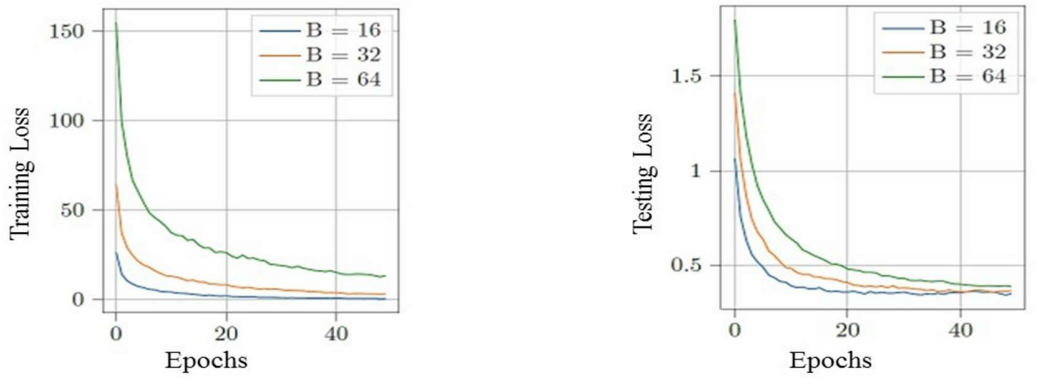
The purpose of this experiment is to evaluate the architecture and performance of ML or centralized learning algorithms. Moreover, later, the results were used for comparison. As a result, the rate of calculated accuracy after testing and training can be seen in Figures 9 and 10. The number of epochs and batch size (BS) value keep the same for further validation. By taking less BS, the computational power is higher for the training and testing phase. After passing from 20 epochs and having BS=16, the training accuracy rate is 95\%, and the testing accuracy is 90\% with a small quantity of overfitting. This result will be used for the following comparison in the experiment. Figure 11 shows the confusion matrix of the performed model.



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

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

Figure 9: Training & Testing Accuracy rate by using centralized learning algorithms where batch size varies and has epochs=20.



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

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

Figure 10: Training & Testing Loss rate by using centralized learning algorithms where batch size varies

and has epochs=20.

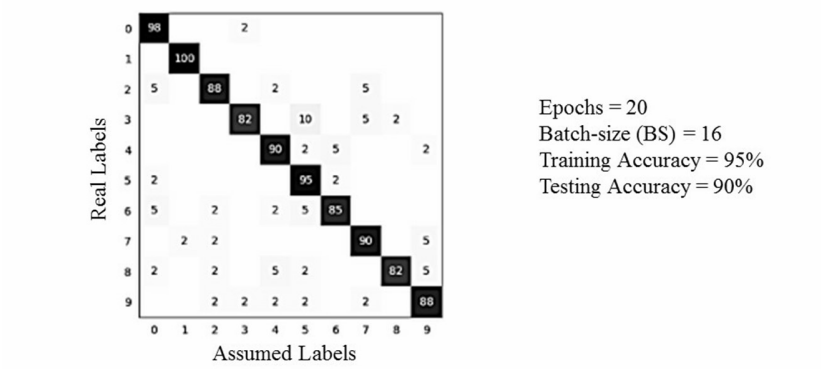
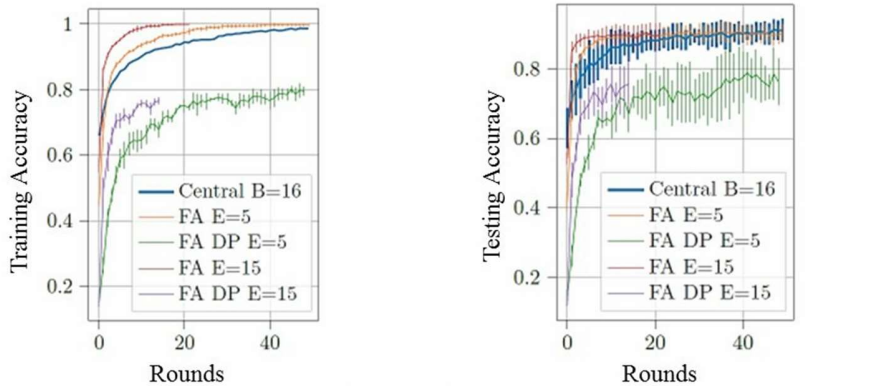


Figure 11: Diagram of Confusion Matrix: Training=95\% \& Texting=90\% by using centralized learning algorithms where batch-size=20 vary and having epochs=20.

4.2 Experiment 2: With Local Differential Model

The experiment aims to calculate the accuracy rate of how LDM affects the accuracy rate and data loss rate vs. the effects of FML in large or small data distribution. As a result, the training and testing accuracy rate is presented in Figures 12 and 13, based on multiple epochs, whereas no. of clients X= 5 and BS=16. Furthermore, the matrix of performed experiments is represented in the figure. And lastly, the privacy $\in$ is presented in Figure 10. It can be easily seen that green and purple color lines show the worst output using the private differential method. At this point, we can change by epochs and BS variations. By taking a large epoch size, FMLA stops working. It seems all right because, on the local model, the number of clients X is difficult to handle, which causes a loss of clients at the time of aggregation of the model at the main central server. Lastly, the cost of deploying LDM seems to increase as the number of samples increases. This also proves that as BS and epochs size increases, the accuracy rate in higher security also increases.

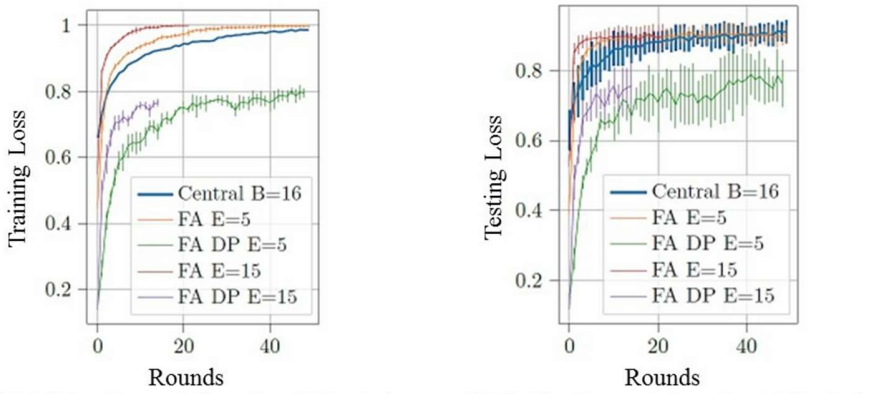


(a) Training Accuracy rate by using Federated averaging algorithm for security analyzing (with or without differential privacy)

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

Figure 12: 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 13: Training & Testing Loss rate by using proposed federated averaging algorithm at global level where BS=16 and no. of client X=5.

4.3 Experiment 3: Time Consumption

The purpose is to compare traditional FMLA and our proposed FMLA working and execution time. As in result, parameters are set as default values like epochs=5, BS=16, and X=5. These parameters help to remove redundancies from the results. The comparison between the proposed algorithm and the traditional federated learning algorithm is shown in Table 3 using different and multiple numbers of epochs, rounds, clients, and batch sizes. The time consumption was computed using the standard deviation formula for almost five rounds.

Table 3: Computation time of traditional and proposed FML by having different epochs, clients, and batch sizes

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	x7.6
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

5. Conclusion

In this paper, we use the concept of explainability in AI and federated machine learning algorithms for the efficiency and security of healthcare systems. We have documented and implemented an optimized federated machine learning averaging model to optimize the system's performance. For result comparison, two more concepts have 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 detailed model with the flowchart of the whole healthcare system. For a few years, many methods have been proposed to measure and evaluate XAI's performance, but a proper platform that shows practical implementation has yet to be proposed. The implementation of standardized data sharing protocols, the development of cooperative frameworks for federated learning, and the prioritization of the integration of explainable AI techniques to improve decision-making transparency are among the urgent steps the healthcare sector must take to adjust to federated machine learning and explainability. Some of the measures taken are just theoretical, from the user and viewpoint (for just user satisfaction). It can only be measured by subjective discussion and clarity. Now the question arises: Does a theoretical explanation fulfill the need for an advanced XAI system? So, the answer is that it is still under processing as future work. Currently, the concept of XAI can be easily explained through models, frameworks, and flowcharts, which help evaluate the XAI-based model's flow.

Acknowledgment: Researchers would like to thank the Deanship of Scientific Research, Qassim University for funding publication of this project

Author Contributions: The authors confirm contribution to the paper as follows: R. Abid, M. Rizwan, A. Alabdulatif and A. Alnajim: Methodology, Investigation, Software, Writing, Funding. R. Abid, M. Rizwan, A. Alabdulatif: Investigation, Writing-Original Draft, Writing-Review and Editing. A. Alnajim, M. Alamro and M. Azrour: Validation, Writing-Review and Editing. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: All data generated or analyzed during this study are included in this article and are available from the corresponding author upon reasonable request.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] C. Zanni-Merk and A. Jeannin-Girardon, "*Towards the joint use of symbolic and connectionist approaches for Explainable Artificial Intelligence*," *Learning and Analytics in Intelligent Systems*, pp. 271–286, 2022.

[2] M. Regona, T. Yigitcanlar, B. Xia, and R. Y. Li, "*Opportunities and adoption challenges of AI in the construction industry: A Prisma Review*," *Journal of Open Innovation: Technology, Market, and Complexity*, vol. 8, no. 1, p. 45, 2022.

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

[4] M.-Y. Kim *et al.*, "*A multi-component framework for the analysis and design of Explainable Artificial Intelligence*," *Machine Learning and Knowledge Extraction*, vol. 3, no. 4, pp. 900–921, 2021.

[5] Sengan, Sudhakar; Sagar, R. Vidya; Ramesh, R.; Khalaf, Osamah Ibrahim; Dhanapal, R., *"The optimization of reconfigured real-time datasets for improving classification performance of machine learning algorithms*," Mathematics in Engineering, Science & Aerospace (MESA), pp. 43–54, 2021.

[6] A. Garg, V. V. Venkataramani, A. Karthikeyan, and U. D. Priyakumar, "*Modern AI/ML methods for healthcare: Opportunities and challenges*," *Lecture Notes in Computer Science*, pp. 3–25, 2022.

[7] A. I. Osman *et al.*, "*Past, present and perspective methodology for groundwater modeling-based machine learning approaches*," *Archives of Computational Methods in Engineering*, vol. 29, no. 6, pp. 3843–3859, 2022.

[8] R. Mukta, H. Paik, Q. Lu, and S. S. Kanhere, "*A survey of data minimisation techniques in blockchain-based healthcare*," *Computer Networks*, vol. 205, p. 108766, 2022.

[9] R. Abid, B. Aslam, M. Rizwan, F. Ahmad, and M. U. Sattar, "*Block-chain - security advancement in medical sector for sharing medical records*," *2019 International Conference on Innovative Computing (ICIC)*, Michigan State University, East Lansing, MI 48824, USA. 2019.

[10] J. Munoz-Gama *et al.*, "Process mining for healthcare: Characteristics and challenges," *Journal of Biomedical Informatics*, vol. 127, p. 103994, 2022.

[11] Chaoyang He, Songze Li, Jinhyun So, Xiao Zeng, Mi Zhang, Hongyi Wang, Xiaoyang Wang, Praneeth Vepakomma, Abhishek Singh, Hang Qiu, Xinghua Zhu, Jianzong Wang, Li Shen, Peilin Zhao, Yan Kang, Yang Liu, Ramesh Raskar, Qiang Yang, Murali Annavaram, Salman Avestimehr, "*FedML: A Research Library and Benchmark for Federated Machine Learning*", 2020, arXiv preprint arXiv:2007.13518.

[12] F. Zerka *et al.*, "*Systematic review of privacy-preserving distributed machine learning from Federated Databases in Health Care*," *JCO Clinical Cancer Informatics*, no. 4, pp. 184–200, 2020.

[13] Y. Zhan, P. Li, Z. Qu, D. Zeng, and S. Guo, "A learning-based incentive mechanism for Federated learning," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6360–6368, 2020.

[14] H. Habibzadeh, T. Soyata, B. Kantarci, A. Boukerche, and C. Kaptan, "Sensing, communication and Security Planes: A new challenge for a Smart City system design," *Computer Networks*, vol. 144, pp. 163–200, 2018.

[15] M. M. Ahsan and Z. Siddique, "Machine learning-based heart disease diagnosis: A systematic literature review," *Artificial Intelligence in Medicine*, vol. 128, p. 102289, 2022.

[16] A. K. Sharma, A. Nandal, A. Dhaka, and R. Dixit, "Medical image classification techniques and analysis using Deep Learning Networks: A Review," *Health Informatics: A Computational Perspective in Healthcare*, Springer, pp. 233–258, 2021.

[17] D. Gunning *et al.*, "XAI—explainable artificial intelligence," *Science Robotics*, vol. 4, no. 37, 2019. DOI: 10.1126/scirobotics.aay7120

[18] F. K. Dosilovic, M. Brcic, and N. Hlupic, "Explainable artificial intelligence: A survey," *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2018.

[19] C. M. Cutillo *et al.*, "Machine Intelligence in healthcare—perspectives on trustworthiness, explainability, usability, and transparency," npj Digital Medicine, vol. 3, no. 47, 2020.

[20] Le, Phuong Quynh, et al. "Benchmarking eXplainable AI-A Survey on Available Toolkits and Open Challenges." International Joint Conference on Artificial Intelligence, Macau, S.A.R. 2023.

[21] A. Holzinger, A. Saranti, C. Molnar, P. Biecek, and W. Samek, “Explainable AI methods - A brief overview,” xxAI - Beyond Explainable AI, Springer, cham, pp. 13–38, 2022.

[22] Saeed, Waddah, and Christian Omlin. "Explainable AI (XAI): A systematic meta-survey of current challenges and future opportunities." Knowledge-Based Systems 263 (2023): 110273.

[23] Schwalbe, Gesina, and Bettina Finzel. "A comprehensive taxonomy for explainable artificial intelligence: a systematic survey of surveys on methods and concepts." Data Mining and Knowledge Discovery (2023): 1-59.

[24] Polley, S., Janki, A., Thiel, M., Hoebel-Mueller, J., Nuernberger, A.: Exdocs: evidence. based explainable document search. In: Workshop on Causality in Search and Recommendations co-located with 44th International ACM SIGIR Conference on Research and Development in Information Retrieval, New York. NY. USA,2021.

[25] J. Zhou, A. H. Gandomi, F. Chen, and A. Holzinger, “Evaluating the quality of machine learning explanations: A survey on methods and metrics,” *Electronics*, vol. 10, no. 5, p. 593, 2021.

[26] J. Gerlings, A. Shollo, and I. Constantiou, “Reviewing the need for explainable artificial intelligence (XAI),” *Proceedings of the Annual Hawaii International Conference on System Sciences*, Kauai, Hawaii, USA, 2021.

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

[28] D. Liu, D. Dligach, and T. Miller, “Two-stage federated phenotyping and patient representation learning,” *Proceedings of the 18th BioNLP Workshop and Shared Task*, 2019. doi:10.18653/v1/w19-5030

[29] Poonguzhali, R., et al. "Automated brain tumor diagnosis using deep residual u-net segmentation model." *Computers, Materials & Continua* 74.1 (2023): 2179-2194.

[30] Agbley, Bless Lord Y., et al. "Federated Fusion of Magnified Histopathological Images for Breast Tumor Classification in the Internet of Medical Things."*IEEE Journal of Biomedical and Health Informatics* (2023). **DOI:** 10.1109/JBHI.2023.3256974

[31] Radanliev, Petar, and David De Roure. "Disease X vaccine production and supply chains: Risk assessing healthcare systems operating with artificial intelligence and industry 4.0." Health and Technology 13.1 (2023): 11-15.