Jashore University of Science and Technology

Jashore-7408, Bangladesh

Decentralized Privacy-Preserving Framework for Sleep Anomaly Detection and Behavioral Pattern Recognition in Healthcare

Submitted By:

Md. Saniul Basir Saz

Student ID: 200103

Session: 2020-2021

Supervisor:

Dr. Mohammad Nowsin Amin Sheikh

Assistant Professor

Dept. of Computer Science and Engineering (CSE)

This thesis report was submitted in partial fulfillment of the
requirements for the degree of B.Sc. Engg.
in the Dept. of Computer Science and Engineering (CSE) under the
Faculty of Engineering and Technology (FET)

May 2026

Jashore University of Science and Technology

Jashore-7408, Bangladesh

This thesis titled **Decentralized Privacy-Preserving Framework for Sleep Anomaly Detection and Behavioral Pattern Recognition in Healthcare** was submitted by **Md. Saniul Basir Saz** and was officially approved after the final defense held in May 2026 for the degree of B.Sc. Engg. in Dept. of Computer Science and Engineering (CSE).

Signature of the Student

Md. Saniul Basir Saz

Signature of the Supervisor

Dr. Mohammad Nowsin Amin Sheikh

Signature of the Chairman

Dr. Md Kamrul Islam

Dedication

To my mother

and to the memory of my father,

whose love, sacrifice and prayers

made me who I am today,

and to my respected supervisor

for his support and direction

during my research journey,

and to all those who dream and work hard

to achieve their goals.

Signature
Md. Saniul Basir Saz
Student Id: 200103

Acknowledgments

First of all, I thank Almighty Allah. By His grace and mercy, I successfully completed this thesis. I also thank my academic supervisor, **Dr. Mohammad Nowsin Amin Sheikh**, Aassistant Professor in the Department of Computer Science and Engineering (CSE) at Jashore University of Science and Technology. He always guided me, gave me helpful advice and supported me during this thesis. I am very grateful to him.

And I also want to thank the Chairman of the Department of Computer Science and Engineering (CSE) and all the faculty members for their helpful advice and constant support during this thesis.

Finally, I would like to thank my dear parents, my brother and my supervisor. They are the main support of my life. Their love, hard work and financial help always inspired me to move forward.

List of Abbreviations

No.	Abbreviation	Full Form
1	JUST	Jashore University of Science and Technology
2	CSE	Computer Science and Engineering
3	FL	Federated Learning
4	DL	Deep Learning
5	ZKPs	Zero Knowledge Proofs
6	XAI	Explainable Artificial Intelligence
7	IPFS	InterPlanetary File System
8	CID	Content Identifier
9	PSG	Polysomnography
10	EEG	Electroencephalogram
11	ECG	Electrocardiogram
12	EMG	Electromyogram
13	EOG	Electrooculogram
14	SHAP	Shapley Additive exPlanations
15	LIME	Local Interpretable Model-agnostic Explanations
16	AES	Advanced Encryption Standard
17	EIP	Ethereum Improvement Proposal
18	RBAC	Role-Based Access Control

Table of Contents

List of Figures

List of Tables

Abstract

Sleep is a fundamental biological need that is crucial for physical, cognitive and mental health. Lack of sleep affects daily activities, reduces productivity and increases the risk of stress, anxiety, depression and burnout. In healthcare, sleep-related data is analyzed using machine learning to understand behavioral patterns and predict health status. However, data privacy and security is a major challenge due to the use of sensitive personal data. To address this problem, Federated Learning (FL) ensures privacy by training models in a distributed environment, instead of storing data centrally. Explainable AI (XAI) enhances transparency and trustworthiness by explaining model decisions. Blockchain provides secure, immutable and tamper-proof storage of data. In combination, FL, XAI and Blockchain create a secure and privacy-preserving healthcare infrastructure. In this study, a decentralized framework is proposed by integrating Federated Learning (FL), Explainable AI (XAI), Blockchain Zero-Knowledge Proofs (ZKPs) and IPFS. The primary goal of this framework is to ensure safe and privacy-preserving sleep-related data analysis in a distributed environment. For validating the proposed framework, an Autoencoder is used for sleep anomaly detection and four deep learning models are evaluated with eight FL algorithms along with XAI. In the performance results, the on-chain process (Blockchain, ZKPs, IPFS) showed high efficiency (22 TPS, 73 ms latency, 100% success rate, block confirmation time 0.2ms and average transaction time 0.07 sec), and in the off-chain process achieved 0.9776 accuracy and 0.9831 F1-score in the best FL-XAI setup (LSTM-Attention with pFedMe) and 0.9223 accuracy and 0.9337 F1-score in validation.

Chapter 1
Introduction

Chapter 1: Introduction

1.1 Overview

Sleep is one of the most fundamental biological processes directly related to human mental health, emotional stability and behavioral outcomes. In the case of youth people in Bangladesh, irregular sleep is emerging as a growing public health problem due to academic pressure, excessive use of digital devices, family problems and socio-economic stress [1]. However, in Bangladesh 13% of adolescents, 44.2% of psychiatric patients, 41.3% of long-term patients, 56.4% of young adults, 59.4% of university students and 72.1% of medical students suffer from different kinds of sleep problems [2] [3] [4] [5] [6]. Global research has demonstrated that sleep irregularities and deprivation can cause behavioral abnormalities, including depression, attention deficit, anxiety and irritability [7].

Blockchain technology first became widely known by introducing a new concept of creating decentralized digital systems. A blockchain basic idea is a cryptographically secure series of blocks that keeps records of timestamps and prevents any unauthorized changes [8] [9]. The healthcare industry has several challenges including secure EMR management, patient data sharing and the doctor referral process. By adopting blockchain technology to ensure privacy, security and transparency, these issues can be overcome [10]. The gold standard for clinical diagnosis of sleep disorders is PSG which records different kinds of physiological signals including respiration, oxygen saturation, EEG, ECG, EMG and EOG. However, sleep disorders are a serious health problem that has significant effects on mental health and general well-being [11]. Furthermore, data privacy is a most important issue that impacts the healthcare industry as well as the research and prediction of sleep disorders and analysis. The increasing use of wearable sensors and Internet of Things (IoT)-based sleep monitoring systems is enabling the collection of huge amounts of sleep pattern data, which is used for predictive modeling. However, due to the use of centralized data storage architecture, serious issues are being raised regarding privacy, data integrity and secure data sharing. Blockchain technology is an opportunity alternative for secure sleep data management and reliable predictive modeling through its decentralized and

tamper-resistant framework [12].

Federated Learning (FL) is a decentralized machine learning approach and providing opportunities to model training without sharing raw data and its reduces the risk and allowing clients to train models locally and share only model updates [13]. On the other hand, privacy and security concerns limit the full potential of centralized deep learning approaches in the healthcare sector. Since, Federated Learning (FL) has emerged as a potential solution, which enables collaborative model training without sharing raw medical data [14]. Yet, machine learning based medical predictive and classification systems remain a security vulnerability. To address these limitations, decentralized solutions based on blockchain technology have become a crucial solution [15]. The FL ensures data privacy during training, but its black-box characteristic constrains transparency and weakens trust in critical decision-making. Integrating XAI with FL allows for interpretable model predictions while maintaining confidentiality, which increases acceptance, reliability and accountability in sensitive areas such as healthcare [16]. Thus, traditional medical prediction systems that use centralized machine learning and deep learning models can put user privacy and trust at risk. A decentralized approach can solve these problems and It can build trust in the healthcare [17].

Blockchain technology can be used as a reliable complementary solution, ensuring tamper-proof data logging, decentralized consensus and transparent audit capabilities. And zero knowledge proofs ensure that participants can check for the correctness of their updates or computation without revealing data [18]. Blockchain, FL, XAI, Smart Contract and ZKPs work together to build a combined structure for building secure, transparent smart systems. For example, in a decentralized healthcare system, these technologies ensure transparency while maintaining patient data privacy. Since adequate sleep is very important for a normal person, at the same time, many types of problems occur due to lack of sleep. Furthermore, health awareness can be enhanced by the examination of sleep data, and it is crucial to maintain the confidentiality of this information.

Sleep data analysis has a wide range of applications but it also faces many difficult problems.

However, simply quantifying the amount of sleep is no longer enough. Developing techniques to precisely identify sleep abnormalities. Such as irregular movements or breathing alterations is crucial to ensuring health. After all, there is a strong reciprocal link between sleep and mental health.

In our proposed framework, where on-chain and off-chain process will work together. User sleep data will be model trained on local devices and raw data should never be shared outside which ensures privacy. Blockchain integrated to ensure data integrity and tamper resistance where metadata and transaction logs will be stored. IPFS is used for storing sleep artifacts to ensure decentralized storage and avoid single point of failure. Smart Contract used for data access control which will be data sharing according to certain rules. Also, through ZKPs, it can be proved that a specific computation or validation is done correctly without revealing any sensitive information. Finally, XAI has been integrated so that clinicians or researchers can clearly understand the reason behind the model decision.

1.2 Background

Sleep is a fundamental part of human health and irregular sleep can often cause mental health problems. But centralized analysis raises privacy and security concerns. On the other hand, Deep learning has proven to be highly effective in identifying mental health and wellbeing and detecting various abnormalities. But in the process of model training, the security of sensitive health information is at risk. Federated learning can be used to solve this problem, where model training takes place on multiple devices but raw data is not shared. Immutable records can be stored using blockchain technology to ensure reliability and accountability. Additionally, zero knowledge proofs enable the verification of results without disclosing personal information.

In addition to privacy and security, another important challenge for models used in mental health assessment is interpretability. Such models often behave like "black boxes," making them difficult for clinicians and users to understand. XAI is very important to overcome these limitations. XAI uses a variety of methods such as attention visualization, feature attribution, and explainable architectural elements to analyze how the model is making decisions. This makes it easier to understand the justification behind the model's outcomes and increases acceptance in clinical use.

Thus, the combination of these technologies FL, DL, blockchain, ZKPs, and XAI creates a secure, transparent and explainable technological foundation. Which is very useful for sleep pattern analysis and mental health assessment in healthcare.

1.3 Problem Statement

Sleep problems are often associated with stress, anxiety and other mental health problems. Existing centralized analysis methods carry the risk of leaking personal health information, while DL models require a lot of data. But it is not safe to share sensitive information. Moreover, clinicians are not able to easily interpret the model's conclusions and the system does not have a reliable audit or verification mechanism. The result is a lack of a secure, transparent and trustworthy framework that can analyze distributed sleep data, identify mental health-related abnormalities and ensure privacy and trust using FL, Blockchain, ZKPs and XAI.

1.4 Objectives

This study has the following main objectives:

1. To propose a secure and privacy-preserving framework that integrates off-chain and on-chain to manage sleep anomaly detection and behavior analysis. Where Blockchain, FL, XAI, ZKPs, Smart Contract and IPFS will work together.

2. In the off-chain process, deep learning is used for sleep anomaly detection. Federated learning and XAI is also used for distributed model training.

3. To evaluate the proposed Off-chain, On-chain integrated framework in the context of security and using MMASH and PAMAP2 datasets.

4. In the on-chain process, blockchain is used to ensure immutable logging, which increases transparency and trust. Smart Contract is used for access control.

5. To use the ZKPs mechanism for verifying the authenticity of the information without sharing data. And to integrate IPFS for storing ZKP hashes, anomaly report data and explainable reports, ensuring decentralized storage and avoiding a single point of failure.

1.5 Research Questions

1. How can we securely detect sleep anomalies using sleep data?
2. How can FL enable distributed model training without sharing sensitive data?
3. How can we ensure the verification and integrity of sleep pattern analysis and mental health and wellbeing framework using FL, DL, XAI, Blockchain and Zero-Knowledge Proof?
4. How can we make model decisions?
5. How can these technologies be integrated to create a secure, privacy-preserving, and explainable framework for sleep pattern analysis, mental health and wellbeing?

1.6 Contribution

The major contributions of this thesis are summarized below:

1. Proposed a decentralized framework integrating FL, XAI, Blockchain, ZKPs and IPFS for privacy-preserving sleep anomaly detection, pattern and behavioral analysis.

2. Evaluated 4 deep learning models with 8 FL algorithms, achieving best accuracy (0.9776) and F1-score (0.9831) with LSTM+Attention and pFedMe. And SHAP XAI was applied to provide explainability for the model decisions. And also contributed to analyzing sleep behavior patterns from sleep data.

3. Implemented an Autoencoder based anomaly detector validated on 220,328 segments with a 1.3% anomaly rate. And validated the full integrated framework on three public benchmark datasets: Sleep-EDF Database Expanded, MMASH and PAMAP2.

4. Achieved high on-chain efficiency with 22 TPS, 73 ms latency and 100% transaction success rate. And applied ZKPs to verify data authenticity without exposing private sleep data.

5. The off-chain module achieves an average CPU utilization of 17.27%, with a high of 70.20% in activity monitoring inference and a GPU usage of 68.45% in anomaly inference.

1.7 Chapter Organization

This study organizes its content as follows: **Chapter 2** outlines related work, **Chapter 3** an overview of related technologies, **Chapter 4** and **Chapter 5** describe the proposed framework and methodology, **Chapter 6** results and discussion and **Chapter 7** conclusions and future work directions of this study.

Chapter 2
Related Work

Chapter 2: Related Work

2.1 Overview

This chapter discusses current research relevant to the proposed framework. The discussion includes federated learning and blockchain-based techniques for sleep monitoring that ensure privacy. In addition to deep learning methodologies for evaluating sleep and processing physiological inputs. In the end, it compares other works based on proposed framework.

2.2 Federated Learning and Blockchain in Sleep Monitoring

Some recent works has to do with the privacy and security of medical AI. Hongjin Li et al. used FL for sleep stage classification [19]. Ziyi Wang et al. focused on anomaly detection in sleep data and also Tahir and Zaheer worked on IoT sleep anomaly detection [20] [21]. On the other hand, Nandini et al. have used Blockchain, ZKPs and IPFS together for safeguarded sharing of genomic data through health record systems [22]. Lanciaux et al. worked on medical AI and used ZKPs and FL together [23]. Sharma er al. also worked on healthcare and used Blockchain, ZKPs and FL [24]. Additionally, Albalwy et al. worked on EHR and used ZKPs, Blockchain and IPFS together [25]. Raghav et al. also worked on healthcare and used ZKPs and IPFS for data exchnage [26]. But their work is outside the sleep domain.

On the other hand, Borges et al. presented a HiTLCPS for smartphone-based sleep detection. Their study compared traditional ML (MLP, LSTM) and FL (FedAvg) using the ISABELA dataset. The model achieved 84% accuracy and also preserved user privacy [27]. Asad Ali et al. proposed a federated ensemble model using multi-sensor wearable data, achieving 99.3% accuracy, 99.17% sensitivity and 99.8% specificity in sleep stage classification and maintaining data privacy through on-device learning [28]. Moon et al. introduced a distributed methodology for sleep stage diagnosis on edge devices [29]. Parul Dubey et al. proposed a CNN-LSTM based Federated Learning model that combines behavioral and physiological data to predict mental health diagnostics and achieved 92% accuracy, 0.905 F1-score, and 0.90 AUC-

ROC [30]. Adri-ana Anido-Alonso et al. proposed a non-centralized deep-learning methodology that enhances inter-database generalization in automatic sleep staging across various public sleep databases through ensemble models and a novel federated learning algorithm (ssFedSGD), enabling model training without the exchange of raw patient data [31]. Overall, a summary of existing FL approaches for sleep and health monitoring is shown in Table 2.1.

Table 2.1: Summary of Federated Learning Approaches for Sleep and Health Monitoring.

Authors	**Approach / Models**	**Datasets**	**Performance**	**Criticism**
Guilherme A. et al.	FL (FedAvg), MLP, LSTM, SMOTE	ISABELA Sleep Detection Dataset (30 users, 4 weeks)	84% Accuracy	Small Datasets; Self-Report Noise; Device heterogeneity
Asad Ali et al.	HFL; Ensemble (RF + LR); feature engineering; signal filtering	DREAMT dataset (100 participants, Duke University Sleep Disorder Lab)	99.3% Accuracy; 99.17% Sensitivity; 99.8% Specificity	Network instability; Client Drop Out
SungHwan Moon et al.	FL (FedAvg), 1D CNN, MAML (T1–T2 variant)	Apple Watch + PSG (31 subjects); Raspberry Pi validation	58.2% F1; 12.1% AUC (FL-ML); 22.6s inference on edge	MAML pre-training performed on GPU server, not on edge; Small dataset
Parul Dubey et al.	CNN-LSTM; Differential Privacy (Gaussian noise); Homomorphic Encryption; Adam optimizer	Kaggle Behavioral Multimodal Dataset	92% Accuracy; 0.905 F1-score; 0.90 AUC-ROC	High comm. and compute overhead; Real time delay from aggregation rounds; Data quality and heterogeneity issues
Adriana Anido-Alonso et al.	Ensemble models (voting, averaging, weighting, Nelder-Mead); ssFedSGD; CNN-LSTM	DREAMS, Dublin, SHHS, Telemetry, ISRUC, HMC	Improved inter-database generalization	Batch normalization caused convergence problems; FedAvg and FedSGD unstable in non-IID data

2.3 Deep Learning Based Sleep Analysis

Gengalakshmi G. et al. proposed an LSTM-based deep learning model that analyzes wearable sensor data (accelerometer, heart rate) for sleep stage classification and insomnia detection, the model achieved 96.75% accuracy in sleep stage detection and 93.50% sensitivity in insomnia detection, which is 18–20% more effective than conventional methods [32]. Sumit Satoiya et al. proposed ScaloNet-121 for insomnia detection using DenseNet-121 by converting EEG signals into scalograms with CWT, which achieved 99.51% accuracy on the CAP dataset [33]. Kaicheng Feng et al. proposed a new method for sleep apnea detection using ECG signals and their model uses an unsupervised feature learning module called FSSAE and a TDCS classifier composed of HMM and modified MetaCost. They achieved 85.1% accuracy, 86.2% sensitivity and 84.4% specificity on the PhysioNet Apnea-ECG dataset and the method improves apnea detection by reducing dependence on labeled data and dealing with class imbalance. However, the model is trained on limited unlabeled data and has some limitations [34].

Asma Gasmi et al. proposed a new Deep Learning (DL) based method to detect sleep abnormalities in elderly patients, creating a synthetic dataset with five sleep profiles for 2,500 patients. Mean-Shift clustering is used to model sleep behavior and LSTM-based autoencoder is used to detect abnormalities, which analyzes the differences between reconstructed and real sleep data. This method achieves 91.2% accuracy and 100% precision on synthetic data and 93% accuracy on real data [35]. Ning Han et al. proposed a dual DL framework for activity classification and anomaly detection using CNN + SVM and LSTM, and in this study, only 1 volunteer was observed for 2 days, and $> 95\%$ activity prediction success was achieved without real anomalies [36].

Rana Alabdan et al. proposed the MBES-DLSQP framework, where MBESA is used to tune the model settings and SSAE is used to predict sleep quality, and they tested it on a small Kaggle sleep dataset (400 instances, 4 sleep classes) and obtained 98.33% accuracy, but it has not been tested on clinical-grade PSG data [37]. Overall, a summary of existing DL approaches for sleep

and health monitoring is shown in Table 2.2.

Table 2.2: Summary of Sleep and Physiological Monitoring Studies.

Authors	**Approach / Models**	**Datasets**	**Performance**	**Criticism**
Gengalakshmi G. et al.	LSTM	Sleep-EDF Database (Expanded)	96.75% Accuracy	Minor light sleep vs. wake,REM errors; Uses simulated, not real-world, wearable data; Limited demographic diversity
Sumit Satoiya et al.	EEG scalogram + CNN	CAP dataset	99.51% Accuracy	Computational cost and inference time not reported; No comparison with other CNNs or transformers.
Kaicheng Feng et al.	FSSAE + TDCS classifier + HMM	PhysioNet Apnea-ECG	85.1% Accuracy; 86.2% Sensitivity; 84.4% Specificity	Limited ublabeled data; Requires labeled data for classification
Asma Gasmi et al.	Mean-shift clustering + LSTM autoencoder + synthetic data generation	Synthetic dataset	91.2% Accuracy (synthetic); 93% (real data)	Depends heavily on synthetic data; Assumes linear sleep degradation trend
Ning Han et al.	CNN + SVM; LSTM (signal prediction & anomaly detection)	Microwave sensor dataset (1 subject, 2 days, 12 activities)	>95% Accuracy	Extremely limited dataset (1 subject, 2 days)
Rana Alabdan et al.	MBESA hyperparameter optimization + SSAE + MBES-DLSQP framework	Kaggle Sleep Dataset (400 samples, 4-class labels)	98.33% Accuracy	Small datasets;Not Validated on clinical-grade PSG data

2.4 Comparison with Existing Works

Most existing works focus on different healthcare domain. Li et al. Works with sleep analysis with FL, but does not include privacy-preserving methods like Blockchain, ZKPs [19]. On the other hand, Nandini et al. Emphasizes Blockchain, ZKPs [22]. Similar, studies like Lansiaux and Sharma et al [23] [24]. incorporate XAI but they are limited to general medical AI applications rather than sleep analysis. Several works such as Albalwy and Raghav et al. focus primarily on secure data sharing but no target the sleep domain [25] [26]. Overall, a comparative analysis of the proposed framework against existing works is as shown in Table 2.3.

In our proposed framework includes FL to perform sleep pattern analysis, anomaly detection and behavioral analysis to ensure privacy, as well as Blockchain to ensure security and decentralization. XAI has been apply to make model decisions interpretable and transparent and zkps is being apply to ensure strong privacy protection. Finally, IPFS has also been used to make data storage and sharing more efficient and decentralized. This approach can be used in the healthcare sector, where privacy-preserving technologies can work together to create a more secure sleep monitoring system.

Table 2.3: Comparison of Proposed Framework with Existing Works.

Study	**Sleep Pattern and Anomaly Detection**	**FL**	**XAI**	**Blockchain**	**ZKPs**	**IPFS**	**Healthcare Domain**
Li et al. 2025	✓	✓	×	×	×	×	Sleep
Nandini et al. 2025	×	×	×	✓	✓	✓	Genomics
Lansiaux 2026	×	✓	×	×	✓	×	Medical AI
Sharma et al. 2025	×	✓	×	✓	✓	×	Medical AI
Albalwy 2026	×	×	×	✓	✓	✓	No Sleep Domain
Raghav et al. 2026	×	×	×	×	✓	✓	No Sleep Domain
Our Work	✓	✓	✓	✓	✓	✓	Sleep

Chapter 3
Overview of Related Technologies

Chapter 3: Overview of Related Technologies

3.1 Overview

This chapter discusses the fundamental technologies employed in the proposed framework. It covers several blockchain types, Zero Knowledge Proofs, smart contracts, federated learning and explainable AI to provide the technical foundation.

3.2 Blockhain and Types

The distributed, tamper-proof ledger technology known as blockchain [8]. Blockchain cloud services make it simple to gather, combine and exchange transactional data from multiple sources. Blocks of data are kept and cryptographic hashes are used as unique IDs to refer to the material in chronological sequence. Every block contains a hash of the one before it, forming an unchangeable and impenetrable data chain [38]. Blockchain protects data integrity, avoids data duplication and improves security. Blockchain is now a useful tool for reliable data management. Because data in a blockchain system cannot be altered without the approval or consent of the participating network nodes, fraud and data tampering are also prevented. Its decentralized consensus method nearly impossible to make unauthorized changes [39].

As shown in Figure 3.1, how blockchain stores data in an organized block format with important parts like a header, previous hash, timestamp, nonce and Merkle root [40]. This makes it safe, honest, and easy to trace without a central authority. In general, blockchain architectures can be classified into four primary categories namely public, private, consortium and other is hybrid blockchains [41]. These types are based on how decentralized, accessible, and governed they are. As shown in Figure 3.2, different industries and applications have different needs for each type. For example, areas such as healthcare and finance typically require strong governance and limited access to maintain safety and regulations. On the other hand, decentralization and transparency are usually more important in public blockchain or open systems. So what kind of system will be used depends on the needs, limitations and goals of the particular application.

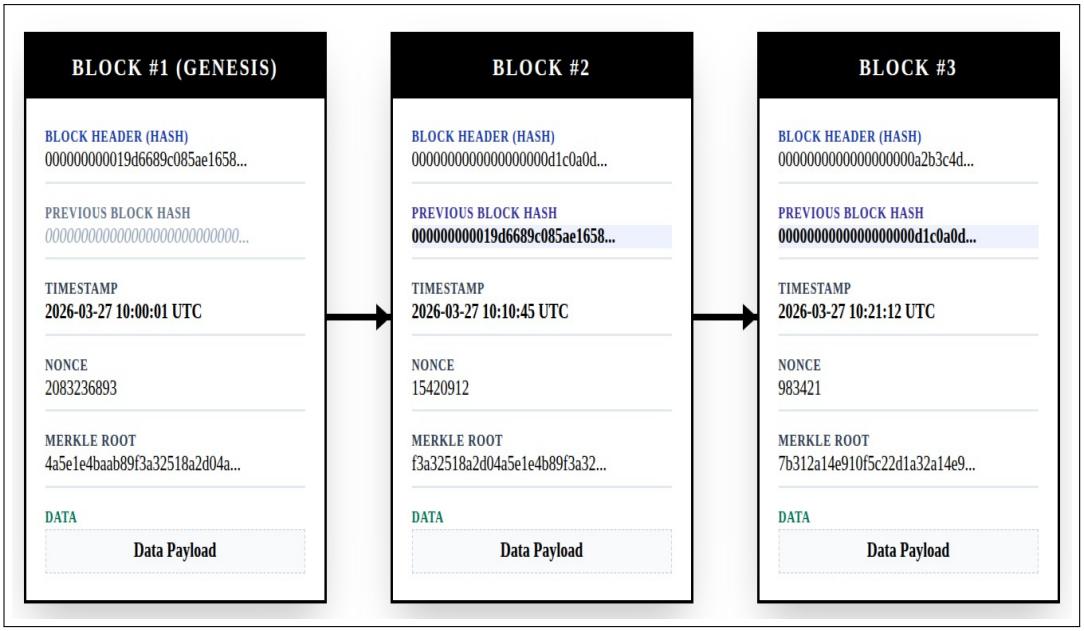


Figure 3.1: Internal Components of a Blockchain Block Header Structure and Data Linkage.

3.2.1 Public Blockchain

A public ledger is a kind of decentralized ledger technology that anybody may use. This means that anyone can see, add to and access the network without having permission from a central authority. Public blockchain must have decentralisation, open ledgers, data that can't be changed, Proof of Work and Proof of Stake (PoW & PoS) consensus, and access that doesn't require permission. The Ethereum Virtual Machine (EVM) is a basic blockchain and it possible to use decentralised apps (dApps) and programmable smart contracts. It has helped DeFi, NFTs and DAOs grow a lot and it is now a key part of the Web3 infrastructure [42]. This study critically examines the transformative role of blockchain in healthcare, elucidating its potential to enhance data integrity and interoperability while addressing persistent challenges related to scalability, privacy and regulatory compliance [43].

3.2.2 Private Blockchain

Private blockchains also known as permissioned ledgers only let trusted users access the system. This makes it easier to control and govern than open systems. This approach makes sure that

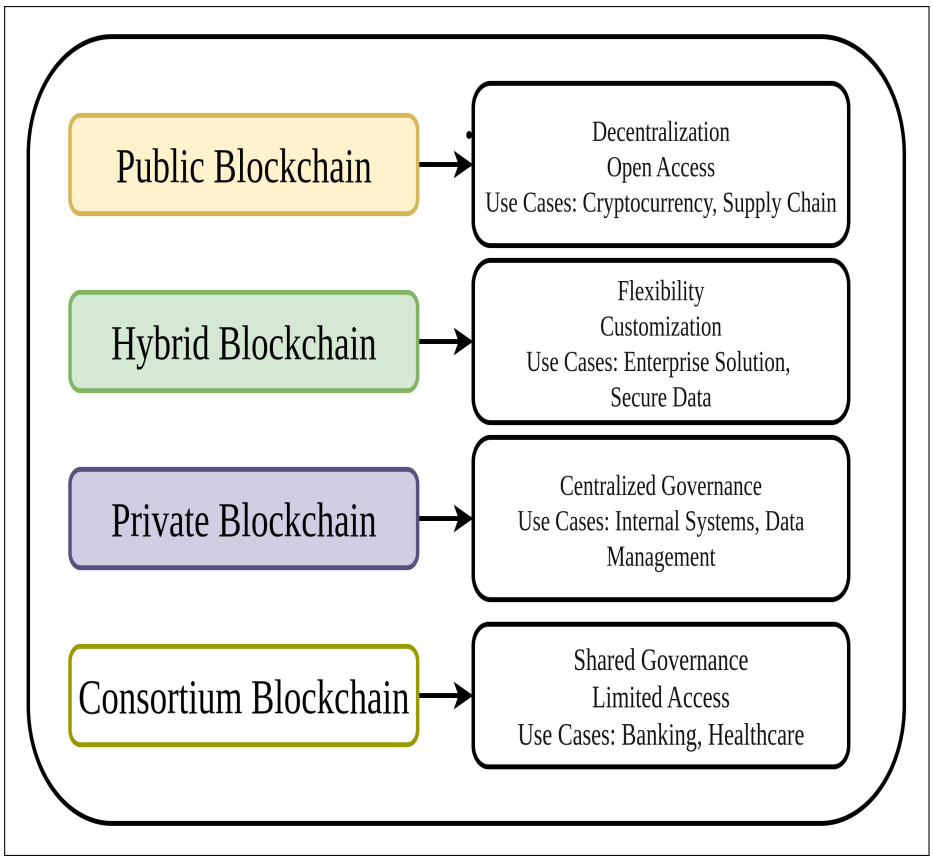


Figure 3.2: Types of Blockchain: Features and Use Case.

healthcare providers follow the rules, keep patient information private and keep the integrity of patient information while still keeping important blockchain features like immutability and decentralisation [44].

In a permissioned blockchain network for healthcare systems, all the nodes are cryptographically identified so that only hospitals, insurers and regulatory agencies can join. To make things work better, consensus protocols are used instead of the traditional Proof-of-Work models.. Smart contracts are used to automate important tasks like managing patient consent controlling who can access data and giving permission to share data. This makes health information systems more open and trustworthy. To protect patient privacy, sensitive medical records are kept off-chain in decentralized storage systems like IPFS or encrypted cloud storage. Tamper-evident cryptographic hashes and their corresponding metadata are kept securely on-chain so that they can be checked and audited [45][46].

3.2.3 Zero Knowledge Proofs

A zero knowledge proofs is an encrypted method allowing one party (the prover) to provide proof to another party (the verifier) the legitimacy of a statement without publicly revealing any information outside the proof of its truth. ZKP mechanisms can be added to healthcare systems to check a patient's credentials or consent without giving away private medical information, which is required by privacy regulations [47][48].

3.2.4 Smart Contract

In healthcare, smart contracts [49] are rules that run themselves and allow only authorized people access patients' private data safely. Patients can give or reject medical professionals access to their data without going through middlemen by including pre-agreed consent rules in blockchain contracts. The contracts automatically make sure that everything is consistent. They only let authorized people see certain medical information under open and permanent terms.

3.2.5 Consortium Blockchain

The Consortium Blockchain is a distributed ledger system that only certain people can use. It includes hospitals, drug companies, and health authorities, and it can help solve tough problems in the health sector. This technology makes sure that all parties can access health data that can't be changed in real time. It also automates patient compliance and insurance claim processing through smart contracts. It also gives a fully open audit trail to meet regulatory requirements, which guarantees data security, efficient management and compliance with the law [50].
This role-based structure provides a strong base for safe, scalable and able to communicate healthcare data exchange that protects patient privacy and holds people accountable [51]. Role-Based Access Control (RBAC) also makes sure that only patients who have permission can use the network. This multi-tiered design makes it easier to share data safely, reliably and in a way that works with other systems in healthcare ecosystems [52].

3.3 Federated Learning

Federated learning is a modern machine learning technique that trains models using the device's own (local) data instead of collecting data from a central server. Google was the first to propose distributed learning as a way to train models in a decentralized way with the main goal of protecting users' privacy. Further evaluations applying the FedAvg algorithm showed the efficiency of this method across several neural network architectures [53].

Centralized learning in modern healthcare means putting together patient data from many different places, like electronic health records, X-ray images, lab test results and clinic records, into one big server or database to train models. This makes it easier for data specialists to do their jobs because they can do a good job of pre-processing and cleaning the whole dataset. But keeping so much patient information in one place is a big risk to privacy and security [53]. Federated learning efficiently trains models while preserving data privacy in healthcare; however, it faces many technical and policy-related challenges [54]. Federated learning has several algorithms. FedProx [55] is an upgraded version of FedAvg that adds an extra proximal term to the local training of each client. The server picks a few clients at random for each round. SCAFFOLD [56] is a new version of FedAvg that uses control variables to make sure that clients' local updates are not biased or misdirected. This method keeps separate control vectors for the server and the client. Every round the server picks certain clients, trains them on their own data and sends control vectors to the server with updates. The server makes those changes and builds a new global model.

FedOPT [57] is a flexible federated optimization framework that uses both client and server-side optimizers to make global models converge faster by updating them based on local gradients and global aggregation. FedNova [58] is a method for normalizing averages that fixes the problem of objective inconsistency caused by differences in the clients' local updates. It also helps the global model converge to the right target by naturally averaging all the clients' updates. FedDyn [59] method uses dynamic regularization to change the local loss function of the devices

that take part in each round of FedDyn. This means that the optimized model of the device will slowly move closer to the servers global loss function's fixed point. Every device adds a linear and a quadratic penalty term to its own loss. FedBN also has its own batch normalization layer

Table 3.1: Core Properties of Federated Learning Algorithms (Part I).

Feature	**FedAvg**	**FedProx**	**SCAFFOLD**	**FedOpt**	**FedBN**	**Per-FedAvg**
Handles Non-IID Data	Moderate	✓	✓	✓	✓	✓
Personalization Support	×	×	×	×	✓	✓
Server-Side Optimizer	×	×	×	✓	×	×
Communication Efficiency	✓	✓	✓	✓	✓	Moderate

for each client, which it doesn't share with anyone else [60]. This method helps non-IID data come together better and the performance is also better. Theoretical analysis and experimental findings indicate that FedBN significantly surpasses FedAvg and FedProx. Additionally, the Personalized Federated Learning (FL) framework, utilizing MAML, introduces a tailored variant of Federated Averaging termed Per-FedAvg [61],which is shown in Table 3.1.

Experimental results indicate that customization is markedly more effective in heterogeneous datasets and can also achieve convergence with a non-convex loss function. One big problem is that clients don't have IID data, which makes performance worse. To tackle this issue, the model-level contrastive learning methodology termed MOON (Model-Contrastive Federated Learning) has been introduced [62]. Table 3.2 and Table 3.3 shows a feature-based comparison.

Table 3.2: Advanced Federated Learning Methods (Part II).

Feature	**MOON**	**FedDyn**	**Ditto**
Handles Non-IID Data	✓	✓	✓
Personalization Support	Moderate	×	✓
Server-Side Optimizer	×	×	×
Communication Efficiency	✓	✓	✓
Convergence Speed	✓	✓	✓
Robust to System Heterogeneity	✓	✓	✓

Table 3.3: Comparison of Federated Learning Algorithms.

Algorithm	**Non-IID**	**Pers.**	**Optimization Type**	**Comm. Eff.**
FedAvg	Moderate	×	SGD-based averaging	✓
FedProx	✓	×	Proximal SGD	✓
SCAFFOLD	✓	×	Variance reduction	✓
FedOpt	✓	×	Adam / Yogi / server-side optimization	✓
FedDyn	✓	×	Regularization-based optimization	✓
FedBN	✓	✓	Local batch normalization	✓
Per-FedAvg	✓	✓	Meta-learning	Moderate
MOON	✓	✓	Contrastive learning	✓
FedMA	✓	✓	Model matching / merging	× (High cost)
Ditto	✓	✓	Bi-level optimization	✓

3.4 Explainable AI

AI has changed healthcare a lot by automating diagnosis, risk assessment and medical advice. Most AI models especially deep learning models, are called black boxes because their decision-making processes are so complicated [63]. This is where the need for explainability comes in. Explainability Models make it easy for the patient to understand and trust a choice or prediction by breaking down the reasoning and method behind it [64].

Both the doctor and the patient need to know why the AI made those choices when it is used to make important decisions about a patients life. They can trust the model more if it can explain why it made a decision. So, explainability is important to make sure that AI models in healthcare are clear and trustworthy. In ML and DL explainability techniques are broadly divided into two major categories intrinsic explainability and post-hoc explainability [65]. Intrinsic explainability relates to models that can be understood by themselves because their design is simple and transparent. Such models, such as regression, logistic regression, decision trees, rule-based systems and generalized additive models (GAMs), provide a simple understanding

of how input features affect output. For instance, the correlation coefficients of linear regression clearly measure the relationship between features and predictions, and the decision tree gives a clear decision path with hierarchical splitting rules. The major benefit of intrinsic models is their transparency and ease of interpretation, which makes debugging easier and increases user trust [66].

Post-hoc explainability techniques aim to describe complex black-box models without modifying their architecture. Feature importance scores and LIME are two examples of these methods. They use simple substitute models to guess how things will behave in a certain area [67]. These methods can be specific to neural network architectures or useful to various model types. SHAP, on the other hand, uses game theory to figure out how much each feature adds to the model. PDP and ICE plots [68] make it easy to see how global and local features affect the model. These post-hoc methods can be used in healthcare to make sense of complicated predictive models for diagnosis, treatment suggestions, or risk assessment. This makes things clearer and builds trust between doctors and patients.

Chapter 4
Proposed Framework

Chapter 4: Proposed Framework

4.1 Overview

In this chapter, we discuss our proposed multi-module framework to address the deficiencies in sleep pattern analysis systems, including centralized privacy vulnerabilities and lack of data verifi- cation. The framework integrates deep learning for pattern extraction and anomaly detection, federated learning for decentralized model training, explainable AI (XAI) for interpretable model decisions, blockchain with zero-knowledge proofs (ZKP) for immutable privacy preservation, smart contracts for controlled access and IPFS for decentralized storage.
This chapter organized into five sections: **Section 4.2** Proposed framework, **Section 4.3** Architecture of Both Off-chain and On-chain Modules, **Section 4.5** Off-Chain Module with FL/XAI and Anomaly Detection, **Section 4.5** Off-Chain FL module with privacy and XAI, and **Section 4.6** On-chain Module.

4.2 Proposed Framework

Our proposed framework integrates blockchain, federated learning and privacy-preserving computation to ensure the secure and verifiable management of sleep data, as shown in Figure 4.1. This framework starts with sleep data which is first processed through preprocessing to remove noise and normalize features. Off-chain modules handle heavy computational tasks including sleep classification, deep learning based anomaly detection, real-time alert and FL / XAI modules. A global federated server coordinates multiple client nodes using differential privacy and secure aggregation, so that raw data never goes out of the local device. For secure storage and verification creates Zero-Knowledge Proofs (ZKPs) for private validation, stores metadata in IPFS with Content Identifier (CID) and stores only the CID, ZKP proof and timestamps in the blockchain. Smart contracts implement access control and verification rules. Lastly, parallel processing between on-chain and off-chain modules ensures real-time monitoring, integrity of dataand transparency with privacy rules.

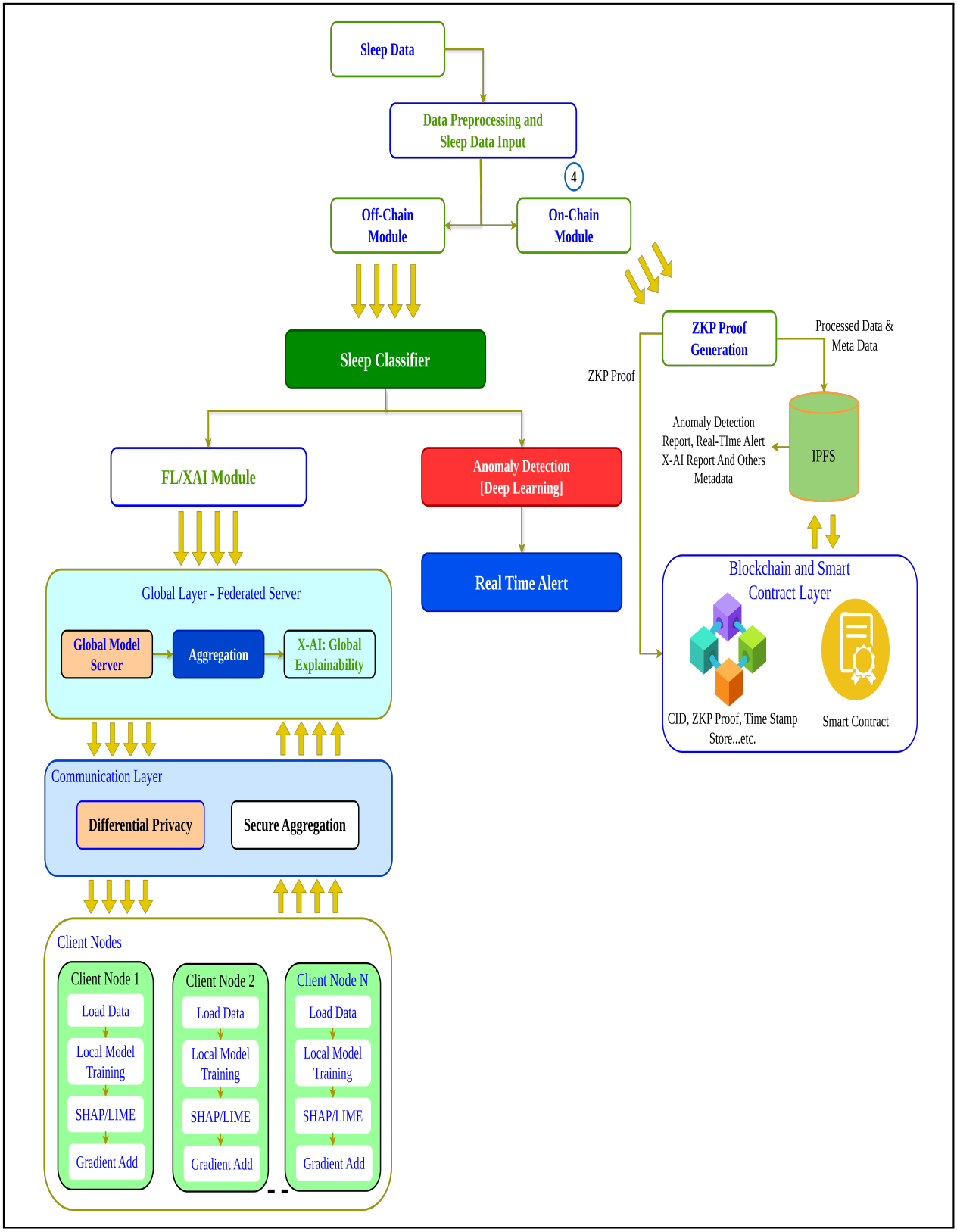


Figure 4.1: Proposed Framework Architecture Integrating Off-Chain and On-Chain Modules.

4.3 Architecture of Both Off-Chain and On-Chain Modules

The first step is to collect sleep data. Second, the data is cleaned up and sent to the off-chain and On-chain module, as shown in Figure 4.2. The procedure begins with processed sleep data. This data undergoes preprocessing and sleep data input during which it is cleansed, standardized and prepared for further analysis. The preprocessed data undergoes analysis, feature extraction and is subsequently stored in the off-chain module. This ensures that the blockchain avoids excessive computational demands. Simultaneously, the on-chain module performs critical functions including as hashing data, appending timestamps and executing smart contracts to ensure data accuracy and transparency.

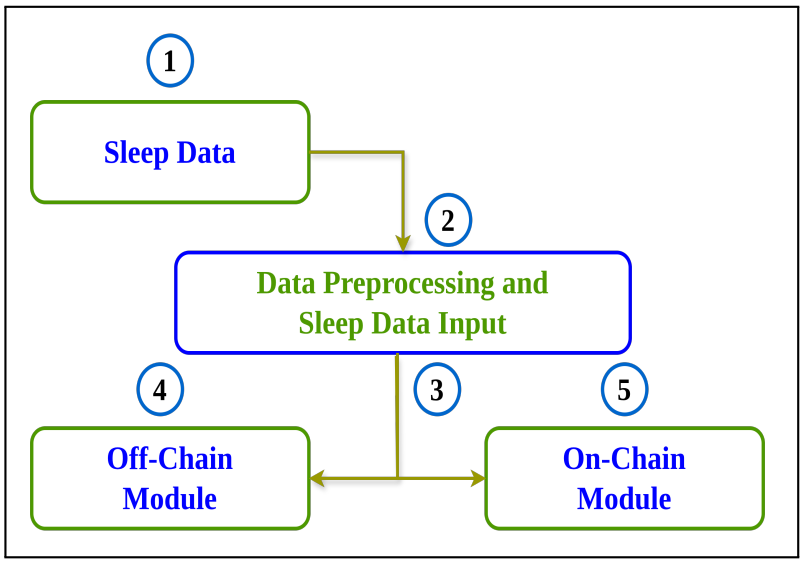


Figure 4.2: On-Chain and Off-Chain Module Integration.

4.4 Off-Chain Module

The Off-chain module performs computationally heavy tasks to reduce blockchain load. It includes four components. First, a sleep classifier module identifies sleep stages. Second, a deep learning–based anomaly detection module detects unusual sleep patterns. Third, a real-time alert mechanism sends alerts. Fourth, an FL/XAI module uses federated learning for for

further processing, as shown in Figure 4.3. Together, these components improve security and user trust.

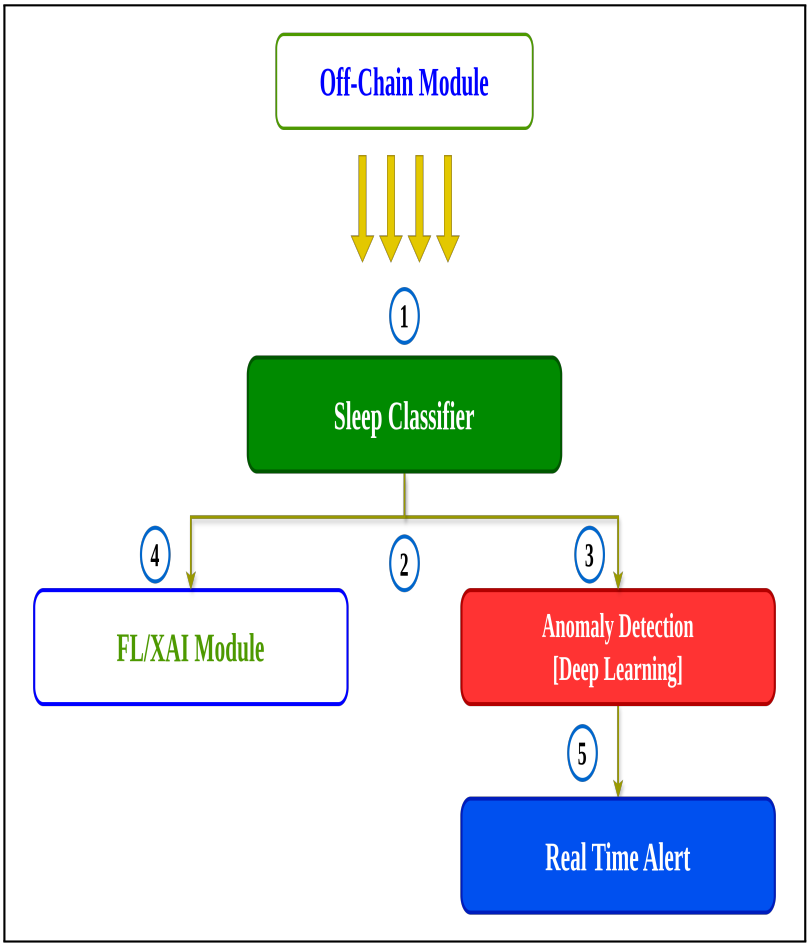


Figure 4.3: Off-Chain Module with FL/XAI and Anomaly Detection.

4.5 Off-Chain FL Module with Privacy and XAI

The Federated Learning (FL) with XAI module includes a global layer and multiple client nodes. The global layer contains a global model server with XAI for explainability and aggregatipn component to combine client updates. And communication Layer that uses differential privacy and secure user data. Each client node loads local sleep data, trains a model locally, uses SHAP or LIME to explain predictions. And Send only gradients not raw data to dathe federated server, as shown in Figure 4.4. This ensures privacy, security and transparency,

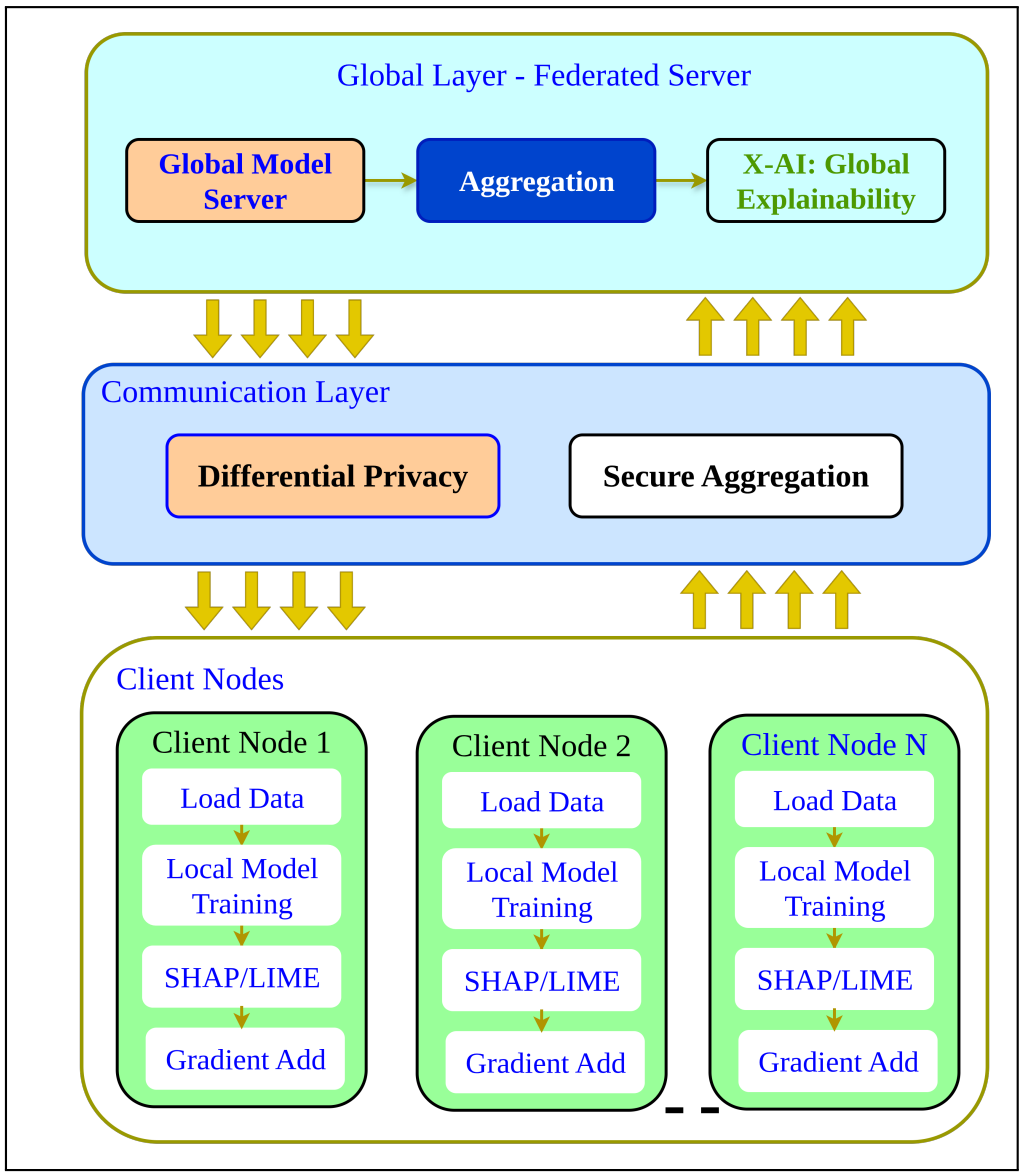


Figure 4.4: Off-Chain Federated Learning Module with Privacy and XAI.

4.6 On-Chain Module

The blockchain and smart contract module works with ZKPs and IPFS. First, ZKP proof generation creates cryptographics proofs that allow verification of sleep data without exposing the raw information. Second, IPFS (InterPlanetary File System) stores metadata off-chain and it returns unique CID (content identifier). IPFS is peer-to-peer decentralized storage networks.

Then blockchain stores only the CID, ZKP proof and timestamp. Which keeps costs low and privacy high. Finally, Smart contract manages access control with verification rules, as shown in Figure 4.5.

Together, these components ensure that sleep data is stores securely, verified privately and shared only with proper authorization.

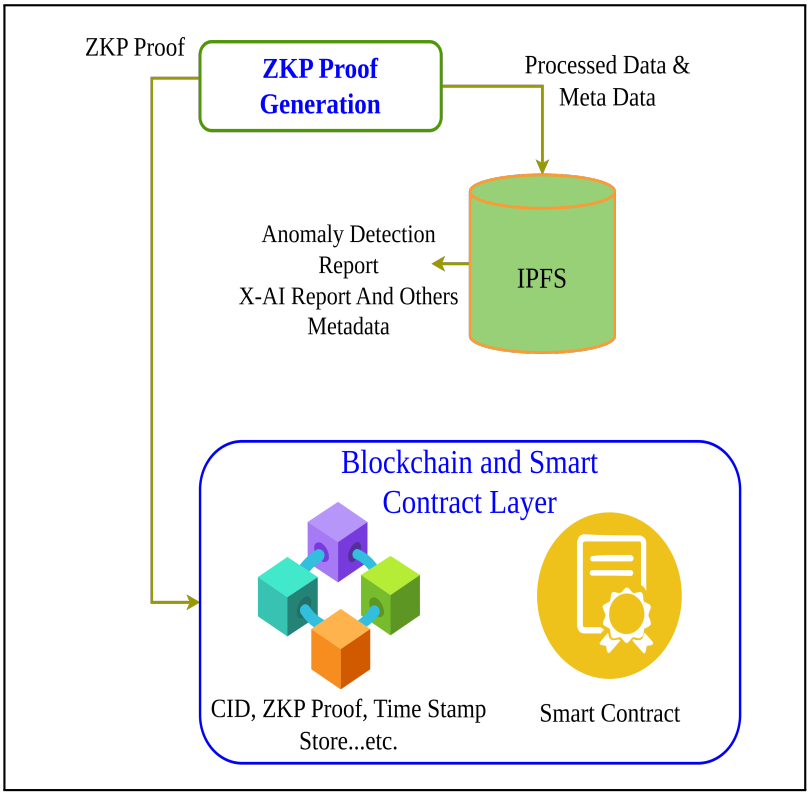


Figure 4.5: On-Chain Blockchain Module with ZKPs, IPFS and Smart Contract.

Chapter 5
Methodology

Chapter 5: Methodology

5.1 Overview

In this study, we proposed a framework for analyzing sleep patterns and protecting user data. The method that we have followed to verify the validity of the framework will be discussed in this section. We have used the deep learning model to detect sleep anomalies. FL is used to keep personal information as safe as possible. Explainable Artificial Intelligence (XAI) has been used to understand model decisions. Blockchain and smart contracts, Zero Knowledge Proofs (ZKPs) have been used to enhance the security and authenticity of data. Thus, we have proposed a secure, privacy-preserving and interpretable framework, which is useful for analyzing sleep patterns and user behavior. as shown in Figure 4.5. Our existing work for the environment setup, as shown in Table 5.1.

Table 5.1: Experimental Environment Configuration.

Category	**AI/ML Environment (Windows)**	**Blockchain Environment (Linux)**
OS	Windows 11 Enterprise multi-session	Linux Ubuntu 25.04
CPU	Intel i9 @ 12.2 GHz (Turbo)	AMD Ryzen 5 5600
AI Accelerator	NVIDIA GPU (16 GB VRAM)	—
RAM	128 GB	16 GB
Primary Storage	Samsung SSD 980 PRO (1 TB)	SSD (512 GB)
Secondary Storage	TOSHIBA F100 (4 TB)	—

This chapter is organized as follows: **Section 5.2** describes dataset description, **Section 5.3** presents data preprocessing, **Section 5.4 to 5.6** cover the off-chain and on-chain methodology and **Section 5.7** presents the off-chain evaluation measures.

5.2 Dataset Description

This study used three publicly available datasets: Sleep-EDF Database Expanded [69], MMASH [70] and PAMAP2 [71]. Both datasets include detailed physiological and behavioral signals necessary for sleep and psychophysiological assessments.

5.2.1 Sleep-EDF Database Expanded

The Sleep EDF Database Expanded contains complete nightly PSG recordings that have been collected from healthy individuals and individuals with minor sleep problems. Each recording includes EEG, EOG, chin EMG and event markers. Some recordings also include breathing and body temperature. The sleep stages are manually scored where the stages are W (Wake) R (REM) 1-4 (non-REM stages) M (Movement) and unknown.

The Sleep-EDF dataset contains PSG files in EDF format and hypnograms in EDF + format, which makes it possible to directly analyze sleep stages and electrophysiological signals. Overall, summary of Sleep-EDF dataset studies is as shown in Table 5.2.

Table 5.2: Summary of the Sleep-EDF Dataset Used in This Study.

Study	**Subjects / Recordings**	**Signal Sampling**
Sleep Cassette Study (SC)	Subjects	25–101 healthy adults
	Signals	EEG & EOG: 100 Hz EMG: 1 Hz Respiration: 1 Hz Body Temp: 1 Hz Event Marker: 1 Hz
Sleep Telemetry Study (ST)	Subjects	22 healthy adults, 44 recordings
	Signals	EEG: 100 Hz EOG: 100 Hz EMG: 100 Hz Event Marker: 1 Hz

5.2.2 MMASH

The MMASH dataset contains 24 hour continuous recordings of healthy participants that include a variety of physiological, behavioral and psychological data. Summary of MMASH dataset is as shown in Table 5.3. Participants wore 24-hour heart rate monitors and actigraphy

Table 5.3: Summary of MMASH Dataset Used in This Study.

Data Type	**File**	**Features**
Anthropometric	user_info.csv	Gender, Age, Height, Weight
Sleep	sleep.csv	Sleep onset, Total sleep time, Wake after sleep onset, Sleep efficiency, Movement, Fragmentation index
Cardiovascular	RR.csv	Beat-to-beat interval (RR intervals)
Psychological Assessment	questionnaire.csv	MEQ, STAI, PSQI, BIS/BAS, DSI, PANAS
Daily Activity	Activity.csv	Daily activity, Physical activity, Specific behaviors, Screen-related behavior
Actigraphy	Actigraph.csv	X, Y, Z axes raw accelerometer signals, Step count, Inclinometer data
Biomarkers	saliva.csv	Cortisol, Melatonin, Clock gene expression (before sleep and after wake-up)

devices, and filled out questionnaires at specific times. This dataset provides an opportunity to analyze the relationship between sleep quality, physical activity, cardiovascular response and mental status. Both datasets provide comprehensive and multimodal signals for sleep and psycho-physiological research, making it possible to analyze sleep stages, stress responses, activity and physiological markers using the Deep Learning model.

5.2.3 PAMAP2

The PAMAP2 [71] Physical Activity Monitoring dataset. This dataset contains multivariate time-series data collected from 9 subjects performing 18 different physical activities including

walking, running, cycling, soccer, rope jumping, and household chores. Each subject wore three inertial measurement units (IMUs) on the wrist, chest and ankle,along with a heart rate monitor. The data were recorded at a sampling frequency of 100 Hz for the IMUs and approximately 9 Hz for heart rate. Missing values are present and were handled appropriately during preprocessing.

Table 5.4: PAMAP2 Dataset Feature Description.

Data Type	**Features**
Physical Activity	Timestamp, Activity ID, Heart rate, IMU hand (17), IMU chest (17), IMU ankle (17)
IMU Hand	Temperature, 3D acceleration (±16g), 3D acceleration (±6g), 3D gyroscope, 3D magnetometer, orientation
IMU Chest	Temperature, 3D acceleration (±16g), 3D acceleration (±6g), 3D gyroscope, 3D magnetometer, orientation
IMU Ankle	Temperature, 3D acceleration (±16g), 3D acceleration (±6g), 3D gyroscope, 3D magnetometer, orientation
Heart Rate	Heart rate (bpm)
Activity Labels	Activity ID: 1 (lying), 2 (sitting), 3 (standing), 4 (walking), 5 (running), 6 (cycling), 7 (Nordic walking), 9 (watching TV), 10 (computer work), 11 (car driving), 12 (ascending stairs), 13 (descending stairs), 16 (vacuum cleaning), 17 (ironing), 18 (folding laundry), 19 (house cleaning), 20 (soccer), 24 (rope jumping), 0 (other)

5.3 Data Preprocessing

In this section we have presented an overall overview of the dataset preparation process, which is Anomaly Detection Module and FL and XAI Module.

5.3.1 Data Preprocessing for Anomaly Detection Module

In the process of data preprocessing raw PSG signals are collected from EDF files and converted into a clean and standardized segment by step-by-step processing which is suitable as an input to the deep learning model. This process includes signal loading, noise filtering, segmentation, normalization and memory-efficient data handling.

The data prepared at the end of the entire preprocessing pipeline is fed into a convolutional autoencoder model for the purpose of anomaly detection, as shown in Figure 5.1.

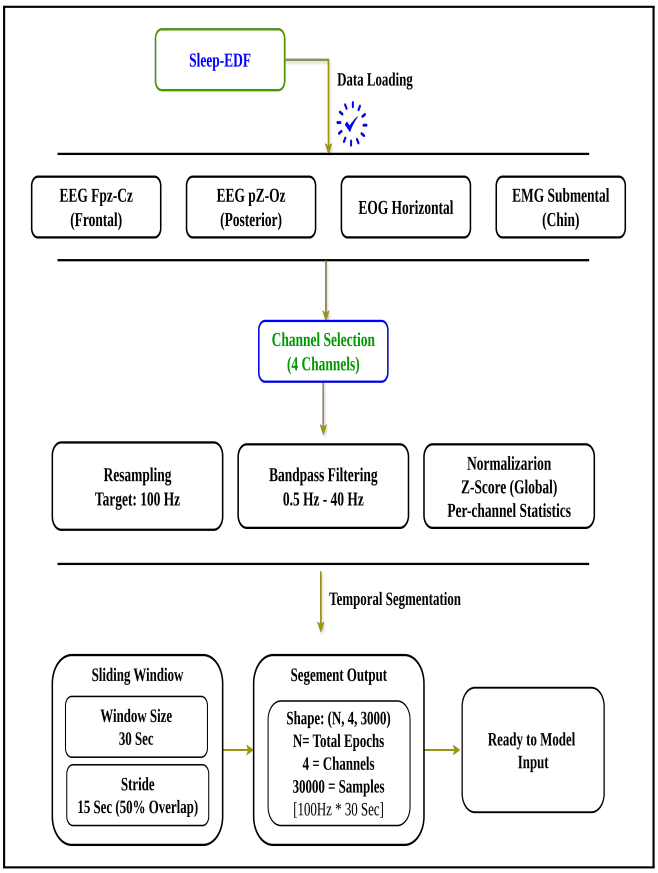


Figure 5.1: Data Preparation Pipeline Flow Diagram for Anomaly Detection.

Overall, data processing overview for sleep-EDF PSG signals is summarized as shown in Table 5.5.

Table 5.5: Data Processing Overview for Sleep-EDF PSG Signals.

Stage	**Step**	**Parameters**	**Output**
Data Loading	1	Sleep-EDF	PSG signals
	2	4 Channels (EEG Fpz-Cz, EEG Pz-Oz, EOG Horizontal, EMG Submental)	Selected channels
Preprocessing	3	Target: 100 Hz	Uniform sampling rate
	4	0.5–40 Hz (Butterworth, 4th order, filtfilt)	Filtered signals
	5	Per-Channel ($\varepsilon = 10^{-8}$)	Normalized signals
Segmentation	6	30s window, 15s stride (50% overlap)	Overlapping segments
	7	Shape: $(N \times 4 \times 3000)$	Uniform segments

5.3.2 Data Preprocessing for FL and XAI Module

This study also uses the MMASH dataset which includes multi-modal physiological and behavioral data recorded over 2 days. This dataset contains heart rate, step count, inclinometer data, sleep logs, RR intervals, cortisol levels and questionnaires, as well as signals from an accelerometer and a gyroscope.

For feature extraction, Raw Actigraph data is aggregated into hourly windows based on timestamps. Windows with fewer than 30 samples are discarded. For each valid window six statistical features (mean, standard deviation, maximum, minimum, 25th percentile, and 75th percentile) are computed across ten channels. Additional temporal features (hour, day, sample count) are included, resulting in 63 features per window.

The MMASH data processing technique is applied in this study for FL and XAI module, as shown in Figure 5.2.

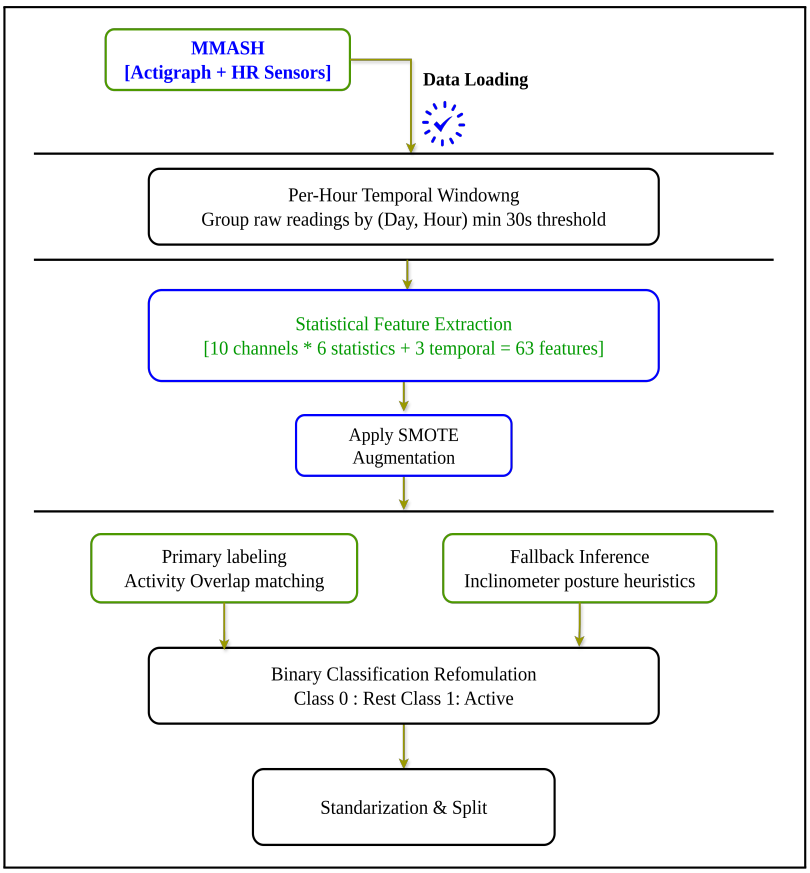


Figure 5.2: Data Preparation Pipeline Flow Diagram for FL and XAI Module.

5.4 Anomaly Detection Module Methods

Raw multi-channel recording be defined as:

$$\mathbf{X}_{\text{raw}} \in \mathbb{R}^{C \times T} \tag{5.1}$$

where C = 4 is the number of EEG/EOG/EMG channels:EEG Fpz-Cz, EEG Pz-Oz, EOG horizontal and EMG submental and T is the total number of time samples. To ensure uniform temporal resolution across recordings with varying acquisition frequencies, each signal is resampled to a defined sampling frequency:

$$\mathbf{X}_{\text{resampled}} = \text{Resample}\left(\mathbf{X}_{\text{raw}},\ f_s^{\text{orig}} \rightarrow f_s^*\right), \quad f_s^* = 100 \text{ Hz} \tag{5.2}$$

A 4th-order Butterworth bandpass filter is used to filter each channel to get rid of baseline drift and high-frequency noise:

$$\mathbf{X}_{\text{c, filtered}} = \text{filtfilt}(b, a, \mathbf{X}_c) \tag{5.3}$$

The filter transfer function $H(z)$ is designed with passband $[f_l, f_h] = [0.5, 40.0]$ Hz. The normalized cutoff frequencies are:

$$\Omega_l = \frac{f_l}{f_s^*/2} = \frac{0.5}{50} = 0.01, \quad \Omega_h = \frac{f_h}{f_s^*/2} = \frac{40}{50} = 0.8 \tag{5.4}$$

The filtfilt function uses zero-phase forward-backward filtering to get rid of phase distortion:

$$\mathbf{X}_{c,\text{filtered}} = \mathscr{F}^{-1}\Big\{H(j\omega) \cdot H^*(j\omega) \cdot \mathscr{F}\{\mathbf{X}_c\}\Big\} \tag{5.5}$$

The continuous filtered signal is partitioned into overlapping segments using a sliding window approach. For channel c, a segment beginning at sample index τ is defined as:

$$\mathbf{s}_c^{(\tau)} = \mathbf{x}_c^{\text{filtered}}\big[\tau : \tau + W\big] \tag{5.6}$$

The window length W and stride S are defined as:

$$W = f_s^* \cdot T_{\text{win}} = 100 \times 30 = 3000 \text{ samples}, \tag{5.7}$$

$$S = f_s^* \cdot T_{\text{stride}} = 100 \times 15 = 1500 \text{ samples} \tag{5.8}$$

The full set of segments across all C channels forms a 3D tensor:

$$\mathbf{S}^{(n)} \in \mathbb{R}^{C \times W}, \quad n = 0, 1, \ldots, N_{\text{seg}} - 1 \tag{5.9}$$

where the total number of segments per recording is:

$$N_{\text{seg}} = \left\lfloor \frac{T - W}{S} \right\rfloor + 1 \tag{5.10}$$

The 50% overlap, $T_{\text{stride}} = T_{\text{win}}/2$, ensures temporal continuity between adjacent segments. To normalize amplitude scale across heterogeneous channels, a global per-channel z-score normalization is computed over all segments from all recordings. For channel c:

$$\mu_c = \frac{1}{N_{\text{total}}} \sum_{n=1}^{N_{\text{total}}} \sum_{t=1}^{W} \mathbf{S}_{c,t}^{(n)} \tag{5.11}$$

$$\sigma_c^2 = \frac{1}{N_{\text{total}}} \sum_{n=1}^{N_{\text{total}}} \sum_{t=1}^{W} \left(\mathbf{S}_{c,t}^{(n)}\right)^2 - \mu_c^2 \tag{5.12}$$

The normalized segment $\hat{\mathbf{S}}^{(n)} \in \mathbb{R}^{C \times W}$ is passed through a Conv1D encoder f_θ to produce a compressed latent representation: Encoder stages each Conv1D layer with kernel k, stride s, padding p, and output channels d. The decoder g_ϕ reconstructs the input from $\mathbf{z}^{(n)}$:

Table 5.6: Conv1D Encoder Architecture.

Layer	**Operation**	k	s	p	**Output Channels**
1	Conv1D + ReLU	7	2	3	32
2	Conv1D + ReLU	5	2	2	64
3	Conv1D + ReLU	5	2	2	128
4	FC Projection	–	–	–	$d_z = 64$

The temporal dimension after each strided convolution is:

$$L_{\text{out}} = \left\lfloor \frac{L_{\text{in}} + 2p - k}{s} \right\rfloor + 1 \tag{5.13}$$

After three stages, the flattened representation is projected to the latent code:

$$\mathbf{z}^{(n)} = \mathbf{W}_{\text{enc}} \cdot \text{Flatten}\left(f_\theta\left(\hat{\mathbf{S}}^{(n)}\right)\right) + \mathbf{b}_{\text{enc}}, \quad \mathbf{z}^{(n)} \in \mathbb{R}^{64} \tag{5.14}$$

$$\hat{\mathbf{S}}^{(n)} = g_\phi\left(\mathbf{W}_{\text{dec}} \cdot \mathbf{z}^{(n)} + \mathbf{b}_{\text{dec}}\right) \tag{5.15}$$

The model is trained to minimize the mean squared reconstruction loss:

$$\mathscr{L} = \frac{1}{N}\sum_{n=1}^{N} \frac{1}{C \cdot W} \left\| \hat{\mathbf{S}}^{(n)} - \mathbf{S}^{(n)} \right\|_F^2 \tag{5.16}$$

And the per-segment anomaly score $\delta^{(n)}$ is defined as the reconstruction MSE:

$$\delta^{(n)} = \frac{1}{C \cdot W} \left\| g_\phi\left(f_\theta(\mathbf{S}^{(n)})\right) - \mathbf{S}^{(n)} \right\|_F^2 \tag{5.17}$$

The anomaly decision boundary is derived from the empirical score distribution using a 3-sigma rule:

$$\delta^* = \mu_\delta + 3\,\sigma_\delta \tag{5.18}$$

The mean and standard deviation of the anomaly scores are:

$$\mu_\delta = \frac{1}{N}\sum_{n=1}^{N} \delta^{(n)}, \qquad \sigma_\delta = \sqrt{\frac{1}{N}\sum_{n=1}^{N} \left(\delta^{(n)} - \mu_\delta\right)^2} \tag{5.19}$$

A binary anomaly label is then assigned as:

$$y^{(n)} = \begin{cases} 1 & \text{if } \delta^{(n)} > \delta^* \quad \text{(anomalous)} \\ 0 & \text{if } \delta^{(n)} \leq \delta^* \quad \text{(normal)} \end{cases} \tag{5.20}$$

5.5 FL and XAI Module Methods

The original MMASH dataset contained 22 participants. To address class imbalance and sample size for FL and XAI training SMOTE was applied during preprocessing. And for validation use PAMAP2 datasets. For cross-dataset validation, PAMAP2 activities were mapped to bi-

nary classes as follows: Rest = lying, sitting, standing; Active = walking, cycling, vacuum cleaning, ironing. In MMASH, For each user u, raw actigraph recordings are segmented into non-overlapping hourly windows. Let $\mathscr{W}_u$ denote the set of hourly windows for user u. Each window $w \in \mathscr{W}_u$ represents one hour of continuous recording and contains at least 30 samples.

For each sensor signal $s \in \{\text{Axis1, Axis2, Axis3, Steps, HR, VectorMagnitude, Inclinometer}\}$, we extract a statistical feature vector:

$$\mathbf{f}_s(w) = [\mu_s,\ \sigma_s,\ \max(s),\ \min(s),\ Q_{25}(s),\ Q_{75}(s)] \tag{5.21}$$

where μ_s and σ_s are the sample mean and standard deviation over the window. Combined with temporal context features $\{\text{hour}, \text{day}, n_{\text{samples}}\}$, the full feature vector for window w is:

$$\mathbf{x}_w \in \mathbb{R}^d, \quad d = 6 \times |\mathscr{S}| + 3 = 63 \tag{5.22}$$

Each window receives a binary label $y_w \in \{0, 1\}$ (Rest vs. Active). The dominant activity label is assigned via maximum-overlap matching with the Activity:

$$y_w = \arg\max_a \sum_{i \in \mathscr{A}} \mathbf{1}[a_i = a] \cdot \Delta t_i(w) \tag{5.23}$$

where $\Delta t_i(w)$ is the temporal overlap (in seconds) between activity interval i and window w. Activity codes are binarized as:

$$y_w = \begin{cases} 0 & \text{(Rest/Sleep)} \\ 1 & \text{otherwise} \quad \text{(Active)} \end{cases} \tag{5.24}$$

All features are normalized using global statistics computed across all users before distribution to clients:

$$\tilde{\mathbf{x}} = \frac{\mathbf{x} - \mu_{\text{global}}}{\sigma_{\text{global}} + \varepsilon}, \quad \varepsilon = 10^{-6} \tag{5.25}$$

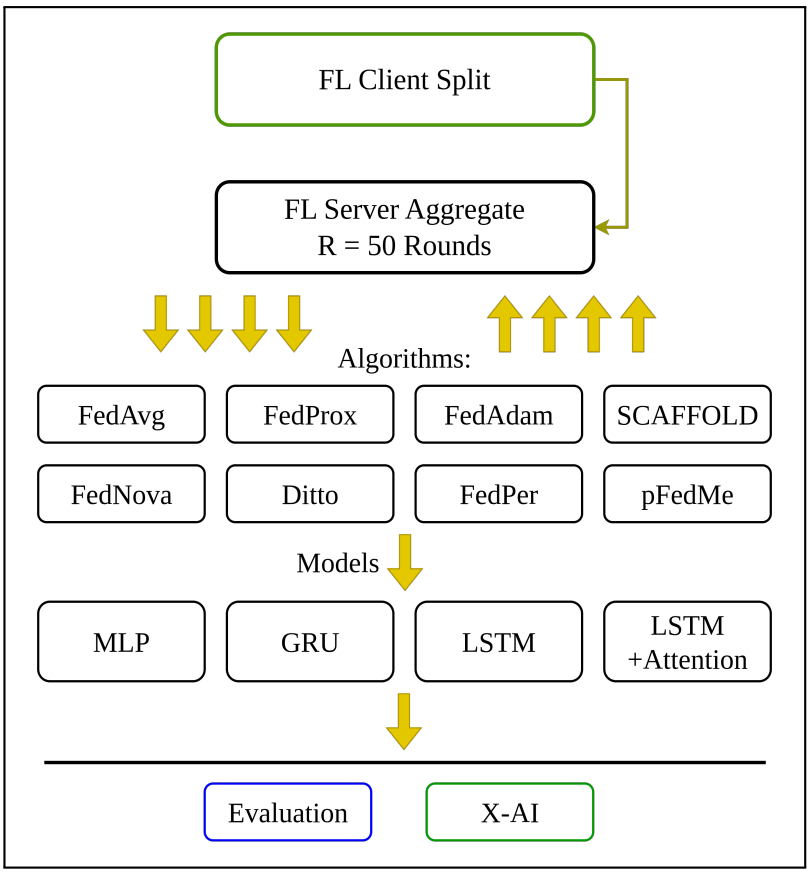


Figure 5.3: Federated Learning Algorithm Comparison and Explainable AI Integration.

We evaluate four neural architectures. Let $d = 63$ be the input dimension.

1. **MLP.** A two-hidden-layer perceptron with dropout regularization [72]:

$$\hat{y} = \sigma\Big(W_3 \cdot \mathrm{ReLU}\big(W_2 \cdot \mathrm{Dropout}(\mathrm{ReLU}(W_1\mathbf{x} + b_1)) + b_2\big) + b_3\Big) \tag{5.26}$$

   with hidden dimensions $[64, 32]$ and dropout rate $p = 0.3$.

2. **GRU.** A single-layer Gated Recurrent Unit [73]. Each window is treated as a sequence of length $T = 1$:

$$\mathbf{h}_t = \mathrm{GRU}(\mathbf{x}_t, \mathbf{h}_{t-1}; \theta_{\mathrm{GRU}}), \quad \hat{y} = \sigma(W_o\mathbf{h}_T + b_o) \tag{5.27}$$

   with hidden size 32 and dropout 0.3.

3. **LSTM.** A two-layer Long Short-Term Memory network [74]:

$$(\mathbf{h}_t, \mathbf{c}_t) = \mathrm{LSTM}(\mathbf{x}_t, \mathbf{h}_{t-1}, \mathbf{c}_{t-1}; \theta_{\mathrm{LSTM}}) \tag{5.28}$$

$$\hat{y} = \sigma(W_o \mathbf{h}_T + b_o)$$

with hidden size 48, 2 layers and dropout 0.2.

4. **LSTM + Attention.** Extends the LSTM with a scaled dot-product attention mechanism over all hidden states [75]:

$$\alpha_t = \frac{\exp\left(\mathbf{v}^\top \tanh(W_a \mathbf{h}_t)\right)}{\sum_{t'} \exp\left(\mathbf{v}^\top \tanh(W_a \mathbf{h}_{t'})\right)} \tag{5.29}$$

$$\mathbf{c} = \sum_t \alpha_t \mathbf{h}_t, \quad \hat{y} = \sigma(W_o \mathbf{c} + b_o) \tag{5.30}$$

All models are trained with Binary Cross-Entropy with Logits loss:

$$\mathscr{L}(\hat{y}, y) = -\left[y \log \sigma(\hat{y}) + (1-y) \log\left(1 - \sigma(\hat{y})\right)\right] \tag{5.31}$$

For Federated Server K clients (users) with a global server coordinating training. Let θ denote the global model parameters. Each client k holds a local dataset $\mathscr{D}_k = \{(x_i, y_i)\}$. Randomly partitioned into training clients (85%) and held-out test clients (15%).

FedAvg: The canonical weighted average aggregation rule:

$$\theta^{(r+1)} = \sum_{k=1}^{K} \frac{n_k}{n} \theta_k^{(r)} \tag{5.32}$$

where $n_k = |\mathscr{D}_k|$ and $n = \sum_{k=1}^{K} n_k$.

FedProx: Augments the local objective with a proximal term to control client drift:

$$\min_{\theta_k} \mathscr{L}_k(\theta_k) + \frac{\mu}{2} \left\| \theta_k - \theta^{(r)} \right\|^2 \tag{5.33}$$

with $\mu = 0.1$ in our experiments. Global aggregation follows FedAvg.

FedAdam: Applies adaptive server-side updates. $\Delta^{(r)} = \bar{\theta}^{(r)} - \theta^{(r)}$ denote the global pseudo-gradient (aggregated client update):

$$\mathbf{m}^{(r)} = \beta_1 \mathbf{m}^{(r-1)} + (1-\beta_1)\Delta^{(r)} \tag{5.34}$$

$$\mathbf{v}^{(r)} = \beta_2 \mathbf{v}^{(r-1)} + (1-\beta_2)\left(\Delta^{(r)}\right)^2 \tag{5.35}$$

$$\theta^{(r+1)} = \theta^{(r)} + \eta_s \frac{\hat{\mathbf{m}}^{(r)}}{\sqrt{\hat{\mathbf{v}}^{(r)}} + \varepsilon} \tag{5.36}$$

$\eta_s = 10^{-3}$ and bias-corrected moments:

$$\hat{\mathbf{m}}^{(r)} = \frac{\mathbf{m}^{(r)}}{1-\beta_1^r}, \quad \hat{\mathbf{v}}^{(r)} = \frac{\mathbf{v}^{(r)}}{1-\beta_2^r} \tag{5.37}$$

SCAFFOLD: Addresses client drift via control variates. Each client k maintains a local control variate $\mathbf{c}_k$ and the server maintains $\mathbf{c}$. The corrected local update is:

$$\theta_k \leftarrow \theta_k - \eta_l \left(\nabla \mathscr{L}_k(\theta_k) + \mathbf{c} - \mathbf{c}_k \right) \tag{5.38}$$

After local training the control variates are updated as:

$$\mathbf{c}_k^+ = \mathbf{c}_k - \mathbf{c} + \frac{\theta^{(r)} - \theta_k^+}{\eta_l \cdot E} \tag{5.39}$$

where E is the number of local epochs.

The server performs aggregation as:

$$\mathbf{c}^{(r+1)} = \frac{1}{K}\sum_{k=1}^{K}\mathbf{c}_k^{+}, \quad \theta^{(r+1)} = \theta^{(r)} + \eta_s \cdot \bar{\Delta}^{(r)} \tag{5.40}$$

FedNova: Normalizes local updates by the effective number of local steps τ_k to remove objective inconsistency [76].

$$\tilde{\Delta}_k = \frac{\theta^{(r)} - \theta_k^{+}}{a_k + \varepsilon}, \quad a_k = \tau_k \tag{5.41}$$

$$\tau_{\text{eff}} = \sum_{k=1}^{K}\frac{n_k}{n}a_k \tag{5.42}$$

$$\theta^{(r+1)} = \theta^{(r)} + \eta_s \cdot \tau_{\text{eff}} \cdot \sum_{k=1}^{K}\frac{n_k}{n}\tilde{\Delta}_k \tag{5.43}$$

FedPer: Separates model parameters into a shared base θ_{base} and a personalized head θ_{head} [77]. Only the base layers are federated:

$$\theta_{\text{base}}^{(r+1)} = \text{FedAvg}\left(\{\theta_{\text{base},k}\}_{k=1}^{K}\right), \quad \theta_{\text{head},k} \text{ is retained locally} \tag{5.44}$$

The split point is set at the last two parameter tensors of the network.

pFedMe: Decouples personalized models θ_k from the global model θ via a proximal objective [78]:

$$\min_{\theta_k} \mathscr{L}_k(\theta_k) + \frac{\lambda}{2}\left\|\theta_k - \theta\right\|^2 \tag{5.45}$$

with $\lambda = 0.5$. The global model is updated by averaging from the clients.

Ditto: Jointly trains global and personalized models. The personalized objective for client k is:

$$\min_{\theta_k} \mathscr{L}_k(\theta_k) + \frac{\lambda}{2} \left\| \theta_k - \theta^{(r)} \right\|^2 \tag{5.46}$$

where $\theta^{(r)}$ is the frozen global model updated independently via FedAvg in the same communication round.

Each client performs $E = 10$ local epochs per round over $R = 50$ communication rounds. The local optimizer is Adam:

$$\theta_k \leftarrow \theta_k - \eta \nabla_{\theta_k} \mathscr{L}_k(\theta_k), \quad \eta = 10^{-3}, \quad \lambda_{\text{wd}} = 10^{-3} \tag{5.47}$$

with mini-batch size $B = 32$.

Apply four complementary attribution methods to the final global model. For feature j and baseline metric m_0:

$$\text{PI}_j = \frac{1}{R} \sum_{r=1}^{R} \left[m\left(\tilde{\mathbf{X}}^{(j,r)} \right) - m_0 \right] \tag{5.48}$$

where $\tilde{\mathbf{X}}^{(j,r)}$ denotes the dataset with feature column j randomly permuted in repetition $r (R = 10)$.

KernelSHAP uses a background reference set of size $B = 10$ to figure out feature attributions. The global feature importance is defined as:

$$\phi_j = \frac{1}{N} \sum_{i=1}^{N} \left| \phi_j^{(i)} \right| \tag{5.49}$$

For a baseline input $\mathbf{x}'$ and input $\mathbf{x}$ along a straight-line path:

$$\text{IG}_j(\mathbf{x}) = (x_j - x_j') \cdot \int_0^1 \frac{\partial F(\mathbf{x}' + \alpha(\mathbf{x} - \mathbf{x}'))}{\partial x_j} \, d\alpha \tag{5.50}$$

The integral is approximated using 30 uniform steps. And local surrogate model $g \in \mathscr{G}$ is fitted around each sample $\mathbf{x}_i$ using N_s samples.

$$\xi(\mathbf{x}_i) = \arg\min_{g \in \mathscr{G}} \mathscr{L}(F, g, \pi_{\mathbf{x}_i}) + \Omega(g) \tag{5.51}$$

where $\pi_{\mathbf{x}_i}$ is a proximity kernel measuring similarity to $\mathbf{x}_i$ and $\Omega(g)$ is a complexity regularization term. Also feature importance scores are obtained by averaging rank positions across all attribution methods:

$$\text{Score}_j = \frac{1}{|\mathscr{M}|} \sum_{m \in \mathscr{M}} (d - \text{rank}_m(j) + 1) \tag{5.52}$$

where d is the total number of features and $\mathscr{M} = \{\text{Permutation, SHAP, IG}\}$.

5.5.1 External Validation

External validation is an essential process for evaluating the generalizability and stability of FL models. External validation assesses the models performance on an entirely separate data source, whereas internal validation assesses how well a model generalizes to new individuals within the same methodology. The objective of this study was to analyze the performance of the off-chain module in different datasets. We evaluated and validated the performance of our models using the MMASH and PAMAP2 datasets and also observe the demographic differences of the participants in this process.

To improve cross-dataset validation, we constructed a uniform feature space comprising 16 shared properties between MMASH and PAMAP2 and hese qualities emphasize the most separate physiological and behavioral indicators heart rate and limb acceleration. The 16 shared features are categorized as follows: physiological (4 features) hr mean, std, max and min. Also biomechanical (12 features) three axis accelerometer readings from the hand, wrist area, each represented by its mean, std, max and min. We measured and observed performance using evaluation metrics.

5.6 On-Chain Module Methods

AES-256-CBC encryption [79] is used to protect local sleep pattern metadata, anomalies, FL/XAI outputs, and feature attributions before they are stored on IPFS. The blockchain only keeps cryptographic references. A ZKPs hash is generated from the FL/XAI output using SHA-256 as a cryptographic commitment that is stored on the blockchain. EIP-191 [80] checks the user's authenticity by recovering the Ethereum address from the signature before blockchain transactions. The smart contract on the blockchain checks the roles of the caller before saving records that can't be changed and include IPFS hash, ZKP hash, timestmaps and FL/XAI metadata. Overall procedure is followed as shown in Algorithm 1.

Algorithm 1 Data Recording with RBAC and ZK Proofs in On-Chain Module

Input:
  User address A_{user}
  IPFS hash H_{ipfs}
  ZK proof hash H_{zk}
  Caller role R_{caller}
  Operation O_{store}
$\text{role}_{\text{caller}} \leftarrow$ query role of `msg.sender` from role mapping
$\text{authorized} \leftarrow (\text{role}_{\text{caller}} = \text{ADMIN} \vee \text{role}_{\text{caller}} = \text{DATA\_MANAGER} \vee \text{role}_{\text{caller}} = \text{USER})$
$\text{valid}_{\text{user}} \leftarrow (A_{\text{user}} \neq \mathbf{0})$
$\text{valid}_{\text{hash}} \leftarrow (H_{\text{ipfs}} \neq \emptyset \wedge H_{\text{zk}} \neq \emptyset)$
if $\text{authorized} \wedge \text{valid}_{\text{user}} \wedge \text{valid}_{\text{hash}}$ **then**
    timestamp $\leftarrow$ current block timestamp
    Execute O_{store}: append new record to userRecords$[A_{\text{user}}]$
    Emit $(A_{\text{user}}, H_{\text{ipfs}}, H_{\text{zk}}, \text{timestamp}, \text{role}_{\text{caller}})$
end if

5.7 Off-Chain Evaluation Measures

In this study, various standard metrics were used to determine the performance of the models applied in the Off-Chain Module. The main terms of the confusion matrix used for classification evaluation, as shown in Table 5.7. Also, the mathematical definitions of the evaluation metrics, as shown in Table 5.8. Overall, these evaluation metrics were highly significant for evaluating the performance of the models applied in this study.

Table 5.7: Classification Outcome Labels.

Symbol	**Full Form**
TP	True Positive
TN	True Negative
FP	False Positive
FN	False Negative

Table 5.8: Mathematical Definitions of Evaluation Metrics.

Metric	**Formula**
Precision	$\frac{TP}{TP+FP}$
Recall	$\frac{TP}{TP+FN}$
Accuracy	$\frac{TP+TN}{TP+FP+FN+TN}$
F1-Score	$\frac{2\times Precision\times Recall}{Precision+Recall}$
Specificity	$\frac{TN}{TN+FP}$
True Positive Rate	$\frac{TP}{TP+FN}$
False Positive Rate	$\frac{FP}{FP+TN}$
AUC	$\int_0^1 True\ Positive\ Rate\, d(False\ Positive\ Rate)$

Chapter 6
Results and Discussion

Chapter 6: Results and Discussion

6.1 Overview

The results based on the proposed framework are presented in this chapter. The proposed framework is discussed in Figure 4.5 of Chapter 4. The results are divided into four subsections based on the datasets used: Sleep anomaly detection, Federated learning and explainable AI with validation, Behavioral pattern analysis and Blockchain based On-Chain module results.

6.2 Sleep Anomaly Detection Results

Initially 153 PSG records from the sleep-cassette subset of the Sleep-EDF Database Expanded were explored. After applying the preprocessing steps in Chapter 5, 150 PSG records (N = 150) were kept for the final analysis. As shown in Table 6.1, a total of 220,328 segments were

Table 6.1: Reconstruction Error Statistics for Autoencoder-Based Anomaly Detection.

Metric	**Value**
Total Segments	220328
Normal Segments	217497 (98.7%)
Anomaly Segments	2831 (1.3%)
Mean Score	0.0336
Std Score	0.0304
Median Score	0.0248
Min Score	0.0002
Max Score	0.3230
Threshold	0.1249

analyzed out of which 217,497 (98.7%) were classified as normal and only 2,831 (1.3%) as anomalies. This low anomaly a percentage (1.3%) shows that the dataset is very unbalanced which is common in real-world physiological anomaly detection where anomalies happen only rarely. The reconstruction error scores range from 0.0002 to 0.3230 with a mean of 0.0336 and a median of 0.0248. If the median mean is less than the mean. It means the data is right-skewed.

Most segments have a low reconstruction error. So they are normal. Some segments have a high error which means they are anomalies. The standard deviation of 0.0304 indicates the variation of the error.

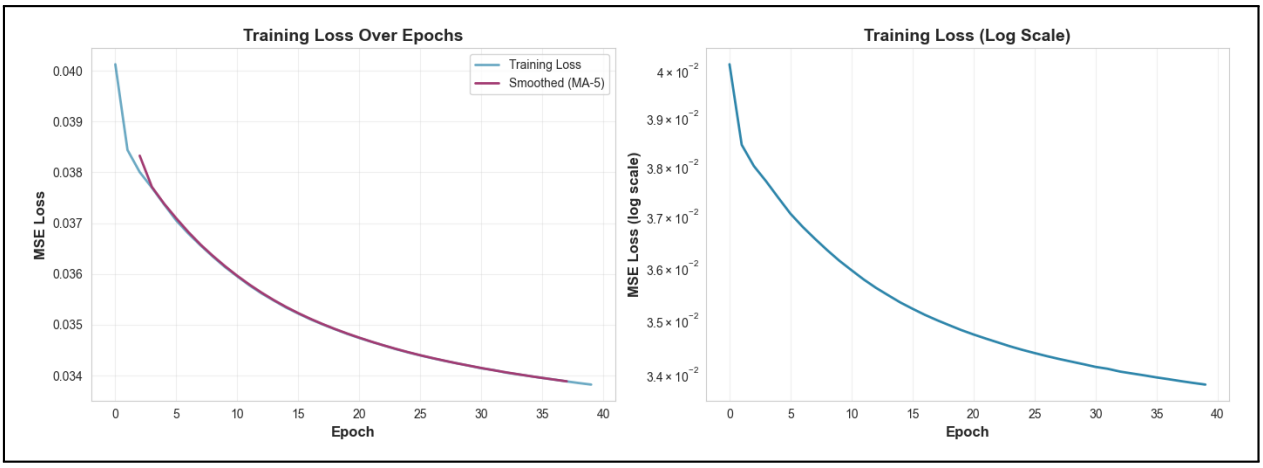


Figure 6.1: Convergence of Autoencoder Training Loss.

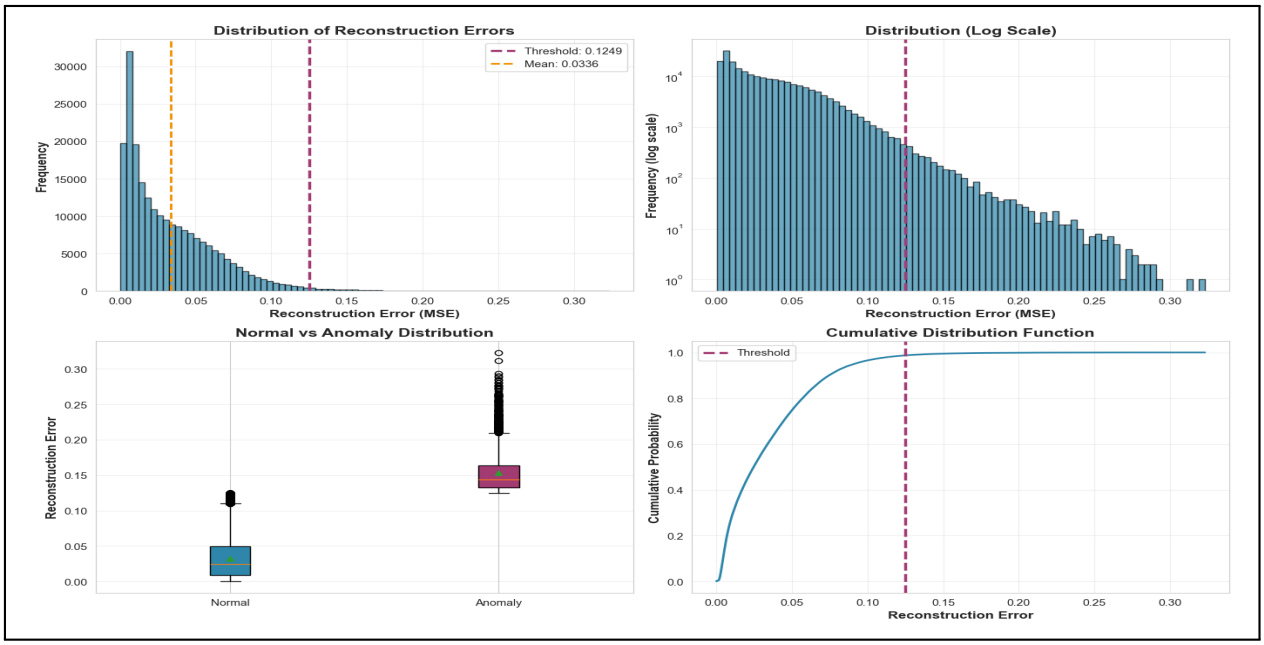


Figure 6.2: Reconstruction Error Analysis for Autoencoder-Based Anomaly Detection.

Autoencoder first learns the data pattern and calculates the reconstruction error. As shown in Figure 6.1, Left: MA-5 Loss (Linear Scale). Right: MSE Loss (Log Scale). Loss Decreases Gradually from 0.040 to 0.034 Over 40 Epochs. Then use the 0.1249 threshold to separate

normal and anomaly. As shown in Figure 6.2, the histogram, log-scale distribution, normal vs anomaly comparison and cumulative distribution function with threshold clearly represent the distributional attributes of the reconstruction error and distinctly differentiate between normal and anomalous samples according to the established decision boundary. Low reconstruction error show normal and high reconstruction show abnormal sleep pattern.

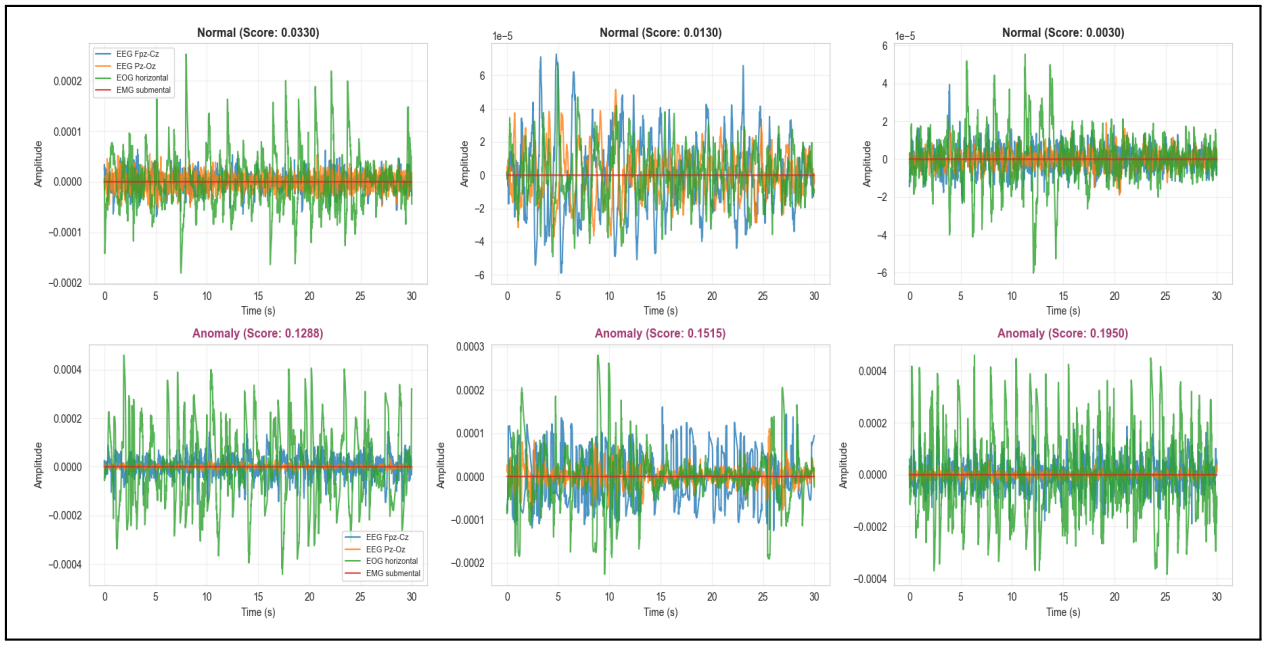


Figure 6.3: Reconstruction Error Comparison Between Normal Samples and Anomalies Across Data Instances.

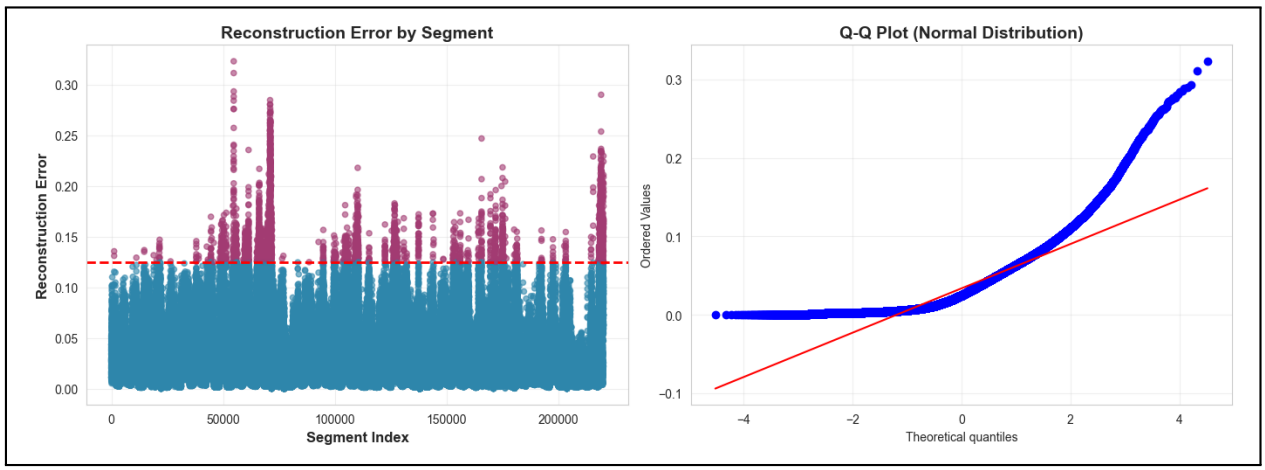


Figure 6.4: Reconstruction Error for Each Segment Index Across All Signal Channels, with Color-coded Traces Showing Patterns of Anomalies.

The violin plot and Q-plot compares reconstruction error distributions between normal and anomalous samples. Normal data shows a very low and tightly clustered error distribution, indicating stable reconstruction by the model, as shown in Figure 6.4 and 6.5.

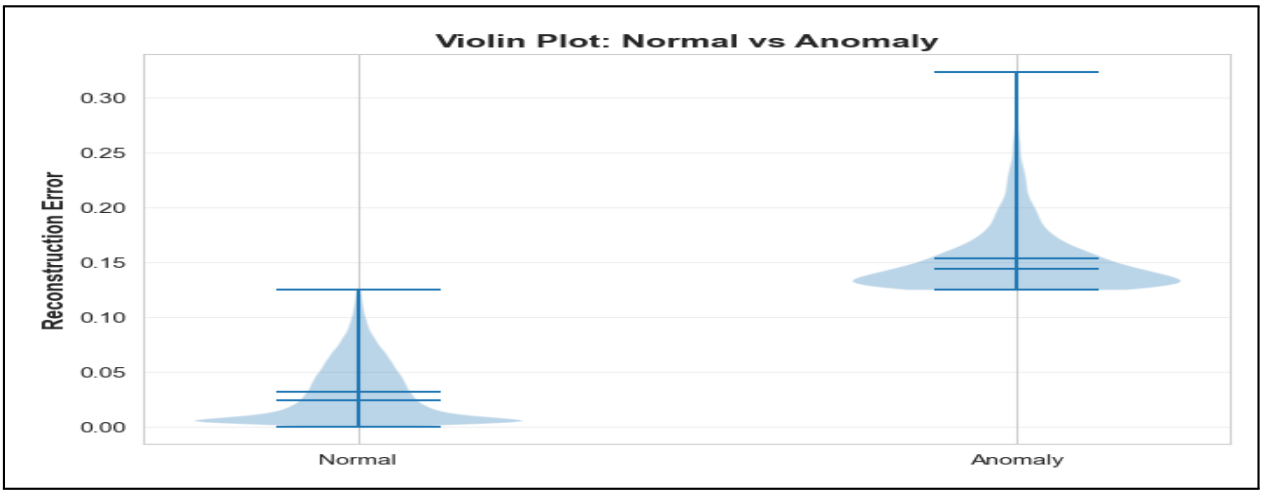


Figure 6.5: Distribution of Reconstruction Errors for Normal vs Anomaly Classes Using Violin Plot Visualization.

As shown in Figure 6.6, low error means normal pattern and high error mean abnormal pattern. This figure compares normal vs abnormal segments based on sleep signals.

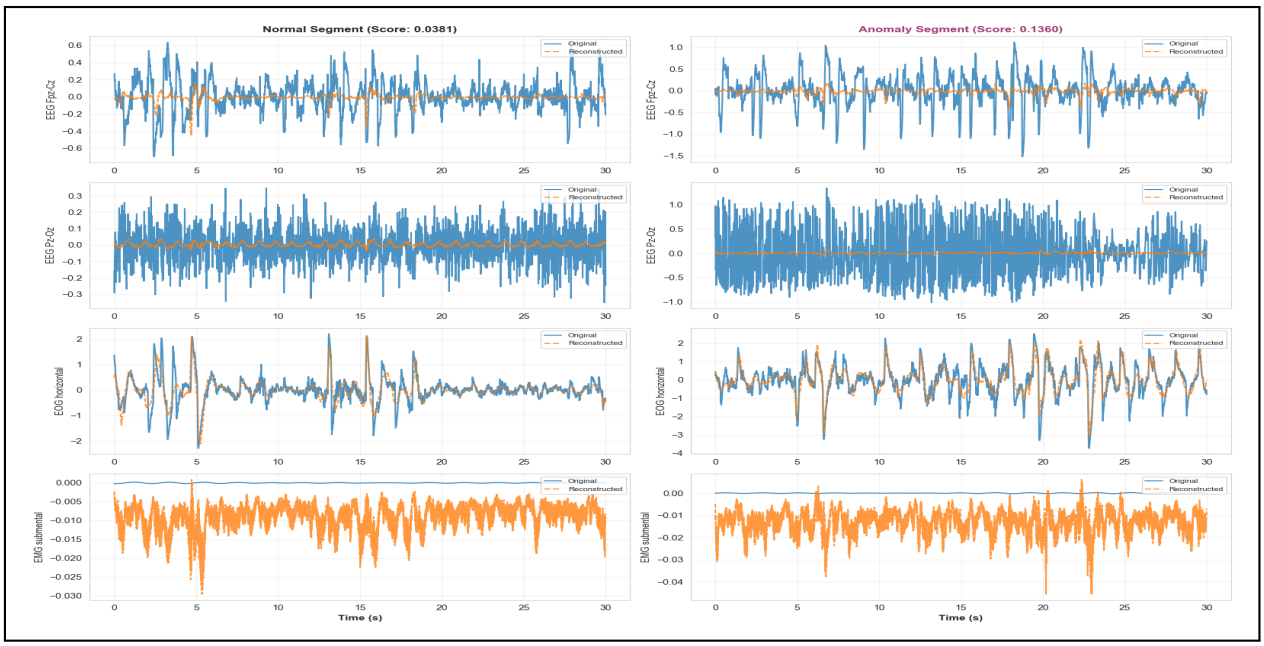


Figure 6.6: Comparison of reconstruction errors for normal and abnormal segments using a threshold-based anomaly detection boundary.

6.3 FL and XAI Module Results

The MMASH dataset used in FL and XAI modules and compared the performance of eight federated learning algorithms FedAvg, FedProx, FedAdam, SCAFFOLD, FedNova, FedPer, pFedMe and Ditto on four different model architectures (MLP, GRU, LSTM, and LSTM + Attention). The PAMAP2 [71] dataset is then used to validate these models. LSTM+Attention (pFedMe) performed well better than any other model for the classification of Rest vs. Active states. The performance of the models is evaluated using accuracy, precision, recall and F1-score metrics.

Table 6.2: Best Model Performance with Cross-Dataset Validation.

Metric	**MMASH (Test)**	**PAMAP2 (Validation)**
Model	LSTM_ATTENTION	LSTM_ATTENTION
FL Algorithm	pFedMe	pFedMe
Accuracy	**0.9776**	0.9223
F1 Score	**0.9831**	0.9337
AUC-ROC	**0.9932**	0.9743
AUC-PR	**0.9962**	0.9831

Table 6.3: Performance Comparison between MMASH Training and PAMAP2 Validation.

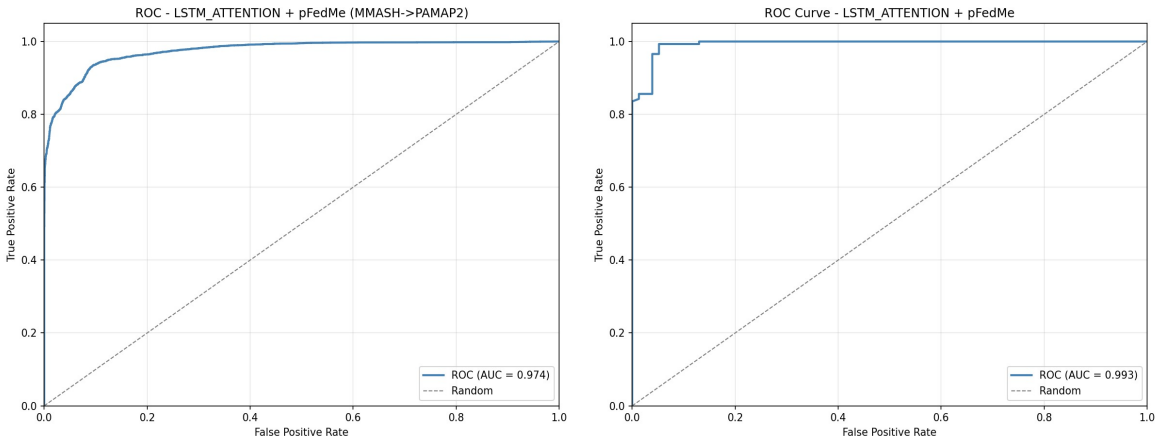
Category	**Algorithms**	**MMASH Training Acc**	**PAMAP2 Validation Acc**	**Transfer Gap**
Personalized	pFedMe, Ditto, FedPer	0.9308	0.9215	-0.0093 (-1.0%)
Non-Personalized	FedAvg, FedProx, FedAdam, SCAFFOLD, FedNova	0.9123	0.9218	+0.0095 (+1.0%)

Total model tested on MMASH test set is 32 (4 models x 8 FL algorithms) and the best performing model is LSTM+Attention with pFedMe algorithm with an accuracy of 97.76%, F1 score

of 98.31%, AUC-ROC of 99.32% and AUC-PR of 99.62%. When validated on the PAMAP2 dataset, the same model achieved an accuracy of 92.23%, F1 score of 93.37%, AUC-ROC of 97.43% and AUC-PR of 98.31%. The top 8 best-performing ranked by two datasets MMASH for personalized performance and PAMAP2 for external validation, as shown in Table 6.4.

Table 6.4: Ranking of Models Based on MMASH and PAMAP2 Performance.

Rank	**Model**	**FL Algorithm**	**MMASH**		**PAMAP2**	
			Acc	**F1**	**Acc**	**F1**
1	LSTM+Attention	pFedMe	**0.9776**	**0.9831**	0.9223	0.9337
2	MLP	pFedMe	0.9641	0.9728	0.9219	0.9331
3	LSTM	pFedMe	0.9596	0.9695	0.9215	0.9335
4	GRU	pFedMe	0.9507	0.9625	0.9217	0.9336
5	LSTM+Attention	FedPer	0.9327	0.9495	0.9196	0.9318
6	LSTM+Attention	FedAvg	0.9283	0.9463	**0.9224**	**0.9341**
7	LSTM+Attention	SCAFFOLD	0.9238	0.9435	0.9212	0.9329
8	LSTM	FedAdam	0.9103	0.9315	0.9204	0.9327



(a) ROC on PAMAP2 Validation Dataset. (b) ROC for Best Performing Model.

Figure 6.7: ROC Curve Comparison for The Best Performing Model Across Validation and Test Datasets.

The SHAP analysis of the LSTM+Attention model with pFedMe model indicated that activity based features particularly incl_stand_mean and steps_p75 contribute most important to the

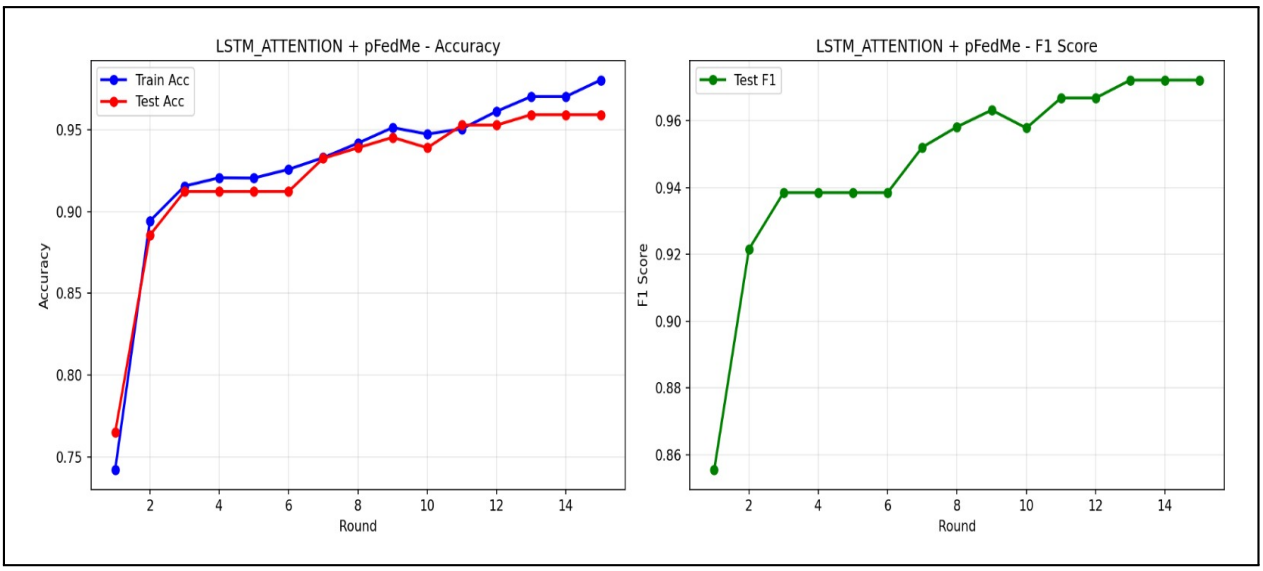


Figure 6.8: Training Curve Comparison for The Best Performing Model.

model predictions, as shown in Figure 6.9. Features associated with the 75th percentile of step counts and axis1 shown significant predictive capability. The majority of step related variables indicates that mobility and body orientation are the main contributors of the models predictions, surpassing cardiac or more detailed acceleration properties.

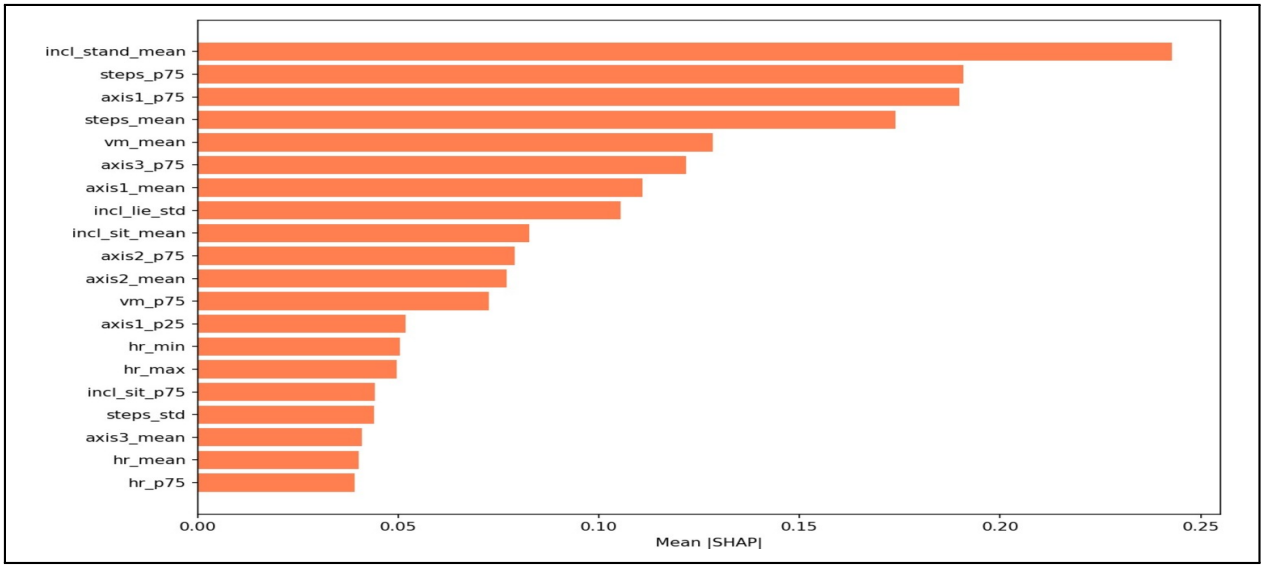


Figure 6.9: SHAP Based Feature Importance Analysis of Best Performing Model.

6.4 Behavioral Pattern Analysis

Heart rate variability (HRV) accelerometry and sleep-related physiological signals were collected over a 24-hour period from healthy participants in the MMASH dataset. The behavioral patterns of each participant were analyzed for the classification of REST vs ACTIVE states. These include daily activity cycles, rest intervals and changes in movement. Individual behavioral characteristics were observed in each participant. For behavioral analysis, only 22 male participants were selected and aged between 20 and 40 years. With BMI of 17.5–33 kg/m² and weight of 60–116 kg. Average weight 75 kg. Their height ranges from 168 to 200 cm.The participants BMI distribution shows that most of the values are in the normal range (18.5–24.9 kg/m²) with an average BMI is 23.1 kg/m², as shown in Table 6.5. Physical activity followed a

Table 6.5: Demographic Characteristics of Participants (N = 22).

Variable	**Min**	**Max**	**Mean ± SD**	**Median**	**Key Finding**
Age (years)	20.0	40.0	26.8 ± 4.5	26.5	Mostly 23.5–28.5
BMI (kg/m²)	17.5	33.0	22.8 ± 3.2	22.5	Peak density at 22.5
Weight (kg)	60	116	74.5 ± 12.5	71.5	Mostly 62–92
Height (cm)	168	200	177.5 ± 6.8	177	Mostly 175–180

clear bimodal circadian rhythm in participants aged 20–40 years. The lowest activity was seen between 2–4 AM (28–35). Two peaks occurred at 8–9 AM (46–57) and 12–2 PM (44–47). Activity gradually decreased after 9 PM. The participants sleep time an average of 5.2 hours. Most perticipant sleep for 5 to 6 hours. Some participant get 4 hours of sleep and some participant get 7 hours. There are very few perticipnt who sleep less than 4 hours or more than 7 hours. No one fell asleep more than 8 hours. Sleep efficiency was different among the participants. The most observed was 75%, which was 3 perticipant. Two participant efficiency was 85%. And 1 each had 80%, 90% and 95% efficiency. And others participant efficiency was between 75% and 95%.

The total sleep time was between 2.8 and 9.6 hours. And the time in bed was between 3.0 and

10.4 hours. Most perticipant slept 4.0 to 5.8 hours and were in bed for 5.4 to 7.6 hours. WASO (waking time in sleep) was between 19 and 118 minutes. And the number of waking up in sleep was 14 to 106 times. Some participant sleep was broken many times and they woke up repeatedly. The participants RMSSD values were between 25 ms and 610 ms. The normal rest and recovery conditions of each participant body were very different, as shown in Table 6.6. The normalized HRV before bedtime was between 0.020 and 0.150. It was between 0.020 and

Table 6.6: Sleep Parameters of Participants.

Variable	**Min**	**Max**	**Mean ± SD**	**Median**	**Key Finding**
Sleep Duration (hours)	2.8	9.6	5.4 ± 1.3	5.2	Mean = 5.2 h
Time in Bed (hours)	3.0	10.4	6.5 ± 1.5	6.2	Majority 5.4–7.6
Sleep Efficiency (%)	75	95	82.5 ± 6.5	85	Most common: 75%
WASO (minutes)	19	118	65.5 ± 28.5	59	High variability
Awakenings	14	106	55.5 ± 25.5	50	High variability
PSQI Score	2.0	9.6	5.6 ± 2.2	5.2	59% poor sleep

0.145 after waking up. For most participants HRV increases a bit after waking up. The cortisol response (CAR) after waking up was between 0.025 and 0.240. NORM values before bedtime ranged from almost zero (1.05 e-7) to 2.40. After waking up it was between 0.05 and 2.80. But not everyone has seen the same changes. Some participants have increased, some participants have decreased. And many participants have not changed at all, as shown in Table 6.7.

Table 6.7: Autonomic Nervous System Measures.

Variable	**Min**	**Max**	**Mean ± SD**	**Median**	**Key Finding**
RMSSD (ms)	25	610	165 ± 135	130	Mostly 95–180
NORM (Before Sleep)	0.020	0.150	0.045 ± 0.035	0.035	Scale-dependent
NORM (Wake Up)	0.020	0.145	0.065 ± 0.040	0.060	Slight increase after wake

The change in melatonin from pre-sleep to wake-up was between -1.3×10^{-8} and 1.2×10^{-8}. It has increased for about half of the participants and decreased for the other half, as shown in 6.8. The participants had a Behavioral Inhibition Score between 18.5 and 26.5. The average score is around 22.5. Most participants had a score between 20.0 and 24.5. The average daily stress score was 31.5 between 10 and 69. The behavioral inhibition score ranged from 18.5 to 26.5 with an average of about 22.5. Everyday stress was much more variable in participants but behavioral inhibition was relatively more stable, as shown in 6.9. The partic-

Table 6.8: Endocrine Response Measures.

Variable	**Min**	**Max**	**Mean ± SD**	**Median**	**Key Finding**
Wake - Before Sleep	-0.025	0.240	0.055 ± 0.065	0.045	81% positive response
Melatonin Change	-1.3×10^{-8}	1.2×10^{-8}	$0.05 \times 10^{-8} \pm 0.6 \times 10^{-8}$	0.01×10^{-8}	Minimal change overall

ipants morningness-eveningness score ranged from 38 to 64, with an average of about 51.5. Some participants like it in the morning and some participants like it in the evening. The Trait

Table 6.9: Psychological and Behavioral Measures.

Variable	**Min**	**Max**	**Mean ± SD**	**Median**	**Key Finding**
Behavioral Inhibition Score	18.5	26.5	22.5 ± 2.5	22.5	Most common: 22.5
Daily Stress Score	10	69	31.5 ± 14.5	31	High variability
Morningness-Eveningness Score	38	64	51.5 ± 6.5	51.5	77% intermediate type
State Anxiety Score	25	54	36.5 ± 7.5	36	Mixed moderate/high levels
Trait Anxiety Score	32	49	41.5 ± 4.5	42	68% moderate anxiety

Anxiety Score ranged from 32.0 to 49.0 with an average of about 41.5. Most participants (68%) had moderate levels of anxiety. And in a very few cases there was less anxiety.

6.5 On-Chain Module Results

In this section, the performance of the proposed framework On-Chain module (Figure 4.5) is evaluated. The analysis focuses on transaction efficiency, security behavior, ZKPs generation with IPFS and smart contract execution reliability based on simulation results. This simulation was evaluated in a local Ethereum Virtual Machine (EVM) environment with Proof-of-Authority consensus and decentralized storage protocols to test this simulation. The average

Table 6.10: Transaction Performance Metrics.

Metric	**Measured Value**	**Description**
Avg. Transaction Time	0.07 sec	Record save time
Throughput	22 TPS	Maximum transactions processed per second
Network Latency	73 ms	Communication delay
Success Rate	100.00%	Successfully mined transactions
Failure Rate	0.00%	Failed transactions

Table 6.11: Smart Contract Performance Metrics.

Metric	**Measured Value**
VM Execution Time	11 ms
Gas per Execution	194,215 GWEI
Block Confirmation Time	0.2 ms
Finality Time	Instant (1 block)
Deterministic Rate	100%

transaction time of 0.07 seconds proves that the proposed methods are much faster, as shown in Table 6.10. The reason for this speed is the EVM environment and the optimized smart contract design. The cost of 194,215 gas per record is medium-level and cost-effective. This makes the system usable for frequent sleep data logging, as shown in Table 6.11. Zero-fault integrity and access control scores indicate that zero-knowledge proofs and EIP-191 signatures together provide strong protection against unauthorized data access and data tampering. However, the

Table 6.12: Security and Privacy Evaluation.

Metric	**Measured Value**	**Assessment**
Data Integrity Score	100.00%	Data is fully correct after retrieval
Access Control Level	100.00%	Signature check works properly
Attack Resistance	Advanced	System is safe from attacks
Encryption Overhead	125 ms	Encryption takes small time cost
Immutability Score	High	Data cannot be changed

AES-256 encryption takes an extra 125 milliseconds. The method provides attack resistance. Especially against replay attacks and man-in-the-middle attacks, because the blockchain ledger is immutable, as shown in Table 6.12. Proposed methods achieves 22 TPS with an average

Table 6.13: Scalability Analysis under Varying Load Conditions.

Load (Transactions)	**Latency (ms)**
10 Transactions	1,200
50 Transactions	1,450
100 Transactions	1,800
200 Transactions	2,500

latency of 1.42 seconds, low cost and strong security using ZKPs combined with AES-256 encryption, as shown in Table 6.13. The proposed method performs well. It processes 22 trans-

Table 6.14: Gas Cost Audit.

Interaction Phase	**Total Gas Units**
Contract Deployment	1,020,131
System Initialization	211,315
Steady-State Logging (19 logs)	3,690,085
Total	**4,921,531**
Average per record	**194,215 gas units**

actions per second and provides a fast response time of 73 ms. The cost is moderate (194,215 gas units) and all transactions are successful (100%). It takes 125 ms extra time for encryption to ensure privacy, as shown in Table 6.15.

Table 6.15: Overall Performance Summary.

Category	**Primary Metric**	**Result**
Efficiency	Throughput	22 TPS
Response	Avg Latency	73 ms
Economics	Operational Gas	194,215
Reliability	Success Rate	100.00%
Privacy	Encryption Overhead	125 ms
Stability	Consensus Finality	Instant

6.6 System Performance Evaluation

The off-chain module execution of the activity recognition pipeline was evaluated during 10 rounds with 3 simultaneous users. The findings indicate that the system sustains an average CPU use of 17.27%, with transient peaks of 70.20% during initialization, as shown in Figure 6.10. This verifies that off-chain FL/XAI module processing is efficient and appropriate for practical uses. The sleep anomaly inference off-chain module maintains a structured GPU usage of 68.45%, indicating a well partitioned pipeline design, as shown in Figure 6.11.

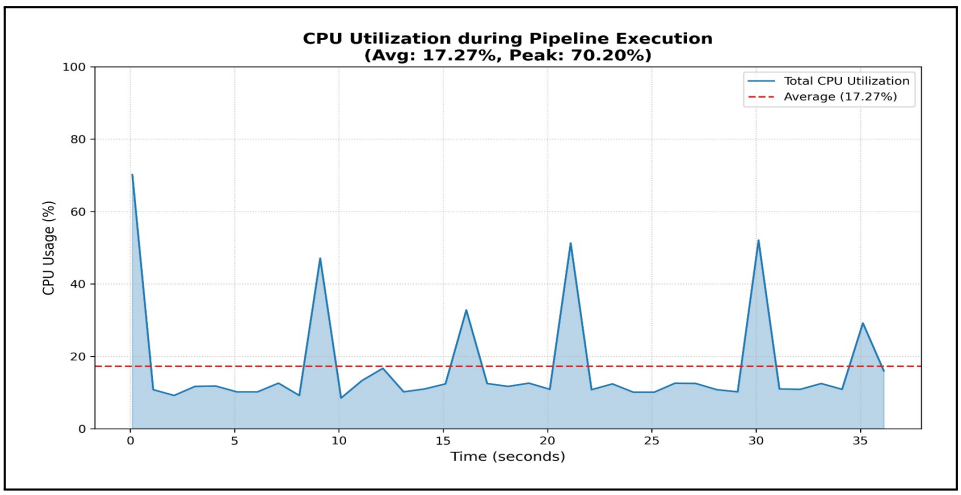


Figure 6.10: Off-Chain CPU Utilization Under Concurrent Workload.

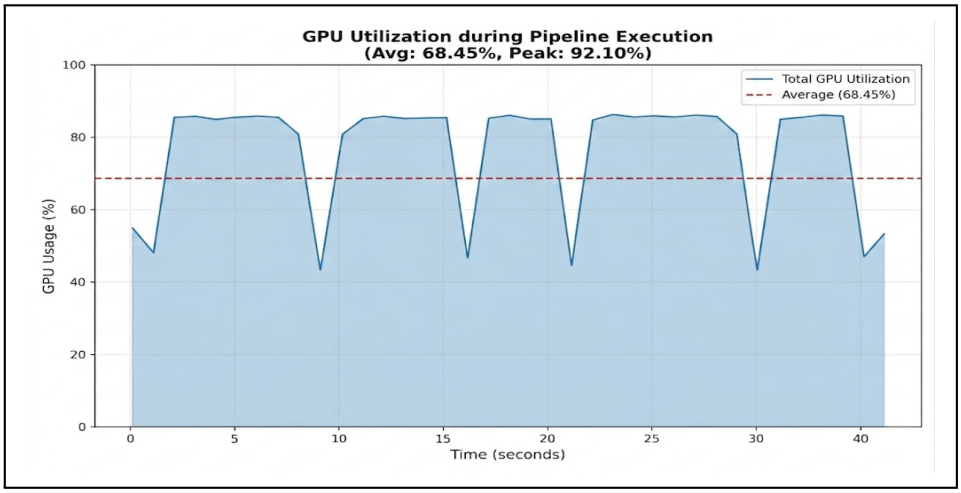


Figure 6.11: GPU Utilization During Off-Chain Anomaly Detection Pipeline Execution.

Chapter 7
Conclusion

Chapter 7: Conclusion

7.1 Overview

In this study, a decentralized framework is proposed combining Deep Learning (DL), Federated Learning (FL), Explainable AI (XAI), Blockchain and Zero-Knowledge Proofs (ZKPs). This framework will ensure safe and privacy-preserving sleep analysis in healthcare sector. Using an autoencoder for anomaly detection on the Sleep-EDF dataset. Good performance was achieved by evaluating activity states with four deep learning models and eight federated learning algorithms using MMASH and PAMAP2 datasets. Also the off-chain module achieves an average CPU utilization of 17.27%, with a high of 70.20% in activity monitoring inference and a GPU usage of 68.45% in anomaly inference. Data security, transparency and trust were ensured through the use of Blockchain, ZKPs and IPFS.

7.2 Limitations

The proposed framework has several practical limitations that should be considered when interpreting the results. These limitations mainly arise from environment setup difficulties, resource constraints and data availability. Overall limitations are as follows:

1. Due to limited computational resources, it was not possible to run large-scale experiments on the dataset.
2. The environment setup for the proposed framework is complex and time-consuming, which limits the ability to conduct extensive testing and validation.
3. The model has not yet been fully validated in large-scale real-world deployment environments, which may affect its generalization to real applications.

7.3 Future Work

In the future, this work will focus on improving data quality, model scalability, and real-world use. More data will be collected from different real-life environments so that sleep patterns

can be understood more clearly. This will make the model more reliable and useful in practice. And future work will also focus on improving system efficiency and making the model easier to understand. Advanced Explainable AI methods will be used to better explain model decisions. A lightweight model will also be developed so that it can run on small devices like wearable devices. Overall future work directions are as follows:

1. Improve the environment setup process and create more complete and diverse datasets by collecting data from different real-life conditions.
2. Enable large-scale real-time data processing by using multiple devices and continuous data collection methods to handle streaming sleep data.
3. Improve the efficiency of the Federated Learning (FL) system so that training can be done faster and more smoothly across many devices.
4. Apply advanced Explainable AI (XAI) techniques to better understand how the model makes decisions and to make the results more transparent.
5. Develop a lightweight model for sleep anomaly detection so that it can run easily on devices with limited resources such as wearable and mobile devices.

References

[1] T. Kairi, S. Dey, R. Jahan, S. Fuad, "Stress and sleep quality among medical students in Bangladesh: a cross-sectional study," J Yeungnam Med Sci., vol. 42, p. 42, 2025, doi:10.12701/jyms.2025.42.42.

[2] S. Mousum, Y. Yang, A. Anjum, M. Salwa, R. Ishra, and A. Haque, "A Theory-Driven Analysis of Adolescent Insomnia in Bangladesh: Testing the 3P Model with Structural Equation Modeling Background," Nov. 2025.

[3] J. Datta, M. Alam, T. Zahangir, S. Afrin, A. A. Sarkar, M. Haque, A. Fariduzzaman, and B. Dutta, "Prevalence and Associated Factors of Insomnia in Adult Psychiatric Patients: A Hospital-Based Study," Sleep Medicine Research, vol. 16, pp. 121-128, 2025, doi:10.17241/smr.2025.02824.

[4] P. Das, M. Arif, M. E. Hasan, et al., "Prevalence and Factors Associated with Insomnia Among Chronic Disease Patients in Bangladesh: A Machine Learning Study," Nature and Science of Sleep, vol. 17, pp. 2541-2567, Oct. 2025, doi:10.2147/NSS.S547335.

[5] F. Rahaman, S. Kamal, R. U. Islam, et al., "The impact of sleep quality on body weight among young adults: a cross-sectional study," BMC Research Notes, vol. 18, p. 486, 2025, doi:10.1186/s13104-025-07544-1.

[6] M. Nurunnabi, M. K. Khan, F. R. Kaiser, M. G. Abbas, T. T. Tabassum, T. Farha, F. Akter, and M. A. Tarafdar, "Exploring Sleep Quality in Bangladeshi University Students during the COVID-19 Pandemic," medRxiv, 2025, doi:10.1101/2025.04.06.25325308.

[7] Yang Jiao, Claudette Butoyi, Qian Zhang, Swailla Amina Araújo Intchasso Adotey, Mengxue Chen, Wen Shen, Dong Wang, Guoyue Yuan and Jue Jia, "Sleep disorders impact hormonal regulation: unravelling the relationship among sleep disorders, hormones and metabolic diseases," Diabetology and Metabolic Syndrome, vol. 17, 2025, doi:10.1186/s13098-025-01871-w.

[8] Nakamoto, Satoshi. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. Cryptography Mailing list at https://metzdowd.com.

[9] S. Haber and W. Stornetta, "How to Time-Stamp a Digital Document," Journal of Cryptology, vol. 3, 1999, doi:10.1007/BF00196791.

[10] Pandey, Shraiyash and De, Abhik Kumar and Choudhary, Shrishti and Asim, Mohammad, "A Decentralized Blockchain-Based Architecture for Healthcare Industry," in 2023 International Conference

on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI), vol. 1, pp. 1-5, 2023, doi:10.1109/ICAIIHI57871.2023.10489491.

[11] Soundarrajan, Srinidhi and Shedge, Prachi and Mahajan, Samiksha and Yenkikar, Anuradha and Sable, Nilesh, "SomnoGuide: AI Based Sleep Disorder Diagnosis," in 2025 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), pp. 1-6, 2025, doi:10.1109/ICBDS67396.2025.11379807.

[12] L. Rachakonda, A. Bapatla, S. Mohanty, and E. Kougianos, "SaYoPillow: A Blockchain-Enabled, Privacy-Assured Framework for Stress Detection, Prediction and Control Considering Sleeping Habits in the IoMT," arXiv preprint, 2020, doi:10.48550/arXiv.2007.07377.

[13] Sana, Tamanna Zubairi and Abdulla, Shahab and Nag, Anindya and Das, Ayontika and Hassan, Md. Mehedi and Fiza, Zoya Zubairi and Karim, Asif and Kabir, Sheikh Ridwan Raihan, "Advancing Federated Learning: A Systematic Literature Review of Methods, Challenges, and Applications," IEEE Access, vol. 13, pp. 153817-153844, 2025, doi:10.1109/ACCESS.2025.3605165.

[14] Sajid Nazir and Mohammad Kaleem, "Federated Learning for Medical Image Analysis with Deep Neural Networks," Diagnostics, vol. 13, p. 1532, 2023, doi:10.3390/diagnostics13091532.

[15] Lang Wu, Weijian Ruan, Jinhui Hu and Yaobin He, "A Survey on Blockchain-Based Federated Learning," Future Internet, vol. 15, p. 400, 2023, doi:10.3390/fi15120400.

[16] Luis M. Lopez-Ramos, Florian Leiser, Aditya Rastogi, Steven Hicks, Inga Strumke , Vince I. Madai, Tobias Budig, Ali Sunyaev and Adam Hilber "Interplay between Federated Learning and Explainable Artificial Intelligence: a Scoping Review," 2024, doi:10.48550/arXiv.2411.05874.

[17] Rosenbacke, Rikard and Melhus, Åsa and McKee, Martin and Stuckler, David, "How Explainable Artificial Intelligence Can Increase or Decrease Clinicians' Trust in AI Applications in Health Care: Systematic Review," JMIR AI, vol. 3, p. e53207, 2024, doi:10.2196/53207.

[18] Sun, Xiaoqiang and Yu, F. Richard and Zhang, Peng and Sun, Zhiwei and Xie, Weixin and Peng, Xiang, "A Survey on Zero-Knowledge Proof in Blockchain," IEEE Network, vol. 35, no. 4, pp. 198-205, 2021, doi:10.1109/MNET.011.2000473.

[19] H. Li, X. Zhao, H. Liu, Z. Wang, Y. Cai, C. Yang, and F. Cong, "Distributed data-privacy preserving federated learning method for sleep stage classification," Biomedical Signal Processing and Control, vol. 109, p. 108032, 2025, doi:10.1016/j.bspc.2025.108032.

[20] Z. Wang, H. Liu, Y. Cai, H. Li, C. Yang, X. Zhang, and F. Cong, "Point out the mistakes: An HMM-based anomaly detection algorithm for sleep stage classification," Biomedical Signal Processing and Control, vol. 99, p. 106805, 2025, doi:10.1016/j.bspc.2024.106805.

[21] S. Tahir and A. Zaheer, "A Distributed Model for IoT Anomaly Detection Using Federated Learning," in *Handbook of Research on AI-Based Technologies and Applications in the Era of Industry 4.0*, pp. 75–91, 2023, doi:10.4018/978-1-6684-7625-3.ch003.

[22] N. Krishappa, G. G. Shivappa, S. Zachariah, P. Thanushree, K. I. Pattan, A. Paria, S. Hiremath, and R. Vaithiyanathan, "A Blockchain-Based Framework With Zero-Knowledge Proof Incorporated for Safeguarded Sharing of Genomic Data Through Health Record Systems," Blockchain Healthc Today, vol. 8, no. 3, Nov. 2025, doi:10.30953/bhty.v8.419.

[23] E. Lansiaux, "Zero-Knowledge Federated Learning with Lattice-Based Hybrid Encryption for Quantum-Resilient Medical AI," arXiv preprint, 2026, doi:10.48550/arXiv.2603.03398.

[24] S. Sharma, G. Petrovic, and S. Kaushik, "zkFL-Health: Blockchain-Enabled Zero-Knowledge Federated Learning for Medical AI Privacy," arXiv preprint, 2025, doi:10.48550/arXiv.2512.21048.

[25] F. Albalwy, "Zero-Knowledge-Based Policy Enforcement for Privacy-Preserving Cross-Institutional Health Data Sharing on Blockchain," Systems, vol. 14, p. 385, 2026, doi:10.3390/systems14040385.

[26] A. Raghav, A. M. Tripathi, N. A. Wani, et al., "Secure, scalable, and interoperable healthcare data exchange using layer-2 ZK-rollups, smart contracts, and IPFS," Scientific Reports, vol. 16, p. 6132, 2026, doi:10.1038/s41598-026-35289-9.

[27] Antonio Borges, Guilherme and Cesar Santos dos Anjos, Julio and Sá Silva, Jorge, "Federated Learning for Sleep Detection Problems," in 2024 IEEE International Conference on Smart Computing (SMARTCOMP), pp. 368-373, 2024, doi:10.1109/SMARTCOMP61445.2024.00083.

[28] A. Ali, H. Jianjun, A. Jabbar and M. Kashif Jabbar, "Multi-Sensor Wearable-Based Sleep Stage Classification Using Federated Learning for Enhanced Privacy," in IEEE Access, vol. 13, pp. 157842-157862, 2025, doi: 10.1109/ACCESS.2025.3607720

[29] S. Moon, T. S. Kim, J. Ryu and W. H. Lee, "Federated Learning for Sleep Stage Classification on Edge Devices via a Model-Agnostic Meta-Learning-Based Pre-Trained Model," 2023 IEEE 13th International Conference on Consumer Electronics - Berlin (ICCE-Berlin), Berlin, Germany, 2023, pp. 188-192, doi: 10.1109/ICCE-Berlin58801.2023.10375664.

[30] Dubey, P., Dubey, P., and Bokoro, P. N. (2025). Federated learning for privacy-enhanced mental health prediction with multimodal data integration. Computer Methods in Biomechanics and Biomedical Engineering: Imaging and Visualization, 13(1). https://doi.org/10.1080/21681163.2025.2509672

[31] A. Anido-Alonso and D. Alvarez-Estevez, "Decentralized Data-Privacy Preserving Deep-Learning Approaches for Enhancing Inter-Database Generalization in Automatic Sleep Staging," IEEE Journal of Biomedical and Health Informatics, vol. 27, no. 11, pp. 5610-5621, Nov. 2023, doi:10.1109/JBHI.2023.3310869.

[32] G. G, C. S. Devi, A. Chandravadhana, S. Vijayalakshmi, I. M. V and S. Murugan, "Deep Learning for Sleep Pattern Recognition in Wearables for Detecting Insomnia," 2025 3rd International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India, 2025, pp. 1369-1374, doi: 10.1109/ICSCDS65426.2025.11166889.

[33] S. Satoiya, S. Jain and B. Roy, "EEG-Based Scalogram Imaging and Deep Learning for Insomnia Classification," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-6, doi: 10.1109/ICCCNT61001.2024.10725371.

[34] K. Feng, H. Qin, S. Wu, W. Pan and G. Liu, "A Sleep Apnea Detection Method Based on Unsupervised Feature Learning and Single-Lead Electrocardiogram," in IEEE Transactions on Instrumentation and Measurement, vol. 70, pp. 1-12, 2021, Art no. 4000912, doi: 10.1109/TIM.2020.3017246.

[35] A. Gasmi, V. Augusto, J. Faucheu, C. Morin and X. Serpaggi, "Anomaly Detection in Sleep Habits Using Deep Learning," 2023 IEEE 19th International Conference on Automation Science and Engineering (CASE), Auckland, New Zealand, 2023, pp. 1-7, doi: 10.1109/CASE56687.2023.10260617.

[36] N. Han, S. Gao, J. Li, X. Zhang and J. Guo, "Anomaly Detection in Health Data Based on Deep Learning," 2018 International Conference on Network Infrastructure and Digital Content (IC-NIDC), Guiyang, China, 2018, pp. 188-192, doi: 10.1109/ICNIDC.2018.8525737.

[37] R. Alabdan, H. A. Mengash, M. Maray, F. Alotaibi, S. Abdelbagi and A. Mahmud, "Modified Bald Eagle Search Algorithm With Deep Learning-Driven Sleep Quality Prediction for Healthcare Monitoring Systems," in IEEE Access, vol. 11, pp. 135385-135393, 2023, doi: 10.1109/ACCESS.2023.3337647.

[38] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 2017, pp. 557-564, doi: 10.1109/BigDataCongress.2017.85.

[39] Yli-Huumo, Jesse and Ko, Deokyoon and Choi, Sujin and Park, Sooyong and Smolander, Kari. (2016). Where Is Current Research on Blockchain Technology?—A Systematic Review. PLOS ONE. 11. 10.1371/journal.pone.0163477.

[40] Gautami Tripathi, Mohd Abdul Ahad, Gabriella Casalino,, "A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges," Decision Analytics Journal, vol. 9, p. 100344, 2023, doi:10.1016/j.dajour.2023.100344.

[41] Aditya Pratap Singh, "Blockchain Technology: Core Mechanisms, Evolution, and Future Implementation Challenges," arXiv preprint, 2025, doi:10.48550/arXiv.2505.08772.

[42] William Metcalfe, "Ethereum, Smart Contracts, DApps," in Blockchain and Distributed Ledger Technology Use Cases, 2020, DOI: 10.1007/978-981-15-3376-1_5.

[43] Seyednima Khezr1, Md Moniruzzaman1, Abdulsalam Yassine and Rachid Benlamri, "Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research," Applied Sciences, vol. 9, no. 9, p. 1736, 2019, doi:10.3390/app9091736.

[44] I. Purwono, K. Nisa, S. Wibisono, and B. Dewa, "Private Blockchain in the Field of Health Services," Journal of Advanced Health Informatics Research, vol. 1, pp. 10-15, 2023, doi:10.59247/jahir.v1i1.14.

[45] Ghosh, P.K.; Chakraborty, A.; Hasan, M.; Rashid, K.; Siddique, A.H. Blockchain Application in Healthcare Systems: A Review. Systems 2023, 11, 38. https://doi.org/10.3390/systems11010038

[46] Fonsêca, A.L.A.; Barbalho, I.M.P.; Fernandes, F.; Arrais Júnior, E.; Nagem, D.A.P.; Cardoso, P.H.; Veras, N.V.R.; Farias, F.L.d.O.; Lindquist, A.R.; dos Santos, J.P.Q.; et al. Blockchain in Health Information Systems: A Systematic Review. Int. J. Environ. Res. Public Health 2024, 21, 1512. https://doi.org/10.3390/ijerph21111512

[47] X. Sun, F. R. Yu, P. Zhang, Z. Sun, W. Xie and X. Peng, "A Survey on Zero-Knowledge Proof in Blockchain," in IEEE Network, vol. 35, no. 4, pp. 198-205, July/August 2021, doi: 10.1109/MNET.011.2000473.

[48] Goldwasser, S., Micali, S., & Rackoff, C. (1985). The knowledge complexity of interactive proof-systems. Symposium on the Theory of Computing.

[49] B. K. Mohanta, S. S. Panda and D. Jena, "An Overview of Smart Contract and Use Cases in Blockchain Technology," 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Bengaluru, India, 2018, pp. 1-4, doi: 10.1109/ICCCNT.2018.8494045.

[50] J. L. Covarrubias and I. L. Covarrubias, "Different types of government and governance in the blockchain," Journal of Governance and Regulation, vol. 10, pp. 8-21, 2021, doi:10.22495/jgrv10i1art1.

[51] G. Wu, H. Wang, Z. Yang, D. He, and S. Chan, "Electronic Health Records Sharing Based on Consortium Blockchain," Journal of Medical Systems, vol. 48, 2024, doi:10.1007/s10916-024-02120-9.

[52] A. Tawfik, A. Al-Ahwal, A. Eldien, and H. Zayed, "ACHealthChain blockchain framework for access control and privacy preservation in healthcare," Scientific Reports, vol. 15, 2025, doi:10.1038/s41598-025-00757-1.

[53] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. Agüera y Arcas, "Communication-Efficient Learning of Deep Networks from Decentralized Data," arXiv preprint, 2023, doi:10.48550/arXiv.1602.05629.

[54] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated Learning: Challenges, Methods, and Future Directions," IEEE Signal Processing Magazine, vol. 37, no. 3, pp. 50-60, May 2020, doi:10.1109/MSP.2020.2975749.

[55] T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith, "Federated Optimization in Heterogeneous Networks," arXiv preprint, 2020, doi:10.48550/arXiv.1812.06127.

[56] S. P. Karimireddy, S. Kale, M. Mohri, S. J. Reddi, S. U. Stich, and A. T. Suresh, "SCAFFOLD: Stochastic Controlled Averaging for Federated Learning," arXiv preprint, 2021, doi:10.48550/arXiv.1910.06378.

[57] S. Reddi, Z. Charles, M. Zaheer, Z. Garrett, K. Rush, J. Konečný, S. Kumar, and H. B. McMahan, "Adaptive Federated Optimization," arXiv preprint, 2021, doi:10.48550/arXiv.2003.00295.

[58] J. Wang, Q. Liu, H. Liang, G. Joshi, and H. V. Poor, "Tackling the Objective Inconsistency Problem in Heterogeneous Federated Optimization," arXiv preprint, 2020, doi:10.48550/arXiv.2007.07481.

[59] D. A. E. Acar, Y. Zhao, R. M. Navarro, M. Mattina, P. N. Whatmough, and V. Saligrama, "Federated Learning Based on Dynamic Regularization," arXiv preprint, 2021, doi:10.48550/arXiv.2111.04263.

[60] X. Li, M. Jiang, X. Zhang, M. Kamp, and Q. Dou, "FedBN: Federated Learning on Non-IID Features via Local Batch Normalization," arXiv preprint, 2021, doi:10.48550/arXiv.2102.07623.

[61] A. Fallah, A. Mokhtari, and A. Ozdaglar, "Personalized Federated Learning: A Meta-Learning Approach," arXiv preprint, 2020, doi:10.48550/arXiv.2002.07948.

[62] Q. Li, B. He, and D. Song, "Model-Contrastive Federated Learning," arXiv preprint, 2021, doi:10.48550/arXiv.2103.16257.

[63] Z. Sadeghi, R. Alizadehsani, M. A. Cifci, S. Kausar, R. Rehman, P. Mahanta, P. K. Bora, A. Almasri, R. S. Alkhawaldeh, S. Hussain, B. Alatas, A. Shoeibi, H. Moosaei, M. Hladík, S. Nahavandi, and P. M. Pardalos, "A review of Explainable Artificial Intelligence in healthcare," Computers and Electrical Engineering, vol. 118, p. 109370, 2024, doi:10.1016/j.compeleceng.2024.109370.

[64] Hildt, E. What Is the Role of Explainability in Medical Artificial Intelligence? A Case-Based Approach. Bioengineering 2025, 12, 375. https://doi.org/10.3390/bioengineering12040375

[65] Chaddad A, Peng J, Xu J, Bouridane A. Survey of Explainable AI Techniques in Healthcare. Sensors. 2023; 23(2):634. https://doi.org/10.3390/s23020634

[66] Linardatos P, Papastefanopoulos V, Kotsiantis S. Explainable AI: A Review of Machine Learning Interpretability Methods. Entropy. 2021; 23(1):18. https://doi.org/10.3390/e23010018

[67] J. M. Steinkamp, W. Bala, A. Sharma, and J. J. Kantrowitz, "Task definition, annotated dataset, and supervised natural language processing models for symptom extraction from unstructured clinical notes," Journal of Biomedical Informatics, vol. 102, p. 103354, 2020, doi:10.1016/j.jbi.2019.103354.

[68] S. Lundberg and S.-I. Lee, "A Unified Approach to Interpreting Model Predictions," arXiv preprint, 2017, doi:10.48550/arXiv.1705.07874.

[69] B. Kemp, A. H. Zwinderman, B. Tuk, H. A. C. Kamphuisen, and J. J. L. Oberye, "Analysis of a sleep-dependent neuronal feedback loop: the slow-wave microcontinuity of the EEG," IEEE Transactions on Biomedical Engineering, vol. 47, no. 9, pp. 1185-1194, Sept. 2000, doi:10.1109/10.867928.

[70] A. Rossi, E. Da Pozzo, D. Menicagli, C. Tremolanti, C. Priami, A. Sirbu, D. Clifton, C. Martini, and D. Morelli, "Multilevel Monitoring of Activity and Sleep in Healthy People," PhysioNet, Version 1.0.0, June 2020, doi:10.13026/cerq-fc86.

[71] Reiss, A. (2012). PAMAP2 Physical Activity Monitoring [Dataset]. UCI Machine Learning Repository. https://doi.org/10.24432/C5NW2H.

[72] M.-C. Popescu, V. Balas, L. Perescu-Popescu, and N. Mastorakis, "Multilayer perceptron and neural networks," WSEAS Transactions on Circuits and Systems, vol. 8, July 2009.

[73] G. Shen, Q. Tan, H. Zhang, P. Zeng, and J. Xu, "Deep learning with gated recurrent unit networks for financial sequence predictions," Procedia Computer Science, vol. 131, pp. 895-903, 2018, doi:10.1016/j.procs.2018.04.298.

[74] S. Hochreiter and J. Schmidhuber, "Long Short-Term Memory," Neural Computation, vol. 9, no. 8, pp. 1735-1780, Nov. 1997, doi:10.1162/neco.1997.9.8.1735.

[75] Q. Kang, E. J. Chen, Z.-C. Li, H.-B. Luo, and Y. Liu, "Attention-based LSTM predictive model for the attitude and position of shield machine in tunneling," Underground Space, vol. 13, pp. 335-350, 2023, doi:10.1016/j.undsp.2023.05.006.

[76] J. Wang, Q. Liu, H. Liang, G. Joshi and H. V. Poor, "A Novel Framework for the Analysis and Design of Heterogeneous Federated Learning," in IEEE Transactions on Signal Processing, vol. 69, pp. 5234-5249, 2021, doi: 10.1109/TSP.2021.3106104.

[77] M. G. Arivazhagan, V. Aggarwal, A. Singh, and S. Choudhary, "Federated Learning with Personalization Layers," arXiv preprint arXiv:1912.00818, 2019, doi:10.48550/arXiv.1912.00818.

[78] C. T. Dinh, N. H. Tran, and T. D. Nguyen, "Personalized Federated Learning with Moreau Envelopes," arXiv preprint arXiv:2006.08848, 2022.

[79] M. Nurhandhi and A. Suhendar, "Improving Firebase BaaS Service Security in Counseling Chat Applications: AES-256 and CBC Approach for End-to-End Encryption," Jurnal Informatika dan Sains, vol. 6, no. 2, pp. 153-160, Dec. 2023, doi:10.31326/jisa.v6i2.1783.

[80] M. H. Swende (Holiman) and N. Johnson, "ERC-191: Signed Data Standard," Ethereum Improvement Proposals, EIP-191, Jan. 2016. Available: https://eips.ethereum.org/EIPS/eip-191.