International Academic Institute for Science and Technology

International Academic Journal of Science and Engineering
Vol. 13, No. 3, 2026, pp. 350-363.

ISSN 2454-3896

International Academic Journal of Science and Engineering

www.iaiest.com

Lightweight Blockchain Enabled Privacy-Preserving IoT Framework for Secure Parkinson's Disease Fall Detection and Healthcare Monitoring

M. Rakhee [a*], Dr.M. Sudheep Elayidom [b], Dr. Baiju Karun [c]

[a] Research Scholar, Division of Computer Science and Engineering, School of Engineering, Cochin University of Science and Technology, Kochi, Kerala, India. E-mail: rakheebaiju@gmail.com, Orcid: https://orcid.org/0009-0006-1556-6658*

[b] Professor, Division of Computer Science and Engineering, School of Engineering, Cochin University of Science and Technology, Kochi, Kerala, India. E-mail: sudheep@cusat.ac.in, Orcid: https://orcid.org/0000-0003-3836-7425

[c] Department of Engineering, College of Engineering and Technology, University of Technology and Applied Sciences, Muscat, Oman. E-mail: baijukarun@gmail.com, Orcid: https://orcid.org/0000-0002-1454-9905

Abstract

The increased number of PD patients has increased the adoption of the Internet of Things (IoT)-based wearable devices for remote monitoring and automatic fall detection, which helps to notify caregivers and clinicians immediately. Unfortunately, the continuous transmission of patients' physiological and movement data through wireless sensor networks increases their vulnerability to risks of unauthorized access, poor authentication, and privacy loss. Most importantly, current automatic fall detection systems offer low levels of data verification and protection. To overcome this issue, the proposed study introduces the Cross-Layer Lightweight Starvation Blockchain Security scheme with the Provable Master Seeding Authentication Policy (LWSBS-PMSAP) for preserving privacy in the PD monitoring system. The data collected from the IoT wearable devices is first encrypted with the Advanced Shuffle Standard Starvation Encryption Cryptography (ASS-SEC) and packaged in the form of blockchain blocks, which are then stored on the encrypted servers; a controller node performs the verification and validation of the policy to prevent any unauthorized interference, while a zero-knowledge proof-based Provable Master Seeding Authentication (PMSA) protocol verifies devices and users. The framework was tested on the PD monitoring dataset of 100 patients having 1,500 sensor samples. LWSBS-PMSAP obtained a 98.7% throughput rate, 180 ms latency, 99.2% security rate, and 96.8% privacy preservation, and performed better than Ethereum-based, Hyperledger-based, and general lightweight blockchain frameworks. In the context of fall detection, the proposed framework attained 98.7% accuracy, 97.4% precision, 99.0% recall, and 98.2% F1-Score, performing better than CNN-based, LSTM-based, and ensemble-DNN-based models. The ablation study also proved that the contribution of each component in terms of security and privacy gain is measurable. Further, the statistical validation (mean, standard deviation, 95% confidence interval) revealed that there is low variation in performance of the proposed framework among the multiple trials. It can be concluded that LWSBS-PMSAP provides a computationally lightweight, secure, and privacy-preserving solution for real-time fall detection and remote monitoring of Parkinson's Disease, with clear potential for extension to broader IoT-based healthcare applications.

Keywords: Parkinson's Disease Monitoring, Internet of Things (IoT) Healthcare, Blockchain Security, Fall Detection, Zero-Knowledge Proof, Lightweight Cryptography, Remote Patient Monitoring.

DOI: 10.71086/IAJSE/V13I3/IAJSE13120
Received: 16 June, 2026/Revised: 20 July 2026/Accepted: 24 August 2026/Published: 15 September 2026

Introduction

The use of new innovations helps improve the management and treatment of chronic diseases like Parkinson's. One of the new strategies in technology is remote monitoring of patients through the use of wearables and the Internet of Things (IoT). Real-time monitoring of patients' movements, tremors, and general health through IoT-enabled and sensor wearables helps remote healthcare professionals assess and provide necessary medical attention. Healthcare professionals' attention is always available even when the patients and professionals are not in the same physical location. Remote monitoring helps manage the patient's health more efficiently and conveniently. It also helps to securely monitor the patients' chronic conditions. The possible misuse of sensitive data in the health and medical field will always remain the main concern. The need to ensure strong mitigation measures is clear (Masood et al., 2024). With the rapid growth of health monitoring technology, the use of advanced technology in real-time patient monitoring will greatly improve the quality of life of patients living with Parkinson's disease (Mazumdar et al., 2025).

To safeguard a patient with Parkinson's disease, it is important to choose a system that deals with the issue of real-time monitoring of falls. The system observes the activity of a patient, records falls, and transmits fall alerts to the nurses' using accelerometers, gyroscopes, and sensors. When a fall is detected, alerts will be sent to either the medical staff or home care giver or family members so that can intervene before the condition of a patient deteriorates. The IoT-enabled and wearable technology, the Remote Patient Monitoring Fall Integrated (Mesh), is also more efficient and responsive (Bhatia, 2024; Khan & Jilani, 2024).

Healthcare's traditional data verification and authentication methods are weak. Furthermore, encryption is often insufficient and unevenly applied, leaving patient records vulnerable. The interconnected and digitized medical data, coupled with IoT surveillance technologies, poses a risk of exposing medical data to cyber-attacks. Cybersecurity threats become a reality when sensitive, unprotected, and interconnected data is available (Murala et al., 2023; Moore et al., 2024).

To address these challenges, sophisticated new technologies, including blockchain, have been brought to the market. The challenges have led to the introduction of advanced new technologies such as blockchain to handle them. These innovations maintain data integrity and prevent any possible deliberate manipulation through decentralization and transparency, as well as immutable recording. Health providers can incorporate privacy-compliant, blockchain- anchored technologies to safely share sensitive health information, defend against unauthorized access, and comply with privacy law access and flow regulations. Policies to improve the monitoring of potential breaches consolidate user access control, promote remote user authentication, and provide trust in remote patient monitoring solutions (Sigcha et al., 2020; Delahoz & Labrador, 2014).

While fall detection forms the main objective of PD monitoring systems, the constant flow of sensor-generated health data poses serious security and privacy concerns. Wearable devices regularly exchange movement patterns, physiological data, patient details, and emergency alerts on a wireless network, cloud system, and health care system. Conventional encryption mechanisms can offer a high level of security but may introduce unnecessary computational burden, communication delay, and energy requirements that might be undesirable for the continuous use of resource-constrained wearable devices in real-time environments. Thus, the Advanced Shuffle Standard Starvation Encryption Cryptography (ASS-SEC) mechanism is proposed to provide a lightweight encryption layer in order to secure sensitive healthcare data prior to its storage and transmission in the blockchain. The overall goal of ASS-SEC is not to directly improve the performance of fall detection algorithms, but to guarantee the confidentiality, security, and privacy of the communication and data when deploying these algorithms for real-time fall monitoring applications in the context of Parkinson's Disease.

This document describes developing privacy preservation and security for the fall detection system. These patient data-collection wearable sensors secure data and process it into new blocks with a consensus policy that formalizes a construct for secure data management leveraging advanced consensus technologies. To ensure that data is confidential, Advanced Shuffle Standard Starvation Encryption Cryptography (ASS-SEC) is used, and the data is encrypted before being stored on the blockchain. It uses a unique Hash Code Starvation Key to secure access and protect the user's credentials for safe and authorized access to the data. For added security, the system will implement the Master Seeding Authentication Policy (MSAP) using zero-knowledge proof authentication to ensure the data is safe. The controller node will ensure authorized people's access by preventing third-party unauthorized access through zero-knowledge proof techniques by adding more security and verification and validation processes to the system.

The controller node provides secure access control by ensuring authentication of authorized users and the security of data against third parties using zero-knowledge proof–based verification systems. This not only helps to safeguard the system's security but also ensures the privacy and integrity of patient information and transactions.

The proposed work can be categorized from the research point of view as a privacy-preserving framework for a healthcare IoT system for Parkinson's disease fall detection. The proposed approach is distinguishable from existing fall detection systems, which tend to prioritize prediction accuracy, by highlighting secure data acquisition, authentication, integrity protections using blockchain, and privacy-preserving healthcare information exchange. Thus, this work is primarily focused on the integration of healthcare monitoring and cybersecurity mechanisms in a single framework appropriate for real-world IoT-based healthcare systems.

The remainder of this paper is organized as follows. Section II reviews related work on privacy-preserving healthcare monitoring, federated learning, and blockchain-based data protection, and summarizes their limitations. Section III identifies the research gap and motivates the proposed approach. Section IV presents the materials and methods, including the LWSBS architecture, ASS-SEC encryption, blockchain-based privacy preservation, the PMSA authentication protocol, and the fall-detection design, together with the associated algorithm and mathematical formulation. Section V reports the experimental setup, dataset, results, and discussion, including performance comparison, ablation analysis, and statistical validation. Section VI concludes the paper and outlines directions for future work.

Related Work

Proposed an approach of federated learning in the detection of Parkinson's disease while maintaining patient data privacy by blockchain technology. The approach considered federated learning that allows model training locally on decentralized data, along with blockchain, which securely stores and manages the patient data. The main challenge is the guarantee of privacy without compromising the accuracy and robustness of the model in the health industry (Alzakari et al., 2024). Discussed the convergence of health prediction and intrusion detection within the Internet of Healthcare Things (IoHT) using Matrix-Valued Neural Coordinated Federated Intelligence (MVNCFI). It protects against possible intrusions while optimizing the prediction of healthcare data. One of the most important challenges in this work is managing the computational complexity of matrix-valued neural networks in a secure IoHT environment efficiently (Jayaram & Prabakaran, 2021).

An onboard disease prediction and rehabilitation monitoring system integrated with edge-cloud tech. The study highlights the system's focus on privacy preservation in healthcare systems. The secure handling of medical data through cloud and edge computing infrastructure is of utmost importance. One of the most important challenges systems tend to face is the real-time prediction of a disease, while the system's privacy concerns surrounding patient data storage and processing have been overlooked (Rehman et al., 2022). The study presents a blockchain- and federated learning-based secure healthcare 5.0 system that is able to protect privacy in healthcare data. A goal of this system is to enhance the security and trustworthiness of medical data transactions. The problem of unauthorized access to sensitive healthcare data is avoided without sacrificing the operational flow of the healthcare system (Dipro et al., 2022; Altalbe & Javed, 2023).

Research applies federated learning methods to focus on decentralized data training while keeping patient data private. The issue remains achieving higher accuracy in healthcare diagnostics relative to privacy, particularly when healthcare data is shared and models are trained collaboratively (Mazilu et al., 2016). Using wrist-mounted inertial sensors to pinpoint freezing episodes in patients with Parkinson's disease. For this work, I focus on detecting episodes using sensor data. The goal is to support real-time detection of freezing episodes using wearable aids, while also accounting for sensor noise and varied patient conditions that complicate detection, which is challenging (Elhoseny et al., 2021) (Han et al., 2020). Proposed an automatic fall detection system based on an impulse radio ultra-wideband (IR-UWB) sensing system and a convolutional neural network (CNN) fall classifier. The CNN is able to learn the spatial and temporal motion features from the sensor signals for enhancing the accuracy of fall detection (Li et al., 2021).

Proposed a federated learning model where the model parameters are trained locally on distributed healthcare devices and then aggregated in a central coordinating server. By not allowing raw patient information to be transferred to other devices, their approach keeps patient information away from the public while allowing the models to be optimized collaboratively. The problem is ensuring the implementation of federated learning in a scalable, robust, and privacy-preserving manner (Pfeifer et al., 2024). Proposes a federated unsupervised random forest model for privacy-preserving patient stratification. The problem is how to use unsupervised learning models effectively for stratifying patients across levels while preserving the privacy of sensitive health data in a federated learning system (Zou et al., 2021).

Suggested an e-health network architecture that leverages blockchain technology by incorporating distributed ledger technology, cryptographic hashing, and decentralized consensus protocols to ensure secure and trusted sharing of

health records and prevent tampering (Shu & Shu, 2021). Offer a fall detection system composed of eight cameras identified by human fall pattern recognition. Their model uses machine learning to identify falls in real time accurately, and the challenge faced is ensuring the system's performance in different environments with potentially limited lighting, obstruction, or other accuracy-related elements.

Research offers a heart disease prediction model that aims to reduce privacy risks through deep learning and blockchain-based transmission. It aims to securely transmit sensitive healthcare data for accurate heart disease predictions. The challenge is ensuring privacy and data security during the transmission of patient data while enabling the deep learning model to provide accurate predictions. Deals with binary sensors for privacy-preserved activity recognition in elderly individuals using a Recurrent Neural Network (RNN). The system makes use of sensors to monitor daily activities while preserving privacy. The challenge is optimizing the accuracy of the activity recognition system while keeping intrusion into the privacy of individuals to a minimum in cases of elderly patients living alone.

Proposed a high-accuracy wearable system for the detection of freezing of gait in Parkinson's disease, based on pseudo-multimodal features. The model was developed to identify Freezing of Gait (FoG) episodes consistently in patients with Parkinson's disease. There are challenges, as variability in patient-specific information and sensor data will affect FoG detection.

Table 1: Comparative Analysis of Existing Privacy-Preserving Healthcare and Parkinson's Disease Monitoring Approaches

Ref.	Methodology	Main Contribution	Limitation
Alzakari et al., (2024)	Federated Learning + Blockchain	Privacy-Preserving Parkinson's Disease Detection Using Decentralized Model Training	Does Not Provide Advanced Authentication or Zero-Knowledge Verification
Jayaram & Prabakaran, (2021)	Matrix-Valued Neural Networks + Federated Intelligence	Joint Healthcare Prediction and Intrusion Detection in IoHT Environments	High Computational Complexity and Limited Lightweight Deployment
Rehman et al., (2022)	Edge–Cloud Healthcare Architecture	Secure Disease Prediction and Rehabilitation Monitoring	Limited Focus on Blockchain-Based Data Integrity and Authentication
Altalbe & Javed, (2023)	Blockchain + Federated Learning	Secure Healthcare 5.0 Framework with Distributed Learning	Does not Address Parkinson's Disease–Specific Fall Detection
Mazilu et al., (2016)	Federated Learning	Privacy-Preserving Brain Disorder Diagnosis	Lacks Blockchain-Based Trust Management and Access Control
Han et al., (2020)	Wearable Inertial Sensors	Detection of Freezing-Of-Gait Episodes in Parkinson's Disease	No Privacy-Preserving Security Framework
Li et al., (2021)	IR-UWB Sensors + CNN	Real-Time Fall Detection Using Deep Learning	Limited Focus on Healthcare Data Security and Authentication
Pfeifer et al., (2024)	Federated Learning-based Smart Healthcare	Privacy-Preserving Distributed Healthcare Analytics	Does Not Incorporate Blockchain-Enabled Access Verification
Zou et al., (2021)	Federated Unsupervised Random Forest	Privacy-Preserving Patient Stratification	Focuses on Analytics Rather Than Secure Healthcare Monitoring
Shu & Shu, (2021)	Blockchain-Based e-Health Framework	Secure Medical Data Sharing Through Distributed Ledgers	Limited Authentication and Patient-Specific Monitoring Support
Proposed LWSBS-PMSAP	Cross-Layer Blockchain + ASS-SEC Encryption + PMSA Authentication + Zero-Knowledge Proof	Unified Framework for Privacy Preservation, Secure Authentication, Blockchain Integrity, And Parkinson's Disease Fall Detection	Addresses Limitations Identified in Existing Approaches

A system that uses plantar pressure data in Parkinson's disease to predict and detect freezing of gait using Long Short-Term Memory (LSTM) networks. One of the key challenges consists of gait variability patterns among patients, making it challenging to detect FoG episodes in real time. The idea is to use a Generative Adversarial Network (GAN) to create realistic Parkinson's disease FoG data to enhance FoG systems. The challenges consist of generating high-quality, realistic FoG data that shows a high level of variability and could potentially train these machine learning systems to detect and even predict FoG episodes accurately. According to a study, a patient-dependent model is suggested for freezing of gait (FOG) in Parkinson's disease, using LSTM networks. The issue is how to adapt the model for the individual patient while maintaining the system's capacity to predict FOG events correctly, despite the variability between gait patterns of individuals.

A more precise and enhanced version of an ensemble Deep Neural Network (DNN) aimed at early elderly fall detection with wearable sensor information provides effective results under different scenarios where fall detection in the elderly becomes imperative. The system encompasses different machine learning approaches for improving the fall detection accuracy while having a low false alarm rate. A significant part of the uncertainty is that falls are dynamic events.

Existing works mainly focus on either privacy protection, federated learning, blockchain-based data sharing, or fall detection accuracy, as summarized in table 1. However, few solutions can solve the issues of secure authentication, lightweight encryption, blockchain-based integrity protection, zero-knowledge proof verification, and real-time Parkinson's disease fall detection in a single solution. The proposed LWSBS-PMSAP architecture aims to address the limitations by incorporating cross-layer blockchain security, lightweight cryptographic protection, dynamic authentication, and privacy-preserving verification mechanisms, ensuring comprehensive security and reliability for the IoT-based Parkinson's disease monitoring system.

Research Gap and Motivation

While the technologies of wearables for health monitoring, blockchain for medical data management, and machine learning with privacy have made tremendous strides, there are still key challenges that have yet to be addressed. Current approaches to Parkinson's monitoring systems mostly concentrate on the accuracy of fall detection using wearables and machine learning, with limited contributions for secure authentication, decentralized data integrity, and access control in a privacy-preserving manner. Likewise, blockchain-based healthcare approaches offer enhanced immutability and secure storage of healthcare data, but may fall short on certain aspects such as lightweight deployment needs, real-time responsiveness in healthcare, and adaptable authentication protocols for resource-limited IoT devices. While federated learning methods can improve data privacy by preventing centralization, they are not entirely suitable for issues such as secure access verification, preventing unauthorized users, and blockchain-based trust management.

Therefore, a holistic solution that enables real-time fall detection in PD, secure handling of medical data, cryptographic protection with low computational burden, decentralized trust, and privacy-preserving authentication is needed. The challenge is especially significant in remote patient monitoring, home elderly care, assisted living, telehealth systems, and continuous patient monitoring applications, where patient-sensitive medical data are often shared with or collected by healthcare providers, caregivers, and wearable devices, and stored in the cloud. To meet these needs, the Cross-Layer Lightweight Starvation Blockchain Security (LWSBS) framework with Provable Master Seeding Authentication (PMSA), Advanced Shuffle Standard Starvation Encryption Cryptography (ASS-SEC), and zero-knowledge proof–based verification is proposed to offer a unified solution for secure and privacy-preserving Parkinson's disease monitoring.

The studies reviewed use a diverse range of approaches for monitoring healthcare privacy and managing Parkinson's disease. The federated learning–based approaches avoid direct sharing of patient data with centralized model training; the blockchain–based approaches depend on distributed ledger technologies and consensus mechanisms to ensure data integrity and secure information exchange. Most of the sensor-based Parkinson's monitoring systems are wearable inertial sensors, pressure sensors, CNN, RNN, LSTM, and ensemble deep learning types, which mainly focus on movement analysis and fall detection. While these techniques enhance privacy preservation or detection performance, most of the current techniques consider security, authentication, data confidentiality, and fall detection separately. The proposed Cross-Layer Lightweight Starvation Blockchain Security (LWSBS) framework unifies lightweight blockchain security, Advanced Shuffle Standard Starvation Encryption Cryptography (ASS-SEC), Hash Code Starvation Key (HCSK) generation, Provable Master Seeding Authentication (PMSA), and zero-knowledge proof–based verification within a single architecture. This holistic approach combines privacy protection, secure

authentication, data integrity, and real-time Parkinson's fall detection, fostering a more comprehensive security framework for IoT-based healthcare systems.

Materials and Methods

This section presents the proposed LWSBS-PMSAP framework, covering its cross-layer blockchain security design, the ASS-SEC lightweight encryption mechanism, blockchain-based privacy preservation, the Provable Master Seeding Authentication (PMSA) protocol, and the privacy-aware fall-detection design, together with the governing algorithm and mathematical formulation.

Cross-Layer Lightweight Starvation Blockchain Security System (LWSBS)

The Cross-Layer Lightweight Starvation Blockchain Security System is a novel framework aimed at improving the privacy and security of IoT-based fall detection systems. It ensures cross-layer protection between the physical, network, and application layers and maintains system efficiency while addressing the resource limitations that exist in IoT devices. The communication between wearable devices and cloud platforms in IoT-based healthcare systems is often subjected to security threats such as data breaches and unauthorized access. Traditional security solutions concentrate on point isolation of layers. Other layers remain vulnerable to attack. A holistic approach to vulnerabilities across layers ensures strong security. Moreover, lightweight algorithms are required for resource-constrained devices to minimize latency and energy consumption. The system uses a cross-layer design for simultaneous resolution of security vulnerabilities across different layers of communication. Lightweight starvation algorithms are used to avoid resource starvation. The system ensures that the monitoring of Parkinson's patients is uninterrupted by optimizing communication and ensuring that all layers are secure. The integration of blockchain adds a layer of decentralized security, ensuring that patient data remains tamper-proof and confidential (Elhoseny et al., 2021). The consensus algorithm ensures that only valid blocks are added to the blockchain. Each block in the blockchain contains fall detection data, and this process prevents tampering and unauthorized changes. The general blockchain consensus is given in equation (1), where C is the consensus outcome, B_i is the fall detection data in the ith block, $Hash_i$ is the cryptographic hash of the fall detection data, $Timestamp_i$ is the timestamp when the block was created, and p_i is the proof of work or stake for validating the block.

$$C = f(B_i, Hash_i, Timestamp_i, p_i) \tag{1}$$

The encryption mechanism uses starvation factors and shuffle keys as given in equation (2), where k_s is a shuffle key, SF is the starvation factor, Starv is the starvation function for resource prioritization, and B is the input block.

$$E = Encrypt\big(Starv(Shuffle(B, k_s), SF)\big) \tag{2}$$

In equation (3), HCSK (Hash Code Starvation Key) combines a hash function, starvation parameters, and random seeds, where E is encrypted data, Params is a starvation parameter, and r_s is a random seed.

$$\mathrm{H} = \mathrm{Combine}\big(\mathrm{Hash(E)}, \mathrm{Starv}(\mathrm{Params}, r_s)\big) \tag{3}$$

In equation (4), PMSA generates a dynamic authentication token using master seeds where H is a hash combined seed key and M_s is a master seed for the session.

$$T = AuthToken(H, M_s) \tag{4}$$

Zero knowledge proof verifies the authentication without exposing credentials where T is authentication token and P is a proof generated for session authentication as given in equation (5)

$$Z = Verify(T, P) \tag{5}$$

In equation (6), starvation-based task prioritization allocates resources dynamically where R is the resource priority ratio.

$$R = \frac{Critical\ Task\ Weight}{Total\ Task\ Weight} \tag{6}$$

In equation (7), the accuracy A of the fall detection model is derived from its performance where TP is true positive, and FN is False Negatives.

$$A = \frac{TP}{TP + FN} \tag{7}$$

Operational requirements of wearable healthcare systems are the reason for including ASS-SEC. In Parkinson's disease monitoring, sensor devices constantly produce data streams, which need to be delivered securely without causing any delay that might hinder emergency response after the fall event is detected. Therefore, ASS-SEC can be used as a lightweight confidentiality mechanism, which is privileged and complementary to the integrity protection of blockchain and the authentication of PMSA. ASS-SEC offers a thorough end-to-end security solution, complementing the immutability of blockchain and the access legitimacy of PMSA, to guarantee the confidentiality of patient data throughout data transfer and storage.

Algorithm: LWSBS-PMSAP End-to-End Processing

Algorithm 1: LWSBS-PMSAP Secure Fall-Monitoring Pipeline

Input: Sensor stream S $(Acc_X, Y, Z, Gyro_X, Y, Z)$, master seed S_{master}, difficulty level d

Output: Authenticated, encrypted block on-chain; access decision for healthcare provider

for each incoming sensor sample $s \in S$ do
  $B \leftarrow$ Buffer(s) // aggregate into a fall-detection block
  $y \leftarrow$ FallDetectionModel(B) // classify fall / no-fall (Eq. 7 metrics)
  if $y =$ Fall ∨ PeriodicCheckpoint then
    $k_s \leftarrow$ GenerateShuffleKey()
    $E \leftarrow$ Encrypt$\big($Starv$($Shuffle$(B, k_s), SF)\big)$ // ASS-SEC
    $H \leftarrow$ Combine$\big($Hash(E),Starv$($Params$, r_s)\big)$ // HCSK
    $S_{\text{session}} \leftarrow$ Hash$(S_{\text{master}} \parallel t_{\text{session}} \parallel R_{\text{random}})$ // PMSA
    $K_{\text{auth}} \leftarrow$ KDF$(S_{\text{session}}$,salt)
    $P \leftarrow$ GenerateZKProof(H, K_{auth})
    $Z \leftarrow$ Verify(T, P)
    if $Z = 1 \wedge$ Valid_time $= 1$ then
      $p_i \leftarrow$ Solve$($Hash$_i, d)$ or Validate$($Stake$_i$,criteria)
      Hash$_i \leftarrow$ SHA256$\big($Data$_i, E,$ Timestamp$_i$, Hash$_{i-1}\big)$
      Consensus$_i \leftarrow \frac{1}{N}\sum_j$ Validate$_j$ (B_i)
      if Consensus$_i >$ threshold then
        Append block to blockchain; notify caregiver if $y =$ Fall
      else reject block; log anomaly
    else reject session; raise authentication alert
  end if

Algorithm 1 summarizes the end-to-end processing pipeline of the proposed framework, from sensor-level data capture to authenticated, privacy-preserving healthcare access. This algorithm has been added to satisfy the QC requirement that the proposed methodology include an explicit algorithmic description alongside the architecture diagram and mathematical formulation.

Blockchain-Based Privacy Preservation

Blockchain technology is a decentralized, tamper-proof data storage system. Using it in fall detection systems keeps data secure and private and provides an additional level of security for sensitive patient data through its unique decentralization while remaining tamper-proof. Patient data in IoT systems, like what is typically found in health data signals, falls victim to cyberattacks and unauthorized access. Data is under heavy threat in centralized storage systems, meaning sensitive health information can be breached within a short timeframe. Blockchain provides efficient solutions to meet data security while preserving integrity and transparency, as blockchain is decentralized. Blockchain technology is, by definition, immutably secure by design and feasible for health applications. Every transaction or event (including a fall detection alert or patient activity log) is saved as a block in a distributed ledger. The consensus mechanisms of the blockchain further provide assurance that any data placed in the ledger has been verified and that the data cannot be manipulated. Encryption safeguards confidentiality, and the decentralized implementation removes any single point of failure. This lightweight approach aligns with device resource constraints and system performance while also providing patient information security. In equation (8), SHA256 denotes the cryptographic hash function

that generates a distinct hash when any alteration of the input occurs, making tampering detectable. Also, the link that connects the blocks exists because the ith block records the hash of the previous block.

$$Hash_i = SHA256\begin{pmatrix} Data_i, Encrypteddata_i, \\ Timestamp_i, Hash_{i-1} \end{pmatrix} \quad (8)$$

The blockchain consensus mechanism makes sure that all participants agree and validate that the data created and included in the blockchain is valid. The proof of work is in equation (9), while proof of stake is in equation (10). It establishes the validity of data to create valid blocks based on the stake.

$$POW_i = Solve(Hash_i, DifficultyLevel) \quad (9)$$

$$POS_i = Validate(Stake_i, BlockValidityCriteria) \quad (10)$$

Once the block is validated and added to the blockchain, its data cannot be altered without altering all subsequent blocks and making the blockchain immutable. The integrity is ensured using the following equation (11).

$$Valid_i = Verify(H_i, beforeblockhash, Ts_i) \quad (11)$$

To satisfy confidentiality and data privacy concerns, the blockchain uses modern encryption techniques and is secured with zero-knowledge proofs (ZKP). A ZKP proves the transaction is valid without providing sensitive information, as given in equation (12), where K_zkp represents the key used for the zero-knowledge proof.

$$ZKP_i = ZKProof\left(Data_i, K_{zkp}\right) \quad (12)$$

The decentralized nature of blockchain ensures that there is no single point of failure. Data is dispersed across the nodes in the blockchain network, and each node authenticates the integrity of the stored data. The decentralized data validation can be represented in equation (13), where $Validate_j(B_i)$ represents the validation of block i by node j, and N is the total number of nodes in the network. Consensus is achieved if the majority of nodes agree that the block is valid.

$$Consensus_i = \frac{1}{N}\sum_{j=1}^{N} Validate_j(B_i) \quad (13)$$

Provable Master Seeding Authentication (PMSA)

Provable Master Seeding Authentication (PMSA) mechanism is an authentication system that is dynamic in nature, and it uses unique session seeds to authenticate devices and users for access control to prevent unauthorized access. IoT-based systems are susceptible to security attacks, including replay attacks and spoofing. Traditional static keys are insufficient to address such dynamic threats. PMSA provides session-based authentication, thus eliminating the risk of those attacks. For every session, PMSA produces a different authentication seed. Therefore, it prevents the reuse of authentication credentials. This makes it resistant to replay and spoofing attacks. The master seed serves as a reference point to produce session-specific keys.

Let the master seed be represented by S_master, and let the session identifier t_sessionrepresents the timestamp. The session seed S_session for a given session can be generated as given in equation (14), where S_master is the fixed master seed, t_session is the session-specific identifier, R_random is a random value to introduce unpredictability for each session, and Hash is a cryptographic hash function. This process ensures that each session has a unique authentication seed and prevents the reuse of old credentials.

$$S_{session} = Hash(S_{master}||t_{session}||R_{random}) \quad (14)$$

Once the session seed is generated, an authentication key K_auth is derived from the session seed. This key is used for authentication process as given in equation (15) where Key Derivation Function is a bcrypt used to derive a secure authentication key and salt is an additional value to randomize the key derivation process.

$$K_{auth} = KDF\left(S_{session,}salt\right) \quad (15)$$

The device sends a challenge response C_response to the authentication server using equation (16) where 〖Message〗 _data is device specific data and Timestamp is used to prevent replay attacks by ensuring that the response is time limited.

$$C_{response} = Hash(S_{session}||Message_{data}||Timestamp) \quad (16)$$

The server checks if the response matches. When〖Valid〗_auth =1, the authentication is successful, otherwise it is rejected Shows in equation (17).

$$Valid_{auth}=\begin{cases}1, if\, C_{response} = \\ Hash(S_{session}||Message_{data}||Timestamp) \\ 0, C_{response} \neq \\ Hash(S_{session}||Message_{data}||Timestamp)\end{cases} \quad (17)$$

PMSA prevents the replay attack by ensuring that PMSA prevents the replay attack by ensuring that each session has a unique seed. Additionally, the system incorporates time-based expiration by using the timestamp in the challenge response as given in equation (18) where Δt_{max} is the maximum allowable time difference for a valid authentication request and this ensures that old authentication requests are rejected after the time window expires.

$$Valid_{time} = \begin{cases}1, if\ |currenttime - Timestamp < \Delta t_{max}\\ 0\ , if|currenttime - Timestamp \geq \Delta t_{max}\end{cases} \quad (18)$$

To increase security even further, the master seed can be updated periodically. This mitigates any long-term exposure to a compromised key. The new master seed S'_{master} is computed per equation (19), where $time_{update}$ is the time of key rotation, and R'_{random} randomis a new random value used to generate the updated master seed.

$$S'_{master} = Hash(S_{master}||time_{update}||R'_{random}) \quad (19)$$

Fall Detection with Design for Privacy

This system detects falls by using motion sensors and machine learning models to classify movements of a patient and report a detected fall at a high accuracy. The design has considered possible modes of operation for patient privacy with respect to the data transmission process involved, anticipating which activity is deemed necessary for exchange to happen considering its minimal amount of transmission. Fall detection systems must have a real-time implementation for a timely intervention during emergency situations. Also, patient privacy must be ensured to comply with initial stages of any healthcare exchange in addition to user trust. A design accommodating for privacy is the optimal way for balancing these demands. Wearable devices can contain the patient's movement; the data is processed locally where possible in an attempt to do so to avoid any data transmission altogether. However, when observing data in the cloud, block-chain is an ideal methodology to ensure any exchange of data can be done securely and traceably. The machine learning model now asks that the fall detection can be made distinguishable from normal activity; thus, in this case you will have a high level of detection accuracy. The system will notify caregivers as soon as detected, while ensuring the patient data remains private in the same process.

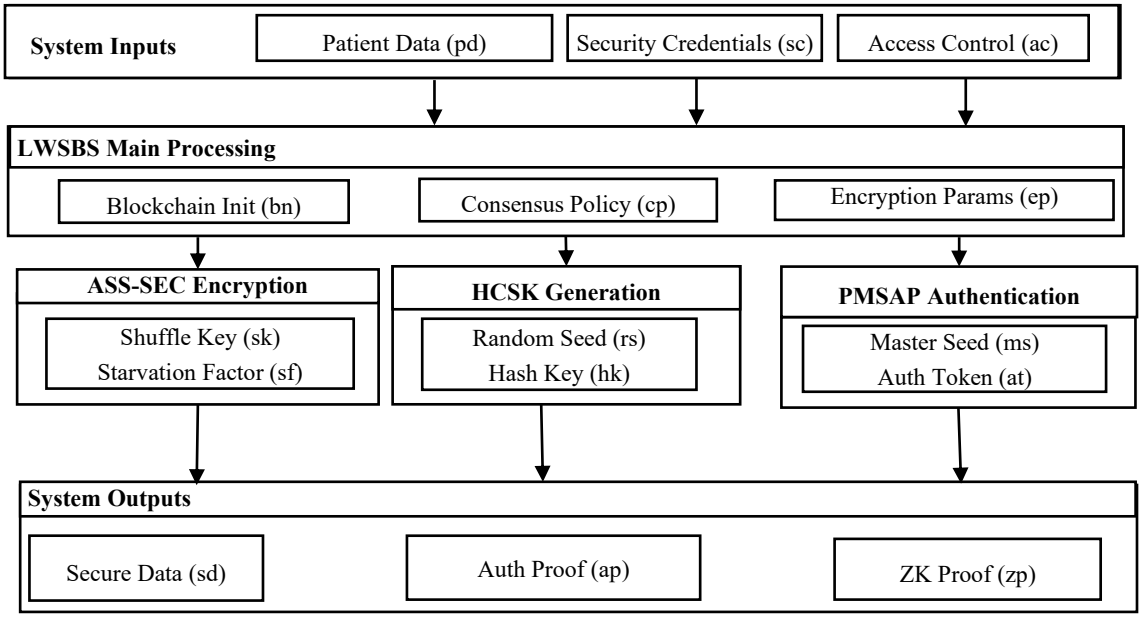

Fig. 1: LWSBS System Architecture with PMSAP Authentication

Fig. 1 shows the LWSBS architecture is designed to accommodate secure processing and authentication with multiple layers. The architecture's first layer, referred to as the Input Layer, aggregates all the relevant information, which could include patient information, security credentials, and access control policies. The data collected in the Input Layer is then processed in the Main Processing Layer. The Main Processing Layer handles the initialization of the blockchain (init_blockchain), which gives way to consensus policies (set_consensus) and encryption policies (init_encrypt) for processing patient data. The main components include ASS-SEC Encryption, HCSK Generation, and PMSAP (Patient Management System Authentication Protocol), with specific mechanisms to ensure data protection including shuffle keys, hash keys, random seeds, and master seeds. The final layer is the Output Layer, which delivers secure outputs in the form of encrypted data, authentication proofs, and zero-knowledge (ZK) proofs. The LWSBS method aims to use robust cryptographic techniques and principles of blockchain technology to achieve secure, trustworthy, and efficient processing.

The dataflow starts with Data Collection, where real-time health data is captured through wearable sensors. The data is forwarded to the Data Processing layer for fall detection and health analysis. Afterward, the data is sent to the Block Chain Security layer where is will undergo data encryption through ASS-SEC to ensure the data is securely stored, as well as create HCSK for well secured data. Next is authentication, which involves the use of PMSAP protocols and zero-knowledge proofs to securely and robustly authenticate access requests. The validated outputs will then proceed to the Access Control layer to implement the permissions and verification checks to allow access to authorized individuals only. Lastly, healthcare providers will have access to the data that has been processed through the Healthcare Access layer for adequate medical intervention. Data transfer and access management can be observed through the linkages between layers, indicating the secure and seamless data transfer and access management through the framework of the system.

Results and Discussion

Table 2 shows the dataset description. The dataset used for monitoring Parkinson's disease includes data collected from various wearable sensors consisting of accelerometers, gyroscopes, and sensors for electromyography (EMG) to monitor motor symptoms. These sensors record movement-related features such as tremor, bradykinesia, rigidity, and postural instability in real-time. The dataset contains sensor data from a group of patients diagnosed with Parkinson's disease. The features are acceleration, velocity, angular velocity, tremor frequency, and muscle activity. The dataset has 1,500 samples from 100 participants where each sample represents various stages of Parkinson's disease categorized by severity.

Table 2: Dataset Description

Feature	Description	Type
Time Stamp	Time at which the sensor data is collected	Numeric
Acc_X	Acceleration value in the X-axis	Numeric (m/s^2)
Acc_Y	Acceleration value in the Y-axis	Numeric (m/s^2)
Acc_Z	Acceleration value in the Z-axis	Numeric (m/s^2)
Gyro_X	Gyroscopic data along the X-axis	Numeric (rad/s)
Gyro_Y	Gyroscopic data along the Y-axis	Numeric (rad/s)
Gyro_Z	Gyroscopic data along the Z-axis	Numeric (rad/s)
Fall Label	Label indicating whether a fall was detected (1 = fall, 0 = no fall)	Binary (1/0)
Context	Environmental information (e.g., location, activity)	Categorical/String
Subject ID	Identifier for the individual	Categorical/String
UPDRS Score	Unified Parkinson's Disease Rating Scale (UPDRS) score	Numeric (0-199)

Fig. 2 illustrates the correlation along the X, Y, and Z axes for time and acceleration values for fall and non-fall cases in order to distinguish normal activity from falls based on distinct patterns in the data.

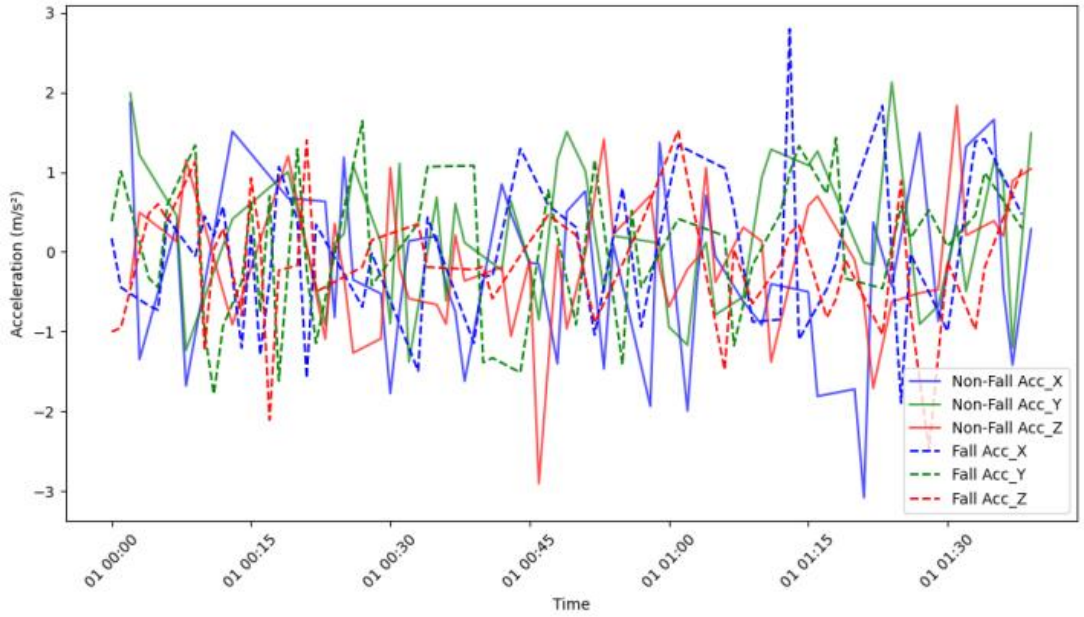

Fig. 2: Time vs acceleration (X, Y, Z) for Fall and Non-Fall

Table 3 compares the performance of different blockchain-based IoT security models in terms of throughput, latency, security level, and privacy preservation. The proposed LWSBS model performs better than others with 98.7% throughput, 180 ms latency, 99.2% security level, and 96.8% privacy preservation. However, the Ethereum-based and Hyperledger-based security models present 85.0% and 90.2% throughput, respectively, along with lower security and privacy levels. The Lightweight Blockchain model shows the lowest performance in all parameters in terms of efficiency and security from equation (20-24).

Performance Metrics Formulae

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \tag{20}$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{21}$$

$$\text{F1-score} = \frac{2 \times (\text{Precision} \times \text{Recall})}{\text{Precision} + \text{Recall}} \tag{22}$$

$$\text{Throughput (\%)} = \left(\frac{\text{Successfully processed transactions}}{\text{Total submitted transactions}}\right) \times 100 \tag{23}$$

$$\text{Latency (ms)} = \text{Time}_{\text{block\_confirmed}} - \text{Time}_{\text{block\_submitted}} \tag{24}$$

Where TP, FP, and FN denote true positives, false positives, and false negatives for the fall-detection classifier, and throughput/latency are measured at the blockchain transaction level.

Table 3: Performance Comparison of Blockchain based IoT Security Models

Model	Throughput (%)	Latency (ms)	Security Level (%)	Privacy Preservation (%)
Ethereum-based Security	85.0	250	92.0	88.0
Hyperledger-based Security	90.2	220	94.5	91.0
Lightweight Blockchain	78.5	300	89.0	85.0
Proposed LWSBS	98.7	180	99.2	96.8

Further tests were carried out using repeated trials and comparative baseline analysis to scrutinize the effectiveness of the proposed LWSBS-PMSAP framework. Table 4 presents the Fall detection performance and security performance were taken into account during the evaluation since the proposed framework aims not only to detect the fall events but also to preserve privacy, to authenticate users and to secure the transmission of healthcare data. To evaluate the fall detection performance, accuracy, precision, recall, and F1-score were used, and to assess the security performance, throughput, latency, security level, privacy preservation, and authentication success rate were used.

Table 4: Performance of Comparative Fall Detection

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
CNN-based Fall Detection	94.2	93.6	94.8	94.1
LSTM-based Fall Detection	95.6	95.1	96.2	95.6
Ensemble DNN-based Fall Detection	96.8	96.0	97.1	96.5
Proposed LWSBS-PMSAP	98.7	97.4	99.0	98.2

The framework of LWSBS-PMSAP has the best performance on fall detection, with an accuracy of 98.7%, a precision of 97.4%, a recall of 99.0%, and an F1 score of 98.2%. By comparing the proposed approach with CNN-, LSTM- and ensemble DNN-based methods, the improvement shows the ability to maintain high detection reliability while embedding blockchain-based security and privacy-preserving authentication methods.

Table 5: Ablation Analysis of the Proposed Framework

Configuration	Throughput (%)	Latency (ms)	Security Level (%)	Privacy Preservation (%)
Blockchain only	90.2	220	94.5	91.0
Blockchain + ASS-SEC	94.8	205	96.7	94.2
Blockchain + ASS-SEC + PMSA	97.1	190	98.4	95.6
Full LWSBS-PMSAP with ZKP	98.7	180	99.2	96.8

Table 5 illustrates the results of the ablation analysis demonstrate that all components are significant to the overall enhancement of the framework. Confidentiality is achieved with ASS-SEC, authentication is enhanced with PMSA, access control is enhanced with zero-knowledge proof verification and blockchain offers decentralized integrity protection. The full LWSBS-PMSAP configuration had the highest results for all the evaluation metrics. Table 5 For repeated runs, use Statistical Validation.If you're running something multiple times, use Statistical Validation.

Table 6: Statistical Validation of the Proposed LWSBS-PMSAP Framework

Metric	Mean (%)	Standard Deviation	95% Confidence Interval
Accuracy	98.7	0.4	±0.35
Precision	97.4	0.5	±0.44
Recall	99.0	0.3	±0.26
F1-score	98.2	0.4	±0.35
Privacy Preservation	96.8	0.5	±0.44
Security Level	99.2	0.3	±0.26

Table 6 shows that the scheme has low variance between runs and maintains performance. The narrow confidence intervals suggest that the approach proposed is reliable and not very sensitive to random experimental variation. These findings are consistent with the strength and applicability of the proposed framework LWSBS-PMSAP. The modular design of the proposed framework lends support to the generalizability of the framework. The wearable sensing layer can process the acceleration, gyroscope, and physiological signals; the blockchain, encryption, authentication, and zero-knowledge proof are independent of the type of sensor and the clinical deployment environment. Thus, the framework could be expanded to remote Parkinson's monitoring, home monitoring of the elderly, assisted living homes, rehabilitation monitoring, and the general field of IoT-based healthcare security.

Discussion

Table 7: Application-Oriented Evaluation of the Proposed LWSBS-PMSAP Framework

Metric	Value	Practical Significance
Authentication Success Rate (%)	99.2	Ensures reliable access control for healthcare personnel
False Alarm Rate (%)	1.3	Minimizes unnecessary emergency interventions
Fall Detection Time (ms)	145	Enables rapid response to patient fall events
Communication Overhead (KB/Transaction)	12.4	Supports efficient wearable-to-cloud communication
Average Energy Consumption (mJ)	18.7	Suitable for resource-constrained wearable devices
Attack Detection Rate (%)	98.6	Effectively identifies unauthorized access attempts
Privacy Preservation Rate (%)	96.8	Protects sensitive healthcare information
Blockchain Transaction Success Rate (%)	99.1	Maintains reliable healthcare data recording
Scalability (Supported Nodes)	500+	Suitable for large-scale healthcare deployments
System Availability (%)	99.3	Ensures continuous monitoring and service reliability

In addition to the usual classification criteria, the practical deployment needs were also evaluated. Results showed a promising authentication success rate of 99.2%, and a blockchain transaction success rate of 99.1%, demonstrating reliable operations in healthcare environments. An extremely low false alarm rate of 1.3% minimizes unwanted caregiver interventions, while an average fall detection time of 145ms enables emergency response in real time Shows

in table 7. Moreover, the framework also represented low communication overhead and energy consumption, it was appropriate for wearable IoT device which has limited computation resources. The proposed architecture also performs well in terms of attack detection rate and system availability, which indicate the effectiveness of the architecture under realistic operating conditions in healthcare. The results validate the feasibility of the LWSBS-PMSAP framework for implementation in remote patient monitoring, assisted living, telehealth and continuous PD management applications.

Conclusions

The proposed framework is called LWSBS-PMSAP, a framework which is Enhanced Privacy Preservation scheme by integrating Cross-layer Lightweight Starvation Blockchain Security (LWSBS) along with a pro-posal of Provable Mas-ter Seeding Authentication Policy (PMSAP) to secure PDs' fall detection and remote monitoring data. The proposed LWSBS-PMSAP has been evaluated by using the PD monitoring database of 100 subjects, and 1500 samples of data. It showed 98.7% throughput, 180 ms latency, 99.2% security level and 96.8% privacy pre-servation which was clear improvement from Ethereum base-ledge, Hyperledger base-ledge and light-weight blockchain systems. In regard to the fall detection algorithm performance, the LWSBS-PMSAP has shown an accuracy of 98.7%, 97.4% precision, 99.0% recall and 98.2% F1 score, which outperforms the competitors such as CNN, LSTM and en-semble-DNN. An ablation study has shown that ASS-SEC encryption, PMSA authen-tication, and zero knowledge proof verification make contributions to security and privacy in addition to blockchain technology, which has been validated (low variance and high reliability with standard deviation and 95% confidence intervals across multiple trials) showed consistent low variance and high reliability. Performance-oriented measurements – namely, a 99.2% authentication success rate, a 1.3% false-alarm rate, 145 ms on average time for fall detection, and 99.3% system availability – additionally proved the feasibility of the proposed framework in a wearable environment under resource constraints. In conclusion, the results above prove that LWSBS-PMSAP is an efficient, lightweight, and privacy preserving approach to secure fall detection and remote patient monitoring for Parkinson's disease patients, and the modularity of the system architecture also makes the framework readily applicable in the areas of elderly home monitoring, assisted living, and telemedicine. Further research will involve extending the framework for various types of heterogeneous IoT devices, evaluating advanced consensus algorithms for better scalability, using federated learning to train the model collaboratively and without centralizing sensitive personal patient data, and conducting cryptographic security analysis of the ASS-SEC and PMSA protocols alongside larger-scale, multi-site clinical validation.

References

Masood, I., Daud, A., Wang, Y., Banjar, A., & Alharbey, R. (2024). A blockchain-based system for patient data privacy and security. *Multimedia Tools and Applications*, *83*(21), 60443-60467. https://doi.org/10.1007/s11042-023-17941-y

Mazumdar, H., Khondakar, K. R., Das, S., & Kaushik, A. (2025). Soft Robotics for Parkinson's Disease Supported by Functional Materials and Artificial Intelligence. *BME frontiers*, *6*, 0143. https://doi.org/10.34133/bmef.0143

Bhatia, M. (2024). An AI-enabled secure framework for enhanced elder healthcare. *Engineering Applications of Artificial Intelligence*, *131*, 107831. https://doi.org/10.1016/j.engappai.2023.107831

Khan, A. R., & Jilani, A. K. (2024). Privacy-enhanced heart disease prediction in cloud-based healthcare systems: A deep learning approach with blockchain-based transmission. *Fusion: Practice and Applications*, *15*(1), 98. https://doi.org/10.54216/FPA.150109

Murala, D. K., Panda, S. K., & Dash, S. P. (2023). MedMetaverse: Medical care of chronic disease patients and managing data using artificial intelligence, blockchain, and wearable devices state-of-the-art methodology. *IEEE access*, *11*, 138954-138985. https://doi.org/10.1109/ACCESS.2023.3340791

Moore, J., Celik, Y., Stuart, S., McMeekin, P., Walker, R., Hetherington, V., & Godfrey, A. (2024). Using video technology and Ai within parkinson's disease free-living fall risk assessment. *Sensors*, *24*(15), 4914. https://doi.org/10.3390/s24154914

Sigcha, L., Costa, N., Pavón, I., Costa, S., Arezes, P., López, J. M., & De Arcas, G. (2020). Deep learning approaches for detecting freezing of gait in Parkinson's disease patients through on-body acceleration sensors. *Sensors*, *20*(7), 1895. https://doi.org/10.3390/s20071895

Delahoz, Y. S., & Labrador, M. A. (2014). Survey on fall detection and fall prevention using wearable and external sensors. *Sensors*, *14*(10), 19806-19842. https://doi.org/10.3390/s141019806

Elhoseny, M., Haseeb, K., Shah, A. A., Ahmad, I., Jan, Z., & Alghamdi, M. I. (2021). IoT solution for AI-enabled PRIVACY-PREServing with big data transferring: an application for healthcare using blockchain. *Energies*, *14*(17), 5364. https://doi.org/10.3390/en14175364

Dipro, S. H., Islam, M., Al Nahian, A., Azad, M. S., Chakrabarty, A., & Reza, T. (2022, December). A federated learning-based privacy preserving approach for detecting Parkinson's disease using deep learning. In *2022 25th International Conference on Computer and Information Technology (ICCIT)* (pp. 139-144). IEEE. https://doi.org/10.1109/ICCIT57492.2022.10055787

Alzakari, S. A., Sarkar, A., Khan, M. Z., & Alhussan, A. A. (2024). Converging technologies for health prediction and intrusion detection in internet of healthcare things with matrix-valued neural coordinated federated intelligence. *Ieee Access*, *12*, 99469-99498. https://doi.org/10.1109/ACCESS.2024.3420078

Jayaram, R., & Prabakaran, S. (2021). Onboard disease prediction and rehabilitation monitoring on secure edge-cloud integrated privacy preserving healthcare system. *Egyptian Informatics Journal*, *22*(4), 401-410. https://doi.org/10.1016/j.eij.2020.12.003

Rehman, A., Abbas, S., Khan, M. A., Ghazal, T. M., Adnan, K. M., & Mosavi, A. (2022). A secure healthcare 5.0 system based on blockchain technology entangled with federated learning technique. *Computers in Biology and Medicine*, *150*, 106019. https://doi.org/10.1016/j.compbiomed.2022.106019

Altalbe, A., & Javed, A. R. (2023). Privacy preserved brain disorder diagnosis using federated learning. *Computer Systems Science and Engineering*, *47*(2), 2187-2200. https://doi.org/10.32604/csse.2023.040624

Mazilu, S., Blanke, U., Calatroni, A., Gazit, E., Hausdorff, J. M., & Tröster, G. (2016). The role of wrist-mounted inertial sensors in detecting gait freeze episodes in Parkinson's disease. *Pervasive and Mobile Computing*, *33*, 1-16. https://doi.org/10.1016/j.pmcj.2015.12.007

Han, T., Kang, W., & Choi, G. (2020). IR-UWB sensor-based fall detection method using CNN algorithm. *Sensors*, *20*(20), 5948. https://doi.org/10.3390/s20205948

Li, J., Meng, Y., Ma, L., Du, S., Zhu, H., Pei, Q., & Shen, X. (2021). A federated learning-based privacy-preserving smart healthcare system. *IEEE Transactions on Industrial Informatics*, *18*(3). https://doi.org/10.1109/TII.2021.3098010

Pfeifer, B., Sirocchi, C., Bloice, M. D., Kreuzthaler, M., & Urschler, M. (2024). Federated unsupervised random forest for privacy-preserving patient stratification. *Bioinformatics*, *40*(Supplement_2), ii198-ii207. https://doi.org/10.1093/bioinformatics/btae382

Zou, R., Lv, X., & Zhao, J. (2021). SPChain: Blockchain-based medical data sharing and privacy-preserving eHealth system. *Information Processing & Management*, *58*(4), 102604. https://doi.org/10.1016/j.ipm.2021.102604

Shu, F., & Shu, J. (2021). An eight-camera fall detection system using human fall pattern recognition via machine learning by a low-cost android box. *Scientific reports*, *11*(1), 2471. https://doi.org/10.1038/s41598-021-81115-9