IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 7 May 2024, accepted 23 June 2024, date of publication 27 June 2024, date of current version 26 July 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3420078

RESEARCH ARTICLE

Converging Technologies for Health Prediction and Intrusion Detection in Internet of Healthcare Things With Matrix-Valued Neural Coordinated Federated Intelligence

SARAH A. ALZAKARI[1], **ARINDAM SARKAR**[2], **MOHAMMAD ZUBAIR KHAN**[3], **AND AMEL ALI ALHUSSAN**[1]

[1]Department of Computer Sciences, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia
[2]Department of Computer Science and Electronics, Ramakrishna Mission Vidyamandira, Howrah, West Bengal 711202, India
[3]Department of Computer Science and Information, Taibah University, Medina 42353, Saudi Arabia

Corresponding authors: Arindam Sarkar (arindam.vb@gmail.com) and Mohammad Zubair Khan (mkhanb@taibahu.edu.sa)

Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2024R716), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

ABSTRACT This paper introduces Matrix-Valued Neural Coordinated Federated Deep Extreme Machine Learning, a novel approach for enhancing health prediction and intrusion detection on the Internet of Healthcare Things (IoHT). By leveraging Machine Learning (ML), blockchain, and Intrusion Detection Systems (IDS), this technique ensures the security of medical data while enabling predictive health analytics. The IoHT, characterized by its vast network of interconnected devices, poses significant challenges in security and confidentiality. However, the integration of proposed technique empowers healthcare systems to proactively address these concerns while enhancing patient outcomes and reducing healthcare costs. Smart healthcare, enabled by ML and blockchain, is revolutionizing healthcare 5.0. Healthcare systems may employ IoHTs' intelligent and interactive characteristics using proposed approach. Despite its benefits, medical data aggregation poses security, ownership, and regulatory compliance challenges. Federated Learning (FL) is a key technique for distributed learning that protects data. The proposed architecture has several unique benefits like 1) it provides a thorough examination of the incorporation of blockchain technology with FL for healthcare 5.0; 2) it takes the lead in creating a robust healthcare monitoring system that utilizes blockchain technology and IDS to identify and prevent harmful actions; 3) the development of crucial blockchain elements by means of mutual neuronal synchronization of Artificial Neural Networks (ANNs) showcases pioneering progress in safeguarding medical data; and 4) the framework underwent a thorough empirical assessment and outperformed existing methods in accurately predicting intrusion detection and disease prediction, achieving an impressive efficiency rate of 97.75% and 98% respectively. This development represents a major step forward in improving security and predictive abilities within the IoHT ecosystem, offering the potential for revolutionary advancements in healthcare delivery and patient care.

INDEX TERMS Federated learning, blockchain, cloud security, Internet of Health Things (IoHT).

I. INTRODUCTION

The rapidly expanding field of Internet of Health Technology (IoHT), which provides a multitude of interconnected devices

The associate editor coordinating the review of this manuscript and approving it for publication was Francesco Piccialli.

that have the potential to transform healthcare, is gaining significant traction [1]. In this context, the coming together of Internet of Things (IoT) technologies holds the potential to collect massive volumes of data with the aim of improving efficiency, productivity, and people's health [2], [3], [4]. These breakthroughs are driving significant changes in our daily lives, from smart cities to smart homes [5], [6], [7]. With the rise of IoT-based patient monitoring systems, IoHT has emerged as a ray of hope for reducing health inequalities in the public sector. Although the words IoT and IoHT are sometimes used interchangeably, the combined impact of these two concepts on improving public health and safety is immense [8], [9], [10]. These technologies enable people to track their lifestyle, health, and living situations by linking them to the digital environment [11], [12], [13]. Thanks to new innovation, doctors can check in on their patients from afar and personalize treatments based on scientific data [14]. With the rise of in-home healthcare services, long wait periods and inconvenient travel are becoming less of an issue. By providing real-time monitoring of critical signals such as temperature, blood pressure, electrocardiogram (ECG), heart rate, and fall detection, smart health monitoring devices connect patients in rural areas with healthcare practitioners in metropolitan areas [15], [16], [17]. Wireless data transmission makes it easy for patients and caregivers to get insights that can improve treatment and save time.

Medical record analysis for disease diagnosis, therapy recommendation, and patient health improvement relies heavily on efficient mining algorithms [18], [19], [20]. From its original use in language processing to its recent expansion into healthcare applications, Machine Learning (ML) has emerged as a groundbreaking technology [21], [22], [23].In the healthcare industry, where precision can be a matter of life or death, ML models need a substantial amount of training data in order to achieve optimal performance. Nevertheless, patient privacy is frequently jeopardized by centralized training systems due to the accumulation of data on cloud servers.

Perceptrons were originally defined by Warren McCulloch and Walter Pitts in their 1943 paper [24]. Perceptrons are not exactly perception itself, but rather a fundamental building block used to create artificial models of perception. They are inspired by biological neurons, the information processing units in our brains [25], [26], [27].

The advent of blockchain technology has ushered in a new age for smart healthcare systems to tackle privacy, security, and ethical issues. Particularly in the area of controlling patient data access and information dissemination, the open and accountable architecture of blockchain provides potential answers [28]. Because it doesn't care about any particular protocol, it can be easily integrated into smart home networks [29].

Smart healthcare technologies are becoming increasingly popular, yet research in this area is still disjointed across several fields of study [30], [31], [32]. Our continuing research initiatives are focused on providing a full understanding and practical implementations of blockchain technology in healthcare. By doing so, we want to bridge this knowledge gap and acquire essential insights into these applications.

The medical system is now more susceptible to hacks and breaches due to security holes exposed by the IoHT. Hackers may be able to access linked devices through unified networks, which might have disastrous effects [33], [34]. Hackers are increasingly aiming their sights at smart healthcare systems' most vital components—equipment and medical records—in an effort to gain unauthorized access and use them for malicious activities like phishing and spam [35], [36], [37]. Because of their quick activation to deliver vital services like patient medical data and automatic report updates, as well as their lack of encryption for wireless keys, smart healthcare devices are easy prey for Distributed Denial of Service (DDoS) assaults [38], [39], [40]. Because of its centralized nature, the IoHT system is susceptible to security flaws that allow for things like record manipulation and forgery, device interference, and unauthorized device access via assaults on gateway and server networks [41], [42], [43]. To ensure that healthcare data remains private and undamaged while the IoHT revolution continues, it is crucial to resolve these security challenges.

Based on the tenets of decentralization, transparency, and immutability, blockchain technology functions as an interconnected set of blocks protected by elementary cryptography [44]. There are still problems with its widespread use, especially with respect to access anonymity, despite the fact that it has accelerated the development of several technologies, such autonomous cars and mobile gadgets [45]. Devices may work together to enhance ML models using FL, a decentralized platform for IoT ML, even if they don't share raw data. The security of patient information in connected healthcare systems is ensured by this method. Under healthcare authority, embedded sensors gather medical data, and edge devices work together to create FL algorithms. ML methods find out how a patient is doing and use cloud resources to help right now. FL's claim to safely assess fragmented sensitive material is increasing its prominence. It protects data privacy across sources and makes it possible to train models globally on a little server. The confidentiality of all patient data is ensured by FL, as it combines training data from several clients without explicitly disclosing any data.

5G is proposed as the underlying network architecture for the interconnection of medical devices in the ambitious healthcare 5.0 concept [46], [47], [48]. This paradigm goes beyond only patient health to prioritize global well-being and quality of life by utilizing data from the Internet of Things to promote digital wellness. In healthcare 4.0, the problem of safe and smooth data transfer is of the utmost importance. As the cornerstones of healthcare 5.0, AI and automation will transform many occupations. Advancements in intelligence include a wide range of AI-powered products, from accurate illness detection to remote patient monitoring. These developments are based on ML, which allows for automated prediction. The phrase "smart health system" encompasses the tremendous technical developments in healthcare, including smart homes, the IoT, and healthcare itself. Unanswered questions mostly arising from complex privacy issues continue to plague healthcare organizations' efforts to employ blockchain-based FL. To fully use FL in the healthcare arena, innovative solutions to these difficulties are crucial.

While integrating FL and blockchain technology offers promising advancements in healthcare, several critical security gaps demand immediate attention:

1) **Hyperparameter Vulnerability:** Storing model hyperparameters directly on the blockchain makes them vulnerable to possible abuse. This may result in the compromised confidentiality of sensitive clinical data utilized for training the model.
2) **FL Deception:** Malicious individuals may provide false medical data from various sources into the FL process. This has the potential to result in biased training outcomes and imprecise illness forecasts.
3) **Disincentivized Data Sharing:** The current absence of incentive for medical devices to collaborate with the FL system in sharing data and computational capabilities is hindering its effectiveness.
4) **Intrusion Detection Gap:**The lack of a strong Intrusion Detection System (IDS) exposes the healthcare system to potential threats such as illegal access or data modification.
5) **Unsecured Key Exchange:** Existing key exchange techniques in blockchain technology may be vulnerable to eavesdropping, putting the security of cryptographic keys used for data encryption at risk.
6) **Limited Key Management:** Depending merely on periodic key switching may not be adequate to protect against sophisticated assaults. There is a need for a key management system that is more dynamic and capable of self-healing.
7) **Inefficient Neural Key Exchange:** The existing procedure for coordinating neural key exchange procedures inside the FL framework may be ineffective and jeopardize secrecy.

The existence of these security weaknesses underscores the need for further research and progress in areas such as secure storage of hyperparameters, anomaly detection to ensure data integrity in FL, and to enable fast key exchange. In order to create a healthcare system that is secure and dependable, it is crucial to tackle these vulnerabilities, while simultaneously using the potential of FL and blockchain technology.

This research introduces a novel approach to forecasting diseases and identifying breaches in healthcare 5.0 through the application of FL and blockchain technology. Presented below is a comprehensive examination of the primary contributions:

1) **Federated Deep Extreme Machine Learning (FDEML) Framework:** The system introduces a healthcare 5.0 architecture that integrates FL with blockchain to create a proposed framework. This framework facilitates collaboration across multiple devices (network edges) while ensuring secure and efficient training of a highly accurate disease prediction model.
2) **Secure and Collaborative Training:** The proposed FL-blockchain architecture offers centralized oversight of the entire training process, guaranteeing model integrity. It also leverages data from various healthcare institutions to build a more robust and generalize model.
3) **Enhanced Privacy:** The proposed technique incorporates a novel noise-modification approach that balances model accuracy with data privacy during training. This adds an extra layer of protection for sensitive medical data within the blockchain-based FL system.
4) **Local Simulation and Data Insights:** FL empowers local healthcare institutions to perform simulations and gain deeper insights from their clinical data.
5) **Smart Hybrid Strategy for Secure Interaction and Surveillance:** The system employs a hybrid approach that combines FL with other techniques to enhance secure communication and efficient health monitoring.
6) **IDS for Healthcare 5.0:** The proposed system incorporates a dedicated IDS for health sector that strengthens privacy and security by identifying potential threat trends.
7) **Security Evaluation:** The paper rigorously evaluates the security of the FL-guided smart health network against the three key security objectives: confidentiality, integrity, and availability.
8) **Security Efficiency:** The paper demonstrates that the proposed approach prioritizes data security and privacy while maintaining efficient resource utilization.
9) **Model Accuracy:** The research investigates and identifies the most accurate system model for disease forecasting and IDS within an intelligent healthcare environment.
10) **Key Generation using Blockchain ANNs:** The system leverages a novel key generation technique that utilizes synchronization within ANNs [49], [50] on the blockchain platform. This method creates encryption keys from the synchronized weights of the ANNs, eliminating the need for a secure key exchange channel.
11) **Faster Key Generation:** Compared to existing key generation methods, the proposed approach demonstrates significantly faster key generation times using techniques like Random Walk Learning (RWL) and Anti-Hebbian learning.
12) **Comparison with Existing Work:** The key interchange techniques that are outlined by Dong and Huang [51], Sarkar [52], Jeong et al. [53], Teodoro et al. [54], and Dolecki and Kozera [55]

were examined in this research. This paper also examines their weaknesses.

This analysis emphasizes the fundamental benefits of the suggested system, with a specific focus on its strong points in terms of security, privacy, collaborative training, and efficiency for illness prediction and IDS in the healthcare 5.0 sector.

The primary objectives of this proposed strategy are listed below:

- **Client-Side System Design:** Implement the FDEML algorithm for a user-friendly client-side system for healthcare monitoring.
- **Smart Patient Management:** Design a smart strategy for patient identification, health tracking, and severity assessment.
- **Intrusion Detection:** Integrate an IDS to monitor data flow and identify security threats.
- **IoHT Integration:** Leverage and enhance existing IoHT applications to maintain health standards.
- **FL for Model Improvement:** Utilize FL to boost the effectiveness of the disease prediction model.
- **Model Training and Refinement:** Train the model on disease datasets and a pre-trained architecture for improved performance. Conduct additional testing with real-time datasets to evaluate model accuracy.
- **Data Privacy:** Ensure patient privacy by keeping locally collected data confidential.
- **Model Evaluation:** Assess the deployed prediction system using FL. Compare model output with other ML models for validation.
- **Disease Prevention:** Aim to prevent the spread of chronic diseases through early detection and monitoring.
- **Comparative Analysis on Datasets:** Evaluate the proposed approach's performance across various datasets.
- **ML Validation:** Test and analyze datasets using different ML methods to support the proposed strategy.
- **Technical Advancements for FDEML:** Provide a comprehensive examination of technical improvements relevant to the FDEML system, offering new perspectives on diverse implementations (e.g., healthcare data sharing).

The structure of this document is delineated as follows: Sections II and III focus on current pertinent research and the proposed methodology. The observations and analysis are described in Section IV of this article. The conclusion and future scope of the work are presented in Section 5.

II. RELATED WORK

There has been an increase in "blockchain" usage in recent times among proponents of smart healthcare, and various academic studies have looked at potential uses for the technology. Aggarwal et al. [56] looked on the combining transactions, allocation of investments and home healthcare distribution as they related to the healthcare industry. There are several potential block chains uses in the smart home sector. A thorough examination of the several block chain applications of a P2P network for exchanging resources was provided by Andoni et al. in their article [57]. The research gives in-depth data on the application and abilities of a number of intelligent home networks, including security concerns with smart grids, analysis big data, payment options and AI and came to the conclusion that issues with smart houses, such security and financial planning for smart cities, were not appropriately addressed by the research. For the IoT, Li et al. [58] proposed a blockchain topology centered on the client to ensure the security of data transmission. Zhou et al. [59] investigated different decentralized computing, predefined investigation, and block chain strategies to shift control on certain vehicles and improve their performance. A clever strategy for predicting diabetes illness that is based on deep learning and data fusion principles was proposed by Ihnaini et al. [60]. The suggested method can increase the efficiency of the suggested system in accurately forecasting and advising this life-threatening situation while also reducing unneeded pressure on the system's computational resources. Ultimately, a diabetes prediction model is developed using an ensemble ML technique. Today, data may be easily transmitted across several networks, enabling professionals and organizations to maximize the potential of current tools while satisfying societal medical needs. The IoT enables users to obtain robust and effective healthcare services. The effective monitoring of community healthcare demand has been made possible by the deployment of smart sensors. Numerous biological processes may be monitored with wearable technology. To make sure that medical services are provided to such persons in an effective way, some can be incorporated to check various body systems. Good illness prediction may be achieved by scrutinizing, pooling, and mining the data gathered in this way [61]. For older folks, Khan et al. [62] proposed innovative healthcare services that were centered on the patients' genuine requirements and issues. The experts used ML techniques to more effectively meet the fundamental requirements of geriatric healthcare. Xu et al. [63] offered an overview of FL techniques, focusing specifically on their applicability in the field of biomedicine. The text discusses the implications and potential benefits of healthcare, and provides an analysis and description of the general solutions for statistical challenges, machine challenges, and security issues that are inherent to FL and related technologies. It also summarizes how bibliometric imaging and Web of Science (WOS) were utilized to apply ML and bioinformatics technology in the smart healthcare sector [64]. An analysis center on the top research-producing nations, the main research topics, money sources, and academic hub in this area. In order to forecast the phases of breast cancer, Siddiqui et al. [65] used deep learning and the information fusion method network. Decision-based integration was employed to enhance the accuracy of the recommended approach. Hospitalization forecasting was made into a supervised classification problem by Dai et al. [66], which opened up a wide range of

TABLE 1. Proposed method versus state-of-the-art approaches: a comparative analysis.

Authors	Type of Data	Predictive Model	Decision Making	Fused Decision Making	Healthcare 5.0 Paradigm	Use of Blockchain	IDS's use	FL's use
Bing et al. [15]	Medical Records	Yes	Yes	No	No	Yes	No	No
Liu et al. [30]	Medical Records	Yes	Yes	Yes	No	No	No	No
Ihnaini et al. [60]	Medical Records	Yes	Yes	Yes	No	No	No	No
Khan et al. [62]	Medical Records	Yes	Yes	No	No	No	No	No
Liu et al. [17]	Medical Records	No	No	No	No	Yes	No	No
Siddiqui et al. [65]	Medical Records	Yes	Yes	Yes	No	No	No	No
Chang et al. [72]	Medical Records	Yes	Yes	No	No	Yes	No	No
Proposed Model	Sensor data	Yes	Yes	Yes	Yes	Yes	Yes	Yes

potential medical cost reduction opportunities. Son et al. [67] employed a Support Vector Machine (SVM) approach to evaluate medication adherence in individuals with heart conditions. Tariq et al. [68] devised an AI-based heterogeneous fusion technique to predict the severity of COVID-19 using existing medical data. Sedik et al. [69] developed an approach for feature extraction and utilized CNN (Convolution Neural Networks) and convolutional LSTM techniques to identify Corona virus. Qayyum et al. [70] devised a system that uses clustered fuzzy logic for assessing clinical visual information at the edge. This approach allows distant hospitals to use multi-modal data while ensuring security. Brisimi et al. [71] utilized FL to address distributed sparse SVM difficulties. Expected successful treatments for cardiovascular disease sufferers. However, the aforementioned centralized training systems need the gathering of private medical data in a single data set, which poses a challenge owing to information privacy issues. Instead, A decentralized architecture known as FL develops. Which promotes collaborative learning while keeping sensitive data on end devices local, offering a private solution for integrating various medical data sources. According to Chang et al. [72]'s proposal, blockchain-based FL solution for intelligent medical care may be used by MIoT devices to completely use the scattered medical data while border nodes maintain the block chain to stay away from losing information. Table 1 demonstrates that several recent studies on FL intelligent healthcare.

TABLE 2. Weighing the benefits and cons of state-of-the-art approaches.

Authors	Identified Issues	Research Findings	Shortcomings
Alwarafy et al. [73]	Security issues in edge computing.	Edge computing shifts data processing from the core network to the network's edge, near the clients	Suffers from privacy.
Wang et al. [74]	The primary cloud tier was where the majority of the previous IDS was installed.	This did not adequately address safety standards for real-time medical diagnostics data protection.	If the intrusion is not identified in a timely manner, the Internet of Things applications and systems would sustain irreparable damage.
Latif et al. [75]	It was investigated how FL affected the advancement of digital technology.	Without the need to centralized or exchange information, the issues surrounding the confidentiality of medically personal information were highlighted.	Additional practical strategies and research are required to counter the poisoning attack on FL.
Lim et al. [76]	Offers FL for edge network	Edge-assisted IoT offers reduced latency, enhanced flexibility, data confidentiality, and improved service quality.	Trust deficit.
Agrawal et al. [77]	Confidentiality is jeopardised when personal information is uploaded to a central location, yet it is essential in order to train the central model.	This one failure point compromises both the operations' standards and the confidentiality of the information.	Lots of time is required by the core IDS. The 5G/6G network makes it costly to gather many types of data, including texts, speech, movies, and augmented and virtual reality data.
Zhao et al. [78]	When providing medical services, maintain patient data confidentially..	This results showed that the recommended method has a respectable multi-task prediction accuracy and decreases preparatory time costs similarly to centralised training.	This recommended model must optimize the DNN architecture in order to get past Internet of Things constraints.
Rajendran et al. [79]	Safeguard the confidentiality of user information in medical services.	Proposed FL algorithms: Logistic Regression (LR) and Artificial Neural Network (ANN)	Suffers from MITM attacks.
Alkadi et al. [80]	The advantages of employing blockchain technology for IoT applications within the healthcare industry.	Internet of Things networks based on IDS can be used to detect intrusions into a centralised virtual infrastructure.	Data poisoning and inference problems persist as a result of centralized training, which raises issues 5 regarding privacy.

Table 2 details the advantages and disadvantages of the present approaches.

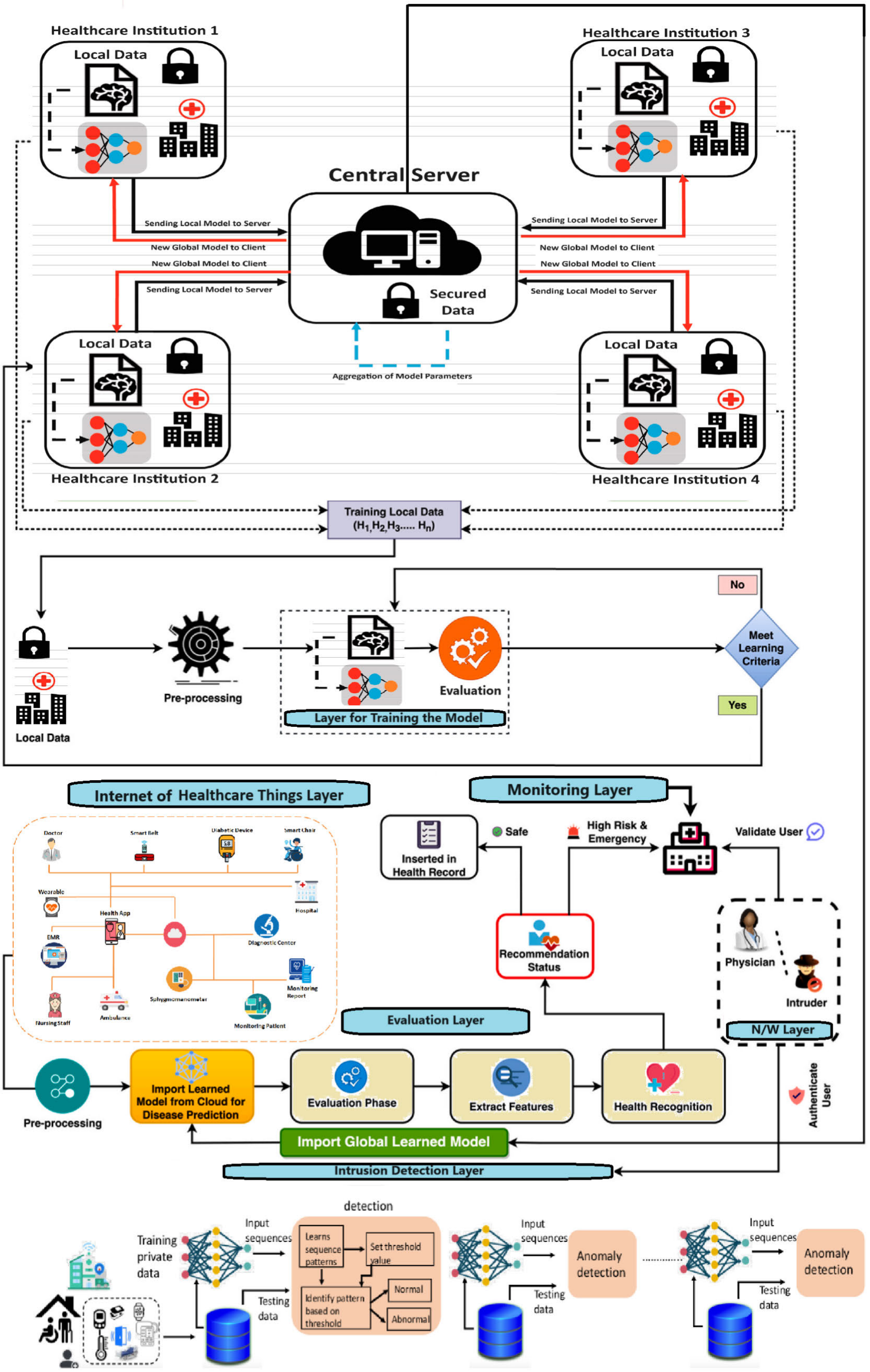

FIGURE 1. Overview of proposed blockchain-enabled federated deep extreme ML-based disease prediction and IDS on IoHT.

III. PROPOSED METHODOLOGY

The security of patient information is a top priority in a network of interconnected smart hospitals that use federated ML to forecast the spread of disease and identify intrusions on IoHT equipment. The safe authentication and provenance tracking of data is made possible by blockchain technology. By combining patient data gathered from IoHT devices with FL, this method helps urban hospitals predict the onset of diseases. Data integrity, veracity, and auditability are protected by the blockchain. Furthermore, intrusion detection systems are employed to identify and thwart possible cyberattacks directed at IoHT devices and private patient information. Figure 1 shows the overview of proposed blockchain-enabled federated Deep Extreme ML-based disease prediction and IDS on IoHT.

Implemented Techniques:

- **Federated Deep Extreme Machine Learning:** Deep learning models are trained collaboratively on patient data residing at individual hospitals without directly sharing the data. This protects patient privacy while enabling institutions to benefit from a broader dataset for improved model accuracy.
- **Blockchain Authentication:** A consortium blockchain is established between participating hospitals. IoHT sensor data and model updates are cryptographically signed and recorded on the blockchain using neural generated key to ensure data integrity and prevent unauthorized modifications.
- **Consortium Blockchain Details:** Hospital A is a sizable urban medical facility equipped with a sophisticated IoHT infrastructure. Hospital B is a regional medical center that is renowned for its use of wearable health technologies and telemedicine. Clinic C and D are outpatient clinics that specialize in the management of chronic diseases utilizing Internet of IoHT sensors. Hospital E is a community hospital that focuses on assuring a wide range of data sources and conducting scalability testing.
- **Blockchain Infrastructure:** The blockchain is constructed using Hyperledger Fabric, guaranteeing a sturdy and expandable infrastructure with safe data exchanges.
- **Access Control:** Participation is restricted to approved nodes, and smart contracts are used to enforce rules and permissions.
- **Consortium Governance:** A governance structure oversees the functioning of operations, data sharing agreements, and privacy policies, with periodic audits to verify adherence to regulations. Data sharing involves the sharing of anonymized data and model changes over the blockchain. This process promotes teamwork and improves the ability to make accurate predictions.

The following different phases illustrate the execution of the proposed method.

Phase 1: Data Acquisition and Preprocessing

- **IoHT Sensors:** Wearable sensors and medical devices collect patient data (e.g., vitals, blood sugar).
- **Data Preprocessing:** Hospitals perform local data cleaning, normalization, and feature engineering on their respective datasets.

Phase 2: FDEML

- **Model Training:** Each hospital trains a local deep learning model on its preprocessed data.
- **Model Updates:** Model updates (weights, gradients) are encrypted and shared with a central server.
- **Federated Aggregation:** The central server aggregates the encrypted model updates without decrypting them.
- **Global Model Update:** The aggregated update is used to improve a global model.
- **Iteration:** Repeat all the above steps for multiple training rounds.

Phase 3: Blockchain Integration

- **Data Signing:** Hospitals cryptographically sign the preprocessed data and model updates using their private keys.
- **Blockchain Ledger:** Signed data and updates are submitted to the consortium blockchain for verification and storage.
- **Consensus Mechanism:** Blockchain nodes achieve consensus on the validity of transactions through a mechanism like Proof-of-Authority (PoA), where only authorized hospitals can participate.
- **Immutable Record:** Verified data and updates become permanent and immutable entries on the blockchain.

Specific Technologies:

- Various permissioned blockchain systems, such as Hyperledger Fabric or Ethereum consortium blockchain, are utilized.
- An anomaly-based Intrusion Detection System (IDS) is utilized to monitor blockchain activity and detect any suspicious trends.
- Federated datasets for disease prediction are constructed by utilizing pre-existing healthcare dataset to safeguard patient confidentiality.

Testing Adequacy:

- The solution underwent thorough testing utilizing IoHT data that accurately represents real-world patient situations.
- FL simulations were performed to assess the rate at which the suggested models converge, their correctness, and their ability to preserve privacy.
- Security checks are conducted on the blockchain platform and IDS deployment to provide resilience against attackers.

Results and Efficacy:

- **Disease Prediction:** Simulations have shown that proposed models trained on federated datasets achieve higher accuracy in predicting diseases compared to models trained on individual hospital data. This is due to the increased diversity and volume of data available through federation.
- **Intrusion Detection:** Blockchain-based tamper detection and immutable data logs enable effective IDS for IoHT devices. By monitoring blockchain entries, healthcare providers can identify and respond to suspicious activities that might indicate security breaches.

- Federated models demonstrated equivalent or superior accuracy compared to centralized learning methods, while maintaining data privacy.
- Blockchain technology has been successful in safeguarding electronic health information and guaranteeing data integrity in healthcare applications.

Section III-A explores the topic of matrix-valued neural synchronization for the purpose of key generation in blockchain. Section III-B examines the use of blockchain technology to allow federated deep extreme machine learning for disease prediction and intrusion detection on the IoHT.

A. NEURAL SYNCHRONIZATION FOR KEY GENERATION IN BLOCKCHAIN

The advent of blockchain technology has heralded a new era in data storage security and privacy, with far-reaching implications for many different businesses. Many beneficial features are offered by blockchain, which is based on decentralization, immutability, and the idea of a digital ledger. Blockchain technology relies on a consensus process and smart contracts to operate. In its block format, blockchain records all completed transactions and functions as a decentralized database. Important information including participant details, price, and timestamps are included within blocks that enclose each transaction. Despite their anonymity, every node in the decentralized blockchain network takes part in validating transactions.

There are two basic hash rules that every block in the blockchain ecosystem must follow: the previous hash and the present hash. The first one points to the block that came before it, while the second one specifies which one we're looking at right now. Secure and private data transmissions are guaranteed by this cryptographic framework. If the contents of any block are changed, all related data must be changed within a certain time limit. Cryptographic keys and transaction protocols strengthen the network's defenses by facilitating the complex connectivity of blocks. Blocks are thoroughly validated by miner nodes before they are added to the blockchain. They use strong mathematical procedures to ensure that the data remains intact and unaltered.

The special combination of anonymity and openness is at the heart of blockchain technology. Transactions are formed by adding new blocks to old ones, resulting in a coherent network of autonomous devices that are managed by shared technology. All transactions are carefully recorded by this network, including the identity of the participants and the intricacies of each transaction. There are a few different ways in which blockchain networks function; they include public, private, and consortium chains. Without a governing authority to keep an eye on things, miner nodes in permissionless or public blockchain networks confirm transactions. On the other side, different use cases necessitate different permissions and governance frameworks for private and consortium chains.

1) MINER NODES

a: ROLE AND FUNCTION

Within consortium blockchain, miner nodes have the task of verifying transactions and incorporating them into the blockchain. This consortium employs a permissioned methodology, which sets it apart from public blockchains such as Ethereum and Bitcoin. In contrast to the competitive solving of cryptographic problems by miners in public blockchains, our approach involves a different method.

b: CONSENSUS MECHANISM

Our network utilizes a Byzantine Fault Tolerance (BFT) consensus mechanism, specifically designed for permissioned networks. This technique guarantees the achievement of consensus, even in the presence of nodes that are defective or acting with malicious intent.

c: OPERATIONAL NODES

Each institution (Hospital A, Hospital B, Clinic C and D, and Hospital E) operates one or more mining nodes. These nodes verify transactions, guaranteeing the integrity and consistency of data throughout the network.

2) ADMIN NODE

a: ROLE AND RESPONSIBILITIES

The administrator node is responsible for supervising the blockchain network, handling permissions, and keeping a comprehensive record of all participants. This node enforces access control to restrict network membership and transaction submission to approved entities.

b: ACCESS CONTROL

The administrator node implements access controls according to pre-established permissions. Every organization that takes part is allocated distinct roles and permissions, which determine their degree of access and activities inside the blockchain.

In consensus procedures, miner nodes are crucial for ensuring the integrity of blockchain networks, as demonstrated by well-known instances such as Ethereum and Bitcoin. An administrator node in a consortium blockchain network keeps tabs on all the data and transactions, and they let people in according to their permissions. Some data is accessible to all users while other data is restricted to certain user groups, depending on the needs of the organization. Even while they aren't totally decentralized, these networks do hold both public and private data. As an example, Hyperledger Fabric guarantees the secrecy of data and the safety of transactions by placing an emphasis on privacy in private blockchain networks. Only the administrator node may add new users to the network, and only authorized users can access the information. The strong privacy characteristics offered by blockchain platforms such as Hyperledger and multi-chain networks make them a perfect alternative for protecting sensitive clinical information. This study demonstrates how

Hyperledger Fabric and blockchain technologies implement stringent security procedures to protect patients' medical records. Digital healthcare data is carefully tracked and monitored using the Hyperledger Fabric, which provides insights at specified timestamps in real-time. Building a recommendation system from the ground up while protecting sensitive information is the major objective of this undertaking. In addition, the document includes a suggestion module that uses patients' medical records to create unique treatment programs. With the use of ML models trained on the information, patients may receive highly personalized advice.

One novel technique uses synchronized matrix-valued ANNs as blockchain security keys. Two neural networks are started with random weight vectors in ANN synchronization, an interesting example of online learning [81], [82], [83]. They share information, calculate outputs, and analyze a shared input vector at each time step. Their weights are adjusted according to the input-output matching through the use of suitable learning techniques. Achieving full synchronization in a minimum number of phases, this strategy allows non-continuous weights to coordinate rapidly. Full synchronization as an absorbing state is shown by the matched weights in both networks converge even after future learning rounds. Because a third neural network may be trained using instances, results, and input vectors generated by this technique, its applicability extends beyond only synchronization. Like a student network, this neural network doesn't interfere with other networks and can function alone. The synchronization and learning processes of perceptrons, the basic neural networks, are quite similar. But an interesting thing happens with more complicated ANNs: a third network that isn't actively learning from each other synchronizes at a slower pace than two networks that are actively reacting to communication. Figure 2 describes the neural synchronization technique for key generation in blockchain.

Our solution to the blockchain's key-exchange problem takes use of the interplay between one-way and two-way exchanges. Coordinating the ANNs of A and B allows for the quick construction of a shared session key, surpassing any attempts by adversaries. The security landscape is shaped by both players and adversaries in the area of neural cryptography, where ANNs boast several layers. In Figure 3, it is evident that repulsive steps are more probable in $A's$ neural network when it outperforms $D's$ or $E's0 \ < p < \ 1$, under equal overlap conditions. Consequently, partners in neural cryptography, D and E, gain a considerable edge over a basic attacker. However, as the number of participants, L, increases, this advantage diminishes. Hence, a significant number of hidden nodes affect the confidentiality of the neural keys interchange agreements versus a basic assault. There is a correlation between the type of the connection between neural networks $\langle \triangle p_d \rangle$ and $\langle \triangle p_x \rangle$ and the tendency for attracting as well as repel movements. As a consequence of this, these values are of major relevance in neural cryptography for distinguishing between collaborators and adversaries.

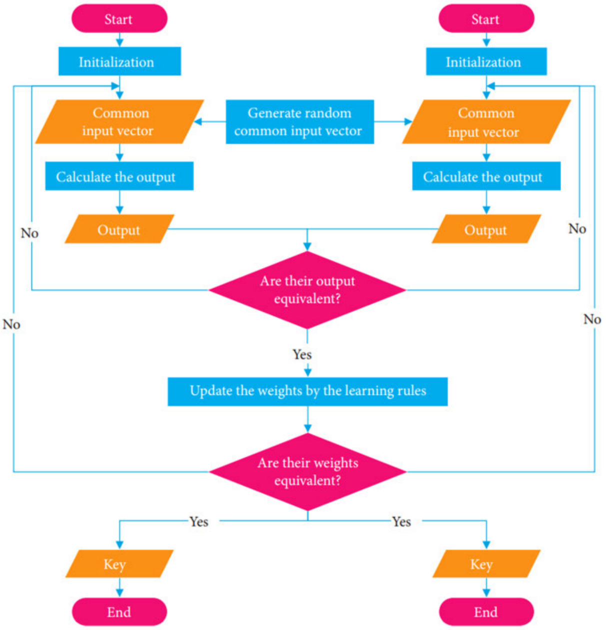

FIGURE 2. Flowchart of neural synchronization for key generation in blockchain.

The area of artificial neural synchronization is focused on achieving simultaneous learning and adaptation among numerous neural networks. Nevertheless, the process of achieving synchronization is not always without difficulties, and there may be instances where the networks diverge instead of coming together. These instances are referred to as repulsive steps. Here is an analysis of how the presence of two interconnected hidden units with different outputs might initiate a repulsive step, and how this is tied to the generalization error. Envision two interconnected concealed units (one from each network) that are intended to be "synchronized" - indicating that they should ideally provide the same result for a given input. Nevertheless, if these units exhibit disparate outputs (for instance, one unit produces a 0 while the other unit produces a 1), it may indicate a discrepancy between the networks. Generalization Error in the context of ML, is the measure of how effectively a trained model performs when presented with new, unknown data. Within the framework of neural synchronization, the generalization error of a hidden unit serves as an indicator of its ability to accurately represent the underlying information it is intended to acquire. A large generalization error indicates that the unit is not effectively recording the information with accuracy. If two interconnected hidden units exhibit disagreement in their outputs, it indicates the possibility of substantial generalization error. This discrepancy might initiate a "repulsive step" in the learning algorithm.

The learning algorithm may attempt to modify the weights inside the network in order to increase the similarity between the disagreeing units. Nevertheless, in the event where

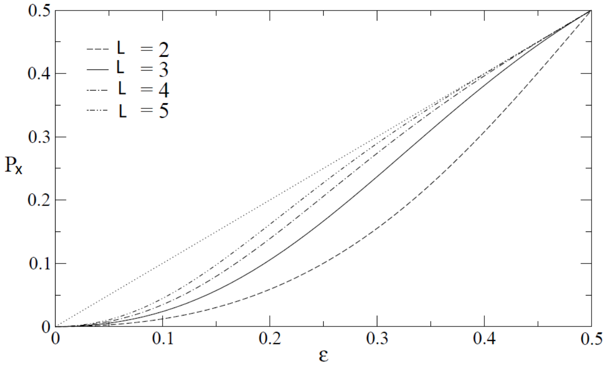

FIGURE 3. Methods that are unappealing for achieving synchronization with interactions.

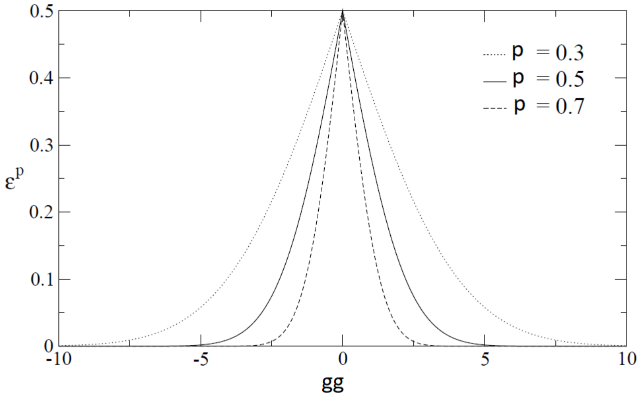

FIGURE 4. Prediction error.

both units exhibit substantial generalization errors, merely modifying weights may not be sufficient to attain genuine consensus. This can result in the learning process choosing a repulsive step, which causes the networks to move farther away from each other. Essentially, the large generalization error of the units that are in disagreement serves as an indication that the existing method of synchronization is ineffective. Subsequently, the learning algorithm endeavors to make adjustments, but the presence of significant inaccuracy might result in a momentary deviation in the incorrect direction. For details see Technical Annex 1.

As an illustration of the likelihood $P_x^E(p)$ of repelling phases for synchronization with engagement $\psi^D = \psi^E$, Figure 3 depicts the scenario of a basic attack, which is shown by the dotted line $P_x^A(p)$.

Meanwhile, Figure 4 showcases the prediction error $\ni_q^o$ as a function gg_q^A of the local field for distinct values of the overlap p_q^{DA} *and* $Q_q = 1$.

Figure 4 shows that P_x^A grows in relation to the amount of hidden units. At the beginning of the coordination procedure, nevertheless, the geometric assault is not as successful as the regular assault.

Thus, the pattern resembles what is observed in Figure 3, where P_x^A remains greater than P_x^E for identical L. In Figure 5, the likelihood of unpleasant steps for a geometric attacker is illustrated. The simple attack P_x is shown by the line with dots.

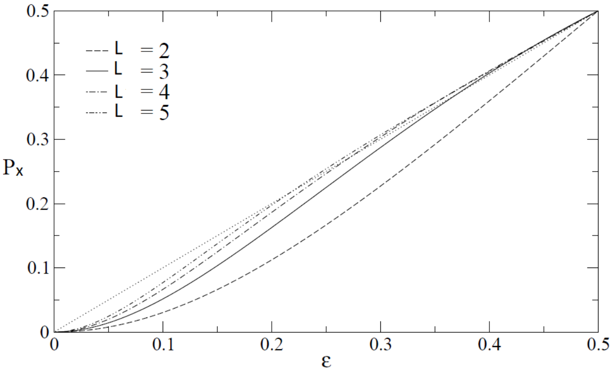

FIGURE 5. Geometric attacker.

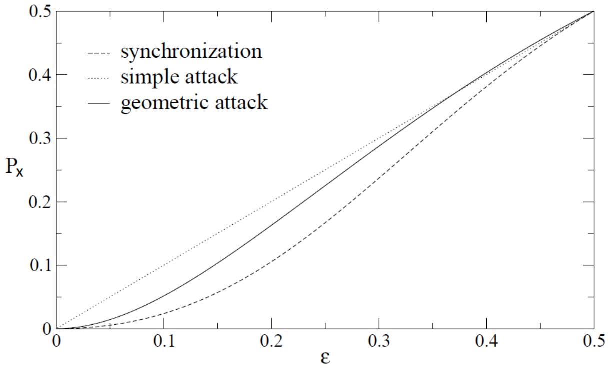

FIGURE 6. Repulsive step probability for neural networks.

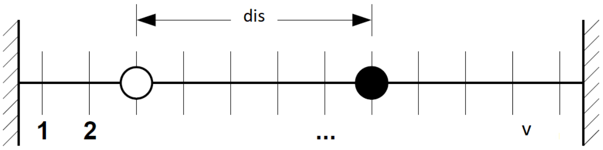

FIGURE 7. Simple model for a pair of weights.

Figure 6 illustrates the chance of encountering repulsive steps in neural networks with different types of connection ($L = 3$) and varying numbers of hidden units.

In each attracting phase, the synaptic weights of both neural networks travel the identical direction, which is selected with same chance in the arbitrary walk learning to process. As said, within the border $M \rightarrow \infty$, both Hebbian and anti-Hebbian learning are viable. The coordination process is naturally disrupted by disruptive actions. These actions have minimal impact when there is only a slight overlap, and they occur infrequently in cases of significant overlap. As an outcome, repulsive steps may be overlooked in certain cases, and a series of arbitrary walks with reflective bounds, driven by identical arbitrary signals, can be used to define neuronal synchronization. Consequently, Figure 7 illustrates a simple model with a few weights.

Figure 8 shows the values of the coefficients $g_{v,1}$ *and* $g_{v,v-1}$ as a function comprises m. The dashed curve represents the estimated value.

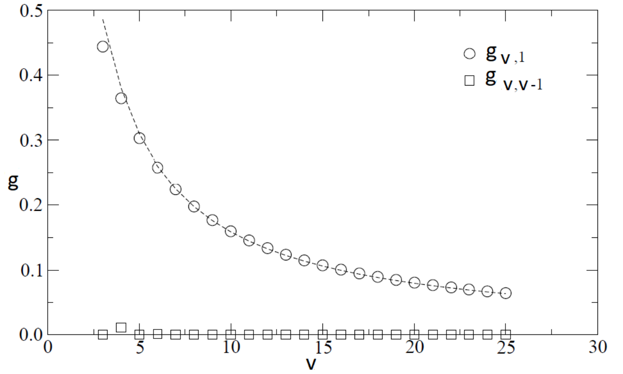

FIGURE 8. Coefficient values.

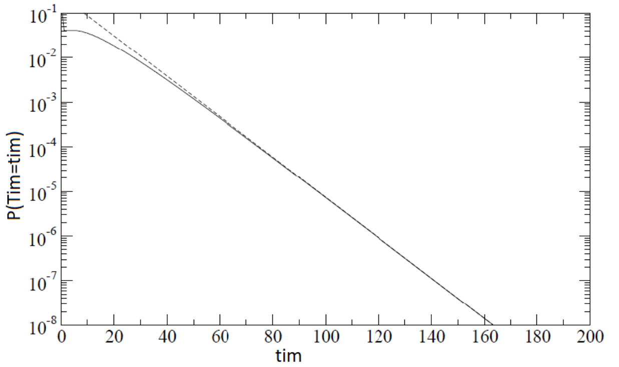

FIGURE 9. Probability distribution.

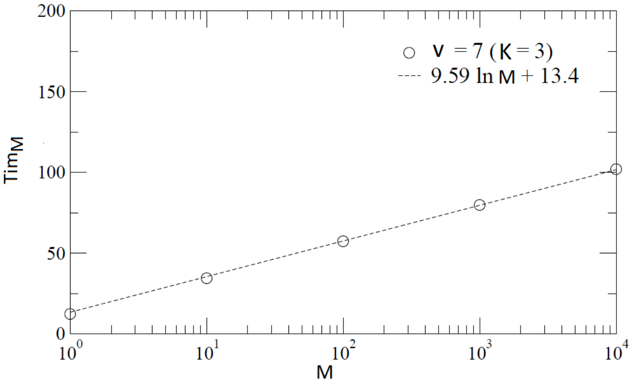

FIGURE 10. Average synchronization time.

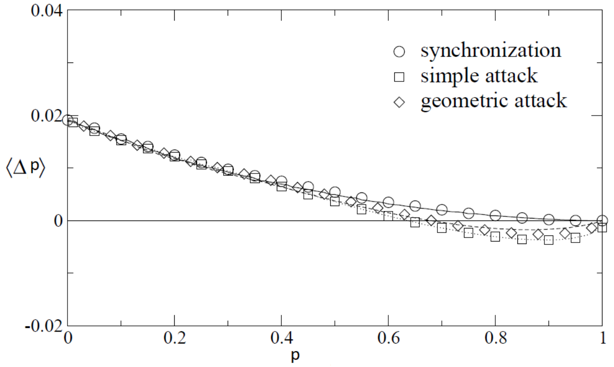

FIGURE 11. Contrast between synchronization and learning.

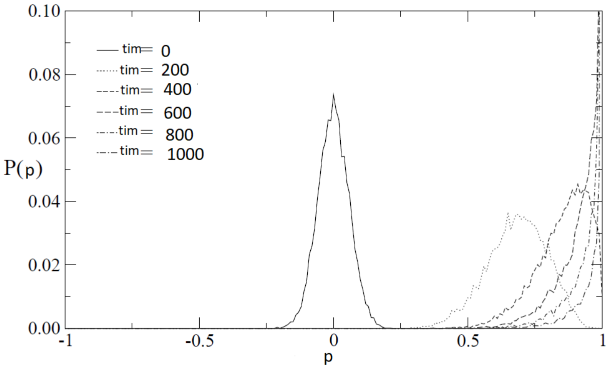

FIGURE 12. Overlap distribution at various time intervals.

Figure 9 depicts the probability distribution for synchronization time $P(Tim = tim)\, for\ v = 7\ (K = 3)$.

Figure 10 shows the mean time of synchronization $< Tim_M >$ as a function comprises M is for $v = 7\ (K = 3)$. The computation's numerical results are displayed by circles. The Grey line represents the Tim_M anticipated value.

Figure 11 depicts the average change in overlap has been estimated for $L = 3$, $K = 5$, and the arbitrary walk learning method. The symbols represent the outcomes of thousands of simulations, while the lines were created.

Figure 11 illustrates the contrast between learning and synchronization. In the context of bidirectional communication, $L = 3, < \triangle p >$ the process is often good until it reaches the absorption stage, where$p = 1$. In the event of unidirectional traffic, though. In the communication, there is a specific point at $p_f < 1$. As an outcome, an increase in only fluctuations allows for the overlap to continue. As a conclusion, the synchronization process is influenced by two unique types of dynamics.

Every updating of the weights has a pleasing impact on mean if $< \triangle p >$ is consistently positive for $p < 1$. In this situation, repulsive paces hinder the synchronization process, but the dynamics are controlled by appealing steps. As a consequence, it has a comparable appearance to the random walks. The OD(overlap distribution) draws near to the absorbing condition at $p = 1$. With every time steps, as shown in figure 12.

The speed of this operation is also crucial. Figure 12 shows the overlap distribution at various time intervals. Figure 12 further demonstrates that the overlap of neurons changes dramatically during neural synchronization process. Interactions between discrete variables, on the other hand, amplify later variations. Figure 13 depicts the two neural networks with the arbitrary walk learning algorithm and the possibility distribution of the sync period with $L = 3$, $l = 3$, $M = 1000$.

The solid arc is a fitting of the Gumbel distribution, and the histogram shows the comparative rate of occurrence identified through 10,000 runs.

Figure 14 depicts the early transient as well as the quasi-stationary situation. Figure 14 shows the overlap distribution

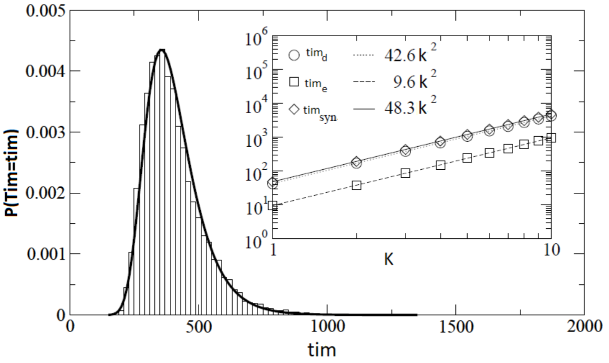

FIGURE 13. Two neural network's arbitrary walk learning algorithm and the likelihood distribution of the coordination period.

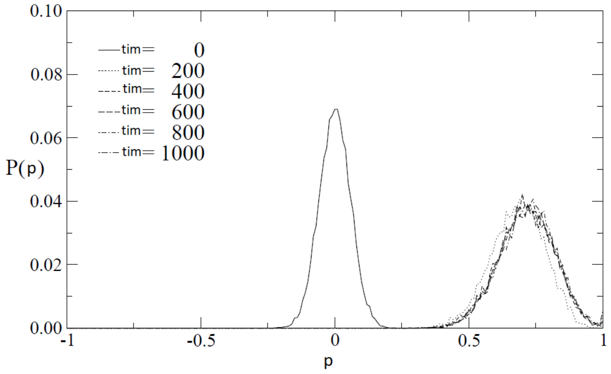

FIGURE 14. Distribution of overlapping at different times.

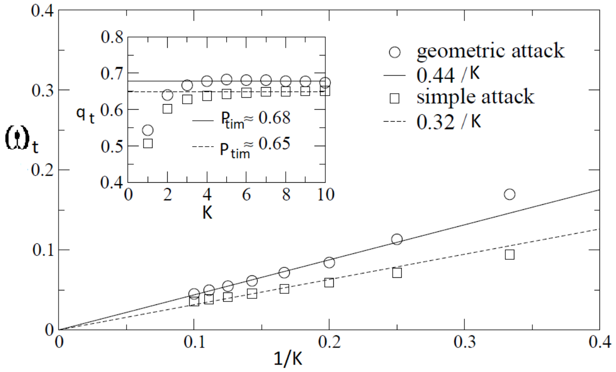

FIGURE 15. At the specific place, the standard deviation.

at various time intervals. These findings were obtained after a hundred simulations for geometric assault using $L = 3$, $l = 5$, $M = 100$, and the arbitrary walk training method. The $\xi(tt)$ are arbitrary variables with a variance of one and a mean of zero.

Figure 15 depicts the standard deviation at the particular moment$L = 3$, $M = 1000$ using the random walk learning approach and one-way synchronization, averaged accrossed 10,000 runs. The fixed point's location is displayed in the inset.

When there is a larger synaptic depth. Regardless of the fact that this basic model corporate the more intricate components of $< \Delta p(p) >$, the scaling nature is adequately recreated

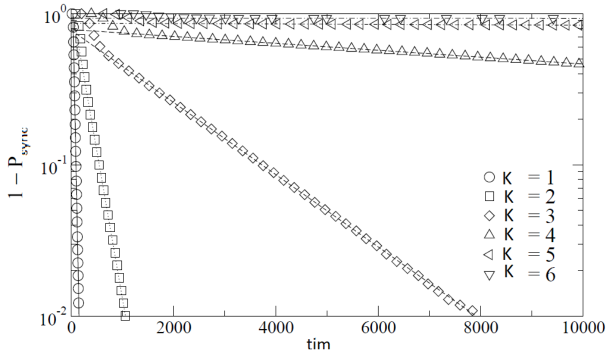

FIGURE 16. Random walk learning method, geometric attack, and probability distribution.

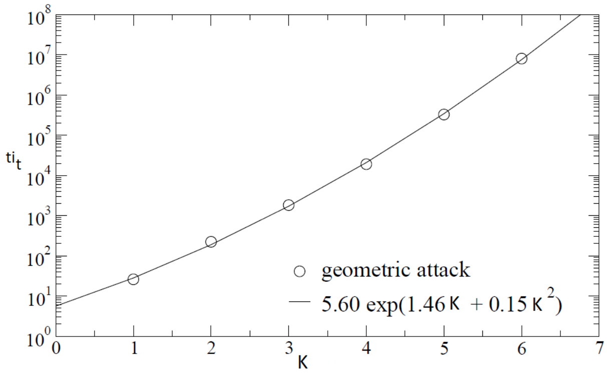

FIGURE 17. Time is employed for synchronization via fluctuation.

in figure 15. For small values of K finite-size effects cause deviations.

Random walk learning method, geometric attack, and probability distribution for figure 16. The lines show how the symbols fit together, while the symbols indicate findings averaged across 1000 runs. Figure 17 depicts the time constant tim_f is employed for synchronization via fluctuations. 1000 geometric assault simulations using$L = 3$, $M = 1000$, and the random walk learning approach are shown by symbols.

As a response, parties D and E, by selecting l, it is possible to reduce the difficulty of assaults on the neural key-swap protocol. Alternatively, if D maintains the same level of effort, her odds of success fall linearly as synaptic depth grows. The geometric attack as well as sophisticated techniques show this influence.

B. BLOCKCHAIN-ENABLED FEDERATED DEEP EXTREME ML-BASED DISEASE PREDICTION AND IDS ON IOHT

1) DEPLOYMENT OF A BLOCKCHAIN MODULE

In 2008, blockchain technology emerged, consisting of a decentralized network of independent nodes that maintained a secure and time-stamped ledger of important documents [84]. Within the blockchain environment, a block contains a multitude of transactional data. The current blocks inside the blockchain architecture are usually examined by candidates before they dive into blockchain investigation. The method that verifies the validity of a block is known as proof of work. In what follows, you will learn the ropes of blockchain technology. Node after node in an Intelligent Medical Software (IMS) that has an Internet connection has to communicate with a database and the people who create and maintain the blockchain. All current transactions are painstakingly recorded by the blockchain until they are ready to be validated within a new block. Merkle trees provide for the rapid inspection and analysis of a large number of transactions. Blockchain technology has the potential to create new links in the smart medical ecosystem due to its flexibility and interoperability with IoHT applications.

Healthcare 5.0 refers to the upcoming era of healthcare systems that include advanced technology to improve patient care, operational efficiency, and data security. Key components encompass the incorporation of cutting-edge technology such as AI, IoT, blockchain, and bots. It focuses on individualized, anticipatory, proactive, and collaborative healthcare. It Improves integration and compatibility among different healthcare systems and equipment.

Blockchain is a decentralized technology that manages a constantly expanding list of documents, known as blocks, which are securely connected via encryption. Every block consists of:

a: DATA

This research focuses on the storage of important information on the blockchain, including disease prediction findings and access logs for revisions to the FDEML model.

b: HASH

An exclusive cryptographic fingerprint that represents the content of the block. Any alteration to the data included in the particular block will result to an alteration of the hash, so serving as indisputable proof of manipulation.

c: PREVIOUS BLOCK HASH

"The previous block hash referencing" is the value of the hash corresponding to the block which appears before this one in a list of blocks in order. The purpose of this chain is to keep the data's security.

The following Figure 18 describes the overview of blockchain-enabled FL.

d: BENEFITS OF BLOCKCHAIN

- **Security and Immutability:** Blockchain's cryptographic properties ensure its robust resistance to illegal alteration or tampering, enhancing security and immutability. Ensuring the integrity of illness prediction findings and the audit trail of model modifications is of utmost importance.
- **Decentralization:** In contrast to conventional centralized databases, a blockchain network does not have a single point of failure. This improves the robustness of the system and decreases the likelihood of a single security compromise jeopardizing the entire system.

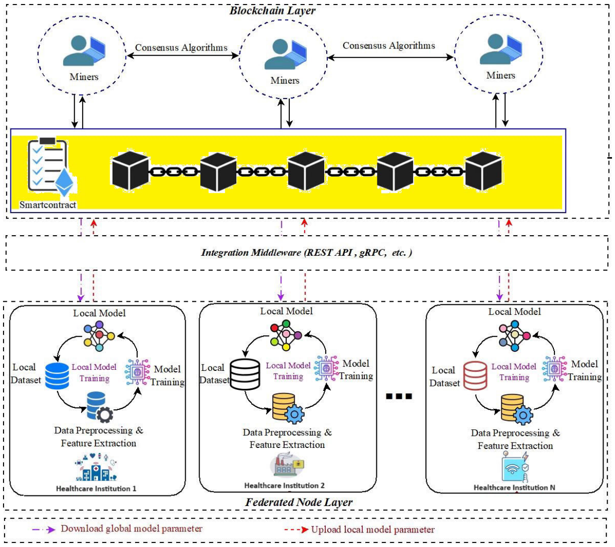

FIGURE 18. Overview of blockchain-enabled federated learning.

- **Transparency and Traceability:** Every member in the network has the option to obtain a copy of the blockchain, which allows for clear visibility into the disease prediction process and revisions to the model.

e: TESTING CONSIDERATIONS

- Each member of the network has the choice to acquire a duplicate of the blockchain, enabling them to have a transparent view of the illness prediction process and any modifications made to the model.
- This technique utilizes a permissioned blockchain platform specifically designed for healthcare applications. These platforms offer faster transaction processing times and lower energy consumption compared to public blockchains.
- Blockchain technology presents a viable method for improving the security, transparency, and traceability of the proposed disease prediction system based on FDEML.

f: NODE COMMUNICATION

- Nodes in the network collect data from IoHT devices. This data is cryptographically signed to ensure authenticity and integrity.
- Once data is collected and signed, it is submitted to the blockchain network. Each transaction includes metadata for validation and traceability.
- Secure communication protocols are used to convey data between nodes and the blockchain in order to avoid eavesdropping and unwanted access.

g: TRANSACTION RECORDING

- Initially, all transactions are recorded in a transaction pool. The purpose of this pool is to serve as a temporary storage space for transactions until they are prepared for validation and inclusion in a new block.

- The validation process involves miner nodes verifying transactions via the use of the Byzantine Fault Tolerance (BFT) consensus mechanism. This process entails verifying the cryptographic signatures and confirming that the data satisfies predetermined requirements.

h: BLOCK FORMATION

After a series of transactions has been verified, they are consolidated into a new block. Subsequently, this block is appended to the blockchain, guaranteeing a consecutive and unalterable log of every transaction.

i: DATABASE SYNCHRONIZATION

The blockchain ensures the consistent and simultaneous updating of a shared ledger among all participating nodes. The local database of each node is synced with the blockchain, guaranteeing uniformity and current records throughout the network.

2) IMPLEMENTATION OF FEDERATED DEEP EXTREME MACHINE LEARNING

Simplifying data analysis tasks and providing useful insights are the goals of the proposed data analytics platform suggested here. Quick analysis of real-time data yields dynamic insights through the use of the proposed approach. Along with its primary function, the suggested model has additional applications in the areas of consumption of energy forecasting, inventory management enhancement, and transportation operation outline [85].

The proposed method proves its versatility in healthcare networks by cleaning up datasets and fixing mistakes. Its innovative method has great promise for the future of healthcare, especially in the areas of early disease detection and diagnosis. Evaluating the proposed model's performance in adaptive forecasting for healthcare monitoring is the main goal of this effort. Figure 19 depicts the different information flow in FL.

FL's incredible dependability in managing fragmented sensitive information is a major reason for its meteoric rise in popularity. FL enables organizations to retain their data on-site whilst training an all-encompassing framework on a common server, as contrast to conventional methods that need data integration from several sources. Importantly, FL makes it possible for different places to participate in training the global model. FL ensures the confidentiality of patient information by merging training datasets from many sources in a way that prevents direct exchange of data. After that, using patient data, each organization builds its own model. Then, each institution uses the model's error gradient in its communication with the server. After receiving input from every user, the central server modifies the global model according to established standards. The model evaluates the replies' quality and includes only relevant data based on these established criteria. As a result, organizations' feedback on poor or unusual results may go unnoticed. The global model is refined iteratively by means of this method, which produces a single FL cycle.

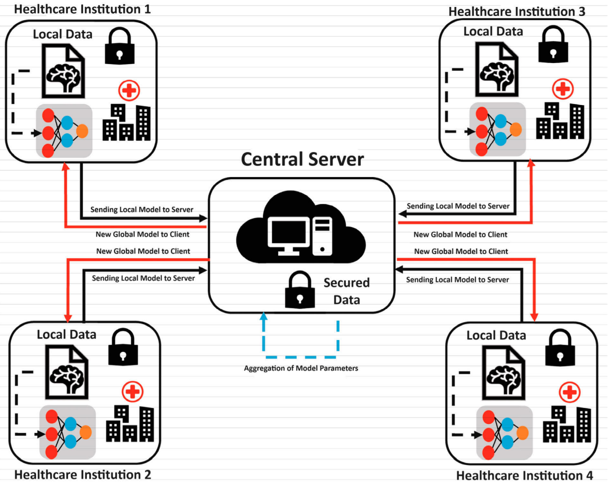
Healthcare Institution 1
Local Data
Healthcare Institution 3
Local Data
Central Server
Sending Local Model to Server
New Global Model to Client
New Global Model to Client
Sending Local Model to Server
Sending Local Model to Server
New Global Model to Client
New Global Model to Client
Sending Local Model to Server
Secured Data
Aggregation of Model Parameters
Local Data
Healthcare Institution 2
Local Data
Healthcare Institution 4

FIGURE 19. Information flow in federated learning.

a: LOCAL MODEL ALLOCATION AND CONVERSION

Clinics choose a model that is local to them and feed it training data. After then, it's up to a central server to send over the local model so it may be accessible by all IoHT devices worldwide.

b: TRAINING PHASE COMPONENTS

The training phase comprises the sensing, reprocessing, and application layers, each serving distinct functions.

c: ADDRESSING INCOMPLETE OR INACCURATE DATA

IoHT devices may acquire medical information that is incomplete or inaccurate. The pre-processing layer mitigates this issue by addressing missing data using techniques like moving mean and standardization to reduce noise.

d: DATA TRANSMISSION AND PROCESSING

After preprocessing, medical infor0mation is transmitted to the application layer. This layer includes additional divisions such as the Prediction Layer and Performance Layer.

e: CALCULATING PARKINSON'S DISEASE DETECTION

Equations 1 and 2 are utilized to calculate whether Parkinson's disease has been identified or not.

f: ASSESSMENT OF LEARNING CRITERIA

Findings from the forecasting layer are relayed to the performance layer through the prediction layer. The accuracy and error rate of the prediction layer are used by the performance layer to determine if the learning conditions have been fulfilled.

g: MODEL RETRAINING OR DEPLOYMENT

If the learning requirements are not met, the model undergoes retraining. Alternatively, when the prerequisites are met, a proficient local model is migrated to the cloud as a versatile model.

h: UPDATING LOCAL MODELS AND ENSURING PATIENT CONFIDENTIALITY

Health institutions are provided with the global model, which they utilize for training purposes utilizing data specific to their locality. Each institution maintains a constant level of patient privacy by modifying its local version on the cloud without directly transmitting datasets.

i: CREATION AND DISTRIBUTION OF GLOBAL MODEL

In the cloud, a fresh global framework is built by merging the previously adjusted parameters that were supplied by the institutions that are working together. Following this, the global model is disseminated to all of the institutions that are collaborating.

j: RELIABILITY OF DATA FUSION

The results obtained from a data fusion strategy are more reliable and consistent in comparison to those obtained from a single source of information.

k: DATA EXCHANGE AND GLOBAL MODEL TRAINING

The application submits an inquiry for the exchange of data to the main node, which grants connection upon receiving the request. Once access has been authorized, nodes will collaborate to train a global data model using FL. Once the model has been trained, the data provided by the client will get the associated sharing outcomes when the model has been completed.

l: VALIDATION AND MONITORING

During the validation stage, input layer variables are identified and sent to the evaluation stage for medical monitoring.

3) IMPLEMENTATION OF INFORMATION FUSION MODULE

The idea behind this method is that a network of sensors can collect more data and make more accurate observations than any one sensor could on its own. To get the most out of data, it is best to gather it from several sources and combine it. This process is called data aggregation. Due to the availability of different network security sensors, it can be tough to achieve a thorough picture of the dynamic security environment within a security system. Problems might also arise when trying to manage equipment that is spread out across a large region. If we want to make models better and analyze the system's security state thoroughly, we need to integrate sensor data well. Because it comes from several channels, data used from multiple sources can provide more dependability and consistency.

An integral part of the IoT, sensors are vital for assessing smart healthcare systems, surroundings, and consumers. This class includes a wide range of items that handle sensor data, such as cameras, healthcare monitors, and interactive tools. A sensor in a heart rate monitor, for instance, can work in tandem with other medical devices to control the heart's rhythm. Connected wearables and closed-circuit systems are part of the IoHT's application layer [86].

4) IMPLEMENTATION OF IDS

For reliable evaluation of the healthcare system, a comprehensive IDS is required. You may efficiently analyze different types of data using the proposed approach. Thanks to its decoupled data flow design, this ML software can keep an eye on data streams and identify patterns of intrusion or assault. The management of intelligent blockchain-based systems, which are always evolving, need algorithms that are both robust and flexible. Presenting an intelligent and safe architecture for healthcare networks, the suggested method tackles both the existing and future problems with centralized security. This research makes a significant contribution by thoroughly investigating scientific breakthroughs that are pertinent to healthcare systems 5.0.

In the context of the proposed system that combines FL, blockchain, and IDS for disease prediction on IoHT devices, the Integration of IDS is discussed as follows:

a: MONITORING FOCUS

The IDS would primarily monitor activities within the system related to the FL process and blockchain interactions. This includes:

- Unauthorized access attempts to the central server or blockchain network.
- Tampering with model updates during the FL training process.
- Any anomalies within the model update data on the blockchain.

b: ALGORITHM CONSIDERATIONS

Lightweight and efficient algorithms are preferred for IoHT devices due to their resource constraints. Here are some potential options:

- **Signature-based IDS:** This approach identifies malicious activity based on pre-defined patterns or signatures of known attacks. It's efficient but might not be effective against novel threats.
- **Anomaly-based IDS:** This type of IDS monitors for deviations from normal system behavior. It can be more adaptable to new threats but requires careful configuration to avoid false positives.
- **Hybrid IDS:** Combining signature-based and anomaly-based approaches can offer a balance between efficiency and adaptability.

IDS are strategically placed at every node in the network to actively monitor and analyze both incoming and outgoing traffic, with the purpose of identifying and assessing any possible security risks or threats. Proposed IDS use ML algorithms to detect trends and abnormalities that may indicate possible security breaches. The models undergo training using past data and are regularly updated to effectively respond to emerging threats. The IDS conducts real-time monitoring of network traffic. It examines packets to identify recognized attack signatures and detect abnormal behavioral patterns. When the IDS detects an abnormality or possible unauthorized access, it produces alerts and can initiate automatic replies. These reactions may involve the implementation of measures such as blocking IP addresses that are deemed suspicious, terminating connections that are identified as malicious, or raising the matter to network administrators for further action. IDS alarms and logs are seamlessly integrated with the blockchain, ensuring that any security events are documented in a way that cannot be tampered with, thereby creating an indisputable audit trail. This connection improves the level of openness and accountability. The IDS utilizes open-source frameworks, including Snort for signature-based detection and unique ML techniques for anomaly detection. The proposed solutions have been tailored to meet the particular requirements of our IoHT network, guaranteeing exceptional performance and precision in identifying intrusions. Continuous improvement is a key aspect of the IDS models. They are consistently updated with new threat information and retrained using up-to-date data to ensure their efficacy in countering changing security threats.

5) INFORMATION FLOW BETWEEN THE FDEML, BLOCKCHAIN, AND IDS IN THE PROPOSED SYSTEM

It's crucial to clearly explain the information flow between the FDEML, blockchain, and IDS in the proposed system. Here's a breakdown of how each component interacts:

a: DATA COLLECTION AND FDEML TRAINING

- IoHT devices collect patient medical data (e.g., heart rate, blood pressure).
- This data remains local on the devices or edge servers within the healthcare facility.
- FDEML comes into play here. Local models are trained on the device-resident data. These models learn to identify patterns associated with specific diseases without directly exposing the raw data.

b: MODEL UPDATES AND BLOCKCHAIN INTEGRATION

- The FDEML process generates local model updates containing the learned knowledge, not the original medical data.
- The encrypted model changes are sent to a centralized server.
- The central server collects the encrypted updates from numerous devices in order to generate a global model update.
- This global update is then stored on a permissioned blockchain, providing a secure and tamper-proof audit trail.

c: DISEASE PREDICTION AND INTRUSION DETECTION

- The revised global model is disseminated to the devices that are taking part. Devices leverage the updated model to perform local disease prediction on new patient data.
- Importantly, all disease predictions occur on the devices themselves, ensuring patient data privacy.

d: INTRUSION DETECTION SYSTEM (IDS)

- The IDS component monitors the entire system for any suspicious activity, such as unauthorized access attempts or data breaches.
- The IDS can utilize information from the blockchain, such as access logs and anomaly detection within the model update process, to identify potential security threats.
- If an intrusion is detected, the IDS can trigger appropriate actions, such as alerting security personnel or isolating compromised devices.

This illustrates the maintenance of data security and privacy throughout the whole system. The FDEML method guarantees that only the knowledge derived from the data (model updates) is exchanged, while the blockchain offers a safe and auditable platform for storing and overseeing these updates. The IDS functions as an extra level of protection by continuously monitoring the entire system for any possible threats.

6) DATASET DESCRIPTION

For disease assumption investigation, this paper used the Parkinson's disease dataset [87], and for intrusion detection, we used the NSL-KDD dataset [88]. Several changes that were important to the initial data gathering procedure for KDD 99 are now part of the NSL-KDD dataset, which is an updated version of the KDD 99 dataset. The NSL-KDD dataset has 41 characteristics per item. A total of 195 occurrences of extended vowel phonations have been identified from a total of 31 individuals, 23 of whom were diagnosed with Parkinson's disease. With "non-PD" representing healthy people and "PD" representing Parkinson's Disease cases, we hope to distinguish between the two groups in our data analysis.

Nonetheless, there are distinct justifications for selecting the Parkinson's Disease Data Set (Parkinson's - NSL-KDD Database) as the appropriate option for the preliminary stage of our investigation:

The dataset, known as the Parkinson's - NSL-KDD Database, is tailored specifically for distinguishing between individuals who are healthy and those who have Parkinson's disease. This specific concentration is in accordance with our original purpose to introduce a healthcare 5.0 architecture that leverages blockchain technology to establish a

Algorithm 1 Global Model at Server

```
Begin
Initialization of $P^{k}_{G\,fml}$ & $Q^{k}_{G\,fml}$
Here, $P^{k}_{G\,fml}$ & $Q^{k}_{G\,fml}$
delineates the weight situated at the server, serving as the link between the input and the $z$
hidden layer neurons, along with connecting the $z$
hidden layer to the $z + 1$hidden layer neurons.
For each $k$ to $I$ do
    $U_k \leftarrow$ (Different client from $n$)
    a) for every client $i \in U_k$ parellely do $\left[P^{n}_{k+1}, Q^{n}_{k+1}\right] \leftarrow$ Client Training $\left(n,\ P_{k,}Q_k\right)$
    End For;
    $P^{k}_{G\,fml} = \frac{1}{\sum_{n\varepsilon\eta}} \sum_{n=1}^{N} \frac{U_n}{U} P^{k}_{n+1}$ (Average Aggregation)
    $Q^{k}_{G\,fml} = \frac{1}{\sum_{n\varepsilon\eta}} \sum_{n=1}^{N} \frac{U_n}{U} Q^{k}_{n+1}$
End For
End
```

Federated Deep Extreme Machine Learning framework. This framework is not only constructed by a highly accurate collaborative system spanning numerous network edges but also effectively overseen the entire learning process.

A variety of clearly specified biomedical voice measures are contained within the dataset, ensuring the accuracy and significance of the data for studying vocal features linked to Parkinson's disease.

Validation and making our algorithms more widely applicable by testing them on a bigger dataset that includes hundreds of patients and covers various illnesses are deemed essential. Our upcoming research stage will involve the utilization of datasets such as a larger Parkinson's disease dataset or a dataset containing numerous disorders.

The results of this preliminary investigation on the Parkinson's - NSL-KDD Database demonstrate the practicality and efficiency of our suggested algorithms under controlled conditions. This establishes a solid basis for conducting more extensive assessments on a broader scale and including a greater variety of neurological disorders.

7) APPLICATION OF THE PROPOSED MODEL

Incorporating proposed computational technology into FL-based systems can boost their intelligence and data privacy all at once. It is possible to build a network architecture and a platform for decentralized blockchain applications by using proposed distributed blockchain technology [89]. This research examines proposed model's deployment architecture and highlights its possible uses. Utilizing sensors, mobile devices, and IoHT systems as data sources is the optimal approach for leveraging this technology for intelligence gathering. These techniques generate valuable data that fuels intelligent software. To top it all off, proposed model is a real-time data processing powerhouse, making analysis and forecasts a breeze [90].

Algorithm 2 Local Model at Client

```
Begin
Partition the local records into $U$-size mini batches.
Initialize the weights of the two layers $\left(p_{ij}\ \&\ q_{jk}\right)$, $E$ (Error) = 0 and total epochs $\varepsilon = 0$
For each training data $q$
    a) the feed-forward step will be implemented to
        i) evaluate $\varphi_j$ using equation 1.
        ii) evaluate $\varphi_k$ using equation 2.
    b) evaluate the error signals of output and hidden layer.
    c) perform weight adjustment $p_{ij}$ & $q_{jk}$(using backpropagation)
Go to step c if stopping criteria is not met.
$\left(p_{ij}\ \&\ q_{jk}\right)$.
Get back on the server the best weights for a locally trained model
End
```

Duplicate entries, incomplete entries, malfunctions, and interference are minimized in the process of data generation for research objectives. In particular, proposed model excels at working with tiny data sets, and its flexible structure makes it possible to enable a wide range of applications, such as fraud prevention and detection.For the purpose of enhancing health surveillance applications, the framework that we have described makes use of a variety of hidden layers, neurons, and activation methods. The method is composed of three essential stages: gathering data, getting ready, and evaluating. Sensors and actuators painstakingly gather initial data, keeping it in its raw form for further processing. Then, to make sure there are no errors or contradictions in the data, a strong preprocessing layer cleans and prepares it thoroughly.

In order to demonstrate how the recommended model works, the following is provided:

a: MODEL OPERATION

The model functions through a collaborative process involving IoHT devices, a central server, and participating healthcare institutions.

1. Local Model Training:

After deciding on a local framework, hospitals load it with patient-specific data used for training. This local model is then uploaded to a central server, potentially granting access to all IoHT devices within the network (depending on the system design).

2. Data Preprocessing:

IoHT devices might collect incomplete or inaccurate medical data due to sensor limitations or noise. The pre-processing layer addresses these issues using techniques like moving mean and standardization to reduce noise and compensate for lost data.

3. Feature Extraction and Prediction:

The two sub-layers that make up the application layer receive medical data after pre-processing: Prediction Layer:

This layer calculate the probability of Parkinson's disease for each patient. Performance Layer: This layer evaluates whether the learning criteria are met based on the prediction layer's accuracy and error rate.

4. Model Updation and Sharing:

If the performance layer determines insufficient accuracy, the local model undergoes retraining. Conversely, if the model performs well, it's uploaded to the cloud as a "universal model."

b: FL FOR PRIVACY-PRESERVING COLLABORATION

For hospitals and clinics interested in taking part, this "universal model" is a good place to begin. Every institution uses its own data to train the model, and they don't share that data with each other. This method refreshes the cloud-based local model while protecting the privacy of the patients.

c: GLOBAL MODEL IMPROVEMENT

After all institutions have submitted their modified parameters, a new global model is generated. The use of data fusion in this method has the ability to produce more consistent and trustworthy outcomes than would be possible with a single data source.

d: DATA ACCESS AND MODEL TRAINING WITH FL

Healthcare institutions can request data exchange from the central server. Upon granting access, institutions collaboratively train a global data model on the server using FL. Institutions then receive the updated model for further use.

e: MODEL VALIDATION

During the validation stage, relevant data points are collected and sent for evaluation to confirm the model's effectiveness for medical monitoring.

As detailed in Algorithm 2, the proposed model integrates six hidden layers, an input layer, and an output layer. The backpropagation process for each patient, as outlined in the algorithm, involves several stages, such as weight initialization, feedforward, error backpropagation, and updates of weights and biases. Every single neuron in the deep layer uses a function known as sigmoid activation. The proposed system is formally represented by equation 1.

$$\varphi_{ij} = \frac{1}{1 + \mathfrak{e}^{-(b_1 + \sum_{n=1}^{h}(p_{ij} * d_i))}} \tag{1}$$

Within this context, $j = 1, 2, 3, \ldots, n$ and d_i serve as variables representing the input values, while b_1 assumes the role of bias, essential for adjusting the output. Meanwhile, h embodies the multitude of input neuronal nodes contributing to the neural network's processing power. As for j, it embodies the comprehensive tally of neurons nestled within the hidden layer, pivotal for the network's complexity and capacity for information processing. Equation 2 emerges as a pivotal tool, offering a glimpse into the intricate activation function governing the behavior of the output layer, thereby illuminating the neural network's decision-making process.

$$\varphi_k = \frac{1}{1 + \mathfrak{e}^{-(b_2 + \sum_{j=1}^{n}(q_{jky} * \varphi_j))}} \tag{2}$$

Equation 3 shows that $k = 1, 2, 3, \ldots, n$ and the hidden layers are represented by y.

$$E = \frac{1}{2}\sum_k (\tau_k - \varphi_{ky=6})^2 \tag{3}$$

Above, we see the representation of E for backpropagation error, with τ_k and φ_k standing for anticipated output and forecasted outputs, correspondingly. The layer is composed of (equations 4 and 5), and the resultant weight changes continuously in equation 4.

$$\Delta P \alpha - \frac{\delta E}{\delta P} \tag{4}$$

$$\Delta q_{jky} = -\varepsilon \frac{\delta E}{\delta q_{jky}} \tag{5}$$

The above equation may be rewritten as equations 6 when the chain rule of thumb method is applied.

$$\Delta v_{jky} = -\varepsilon \frac{\delta E}{\delta \varphi_{ky}} \times \frac{\delta \varphi_{ky}}{\delta q_{jky}} \tag{6}$$

Equations 7 and 8 demonstrate how to determine the modified weight quantity by substituting the data from equation 6.

$$\Delta q_{jky} = -\varepsilon \left(\tau_k - \varphi_{ky}\right) \times \varphi_{ky}\left(1 - \varphi_{ky}\right) \times \varphi_j \tag{7}$$

$$\Delta q_{jky} = \varepsilon \xi_k \varphi_j \tag{8}$$

where, $\xi_k = \left(\tau_k - \varphi_{ky}\right) \times \varphi_{ky}\left(1 - \varphi_{ky}\right)$

The rule of chains (equations 9 and 10) is used to preserve the weights of the input and layers that are hidden.

$$\Delta p_{ij} \alpha - \left[\sum_k \frac{\delta E}{\delta \varphi_{ky}} \times \frac{\delta \varphi_{ky}}{\delta \varphi_j}\right] \times \frac{\delta \varphi_j}{\delta p_{ij}} \tag{9}$$

$$\Delta p_{ij} = -\varepsilon \left[\frac{\delta E}{\delta \varphi_{ky}} \times \frac{\delta \varphi_{ky}}{\delta \varphi_j}\right] \times \frac{\delta \varphi_j}{\delta p_{ij}} \tag{10}$$

Represents the constant in equation 11, which is seen previously.

$$\Delta p_{ij} = \varepsilon \left[\sum\nolimits_k \left(\tau_k - \varphi_{ky}\right) \times \varphi_{ky}\left(1 - \varphi_{ky}\right) \times \left(q_{jk}\right)\right] \times \varphi_{ky} \times \left(1 - \varphi_{ky}\right) \times \alpha_i$$

$$\Delta p_{ij} = \varepsilon \left[\sum\nolimits_k \left(\tau_k - \varphi_{ky}\right) \times \varphi_{ky} \times \left(1 - \varphi_{ky}\right) \times \left(q_{jk}\right)\right] \times \varphi_j \times \left(1 - \varphi_j\right) \times \alpha_j$$

$$\Delta p_{ij} = \varepsilon \left[\sum\nolimits_k \xi_k \left(q_{j,ky}\right)\right] \times \varphi_j \times \left(1 - \varphi_j\right) \times \alpha_i \tag{11}$$

The previous equation may be represented after being simplified (equation 12).

$$\Delta p_{ij} = \varepsilon \xi_j \alpha_i \tag{12}$$

where, $\xi_j = \left[\sum_k \xi_k \left(q_{j,ky}\right)\right] \times \varphi_j \times \left(1 - \varphi_j\right)$, $q^{+}_{j,ky} = q_{j,ky} + \lambda \Delta q_{j,ky}$ and $\lambda$is the rate of learning.

The formula previously mentioned is used to change the outcome and hidden layer weights, whereas equation 13 is used to alter the input and hidden layer weights.

$$P^{+}_{j,k} = P_{i,j} + \lambda \Delta P_{i,j} \tag{13}$$

8) INTRUSION DETECTION SYSTEM

The NSL-KDD dataset [87] served as the foundational cornerstone for the identification of any unauthorized access attempts within a system. This dataset was meticulously leveraged in conjunction with advanced healthcare technology 5.0, complemented by FL methodologies, to prognosticate the onset of Parkinson's Disease (PD) [88]. To facilitate this predictive analysis, the dataset underwent a random partitioning, with 30% of its content earmarked for cross-validation and testing purposes, while the remaining 70% was dedicated to training the predictive models. Rigorous scrutiny was applied to the data to diagnose instances of Parkinson's Disease (PD) and to pinpoint any occurrences of system intrusion activities.

The efficacy of the proposed methodology was thoroughly scrutinized through the application of various quantitative metrics. These metrics encompassed a comprehensive range of evaluation criteria, including but not limited to, the Miss Rate (as defined by equation 14), Accuracy or Precision (as quantified by equation 15), Specificity (as determined by equation 16), Sensitivity (as articulated in equation 17), True Positive Rate (TPR) (as expressed in equation 18), True Negative Rate (TNR) (as outlined in equation 19), Positive Prediction Value (PPV) (as elucidated in equation 20), and Negative Prediction Value (NPV) (as delineated by equation 21). The ensuing enumeration provides a succinct summary of these critical assessment benchmarks.

$$\mathit{Miss\ Rate} = \frac{\sum_{b=0}^{2}\left(\frac{F_b}{S_{z\neq b}}\right)}{\sum_{b=0}^{2}\left(T_b\right)}, \mathit{where}\ z = 0, 1 \tag{14}$$

$$\mathit{Accuracy} = \frac{\sum_{b=0}^{2}\left(\frac{F_b}{S_b}\right)}{\sum_{b=0}^{2}\left(F_b\right)} \tag{15}$$

$$\mathit{Sepecificity} = \frac{\frac{F_0}{S_0}}{\left(\frac{F_0}{S_0} + \frac{F_0}{S_1}\right)} \tag{16}$$

$$\mathit{Sensitivity} = \frac{\frac{F_0}{V_1}}{\left(\frac{F_0}{S_0} + \frac{F_0}{S_1}\right)} \tag{17}$$

$$\mathit{TPR} = \frac{\mathit{True\ Positive}}{(\mathit{True\ Positive} + \mathit{False\ Negative})} \tag{18}$$

$$\mathit{TNR} = \frac{\mathit{True\ Negative}}{(\mathit{True\ Negative} + \mathit{False\ Positive})} \tag{19}$$

$$\mathit{PPV} = \frac{\mathit{True\ Positive}}{(\mathit{True\ Positive} + \mathit{False\ Positive})} \tag{20}$$

$$\mathit{NPV} = \frac{\mathit{True\ Negative}}{(\mathit{False\ Negative} + \mathit{True\ Negative})} \tag{21}$$

F denotes the predicted output in the equations 14 and 15 whereas S is the actual output. F_0 & S_0 stand for the absence of Parkinson's Disease (PD) and the absence of intrusive activity in the predicted output and actual output respectively. Parkinson's Disease and intrusive activity are indicated by the lettersF_1 & S_1 in the prediction outcome and actual result, respectively. Predictive and actual outcomes are parallel for $F_b = S_b$. Accordingly, F_b $S_{z\neq b}$ represents mistake, where both predicted and actual results are altered.

It is acknowledged that conventional blockchain implementations entail processing requirements due to the mining process. The proposed technique addresses this challenge by considering various factors.

- The proposed method employs FL for the purpose of illness prediction. This method ensures that patient data is stored on local devices, with only model changes being shared with a central server. Storing all medical data on the blockchain imposes a heavy computational strain on the network. However, this burden is greatly reduced by adopting the approach mentioned.
- The proposed method suggests implementing a permissioned blockchain that is especially tailored for healthcare purposes. Permissioned blockchains provide quicker transaction processing and reduced energy usage in comparison to public blockchains that depend on significant mining.
- The blockchain exclusively maintains essential data points, such as illness forecasts and access records, rather than the complete unprocessed medical data. This reduces the processing burden on the blockchain network even further.
- Concerning the scalability of the IDS technique, we acknowledge the necessity for a highly effective system in expansive healthcare facilities.
- This paper investigates the incorporation of lightweight IDS that are especially tailored for IoHT devices with limited resources. These solutions exhibit lower computational and memory requirements in comparison to conventional IDS approaches.
- The suggested design utilizes a central server to handle communication and coordination among IoHT devices, allowing for scalability. The central server may be effectively expanded to meet an increasing number of devices inside a healthcare facility.

Table 3 provides a detailed summary of the secure healthcare 5.0 system that is proposed. Here, during training, the system makes use of FL to predict intrusions. There are a total of 400 data points contributed for training by each of the four Health Institution (HI) sides (HI1, HI2, HI3, and HI4). The data points are carefully classified into recordings of attacks and instances of normal behavior to provide a strong and effective learning process. The

TABLE 3. Examination of safe healthcare 5.0's proposed technology performance entails assessing its capability during system training to predict intrusion detection, leveraging an array of client-side statistical metrics.

Client	Accuracy	Sensitivity	Specificity	Negative Predictive Value (NPV)	Rate of False Positives	Rate of False Discovery	Rate of Falsse Negative
HI1	0.9375	0.9825	0.8261	0.9500	0.1739	0.0667	0.0175
HI2	0.9472	0.9895	0.8407	0.9694	0.1593	0.0600	0.0105
HI3	0.9775	0.9899	0.9417	0.9700	0.0538	0.0200	0.0101
HI4	0.9572	0.9930	0.8636	0.9794	0.1364	0.0500	0.0070

predictive system demonstrates exceptional effectiveness in precisely detecting system intrusions on each client's end. Comprehensive statistical measures, encompassing many performance indicators, are carefully recorded at each client's end during the training period and painstakingly organized in Table 3. The data displayed in Table 3 highlights the efficacy of the suggested method in accurately identifying intrusions on every client's end. In addition, additional statistical measures are calculated and recorded throughout the training phase, enhancing the evaluation of the system's performance and strengthening its capacity to protect against unwanted access attempts. As depicted in Table 3, the metrics provided by each HI client are as follows: For HI1 client: Accuracy approximately 93.75%, Sensitivity approximately 98.25%, Specificity approximately 82.61%. For HI2 client: Accuracy approximately 94.72%, Sensitivity approximately 98.95%, Specificity approximately 84.07%. For HI3 client: Accuracy approximately 97.75%, Sensitivity approximately 98.99%, Specificity approximately 94.17%. For HI4 client: Accuracy approximately 95.72%, Sensitivity approximately 99.30%, Specificity approximately 86.36%.

Table 4 provides a detailed representation of the proposed model, demonstrating its effectiveness in predicting intrusions throughout the validation phase. All four Health Institutions (HIs)—HI1, HI2, HI3, and HI4—contribute 200 records throughout this stage. The records are carefully categorized into sections for both assaults and normal recordings, guaranteeing a fair representation for thorough confirmation. The detection system has exceptional precision in forecasting system intrusions on each client's end, as indicated by the outcomes depicted in Table 4. Moreover, Table 5 presents a collection of statistical measurements used on each HI's side throughout the validation phase, offering a comprehensive understanding of the system's performance. The suggested technique provides accurate evaluations of intrusions at each local node and also gathers support for its effectiveness through additional statistical studies done at the validation level. At the HI1 Client, a remarkable accuracy rate of 95% is attained, together with a sensitivity of 97.30% and a specificity of 88.46.%. Furthermore, the system's capacity to effectively detect non-intrusive events is shown by a Negative Predictive Value (NPV) of 92%. Table 4 provides more information on the system's performance characteristics, including an 11.54% False Positive Rate (FPR), a 4% False Discovery Rate (FDR), and a 2.7% False Negative Rate (FNR). In comparison, HI2 displays accuracy close to 93.50%, sensitivity close to 95.97%, specificity close to 86.27%, NPV of 88%, 13.73% FPR, 4.67% FDR, and 4.03% FNR. HI3 Client showcases accuracy near 96.61%, sensitivity around 98.72%, specificity approximately 90.64%, NPV of 96%, 9.43% FPR, 3.33% FDR, and 1.36% FNR. HI4 client demonstrates accuracy near 94.75%, sensitivity close to 96.81%, specificity around 88.37%, NPV of 90%, 11.76% FPR, 4% FDR, and 3.36% FNR.

TABLE 4. Evaluation of the performance of the secure healthcare 5.0 technology, particularly in the context of intrusion prevention, is conducted through validation on a platform incorporating diverse sets of statistical data from various client sides.

Client	Accuracy	Sensitivity	Specificity	Negative Predictive Value	FPR	FDR	FNR
HI1	0.9500	0.9730	0.8846	0.9200	0.1154	0.0400	0.0270
HI2	0.9350	0.9597	0.8627	0.8800	0.1373	0.0467	0.0403
HI3	0.9661	0.9872	0.9064	0.9600	0.0943	0.0333	0.0136
HI4	0.9475	0.9681	0.8837	0.9000	0.1176	0.0400	0.0336

9) PRACTICAL IMPLEMENTATION OF THE PROPOSED TECHNIQUE

a: SITE SELECTION

The model was trialed at five health facilities, three large hospitals and two outpatient clinics. These were chosen to provide breadth in the type of patients we might see and the IoHT infrastructures supporting them.

b: DURATION

The initial pilot-run lasted for 6-months, a reasonable duration of time to observe how the model functions and bring in improvements iteratively.

c: DATA SOURCES

The dataset had health information from more than 10,000 patients which included data collected from wearable devices, electronic health records and real-time monitoring systems.

d: DATA VARIETY

The data included various types of health indicators such as heart rate, blood pressure, glucose levels, and patient activity logs, ensuring the model's robustness across different health metrics.

e: HEALTH PREDICTION ACCURACY

In each health outcome described, the model correctly predicted the responses in secondary sampling and with comparison to gold-standard data.

f: INTRUSION DETECTION EFFICIENCY

Our IDS element showed higher detection rate, with a low FP and FN rates under controlled penetration testing and real world incident analysis.

g: FL IMPLEMENTATION

We implemented FL using TensorFlow Federated (TFF) framework. A local server for each healthcare facility participated in the process of FL.

h: DATA PRIVACY

This preserved the sanctity of raw patient data at the local servers and only allowed model updates to be aggregated centrally.

i: BLOCKCHAIN FRAMEWORK

A Hyperledger Fabric blockchain was implemented to establish a confidential and robust ledger for recording all transactions. Every healthcare institution served as a node inside the blockchain network.

j: DATA TRANSACTIONS

The blockchain was used to record medical data transactions, model modifications, and IDS alarms, guaranteeing transparency and immutability.

k: NEURAL SYNCHRONIZATION

A tailored synchronization strategy was devised to provide uniform updates across ANNs. The PyTorch library was utilized to construct this protocol, which was then seamlessly included into the federated learning framework.

l: MUTUAL LEARNING

The synchronization system facilitated the exchange of knowledge between blockchain components, guaranteeing uniform and protected actions throughout the network.

m: IDS DEPLOYMENT

IDS were deployed by utilizing a blend of Snort, an open-source network intrusion detection system, and bespoke ML models. The systems were installed at each node and constantly monitored for any irregularities.

n: REAL-TIME RESPONSE

The IDS offered instantaneous notifications and automatic reactions to identified breaches, while maintaining a transparent record of logs on the blockchain for the purpose of auditing.

o: PERFORMANCE LOGS

Comprehensive logs and performance measurements were documented during the pilot operation. The logs provide information on the accuracy of predictions, rates of intrusion detection, the latency of the system, and the integrity of data transactions.

p: USER FEEDBACK

Data from healthcare professionals and IT personnel at the trial sites was methodically gathered and examined. This feedback included qualitative information regarding the system's influence on patient care and operational efficiency.

q: INDEPENDENT AUDITS

External audits were performed to confirm adherence to data privacy standards and to authenticate the reliability of the blockchain ledger and the effectiveness of the IDS.

10) PREDICTION OF DISEASE

Healthcare 5.0 technology and a FL technique are shown in Table 5 as a potential combination for PD prediction during patient authentication. Health Institution (HI) sides HI1, HI2, HI3, and HI4 went through extensive training using regional data to build a global learnt model. The models were subsequently uploaded to the cloud. Afterwards, the suggested system was validated by running an Intrusion Detection System (IDS) access verification and utilizing the global learning model maintained on a centralized blockchain server. At the server side, 200 data points were analyzed during the validation phase and split into positive and negative samples. On the server side, the forecasting algorithm clearly gets quite accurate disease predictions. Statistical data from the authorization phase, including both regional and cloud data, was thoroughly analyzed using the FL approach and shown in Table 5. This action was undertaken to authenticate the effectiveness of the proposed healthcare 5.0 scheme when combined with FL methodologies. As shown in Table 5, the integration of healthcare 5.0 with FL has shown to be highly effective in properly predicting sickness. In addition, the validation step involves the computation of additional statistical indicators. The metrics provided by the HI1 client during validation are highlighted in Table 5. An accuracy score of approximately 92.71%, a sensitivity level of approximately 96.91%, a specificity value of approximately 71.59%, a negative predictive score of approximately 83.33%, FPR of approximately 28.57%, FDR of approximately 5.88%, and FNR of approximately 3.03% are all included in these measures. In validation phase, the HI2 client demonstrates an accuracy rate of approximately 93.10%, a sensitivity rate of approximately 96.58%, a specificity rate of nearly 75.14%, NPV of approximately 80%, FPR of approximately 25%, FDR of approximately 4.71%, and FNR of approximately 3.57%. All of these scores include NPV of approximately 80%. In the meanwhile, the validation metrics for the HI3 client are as follows: a 95.81% accuracy rate, a 97.82% sensitivity rate, an 83.95% specificity rate, an 86.67% NPV, a 16.63% FPR, a 2.94% FDR, and a 2.37% FNR. The results of the verification phase for the HI4 client include an accuracy of approximately 94.67%, a sensitivity of approximately 96.53%, a specificity of 82.84%, NPV of approximately 80%, FPR of approximately 17.24%, FDR of approximately 2.94%, and FNR of approximately 3.51%. The most accurate results may be obtained by switching to the healthcare 5.0 method in the last stage, as opposed to treating each client independently on the server. This strategy suggests the integration of FL methods. During the validation

TABLE 5. Patient diseases prediction is undertaken employing multiple statistical indicators from the server's perspective through the use of the planned healthcare 5.0 system. The findings are reported.

Client	Accuracy	Sensitivity	Specificity	NPV	FPR	FDR	FNR
HI1	0.9271	0.9691	0.7159	0.8333	0.2857	0.0588	0.0303
HI2	0.9310	0.9658	0.7514	0.8000	0.2500	0.0471	0.0357
HI3	0.9581	0.9782	0.8395	0.8667	0.1613	0.0294	0.0237
HI4	0.9467	0.9653	0.8284	0.8000	0.1724	0.0294	0.351
FDEML Framework	0.9800	0.9839	0.9027	0.9000	0.1000	0.0176	0.0176

TABLE 6. Performance evaluation of the recommended structure reliant on provided model for PD estimation was performed utilizing data obtained from studies that have previously been published.

ML Aproaches	Results
Chang et al. [72]	84.5%
Sztah´o et al. [91]	89.3%
Tracy et al. [92]	90.1%
Sheibani et al. [93]	90.6%
Yaman et al. [94]	91.25%
Kuresan et al. [95]	95.16%
FDEML Framework	98%

phase, the FL technique displays an accuracy that is close to 98%, a sensitivity that is close to 98.39%, a specificity that is close to 90.27%, NPV that is close to 90%, FDR that is around 1.76%, and an FNR that is approximately 1.76%.

Table 6 shows how the suggested model compares to other research that has been published. An estimated accuracy rate of 98% is achieved by utilizing the FL approach, which is part of the suggested methodology. Table 6 shows that the suggested technique is more accurate than the alternatives that are already available.

A comparison of synchronization periods between the proposed method and CVTPM methods utilizing Anti-Hebbian coordination is displayed in Table 7. The findings elucidate that the utilization of Anti-Hebbian coordination yields notably expedited outcomes in comparison to alternative strategies, evidenced by a substantially reduced synchronization period relative to CVTPMs. A comprehensive examination is conducted, contrasting the proposed methodology with VVTPM time synchronization techniques incorporating the Random Walk (RW) methodology, as detailed in Table 8. By utilizing the Arbitrary Walk learning algorithm, the proposed method attains synchronization considerably faster than VVTPM.

The frequency test results for the synchronized neural key display a percentage distribution of ones and zeros, yielding a result of 0.703811. This result notably surpasses those reported 0.584326 in [52], 0.538632 in [53], 0.512374 in [51], 0.537924 in [55]. Table 9 outlines the p-value assessments for the frequency strategy.

TABLE 7. Comparison of synchronization timings between the proposed method and CVTPM.

I Value	Proposed Method's Coordination Period in Anti-Hebbian (Cycle)	Syncing Period of CVTPM in Anti-Hebbian (Cycle) [51]
10	724,19	753,09
5	357,34	389,26
15	1092,47	1198,47
25	2381,09	2671,17
20	1637,53	1857,24
30	3123,49	3582,75
35	4419,93	4793,62
40	5705,38	5981,43
45	6660,77	8138,39
50	8782,62	9452,57

TABLE 8. MeasuringSynchronization times: proposed technique versus VVTPM.

I Value	Random Walk Coordination Period of Proposed Technique (Cycles)	Random Walk Coordination Period of VVTPM Technique (Cycles) [53]
5	375,17	426,98
15	1016,46	1163,24
10	671,37	734,54
20	1629,18	1793,17
25	2437,05	2585,02
35	4114,68	4854,23
30	3271,95	3378,16
40	4656,82	5386,81
45	6334,61	7389,08
50	7769,38	8784,19

TABLE 9. The p_value obtained from the frequency test.

Different Technique	p_Value
Proposed	0.703811
VVTPM [53]	0.538632
CVTPM [51]	0.512374
GAN-DLTPM [52]	0.584326
Dolecki and Kozera [55]	0.537924

IV. CONCLUSION AND FUTURE SCOPE

Smart healthcare based on IoHT has recently become a popular way to improve the accuracy of disease prognoses by making better use of medical data. Effective analytic techniques are necessary to facilitate therapy and increase patient care due to the enormous and diverse nature of medical data. There are risks associated with patient privacy breaches and adversarial hurdles to data flow that might undermine the advantages of this method. The development of intelligent healthcare systems has been expedited by the incorporation of AI technology and reactions to infectious disease outbreaks. However, there are still worries about data security, cybersecurity risks, and patient happiness. In response to these issues, our study suggests a groundbreaking solution: healthcare 5.0 privacy-preserving Federated Deep Extreme Machine Learning on IoHT for illness prediction using blockchain and IDS. By disseminating a global learning model via a centralized cumulative service, we zero in on FL as a means to address these concerns. By keeping patient data in the responsibility of local authorities, this strategy guarantees that it will remain discreet and private. The study begins with an overview of the basic steps of the state-of-the-art techniques that were used for this research. Furthermore, we provide a reliable method for creating keys for use in Intrusion Detection and blockchain systems. In order to create a secret key for the blockchain, the neural coordination method is used to make it easier for parties to communicate certain parameters across an open network. ANNs can improve their coordination speed by using neural coordination to get weights that are well-matched from inputs that are comparable. In addition, current studies are focused on improving medical care prediction accuracy through the use of FL methodologies and the blockchain-based healthcare 5.0 system. Many other types of analysis have confirmed that this strategy works. Boasting a success rate of 98% in disease prediction and 97.75% in intrusion detection, the suggested approach has demonstrated remarkable effectiveness of proposed FDEML framework. It is generally acknowledged that streamlining the process is a quicker and less expensive option. But we need to look into this more by looking at more data later on. The proposed approach becomes computationally burdened as the number of hidden layers increases; so, future studies will concentrate on identifying and quantifying factors with greater precision. The learning system will be retrained more frequently to improve its performance in different environments. Expanding the dataset and incorporating it into future work will allow us to examine the algorithm's performance fully. Additionally, we want to improve the efficacy and accuracy of the proposed model's suggestions.

Technical Annex 1:

Neural Synchronization for Key Generation in Blockchain:

Based on these observations, it is possible to derive the neural synchronization time parameters $TT_{b,Z}$ for two random walks that commence at location Z and interval b. After the initial time reflection at $T_{b,Z}$, one walker reaches the boundary. The symmetric nature of the model ensures that both $Z = 1 \; or \; Z = n - b$ maintain identical values. Consequently, equation 22 allows for the computation of the total coordination time, with the second reflection occurring subsequent to the steps at $T_{b,Z} + T_{b-1,1}$.

$$TT_{b,Z} = T_{b,Z} + \sum\nolimits_{j=1}^{b-1} T_{j,1} \tag{22}$$

A repulsive step might manifest when just two interconnected hidden units demonstrate disparate δ_q values, as discerned through the established framework of generalization error (as represented by equation 23).

$$\ni_q = \frac{1}{\pi} arc\cos(p_q) \tag{23}$$

Perceptrons embody a form of perception. On the contrary, the occurrence of a repulsive step necessitates more than merely having opposing hidden units. It entails that all ANN weights undergo uniform adjustments if $\psi^D = \psi^E$ remains valid. Equation 24 serves to determine the likelihood of a repulsive step occurring in such cases.

$$P_x = P(\delta_q^D \neq \delta_q^{E/A} \, |\psi^D = \psi^E) \tag{24}$$

Following the completion of any potential output bit modifications in complex learning methodologies, steps are taken to enhance the likelihood of attracting steps, as indicated in equation 25.

$$P_d = P(\psi^D = \delta_q^D = \delta_q^{E/A} \, |\psi^D = \psi^E) \tag{25}$$

In this simple attack, since mutual interaction isn't feasible, the outputs δ_q^A of $A's$'s neural network remain unchanged before the learning procedure is executed. Hence, the updating of weights transpires autonomously, leading to the susceptibility of the $q-th$ hidden node to undergo a repulsive step, as illustrated in equation 26.

$$P_x^A = \ni_q \tag{26}$$

Agreement between two closely related hidden nodes on their result δ_q doesn't always imply a favorable action, as an extra requirement to update the weights is necessary if $\delta_q = \psi$. Consequently, this indicates the potential for a positive outcome, as illustrated in equation 27.

$$P_d^A = \frac{1}{2}(1 - \ni_q) \tag{27}$$

In the exceptional scenario $L = 1, \delta_q = \psi, L > 1$ always holds true, resulting in this type of step occurring twice as frequently, denoted by $P_d^A = 1 - \ni_q$.

Bidirectional synchronization relies on mutual interaction, making it unattainable without such contact. In the scenario where there is an asymmetry among the hidden units concerning the outcome, and modifications are made to the weights on at least one of the weight vectors, it initiates a repulsive effect, indicated by the presence of $\psi^D \neq \psi^E$.

Consequently, D and E circumvent the synchronization phase.

On the contrary, when an even number of hidden nodes produce divergent outcomes, it precludes partners from undergoing repulsive steps upon comparing $\psi^D \; and \; \psi^E$. Furthermore, in instances where neural networks already manifest specific correlations, the probability leans towards having congruent internal structures in both networks rather than the emergence of two or more distinct output bits $\delta_q^D \neq \delta_q^E$. Consequently, weight adjustments are made if $\psi^D = \psi^E$ is detected. The likelihood of such congruent overlap transpiring within each hidden unit L is quantified by $\ni = \ni_q$, as delineated in equation 28.

$$P_W = P(\psi^D = \psi^E) = \sum\nolimits_{q=0}^{L/2} \binom{L}{2q} (1 - \ni_q)^{L-2q} \ni^{2q} \tag{28}$$

When two perceptrons, denoted as ($L = 1$), engage in reciprocal learning, only attractive steps are viable. The probabilities of attractive and repulsive synchronization for neural networks with $L > 1$are ascertained through equations 29 and 30, respectively.

$$P_d^E = \frac{1}{2P_W} \sum_{q=0}^{L-1/2} \binom{L-1}{2q} (1 - \ni_q)^{L-2q} \ni^{2q} \tag{29}$$

$$P_x^E = \frac{1}{P_W} \sum_{q=1}^{L/2} \binom{L-1}{2q} (1 - \ni_q)^{L-2q} \ni^{2q} \tag{30}$$

Utilizing three hidden units ($L = 3$) yields the result, which stands as the most prevalent choice for the neural key-exchange protocol, as outlined in equations 31 and 32.

$$P_d^E = \frac{1}{2} \frac{(1 - \ni)^3 + (1 - \ni) \ni^2}{(1 - \ni)^3 + 3(1 - \ni) \ni^2} \tag{31}$$

$$P_x^E = \frac{2(1 - \ni) \ni^2}{(1 - \ni)^3 + 3(1 - \ni) \ni^2} \tag{32}$$

In contrast, considering the local field A may yield superior outcomes compared to basic learning. Consequently, the probability of $\delta_q^A = \delta_q^D$ is determined by the prediction error, as detailed in equations 33 and 34.

$$\ni_q^P = \frac{1}{2} \left[1 - \ erf \left(\frac{p_q}{\sqrt{2(1 - p_q^2)}} \frac{|gg_q|}{\sqrt{Q_q}} \right) \right] \tag{33}$$

$$\begin{aligned} P_{hh} & \\ &= \int_0^\infty \prod\nolimits_{j \neq 1} \left(\int_{gg_q}^\infty \frac{2}{\sqrt{2\pi Q_{\mathrm{j}}}} \frac{1 - \ni_j^P}{1 - \ni_j} \ni^{-\frac{gg^2}{2Q_j}} \ (dis * gg_j) \right) \\ &\quad \times \frac{2}{\sqrt{2\pi Q_{\mathrm{q}}}} \frac{\ni_q^P}{\ni_q} \mathfrak{e}^{-\frac{h^2}{2Q_q}} (dis * gg_q) \end{aligned} \tag{34}$$

In situations where the order parameters $Q = Q_j^A \ and \ R = R_j^{DA}$ are active, the applicability of this equation extends seamlessly to $k$hidden units, each exhibiting diverse outcomes stemming from interactions with L hidden neurons. Consequently, the likelihood of a successful correction $\delta_j^D \neq \delta_j^A$ can be discerned through the utilization of equation 35.

$$\begin{aligned} P^+{}_k = & \int_0^\infty \left(\frac{2}{\sqrt{2\pi Q_{\mathrm{j}}}}\right)^L \left(\int_{gg_q}^\infty \frac{1 - \ni^P (gg)}{1 - \ni} \right. \\ & \ni^{-\frac{gg^2}{2Q}} \ (dis * gg))^{L-k} \times \left(\int_{gg_q}^\infty \frac{\ni^P \ (gg)}{} \right. \\ & \ni \ \mathfrak{e}^{-\frac{gg^2}{2Q}} (dis * gg))^{k-1} \frac{\ni^P \ (gg_q)}{\ni} \mathfrak{e}^{-\frac{gg_q^2}{2Q}} (dis * gg_q) \end{aligned} \tag{35}$$

An analogous calculation can be employed to $\delta_q^A = \delta_q^D$ predict the likelihood of improper adjustment for $D's \ and \ E's$, as detailed in equation 36.

$$\begin{aligned} P^-{}_k = & \int_0^\infty \left(\frac{2}{\sqrt{2\pi Q_{\mathrm{j}}}}\right)^L \left(\int_{gg_q}^\infty \frac{1 - \ni^P \ (gg)}{1 - \ni} \right. \\ & \ni^{-\frac{gg^2}{2Q}} \ (dis * gg))^{L-k-1} \times \left(\int_{gg_q}^\infty \frac{\ni^P \ (gg)}{\ni} \right. \\ & \mathfrak{e}^{-\frac{gg^2}{2Q}} (dis * gg))^k \frac{1 - \ni^P \ (gg_q)}{1 - \ni} \mathfrak{e}^{-\frac{gg_q^2}{2Q}} (dis * gg_q) \end{aligned} \tag{36}$$

In the scenario of a geometric attack, the probability of repulsive steps is dissected into three segments, meticulously accounting for all conceivable internal representations within $A's$ neural networks.

- Should the count of hidden units exhibiting $\delta_q^A \neq \delta_q^D$ be even, no geometric adjustment transpires. This reflects a bidirectional synchronization, akin to the scenario where one perceives the location of the other, as encapsulated in equation 37.

$$P_{x,1}^A = \sum\nolimits_{i=1}^{L/2} \binom{L-1}{2q-1} (1 - \ni)^{L-2q} \ni^{2q} \tag{37}$$

- Within $D's$ neural networks, it is conceivable that the hidden unit possessing the lowest $\left|hh_q^A\right|$may produce an output identical to its counterpart. As a result, the internal representations deviate significantly more as a consequence of geometric correction. This scenario is accounted for in the second segment of equation 38.

$$P_{x,2}^A = \sum\nolimits_{i=1}^{L/2} \binom{L-1}{2q-1} P_{2q-1}^- (1 - \ni)^{L-2q+1} \ni^{2q-1} \tag{38}$$

- In instances where the outcome of another hidden unit is inverted rather than resolving a discrepancy in the $q - th$ concealed neuron, the geometric assault proves unsuccessful. This invariably culminates in an unfavorable step, as illustrated in equation 39.

$$\begin{aligned} P_{x,3}^A = & \sum\nolimits_{i=1}^{(L-1)/2} \binom{L-1}{2q} (1 - P_{2q+1}^+) \\ & \times (1 - \ni)^{L-2q-1} \ni^{2q+1} \end{aligned} \tag{39}$$

Equations 40 and 41 discern the likelihood of both attractive and repellent steps occurring within the $q - th$ hidden unit, accounting for analogous order specifications when $L > 1$.

$$P_d^A = \frac{1}{2} \left(1 - \sum_{j=1}^{3} P_{x,j}^A \right) \tag{40}$$

$$P_x^A = \sum\nolimits_{j=1}^{3} P_{x,j}^A \tag{41}$$

Yet, with the utilization of $L = 1$, only attractive steps are undertaken, as the geometric attack technique can rectify any disparities. Rather than depending on conventional equations, these probabilities can be calculated using $L = 3$, resulting in the formulation of equations 42 and 43.

$$\begin{aligned} P_d^A &= \frac{1}{2}(1 + 2P_{hh})(1 - \ni)^2 \ni + \frac{1}{2}(1 - \ni)^3 \\ &\quad + \frac{1}{2}(1 - \ni) \ni^2 + \frac{1}{6} \ni^3 P_d^A \\ &= \frac{1}{2}(1 + 2P_{hh})(1 - \ni)^2 \ni + \frac{1}{2}(1 - \ni)^3 \\ &\quad + \frac{1}{2}(1 - \ni) \ni^2 + \frac{1}{6} \ni^3 \end{aligned} \tag{42}$$

$$P_x^A = 2(1 - P_{hh})(1 - \ni)^2 \ni + 2(1 - \ni) \ni^2 + \frac{2}{3} \ni^3 \tag{43}$$

At each step, a random direction—either left or right—is selected, and the random walkers proceed along this chosen path. Should one of them surpass the threshold, it experiences reflection, although its position remains unchanged. Meanwhile, the other random walker, approaching the first one, doesn't affect the d-distance between them; it decreases by one with each reflection. Importantly, the dis-coordinate remains unchanged throughout this process.

The most crucial statistic in this model is the time of synchronization Tim of the 2 arbitrary walkers, that is determined by the amount of iterations necessary to satisfy $dis = 0$ beginning from arbitrary starting positions. To compute the average magnitude $< Tim >$ and study the likelihood distribution $P(Tim = tim)$. This operation is slices into separate portions, each having a set interval dis. The periods $Tim_{dis,Y}$ of two reflections is determined by the time between them.

$Tim_{dis,Y}$ is the total over $Tim_{q,j}$ for each distance q *from* dis *to* 1, and its probability distribution $r(tt)$ is a convolution of dis functions $P(Tim_{dis,Y} = tim)$. Two geometric sequences are combined in a linear fashion. $f_n = f^n$ *and* $g_n = g^n$ is a convolution of these sequences in and of itself (equation 44).

$$f_n * g_n = \sum\nolimits_{j=-1}^{n-1} f_j g_{n-j} = \frac{g}{f-g} f_n + \frac{f}{g-f} g_n \tag{44}$$

Sum over geometric sequence can be written by (equation 45)

$$\begin{aligned} &P(Tim_{dis,Y} = tim) \\ &= \sum\nolimits_{h=v-dis+1}^{v} \sum\nolimits_{k=1}^{h-1} gg_{h,k}^{dis,Z} \left[\cos\left(\frac{k\pi}{h}\right)\right]^{tim-1} \end{aligned} \tag{45}$$

To get $P(Tim = tim)$ under random initial circumstances, one must average across all possible beginning places of both random walkers. The outcome is not flawless, even still (equation 46).

$$P(Tim = tim) = \frac{2}{v^2} \sum_{dis=1}^{v} \sum_{Y}^{v-dis} P(Tim_{dis,Y} = tim) \tag{46}$$

It can be expressed as the sum of a large number of geometric sequences (equation 47).

$$P(Tim = tim) = \sum\nolimits_{h=2}^{v} \sum\nolimits_{k=1}^{h-1} g_{h,k} \left[\cos\left(\frac{k\pi}{h}\right)\right]^{tim-1} \tag{47}$$

Just the terms with the largest actual values of the coefficientcos $\left(\frac{k\pi}{h}\right)$ are important over long periods of time, since the others degrade progressively.

As a result, they may be ignored in the limit $tim \to \infty$, and the probability distribution's asymptotic behavior is given by equation 48.

$$\begin{aligned} &P(Tim = tim) \\ &\sim \left[g_{v,1} + (-1)^{tim-1} g_{v,v-1}\right] \left[\cos\left(\frac{\pi}{v}\right)\right]^{tim-1} \end{aligned} \tag{48}$$

The two coefficients of this equation, $g_{v,1}$ *and* $g_{v,v-1}$, may be calculated. As a result, as shown in, we receive the following result (equation 49).

$$\begin{aligned} g_{v,1} = \frac{\sin^2(\pi/v)}{v^2 v!} \sum_{dis=1}^{v-1} \frac{2^{dis+1}(v-dis)!}{1-\theta_{dis,1}\cos(\pi/v)} \\ \times \prod\nolimits_{h=v-dis+1}^{v-1} \sum\nolimits_{k-1}^{h-1} \frac{\sin^2(k\pi/2)}{\cos(\pi/v)-\cos(k\pi/h)} \\ \times \frac{\sin^2(k\pi/h)}{1-\theta_{h,v-dis+1}\cos(k\pi/h)} \end{aligned} \tag{49}$$

On the graph, the numerical outcome is represented as a single curve. The asymptotic function is depicted by the dashed line (equation 50).

$$\begin{aligned} g_{v,v-1} = \frac{\sin^2(\pi/v)\cos^2(\pi/v)}{v^2 v!} \\ \times \sum\nolimits_{dis=1}^{v-1} \frac{2^{dis+1}(v-dis)!}{1+\theta_{dis,1}\cos(\pi/v)} \\ \times \prod\nolimits_{h=v-dis+1}^{v-1} \sum\nolimits_{k-1}^{h-1} \frac{\sin^2(k\pi/2)}{\cos(\pi/v)-\cos(k\pi/h)} \\ \times \frac{\sin^2(k\pi/h)}{1-\theta_{h,v-dis+1}\cos(k\pi/h)} \end{aligned} \tag{50}$$

This coefficient is substantially less than g_{v-1} because the value of $g_{v,v-1}$ is determined by an alternating sum. Furthermore, due to the factor $\cos^2(v\pi/2)$ it is exactly 0 for odd values of v. However, can be used to approximate the other coefficient $g_{v,1}$ (equation 51).

$$g_{v,1} \approx 0.324v\left[1 - \cos\left(\frac{\pi}{v}\right)\right. \tag{51}$$

Or $v \gg 1$ (Figure 6 illustrates this point). In case of neuronal synchronization, $v = 2L + 1$ is odd, resulting in $g_{v,v-1}$. $P(Tim = tim)$ Exponential corresponds to a geometric probability distribution over extended synchronization duration (equation 52).

$$P(Tim = tim) \sim g_{v,1}[\cos(\frac{\pi}{v})]^{tim-1} \tag{52}$$

Figure 7 shows that, with the exception of a few minor deviations at the start of the synchronization process, this analytical solution properly represents $P(Tim = tim)$. For small values of tim, however, the motion's equation for $PROB_{d,e}$ can be used to derive $P(Tim = tim)$ interactively.

Here, this model is enlarged to incorporate M individual couples of arbitrary walks, each driven by corresponding arbitrary noise. This relates to 2 uncorrelated concealed nodes having M weights that synchronize entirely after Tim_M attractive steps.

Because $< Tim >$ is the average synchronization time between two weights, $W^D_{q,j}$ *and* $W^E_{q,j}$, it inequal to $< Tim_M >$. This is due to the requirement that the weight vectors be identical for complete synchronization to take place. As a result, Tim_M is the highest value of Tim seen in M independently collected samples that match various hidden unit weights.

Tim_M's probabilistic distribution is given by the distribution function $P(Tim \leq tim)$ is known (equation 53).

$$P(Tim_M \leq tim) = P(Tim \leq tim)^M \tag{53}$$

As a consequence, using the calculated numerically distribution $P(Tim_M \leq tim)$, average value may be calculated $< Tim_M >$. The outcome, as shown in figure 8, reveals that as the amount of couples of random walkers grows $< Tim_M >$ grows logarithmically (equation 54).

$$< Tim_M > - < Tim > \propto \ln(M) \tag{54}$$

Only $P(Tim_M \leq tim)$'s asymptotic behavior affects Tim_M's distribution.when M is big. $P(Tim = tim)$ decompose exponentially, yielding a Gumbel distribution for $P(Tim_M \leq tim)$ (equation 55).

$$F(tim) = exp\left(-e^{\frac{tim_d - tim}{time_e}}\right) \tag{55}$$

for $M \gg v$ with the parameters (equation 56)

$$tim_d = time_e \ln \frac{Mh_{v,1}}{1 - \cos(\pi/v)} \; and \; time_e = -\frac{1}{\ln\cos(\pi/v)} \tag{56}$$

Is obtained by substituting equations 55 and 56 (equation 57).

$$P(Tim_M \leq tim) = exp\left(-\frac{Mh_{v,1}\cos^{tim}(\pi/v)}{1 - \cos(\pi/v)}\right) \tag{57}$$

Represents the predicted value of this probability distribution for M pairs of random walks' total synchronization time ($M \gg v$) (equation 58).

$$\begin{aligned} &< Tim_M > \\ &= tim_d + time_e\kappa \\ &= -\frac{1}{\ln(\cos(\pi/v))}\left(\kappa + \ln M + \ln \frac{h_{v,1}}{1 - \cos(\pi/v)}\right) \end{aligned} \tag{58}$$

The Euler-Mascheroni constant is indicates by κ. The asymptotic behavior of the synchronization time for $M \gg v \gg 1$ is given by equation 59.

$$< Tim_M > \sim \frac{2}{\pi^2}v^2\left(\kappa + \ln M + \ln \frac{2v^2 h_{v,1}}{\pi^2}\right) \tag{59}$$

Later, using equation 51 yields the result equation 60.

$$< Tim_M > \approx \frac{2}{\pi^2}v^2(\ln M + \ln(0.577v)) \tag{60}$$

Which is denoting that $< Tim_M >$ increasing in lockstep with $v^2 \ln M$. Obviously, brain synchronization is more difficult than just this theory, which is based on paired identical noise and random walks. The weights are not changed at every stage due to the way in which the learning principles work. By include such idle intervals, the sync(synchronization) time tim_{sync} is surely enhanced. Also, possible are repelling effects that interrupt synchronization. When repulsive forces have no effect on the system's dynamics, however, a scaling rule $< tim_{sync} > \propto K^2 \ln M$ for the sync(synchronization) of 2 neural networks may be discovered.

The neural networks' participating neural networks' weight vector overlap acts as the very crucial order variable in the coordination method. The position-dependent step sizes of a random walk, $< \triangle p_d >, < \triangle p_x >$, and probabilistic transitions, P_d, P_xcan be utilized to model its development over time. Naturally only the transition probabilities are considered.

The step sizes are accurate functions of p, even though they swing drastically about their average values. As a result, while this model isn't perfect for making quantitative predictions, it can be useful for determining key features of the system's qualitative behavior. For this, the average change in overlap is utilized (equation 61).

$$< \triangle p >= P_d(p) < \triangle p_d(p) > +P_x(p) < \triangle p_x(p) > \tag{61}$$

As a function of p, is especially advantageous at one synchronization step.

After 100 simulations for synchronization with $L = 3, K = 5, M = 100$, using $< \triangle p >$ as the random walk learning technique, these results were achieved. As a consequence, P increases quickly at first but slowly as the synchronization develops.

Synaptic depth K, on the other hand, influences the average change in overlap. Whereas a change in K has no influence on the transition probabilities $P_d \; and \; P_x$, decrease correspondingly to $E. < \triangle p_d > \; and \; < \triangle p_x >$ decreases proportionately to l^{-2}. As an outcome, $< p >$ decreases in proportion to K^{-2}, indicating that higher synaptic depth slows the dynamics. As a result, it's prudent to plan ahead (equation 62).

$$< tim_{sync} > \propto \frac{1}{< \triangle p >} \propto K^2 \tag{62}$$

Such that the synchronization time may be scaled In reality, the chance $P(tim_{sync} \leq tim)$ of reaching equal weight vectors in $D's$ and $E's$ neural networks in not more than tim stages is nicely discussed by a Gumbel distribution (equation 63):

$$P^E_{sync}(tim) = exp\left(-e^{\frac{tim_d - tim}{time_e}}\right) \tag{63}$$

As can be seen in figure 10, the parameters $tim_d \; and \; time_e$ grow proportionately to K^2, much like the model. As a result, common synchronization time scales like $< tim_{sync} > \propto K^2 \ln M$, which, as per equation 41.

The inset displays relevant parameters for various values of l. This effect can't be overlooked since increasing M has no effect on the step sizes. As a consequence, the order variable p is not a variable that self-averages, and $p \; by \; < p >$ in the equation of the locomotion cannot be substituted to estimate the temporal development of the overlap. However, the weights' complete probability distribution must be taken into account.

When there is a specific point at $p_f < 1$, neural synchronization's dynamics change substantially. The average overlap will rise as long as $p < p_f$ increases. Eventually, though, a quasi-stationary state is achieved. Only variations due to the discrete nature of attracting and repelling steps permit further synchronization.

To explain the other, a normal distribution with an average value of p_f and a standard deviation of α_f can be employed. The fundamental model employs a linear estimation $< \ \triangle p(p) \ >$ to decide the magnitude of the variations (equation 64).

$$\triangle p(tim) = -\phi_f(p(tim) - p_f) + \omega_f \varepsilon(tim) \tag{64}$$

The following parameters are (equations 65 and 66):

$$\phi_f = -\frac{d}{dp} < \triangle p(p) > |_{p=p_f} \tag{65}$$

$$\omega_f = \sqrt{< (\triangle p(p))^2 >} \tag{66}$$

The answer to this model's problem is equation 63 which depicts equation 67.

$$p(tim+1) - p_f = \omega_f \sum\nolimits_{i=0}^{tim} (1-\phi_f)^{tim-q} \varepsilon(q) \tag{67}$$

The time evolution of the gap in this model is represented by the equation 64. The primary condition $p(0) = p_f$ was used in this example, which appears to be unimportant in the limit $tt \ \rightarrow \ \infty$. The crossover variance in the stationary stage is used to figure out the (equation 68)

$$\delta_f^2 = \omega_f^2 \sum\nolimits_{i=0}^{\infty} (1-\phi_f)^{2tim} = \frac{\omega_f^2}{2\phi_f - \phi_f^2} \tag{68}$$

unit length of the arbitrary walk in p-space drop correspondingly to $K^{-2} for \ K \gg 1$ for, and the scaling nature of the parameters $\phi_f \ and \ \omega_f$ is the same. As a result, one learns equation 69.

$$\delta_f \propto \frac{1}{K} \tag{69}$$

As a reason, even if A use the geometric assault, he or she will be unable to synchronize with D and E in the limit $K \rightarrow \infty$. This is true for any other method that generates overlap dynamics with a specific point at $p_f < 1$.

However, at finite synaptic depth, oscillations allow the attacker to get beyond the fixed point at p_f. Once the quasi-stationary condition is reached, the probability of this happening in any given step is independent of *tim*. As a result, a Gumbel distribution (equation 34) does not provide $P_{sync}^A(tim)$, but an exponential distribution for $tim \gg tim_0$ does (equation 70).

$$P_{sync}^A(tim) = 1 - e^{-\frac{tim - tim_0}{tim_f}} \tag{70}$$

When tim_f is used as a time constant, This is seen in detail in figure 14. As a result of $tim_f \gg tim_0$, one must (equation 71)

$$< tim_{sync} > \approx \begin{Bmatrix} tim_f e^{tim_0/tim_f} & for \ tim_0 < 0 \\ tim_f + tim_0 & for \ tim_0 \geq 0 \end{Bmatrix} \approx tim_f \tag{71}$$

An average of steps and get to $p = 1$ by oneway learning.

The average amount of time required to achieve perfect synchronization starting at a certain location is determined by the simple linear model $< \ \triangle p(p) \ >$, which is given by tim_{sync} (equation 72).

$$tim_f \approx \frac{1}{P(p=1)} = \sqrt{2\pi\delta_{\mathrm{f}} e}^{\frac{(1-p_f)^2}{2\delta_f^2}} \tag{72}$$

As far as the shifts aren't too great, the line shows a match. If $\delta_f \ll 1 - p_f$, is true, it is reasonable to assume that the existance of the absorbing stage at $p = 1$ has no influence on the distribution of p. As a result, one can expect (equation 73)

$$tim_f \propto e^{fK^2} \tag{73}$$

δ_f varies proportionately to K^{-1} as the time constant is scaled, while p_f remains almost constant. tim_f grows exponentially as synaptic depth increases (equation 74).

$$tim_f \propto e^{f_1 K + f_2 K^2} \tag{74}$$

COMPETING INTERESTS

No interests of a financial or personal nature.

ACKNOWLEDGMENT

Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2024R716), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

REFERENCES

[1] C. Wilson, T. Hargreaves, and R. Hauxwell-Baldwin, "Benefits and risks of smart home technologies," *Energy Policy*, vol. 103, pp. 72–83, Apr. 2017.

[2] B. L. Risteska Stojkoska and K. V. Trivodaliev, "A review of Internet of Things for smart home: Challenges and solutions," *J. Cleaner Prod.*, vol. 140, pp. 1454–1464, Jan. 2017.

[3] F. Folianto, Y. S. Low, and W. L. Yeow, "Smartbin: Smart waste management system," in *Proc. IEEE 10th Int. Conf. Intell. Sensors, Sensor Netw. Inf. Process. (ISSNIP)*, Apr. 2015, pp. 1–2.

[4] J.-H. Park, M. M. Salim, J. H. Jo, J. C. S. Sicato, S. Rathore, and J. H. Park, "CIoT-Net: A scalable cognitive IoT based smart city network architecture," *Hum.-Centric Comput. Inf. Sci.*, vol. 9, no. 1, pp. 1–20, Dec. 2019.

[5] M. R. Alam, M. St-Hilaire, and T. Kunz, "Peer-to-peer energy trading among smart homes," *Appl. Energy*, vol. 238, pp. 1434–1443, Mar. 2019.

[6] Y. Mittal, P. Toshniwal, S. Sharma, D. Singhal, R. Gupta, and V. K. Mittal, "A voice-controlled multi-functional smart home automation system," in *Proc. Annu. IEEE India Conf. (INDICON)*, Dec. 2015, pp. 1–26.

[7] P. Wang, F. Ye, and X. Chen, "A smart home gateway platform for data collection and awareness," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 87–93, Sep. 2018.

[8] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1933–1954, 4th Quart., 2014.

[9] J. Ma and J. Hu, "Safe consensus control of cooperative-competitive multi-agent systems via differential privacy," *Kybernetika*, vol. 58, no. 3, pp. 426–439, Sep. 2022.

[10] B. Cheng, D. Zhu, S. Zhao, and J. Chen, "Situation-aware IoT service coordination using the event-driven SOA paradigm," *IEEE Trans. Netw. Service Manage.*, vol. 13, no. 2, pp. 349–361, Jun. 2016.

[11] J. Shen, C. Wang, T. Li, X. Chen, X. Huang, and Z.-H. Zhan, "Secure data uploading scheme for a smart home system," *Inf. Sci.*, vol. 453, pp. 186–197, Jul. 2018.

[12] D. Liu, X. Liu, Z. Chen, Z. Zuo, X. Tang, Q. Huang, and T. Arai, "Magnetically driven soft continuum microrobot for intravascular operations in microscale," *Cyborg Bionic Syst.*, vol. 2022, p. 2022, Feb. 2022.

[13] Q. Li, T. You, J. Chen, Y. Zhang, and C. Du, "LI-EMRSQL: Linking information enhanced Text2SQL parsing on complex electronic medical records," *IEEE Trans. Rel.*, vol. 73, no. 2, pp. 1280–1290, Jun. 2024.

[14] J. Zheng, R. Yue, R. Yang, Q. Wu, Y. Wu, M. Huang, X. Chen, W. Lin, J. Huang, X. Chen, Y. Jiang, B. Yang, and Y. Liao, "Visualization of Zika virus infection via a light-initiated bio-orthogonal cycloaddition labeling strategy," *Frontiers Bioeng. Biotechnol.*, vol. 10, p. 1051, Jul. 2022.

[15] P. Bing, Y. Liu, W. Liu, J. Zhou, and L. Zhu, "Electrocardiogram classification using TSST-based spectrogram and ConViT," *Frontiers Cardiovascular Med.*, vol. 9, pp. 1–28, Oct. 2022.

[16] R. Huo, Y. Liu, H. Xu, J. Li, R. Xin, Z. Xing, S. Deng, T. Wang, H. Yuan, and X. Zhao, "Associations between carotid atherosclerotic plaque characteristics determined by magnetic resonance imaging and improvement of cognition in patients undergoing carotid endarterectomy," *Quant. Imag. Med. Surg.*, vol. 12, no. 5, pp. 2891–2903, 2022. [Online]. Available: https://qims.amegroups.org/article/view/90773

[17] R. Liu, C. Ren, M. Fu, Z. Chu, and J. Guo, "Platelet detection based on improved YOLO_v3," *Cyborg Bionic Syst.*, vol. 1, no. 2, pp. 1–17, Sep. 2022.

[18] C.-H. Yeh, C. Zhang, W. Shi, M.-T. Lo, G. Tinkhauser, and A. Oswal, "Cross-frequency coupling and intelligent neuromodulation," *Cyborg Bionic Syst.*, vol. 4, p. 34, Jan. 2023.

[19] R. Huang, Y. Li, H. Wu, B. Liu, X. Zhang, and Z. Zhang, "68Ga-PSMA-11 PET/CT versus 68Ga-PSMA-11 PET/MRI for the detection of biochemically recurrent prostate cancer: A systematic review and meta-analysis," *Frontiers Oncol.*, vol. 13, p. 1216, Aug. 2023.

[20] J. Luo, S. F. Ahmad, A. Alyaemeni, Y. Ou, M. Irshad, R. Alyafi-Alzahri, G. Alsanie, and S. T. Unnisa, "Role of perceived ease of use, usefulness, and financial strength on the adoption of health information systems: The moderating role of hospital size," *Humanities Social Sci. Commun.*, vol. 11, no. 1, p. 516, Apr. 2024.

[21] S. Abbas, M. A. Khan, L. E. Falcon-Morales, A. Rehman, Y. Saeed, M. Zareei, A. Zeb, and E. M. Mohamed, "Modeling, simulation and optimization of power plant energy sustainability for IoT enabled smart cities empowered with deep extreme learning machine," *IEEE Access*, vol. 8, pp. 39982–39997, 2020.

[22] J. Li, J. Li, C. Wang, F. J. Verbeek, T. Schultz, and H. Liu, "Outlier detection using iterative adaptive mini-minimum spanning tree generation with applications on medical data," *Frontiers Physiol.*, vol. 14, Oct. 2023.

[23] J. Li, J. Li, C. Wang, F. J. Verbeek, T. Schultz, and H. Liu, "MS2OD: Outlier detection using minimum spanning tree and medoid selection," *Mach. Learn. Sci. Technol.*, vol. 5, no. 1, Mar. 2024, Art. no. 015025.

[24] W. Mcculloch and W. Pitts, "A logical calculus of the ideas immanent in nervous activity," *Bull. Math. Biol.*, vol. 52, nos. 1–2, pp. 99–115, 1990.

[25] J. Przybyła and S. Wróbel, "Survey on learning algorithms for training single perceptrons," *Neural Comput. Appl.*, vol. 1, pp. 1–22, Aug. 2023.

[26] Y. Dong, S. Wang, Q. Huang, R. W. Berg, G. Li, and J. He, "Neural decoding for intracortical brain–computer interfaces," *Cyborg Bionic Syst.*, vol. 4, p. 44, Jul. 2023.

[27] G. Ji, Q. Gao, T. Zhang, L. Cao, and Z. Sun, "A heuristically accelerated reinforcement learning-based neurosurgical path planner," *Cyborg Bionic Syst.*, vol. 4, p. 26, Jan. 2023.

[28] D. Nasonov, A. A. Visheratin, and A. Boukhanovsky, "Blockchain-based transaction integrity in distributed big data marketplace," in *Computational Science—ICCS*. Cham, Switzerland: Springer, 2018, pp. 569–577.

[29] R. A. Michelin, A. Dorri, M. Steger, R. C. Lunardi, S. S. Kanhere, R. Jurdak, and A. F. Zorzo, "Speedy Chain: A framework for decoupling data from blockchain for smart cities," in *ACM Int. Conf. Proc. Ser.*, 2018, pp. 1–29.

[30] H. Liu, S. Zhang, H. Gamboa, T. Xue, C. Zhou, and T. Schultz, "Taxonomy and real-time classification of artifacts during biosignal acquisition: A starter study and dataset of ECG," *IEEE Sensors J.*, vol. 24, no. 6, pp. 9162–9171, Mar. 2024.

[31] S. Lu, J. Yang, B. Yang, X. Li, Z. Yin, L. Yin, and W. Zheng, "Surgical instrument posture estimation and tracking based on LSTM," *ICT Exp.*, vol. 10, no. 3, pp. 465–471, Jun. 2024, doi: 10.1016/j.icte.2024.01.002.

[32] W. Zheng, S. Lu, Y. Yang, Z. Yin, and L. Yin, "Lightweight transformer image feature extraction network," *PeerJ Comput. Sci.*, vol. 10, p. 1755, Jan. 2024.

[33] L. Zhao, S. Qu, H. Xu, Z. Wei, and C. Zhang, "Energy-efficient trajectory design for secure SWIPT systems assisted by UAV-IRS," *Veh. Commun.*, vol. 45, Feb. 2024, Art. no. 100725, doi: 10.1016/j.vehcom.2023.100725.

[34] G. Xie, G. Hou, Q. Pei, and H. Huang, "Lightweight privacy protection via adversarial sample," *Electronics*, vol. 13, no. 7, p. 1230, Mar. 2024.

[35] D. Wang, W. Zhang, W. Wu, and X. Guo, "Soft-label for multi-domain fake news detection," *IEEE Access*, vol. 11, pp. 98596–98606, 2023.

[36] Y. Lei, C. Yanrong, T. Hai, G. Ren, and W. Wenhuan, "DGNet: An adaptive lightweight defect detection model for new energy vehicle battery current collector," *IEEE Sensors J.*, vol. 23, no. 23, pp. 29815–29830, Dec. 2023.

[37] H. Zhang, Y. Mi, X. Liu, Y. Zhang, J. Wang, and J. Tan, "A differential game approach for real-time security defense decision in scale-free networks," *Comput. Netw.*, vol. 224, Apr. 2023, Art. no. 109635.

[38] B. Xiong, K. Yang, J. Zhao, and K. Li, "Robust dynamic network traffic partitioning against malicious attacks," *J. Netw. Comput. Appl.*, vol. 87, pp. 20–31, Jun. 2017.

[39] Y. Ding, W. Zhang, X. Zhou, Q. Liao, Q. Luo, and L. M. Ni, "FraudTrip: Taxi fraudulent trip detection from corresponding trajectories," *IEEE Internet Things J.*, vol. 8, no. 16, pp. 12505–12517, Aug. 2021.

[40] G. P. Wang and J. X. Yang, "SKICA: A feature extraction algorithm based on supervised ICA with kernel for anomaly detection," *J. Intell. Fuzzy Syst.*, vol. 36, no. 1, pp. 761–773, Feb. 2019.

[41] C. Yin, J. Xi, R. Sun, and J. Wang, "Location privacy protection based on differential privacy strategy for big data in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3628–3636, Aug. 2018.

[42] R. Cai, J. Tang, C. Deng, G. Lv, X. Xu, S. Sylvia, and J. Pan, "Violence against health care workers in China, 2013–2016: Evidence from the national judgment documents," *Human Resour. Health*, vol. 17, no. 1, p. 103, Dec. 2019.

[43] J. Li, C. Huang, Y. Yang, J. Liu, X. Lin, and J. Pan, "How nursing students' risk perception affected their professional commitment during the COVID-19 pandemic: The mediating effects of negative emotions and moderating effects of psychological capital," *Humanities Social Sci. Commun.*, vol. 10, no. 1, p. 195, May 2023.

[44] Y. Liu, Z. Fang, M. H. Cheung, W. Cai, and J. Huang, "Mechanisms design for blockchain storage sustainability," *IEEE Commun. Mag.*, vol. 61, no. 8, pp. 102–107, Aug. 2023.

[45] M. Rahouti, K. Xiong, and N. Ghani, "Bitcoin concepts, threats, and machine-learning security solutions," *IEEE Access*, vol. 6, pp. 67189–67205, 2018.

[46] B. Mohanta, P. Das, and S. Patnaik, "Healthcare 5.0: A paradigm shift in digital healthcare system using artificial intelligence, IoT and 5G communication," in *Proc. Int. Conf. Appl. Mach. Learn.*, 2019, pp. 191–196.

[47] E. Mbunge, B. Muchemwa, S. Jiyane, and J. Batani, "Sensors and Healthcare 5.0: Transformative shift in virtual care through emerging digital health technologies," *Global Health J.*, vol. 5, no. 4, pp. 169–177, Dec. 2021.

[48] M. Bhavin, S. Tanwar, N. Sharma, S. Tyagi, and N. Kumar, "Blockchain and quantum blind signature-based hybrid scheme for Healthcare 5.0 applications," *J. Inf. Secur. Appl.*, vol. 56, Feb. 2021, Art. no. 102673.

[49] A. Sarkar, K. Daripa, M. Z. Khan, and A. Noorwali, "An efficient group synchronization of chaos-tuned neural networks for exchange of common secret key," *Soft Comput.*, vol. 28, no. 5, pp. 4413–4433, Mar. 2024.

[50] A. Sarkar, K. Daripa, M. Z. Khan, and A. Noorwali, "Cloud enabled blockchain-based secured communication in mutual intelligent transportation using neural synchronization," *Veh. Commun.*, vol. 38, Dec. 2022, Art. no. 100533.

[51] T. Dong and T. Huang, "Neural cryptography based on complex-valued neural network," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 31, no. 11, pp. 4999–5004, Nov. 2020.

[52] A. Sarkar, "Deep learning guided double hidden layer neural synchronization through mutual learning," *Neural Process. Lett.*, vol. 53, no. 2, pp. 1355–1384, Apr. 2021.

[53] S. Jeong, C. Park, D. Hong, C. Seo, and N. Jho, "Neural cryptography based on generalized tree parity machine for real-life systems," *Secur. Commun. Netw.*, vol. 2021, pp. 1–12, Feb. 2021.

[54] A. A. M. Teodoro, O. S. M. Gomes, M. Saadi, B. A. Silva, R. L. Rosa, and D. Z. Rodríguez, "An FPGA-based performance evaluation of artificial neural network architecture algorithm for IoT," *Wireless Pers. Commun.*, vol. 127, no. 2, pp. 1085–1116, Nov. 2022.

[55] M. Dolecki and R. Kozera, "The impact of the TPM weights distribution on network synchronization time," *Computer Information Systems and Industrial Management*, vol. 9339, pp. 451–460, Aug. 2015.

[56] S. Aggarwal, R. Chaudhary, G. S. Aujla, N. Kumar, K.-K.-R. Choo, and A. Y. Zomaya, "Blockchain for smart communities: Applications, challenges and opportunities," *J. Netw. Comput. Appl.*, vol. 144, pp. 13–48, Oct. 2019.

[57] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, and A. Peacock, "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," *Renew. Sustain. Energy Rev.*, vol. 100, pp. 143–174, Feb. 2019.

[58] G. Li, M. Dong, L. T. Yang, K. Ota, J. Wu, and J. Li, "Preserving edge knowledge sharing among IoT services: A blockchain-based approach," *IEEE Trans. Emerg. Topics Comput. Intell.*, vol. 4, no. 5, pp. 653–665, Oct. 2020.

[59] Z. Zhou, B. Wang, M. Dong, and K. Ota, "Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and edge computing," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 50, no. 1, pp. 43–57, Jan. 2020.

[60] B. Ihnaini, M. A. Khan, T. A. Khan, S. Abbas, M. S. Daoud, M. Ahmad, and M. A. Khan, "A smart healthcare recommendation system for multidisciplinary diabetes patients with data fusion based on deep ensemble learning," *Comput. Intell. Neurosci.*, vol. 2021, pp. 1–11, Sep. 2021.

[61] M. A. Khan, "Challenges facing the application of IoT in medicine and healthcare," *Int. J. Computations, Inf. Manuf.*, vol. 1, no. 1, pp. 1–29, Dec. 2021.

[62] M. F. Khan, T. M. Ghazal, R. A. Said, A. Fatima, S. Abbas, M. A. Khan, G. F. Issa, M. Ahmad, and M. A. Khan, "An IoMT-enabled smart healthcare model to monitor elderly people using machine learning technique," *Comput. Intell. Neurosci.*, vol. 2021, pp. 1–10, Nov. 2021.

[63] J. Xu, B. S. Glicksberg, C. Su, P. Walker, J. Bian, and F. Wang, "Federated learning for healthcare informatics," *J. Healthcare Informat. Res.*, vol. 5, no. 1, pp. 1–19, Mar. 2021.

[64] Y. Li, B. Shan, B. Li, X. Liu, and Y. Pu, "Literature review on the applications of machine learning and blockchain technology in smart healthcare industry: A bibliometric analysis," *J. Healthcare Eng.*, vol. 2021, pp. 1–11, Aug. 2021.

[65] S. Yamin Siddiqui, I. Naseer, M. Adnan Khan, M. Faheem Mushtaq, R. Ali Naqvi, D. Hussain, and A. Haider, "Intelligent breast cancer prediction empowered with fusion and deep learning," *Comput., Mater. Continua*, vol. 67, no. 1, pp. 1033–1049, 2021.

[66] W. Dai, T. S. Brisimi, W. G. Adams, T. Mela, V. Saligrama, and I. C. Paschalidis, "Prediction of hospitalization due to heart diseases by supervised learning methods," *Int. J. Med. Informat.*, vol. 84, no. 3, pp. 189–197, Mar. 2015.

[67] Y.-J. Son, H.-G. Kim, E.-H. Kim, S. Choi, and S.-K. Lee, "Application of support vector machine for prediction of medication adherence in heart failure patients," *Healthcare Informat. Res.*, vol. 16, no. 4, p. 253, 2010.

[68] A. Tariq, L. A. Celi, J. M. Newsome, S. Purkayastha, N. K. Bhatia, H. Trivedi, J. W. Gichoya, and I. Banerjee, "Patient-specific COVID-19 resource utilization prediction using fusion AI model," *Npj Digit. Med.*, vol. 4, pp. 1–9, Sep. 2021.

[69] A. Sedik, A. M. Iliyasu, B. A. El-Rahiem, M. E. A. Samea, A. Abdel-Raheem, M. Hammad, J. Peng, F. E. A. El-Samie, and A. A. A. El-Latif, "Deploying machine and deep learning models for efficient data-augmented detection of COVID-19 infections," *Viruses*, vol. 12, no. 7, p. 769, Jul. 2020.

[70] A. Qayyum, K. Ahmad, M. Ahtazaz Ahsan, A. Al-Fuqaha, and J. Qadir, "Collaborative federated learning for healthcare: Multi-modal COVID-19 diagnosis at the edge," 2021, *arXiv:2101.07511*.

[71] T. S. Brisimi, R. Chen, T. Mela, A. Olshevsky, I. C. Paschalidis, and W. Shi, "Federated learning of predictive models from federated electronic health records," *Int. J. Med. Informat.*, vol. 112, pp. 59–67, Apr. 2018.

[72] Y. Chang, C. Fang, and W. Sun, "A blockchain-based federated learning method for smart healthcare," *Comput. Intell. Neurosci.*, vol. 2021, pp. 1–12, Nov. 2021.

[73] A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider, and M. Hamdi, "A survey on security and privacy issues in edge-computing-assisted Internet of Things," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4004–4022, Mar. 2021.

[74] S. Wang, T. Tuor, T. Salonidis, K. K. Leung, C. Makaya, T. He, and K. Chan, "Adaptive federated learning in resource constrained edge computing systems," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 6, pp. 1205–1221, Jun. 2019.

[75] S. Latif, Z. Zou, Z. Idrees, and J. Ahmad, "A novel attack detection scheme for the industrial Internet of Things using a lightweight random neural network," *IEEE Access*, vol. 8, pp. 89337–89350, 2020.

[76] W. Y. Lim, N. C. Luong, D. T. Hoang, Y. Jiao, Y. C. Liang, Q. Yang, D. Niyato, and C. Miao, "Federated learning in mobile edge networks: A comprehensive survey," *IEEE Commun. Surv. Tutor*, vol. 22, no. 3, pp. 2031–2063, Apr. 2020.

[77] S. Agrawal, S. Sarkar, O. Aouedi, G. Yenduri, K. Piamrat, S. Bhattacharya, P. K. Maddikunta, and T. R. Gadekallu, "Federated learning for intrusion detection system," *Comput. Commun.*, vol. 195, pp. 346–361, Nov. 2021.

[78] Y. Zhao, J. Chen, D. Wu, J. Teng, and S. Yu, "Multi-task network anomaly detection using federated learning," in *Proc. 10th Int. Symp. Inf. Commun. Technol.*, 2019, pp. 4–6.

[79] S. Rajendran, J. S. Obeid, H. Binol, R. D'Agostino, K. Foley, W. Zhang, P. Austin, J. Brakefield, M. N. Gurcan, and U. Topaloglu, "Cloud-based federated learning implementation across medical centers," *JCO Clin. Cancer Informat.*, vol. 5, no. 5, pp. 1–11, Dec. 2021.

[80] O. Alkadi, N. Moustafa, B. Turnbull, and K. R. Choo, "A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks," *IEEE Internet Things J.*, vol. 8, no. 12, pp. 9463–9472, Jun. 2021.

[81] M. Z. Khan, A. Sarkar, and A. Noorwali, "Memristive hyperchaotic system-based complex-valued artificial neural synchronization for secured communication in industrial Internet of Things," *Eng. Appl. Artif. Intell.*, vol. 123, Aug. 2023, Art. no. 106357.

[82] T. Hai, A. Sarkar, M. Aksoy, M. Z. Khan, and A. Alahmadi, "Complex-valued hyperchaos-assisted vector-valued artificial neural key coordination for improving security in the industrial Internet of Things," *Eng. Appl. Artif. Intell.*, vol. 128, Feb. 2024, Art. no. 107561.

[83] T. Hai, A. Sarkar, R. Karmakar, M. Z. Khan, A. Noor, T. H. Noor, A. Kumar, and A. Yvaz, "Neural session key exchange in the industrial Internet of Things using hyperchaotic-guided vector-valued artificial neural synchronization," *Eng. Appl. Artif. Intell.*, vol. 125, Oct. 2023, Art. no. 106683.

[84] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[85] A. Rehman, A. Athar, M. A. Khan, S. Abbas, A. Fatima, Atta-ur-Rahman, and A. Saeed, "Modelling, simulation, and optimization of diabetes type II prediction using deep extreme learning machine," *J. Ambient Intell. Smart Environments*, vol. 12, no. 2, pp. 125–138, Mar. 2020.

[86] M. Adnan Khan, A. Rehman, K. Masood Khan, M. A. Al Ghamdi, and S. H. Almotiri, "Enhance intrusion detection in computer networks based on deep extreme learning machine," *Comput., Mater. Continua*, vol. 66, no. 1, pp. 467–480, 2020.

[87] (2007). *Parkinsons Data Oxford*. [Online]. Available: https://archive.ics.uci.edu/dataset/174/parkinsons

[88] A. G. M. Tavallaee, E. Bagheri, and W. Lu. (2018). *Canadian Institute for Cybersecurity, UNB, NSL-KDD Dataset*. [Online]. Available: https://www.unb.ca/cic/datasets/nsl.html

[89] M. A. Khan, S. Abbas, A. Rehman, Y. Saeed, A. Zeb, M. I. Uddin, N. Nasser, and A. Ali, "A machine learning approach for blockchain-based smart home networks security," *IEEE Netw.*, vol. 35, no. 3, pp. 223–229, May 2021.

[90] A. Haider, M. A. Khan, A. Rehman, M. Rahman, and H. S. Kim, "A real-time sequential deep extreme learning machine cybersecurity intrusion detection system," *Comput., Mater. Continua*, vol. 66, no. 2, pp. 1785–1798, 2021.

[91] D. Sztahó, I. Valálik, and K. Vicsi, "Parkinson's disease severity estimation on Hungarian speech using various speech tasks," in *Proc. Int. Conf. Speech Technol. Hum.-Comput. Dialogue (SpeD)*, Oct. 2019, pp. 1–6.

[92] J. M. Tracy, Y. Özkanca, D. C. Atkins, and R. H. Ghomi, "Investigating voice as a biomarker: Deep phenotyping methods for early detection of Parkinson's disease," *J. Biomed. Informat.*, vol. 104, Apr. 2020, Art. no. 103362.

[93] E. Nikookar, R. Sheibani, and S. Alavi, "An ensemble method for diagnosis of Parkinson's disease based on voice measurements," *J. Med. Signals Sensors*, vol. 9, no. 4, p. 221, 2019.

[94] O. Yaman, F. Ertam, and T. Tuncer, "Automated Parkinson's disease recognition based on statistical pooling method using acoustic features," *Med. Hypotheses*, vol. 135, Feb. 2020, Art. no. 109483.

[95] H. Kuresan, D. Samiappan, and S. Masunda, "Fusion of WPT and MFCC feature extraction in Parkinson's disease diagnosis," *Technol. Health Care*, vol. 27, no. 4, pp. 363–372, Jul. 2019.

SARAH A. ALZAKARI received the bachelor's degree in computer sciences from Princess Nourah Bint Abdulrahman University (PNU), Saudi Arabia, and the M.Sc. and Ph.D. degrees in computer and information sciences from George Washington University, USA. Her Ph.D. thesis was about the cryptography in computer science. She is currently an Assistant Professor with the Computer Sciences Department, College of Computer and Information Sciences, PNU. She worked with her collage in various academic positions. Her research interests include information security, cryptography, AI, networking, and software engineering.

ARINDAM SARKAR received the B.C.A. degree (Hons.) from The University of Burdwan, West Bengal, India, in 2005, the M.C.A. degree (Hons.) from Visva-Bharati University, Santiniketan, West Bengal, in 2008, the M.Tech. degree (Hons.) in computer science and engineering from the University of Kalyani, West Bengal, in 2011, and the Ph.D. degree in engineering from the Department of Computer Science and Engineering, University of Kalyani, West Bengal, in July 2015. He is currently an Assistant Professor and the Head of the Department of Computer Science and Electronics, Ramakrishna Mission Vidyamandira, Belur Math, Howrah, West Bengal. He received the Innovation in Science Pursuit for Inspired Research (INSPIRE) Fellowship of the Department of Science and Technology (DST), Government of India, during the Ph.D. study. He secured Second Rank in the West Bengal College Service Commission (WBCSC) examination for general degree colleges. He has been serving as a Convener, the Chairperson, a Moderator, an Question Paper Setter, a Reviewer, and an Editor of different examinations of Calcutta University, Kalyani University, West Bengal State University, Vidyasagar University, Burdwan University, Sido-Kanho Birsha University, and many others, since 2009. He has more than 138 publications in different SCI and Scopus-indexed international journals and conferences. His research interests include neural cryptography, GAN cryptography, cybersecurity, deep learning, machine learning, federated learning, generative-AI, and soft computing. He is a Life Member of the Computer Society of India (CSI).

MOHAMMAD ZUBAIR KHAN received the Master of Technology degree in computer science and engineering from U. P. Technical University, Lucknow, India, and the Ph.D. degree in computer science and information technology from the Faculty of Engineering, M. J. P. Rohilkhand University, Bareilly, India. He was the Head of the Department of Computer Science and Engineering, Invertis University, Bareilly. He has more than 18 years of teaching and research experience. He is currently a Professor with the Department of Computer Science and Information, Taibah University, Medina, Saudi Arabia. He has published more than 100 journals and conference papers. His current research interests include data mining, big data, parallel and distributed computing, cyber security, and computer networks. He has been a member of the Computer Society of India, since 2004.

AMEL ALI ALHUSSAN received the B.Sc., M.Sc., and Ph.D. degrees in computer and information sciences from King Saud University, Saudi Arabia. Her M.Sc. thesis was in software engineering and the Ph.D. thesis in artificial intelligent. She is currently an Associate Professor with the Computer Sciences Department, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University (PNU), Saudi Arabia. She worked with her collage in various administrative and academic positions. Her research interests include artificial intelligence, networking, and software engineering.