Federated Learning and Blockchain-Enabled Privacy-Preserving Healthcare 5.0 System: A Comprehensive Approach to Fraud Prevention and Security in IoMT

Dr.B. Sindhusaranya[1*], R. Yamini[2], Dr.M.A.P. Manimekalai[3] and Dr.K. Geetha[4]

[1*] Assistant Professor, Department of Computer Science and Engineering, Sona College of Technology, India. sindhusaranyabalraj@gmail.com,
Orcid: https://orcid.org/0000-0002-6344-5432

[2] Assistant Professor, Department of Computing Technologies, Faculty of Engineering and Technology, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu, India.
yaminir@srmist.edu.in, Orcid: https://orcid.org/0009-0002-6392-609X

[3] Assistant Professor, Department of ECE, Karunya Institute of Technology and Sciences, Coimbatore, India. manisankar2008@gmail.com, Orcid: https://orcid.org/0000-0001-8854-4579

[4] Professor, Department of CSE, Excel Engineering College, India.
geetharajsri@gmail.com, https://orcid.org/0000-0003-4604-0174

Received: August 19, 2023; Accepted: October 24, 2023; Published: November 30, 2023

Abstract

The proliferation of Internet and Communication Technologies (ICTs) has ushered in a period often referred to as Industry 5.0. The subsequent development is accompanied by the healthcare industry coining Healthcare 5.0. Healthcare 5.0 incorporates the Internet of Things (IoT), enabling medical imaging technologies to facilitate early diagnosis of diseases and enhance the quality of healthcare facilities' service. Nevertheless, the healthcare sector is currently experiencing a delay in adopting Artificial Intelligence (AI) and big data technologies compared to other sectors under the umbrella of Industry 5.0. This delay may be attributed to the prevailing concerns about data privacy within the healthcare domain. In recent times, there has been a noticeable increase in the use of Machine Learning (ML) enabled adaptive Internet of Medical Things (IoMT) systems with different technologies for medical applications. ML is an essential component of the IoMT system, as it optimizes the trade-off between delay and energy consumption. The issue of data fraud in classical learning models inside the distributed IoMT system for medical applications remains a significant research challenge in practical settings. This paper proposes Federated Learning and Blockchain-Enabled Privacy-Preserving (FL-BEPP) for Fraud Prevention and Security (FPS) in the IoMT framework. The system incorporates numerous dynamic strategies. This research examines the medical applications that exhibit hard constraints, such as deadlines, and soft constraints, such as resource consumption, when executed on distributed fog and cloud nodes. The primary objective of FL-BEPP is to effectively detect and safeguard the confidentiality and integrity of data across many tiers, including local fog nodes and faraway clouds. This is achieved by minimizing power use and delay while simultaneously meeting the time constraints associated with healthcare workloads.

Journal of Internet Services and Information Security (JISIS), volume: 13, number: 4 (November), pp. 199-209.
DOI: *10.58346/JISIS.2023.I4.014*

*Corresponding author: Assistant Professor, Department of Computer Science and Engineering, Sona College of Technology, India.

Keywords: Federated Learning, Blockchain, Privacy Preservation, IoMT, Healthcare 5.0.

1 Introduction

The IoMT is a burgeoning technology with significant growth (Sovacool, B.K., 2020). The IoT facilitates the interconnection of several things to gather data that may be used to improve human wellness, productiveness, and efficiency. The ideas of smart cities, smart grids, and smart dwellings have become widely recognized and significantly impact our everyday lives (Alam, M.R., 2019).

One of the most promising emerging technological strategies for mitigating the disparity in global health outcomes is implementing an IoT-enabled health monitoring system for patients (Islam, M.M., 2020). The IoT technologies are often commonly referred to as the IoMT. Despite its specific emphasis on the healthcare sector, this research uses the acronyms IoT and IoMT collectively. In addition, it should be noted that the IoT can greatly enhance wellness and safety in society (Selvaraj, S., 2020). By connecting their personal devices to the Internet, individuals can access information about many aspects of their lives, such as their habits, physical and mental well-being, and living environments, among other factors. This enables healthcare practitioners to monitor individuals' health remotely and continuously in real-time. Moreover, the collected data can be used to advance evidence-based therapies for many health conditions, including illnesses, injuries, protective measures, early diagnosis, and rehabilitation.

In contemporary society, transporting patients from their residences to medical facilities for regular examinations poses significant challenges. Several problems exist within the context, including queuing, journey duration, and the potential for patients to develop diverse viral infections when traversing this contaminated setting. Consequently, the healthcare sector is now prioritizing in-home healthcare services, enabling patients to undergo medical exams inside the confines of their residences. The development of an intelligent health surveillance system aims to facilitate communication between rural patients and healthcare professionals in metropolitan areas. This technology serves as an intermediary between patients and physicians. The device monitors essential physiological indicators such as heart rate, electrocardiogram (ECG) readings, blood pressure, and body temperature and detects instances of collapses (Anikwe, C.V., 2022). The system collects the data and sends it wirelessly to the application for evaluation.

There is a pressing need for the development of efficient mining algorithms to analyze medical data, aiming to facilitate illness detection, provide efficient medical interventions, and improve overall patient care. ML is an advanced computational methodology that has been extensively used across several fields, including but not limited to image recognition, processing languages, and health (Abbas, S., 2020). However, it is important to note that ML models in healthcare need a substantial amount of training data to achieve high accuracy levels. This is particularly significant in the medical sector since precision may often determine the outcome of a patient's life-saving intervention. In most instances, centralized training tactics include acquiring a substantial amount of data from a powerful cloud server. However, this approach might potentially result in significant infringements of customer confidentiality, particularly within the medical domain.

The emergence of BT offers a promising solution for addressing crucial concerns related to privacy, security, and ethics within an intelligent healthcare system. This technology serves as a transparent and responsible data protection method. Nevertheless, BT has shown remarkable achievements in serving as a fundamental component of cybersecurity infrastructure for many intelligent healthcare methods, including but not limited to medical record management and information dissemination (Nasonov, D., 2018). The integration of BT into intelligent household networks may be justified due to its ability to operate independently from the several protocols often used in automated systems (Makhdoom, I., 2020). Nevertheless, despite the growing interest in intelligent medical technology, the present research efforts are fragmented among several academic disciplines. The current research is being conducted to address the existing gap and get valuable insights into the implementation and use of BT in the smart medical industry.

Intelligent healthcare gadgets are often targeted for DDoS attacks due to the presence of unprotected wireless keys. These devices are especially vulnerable since they are promptly activated to provide advanced functionalities, including patient medical information and the automated dissemination of inaccurate medical reports (Yin, C., 2017). The problems discussed arise from the centrally controlled framework of the IoMT system. As the IoMT revolution advances, privacy concerns are becoming more prominent. Specifically, issues such as record fabrication and abuse, device intrusion, and the penetration of illicit IoMT devices via assaults on server and gateway networks are of increasing concern (Ray, P.P., 2020).

The combination of Federated Learning (FL) with BT has facilitated the development of a sophisticated and safe medical system, referred to as Healthcare 5.0, within the context of the IoMT domain. The primary objective of this complete method is to effectively mitigate privacy issues and proactively combat instances of fraud within medical records. FL facilitates the cooperative training of models across distributed devices, enabling healthcare organizations to extract valuable insights while maintaining the confidentiality of sensitive patient data. Concurrently, using BT guarantees preserving medical information in an unchangeable state while offering a transparent platform for healthcare transactions. This results in a secure and tamper-proof ledger for the healthcare industry. By integrating these technologies, the suggested solution not only improves the confidentiality of patient data but also develops a strong defensive mechanism against fraudulent actions in the IoMT, therefore contributing to the development of a safe and patient-centered Healthcare 5.0 ecosystem.

2 Literature Survey

This literature review examines the current research environment, investigating the potential synergies between FL and BT in creating a comprehensive Healthcare 5.0 system. This study examines the dynamic paradigms, obstacles, and inventive approaches that contribute to the avoidance of fraud and the augmentation of security in the IoMT.

In their study, Prasad et al. put out an all-encompassing approach to investigate the utilization of federated learning within the context of the IoMT. The authors thoroughly examine the available literature, providing an organized summary of FL methodologies in the healthcare field (Prasad, V.K., 2022). The implementation entails the analysis of several FL methodologies and their suitability for the IoMT. The provided output offers significant insights into the present scenario, presenting a sophisticated comprehension of the use of FL in medical environments. One of the notable benefits of this approach is its ability to provide a comprehensive perspective on the subject matter, therefore establishing a solid groundwork for potential avenues of future scholarly investigation.

Sezer, Turkmen, and Nuriyev provide a unique approach called PPFchain, which centers on utilizing BT in sensor networks to achieve privacy-preserving FL (Sezer, B.B., 2023). The implementation process entails the creation of a comprehensive framework that guarantees privacy while utilizing BT to facilitate safe and transparent data exchanges. The results illustrate improved PP and security within the context of FL for sensor networks. One of the benefits of utilizing this technology is the enhanced level of data confidentiality and privacy it offers, which is particularly significant in healthcare applications.

Dhasarathan et al. propose a novel approach that combines supervised FL and BT to tackle user privacy issues effectively within the context of the IoMT (Dhasarathan, C., 2023). The process entails the creation of a PP model. One of the benefits of adopting a privacy-centric approach to the IoMT is the assurance of maintaining confidentiality and integrity. Muazu et al. present a technique for an IoMT system that effectively handles medical resources by utilizing edge-empowered blockchain FL (Jung, S.W., 2022). The process entails the development of a system that enhances the allocation of resources in the healthcare sector by utilizing FL at the edge. The results illustrate the effective management of medical resources in the IoMT (Muazu, T., 2023). There are several benefits associated with this approach, such as the utilization of resources and the distribution of decision-making authority. One potential drawback might be the requirement for a robust infrastructure for edge computing.

In this study, Rehman et al. provide a healthcare system prioritizing security by incorporating BT and FL to advance Healthcare 5.0. The technique emphasizes the assurance of security and privacy within the healthcare ecosystem (Rehman, A., 2022). The implementation process entails the integration of BT with FL techniques to increase the security and privacy of data. The presented result demonstrates a Healthcare 5.0 system that prioritizes security and privacy.

Stephanie and her co-authors provide a novel PP model that utilizes hierarchical ensemble and FL techniques within the domain of healthcare 4.0, including BT, to ensure trustworthiness. The technique places significant emphasis on preserving privacy while upholding trustworthiness (Stephanie, V., 2022). The implementation entails the construction of a hierarchical ensemble model. The results illustrate an improvement in the preservation of privacy and the establishment of trust within healthcare systems. One of the advantages of this strategy is its holistic nature, which ensures the preservation of anonymity.

In this study, Lakhan et al. provide a privacy protection model for the IoMT that utilizes FL and incorporates a BT capable of detecting fraudulent activities (Lakhan, A., 2022). The primary objective of the technique is to augment privacy and security measures while concurrently mitigating fraudulent activities inside healthcare data. The deployment process entails the integration of FL and BT to enhance privacy and facilitate Fraud Detection (FD). The results exhibit successful privacy preservation and avoidance of IoMT fraud.

In summary, the literature review highlights the significant importance of FL and BT in influencing the trajectory of healthcare, specifically within the IoMT framework. The studies that have been analyzed demonstrate the potential of these technologies to offer a holistic approach to the avoidance of fraud and enhancement of security, therefore contributing to the advancement of the Healthcare 5.0 vision.

3 Federated Learning and Blockchain-Enabled Privacy-Preserving (FL-BEPP) for FPS in the IoMT Framework

The paper implemented the FL-distributed learning model in a BT-enabled IoMT system. This study aimed to PP and enhance recognition of fraud in medical applications for the IoT. The system architecture is depicted in Fig. 1. The IoMT system comprises many components, including apps, fog nodes, and fog-cloud networks that utilize docker services. The system evaluated a range of IoT services, including E-Healthcare, E-Transport, and smart homes, based on their respective numbers. Each application, denoted as i, is characterized by a coarse-grained nature and completely transfers the workload, denoted as WL_i, to the Fog-Cloud Agent (FCA) for subsequent processing.

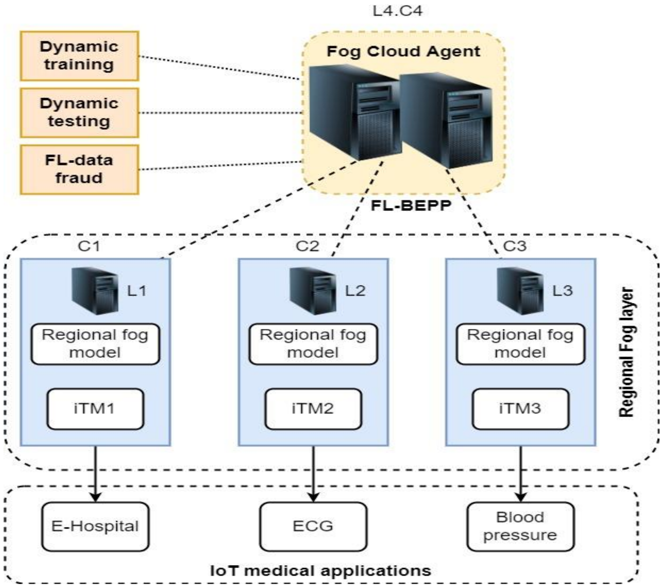

Figure 1: FL-BEPP in the IoMT Framework

The computer nodes, denoted as L, are scattered across various geographical locations inside the network. Every individual node, denoted as l, can train the data model for all IoT applications. Furthermore, these nodes can communicate the trained models with other nodes in the network, including the FCA. The FCA determines the optimal model training at regional fog nodes to minimize applications' energy use and delay while ensuring timely execution within their specified deadlines. The present study introduces the FL-BEPP algorithm framework, which incorporates many dynamic heuristics, as depicted in Algorithm 1. This study uses ML techniques to effectively deploy and enhance a range of FD models that can self-improve and remain sustainable over time. In this study, we illustrate the process of training ML models, both supervised and unsupervised, using past transaction data. The objective is to forecast the fraudulent nature of incoming transactions.

Processing Delay

The study initially computes the validation delay of data using the following methodology.

$$Validation - Delay = xWLi,l \times Valid. \tag{1}$$

Equation (1) guarantees the validation latency of the individual task inside the system. The latency of blockchain and execution is computed as follows.

$$Execution\,Delay = Hashing\ time + (WLi/\,\zeta l) \times xWLi,l + Fraud\ Analysis. \tag{2}$$

Equation (5) determines the execution delay of workload i.

$$Hashing\ time = WLi \leftarrow l,C \leftarrow (SHA - 256) \tag{3}$$

The encryption and decryption process within the blockchain for workload i is determined by equation (3).

$$Fraud\ Analysis = WLi \leftarrow l,C \leftarrow Data - index \tag{4}$$

The analysis of fraud for workload i is determined by equation (4). The energy use of nodes is contingent upon the BT's validation and the fraud analysis for each workload, as established in the subsequent manner. Determining the overall delay of the task is conducted subsequently.

$$Delay = Execution\,Delay + Hashing\ \ time + Fraud\ Analysis. \tag{5}$$

Equation (5) to determine all delays of workload i.

$$Power\ Consumption = Watt \times Delay. \tag{6}$$

Equation (6) is utilized to ascertain the power consumption resulting from the combined execution, BT, and fraud analysis processes within the node concerning the workload.

FL-BEPP Algorithm

This section examines the processes involved in the FL-BETS framework, which encompasses a variety of heuristics, as seen in Algorithm 1. The FL-BETS encompasses several procedures and schemes subsequently. This paper examines task assignment, which aims to find a solution within polynomial time complexity, specifically focusing on meeting the deadlines associated with the assigned job. Generally, it may be stated that the task assignment problem is classified as NP-Hard, requiring solutions to be found within specified deadlines. The input for Algorithm 1 consists of several constraints, such as $I, WL, l, and\ L$. These constraints are then processed through distinct phases.

```
Algorithm 1: FL-BEPP algorithm
Input: $I, WL, L$
Begin
        For ($i = 1\ to\ l = 1\ to\ L$) do
        Order all WL based on timelines
        Get input at a particular time in the system
        Sorting $i \leftarrow WLi, \in I$
        Search and map $l \leftarrow \in l, Delay \in L$
Train and test data on regional fog nodes
Apply training and testing for FL at nodes $l, WLi, L$
Use BT to store secure data at fog nodes with dynamic validation
End for
End
```

FL-based FPS

The concept of dynamic training and testing involves using various models on distinct fog nodes for training and testing. These models are subsequently shared with a centralized cloud for computational processing. Based on the models used for training and testing, it can be observed that all the workloads that underwent training and testing effectively mitigate fraud attacks and address concerns related to privacy. This paper proposes a method called FL-FPS. The method involves training and testing on medical WL to analyze FD in a fog cloud setting, as seen in Fig. 2.

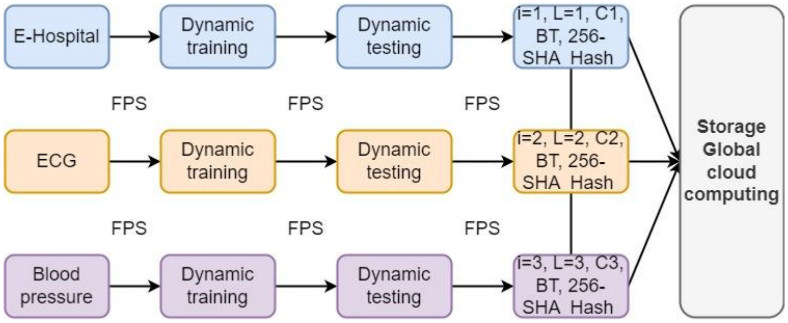

Figure 2: FL-based FPS

Implementing fog and cloud nodes occurs at distinct tiers within the system. Regional federated models are trained on the fog nodes and shared with the global cloud computing infrastructure for BT-enabled storage. The suggested dynamic training and testing strategy in FL-FPS facilitates the discovery of fraud trends by utilizing FL-enabled policies. The model possesses the capability of autonomous learning, enabling it to effectively adjust and accommodate novel and unforeseen instances of fraudulent behavior.

The research classified the fraudulent pattern into two distinct processes: the known pattern and the unknown one. The applications transfer their WL to the fog nodes in the immediate vicinity to do additional processing tasks, such as training and testing, before being executed on the global node. The technique under consideration initially assigns a certain pattern to each WL and offloads them to the corresponding accessible fog nodes. The current consensus mechanisms, namely proof of work and proof of stake, utilize the smart contract rule to facilitate data verification and validation across BT nodes. Consequently, an FD system utilizing ML and random-forest algorithms has been included in the BT to address the ever-changing nature of fraud inside the network. However, the centralized training and testing model for FD algorithms based on ML exhibits a latency issue. Hence, the FL-FPS under consideration reduces delay and precisely manages identified and unidentified instances of fraud inside the system.

4 Results and Discussion

This paper presents an FL-based strategy to optimize the energy consumption of fog-cloud nodes and mitigate application latency in a network-enabled by BT. The prevalence of malfeasance systems is consistently increasing within an IoT-enabled fog-cloud environment. Rule-based FD systems have typically been used to prevent fraud via the Internet, but they depend on an inert set of rules that are adaptable and intelligent expertise. This study uses ML techniques to effectively deploy and enhance numerous FD models capable of self-improvement and long-term sustainability. In this study, we present a methodology for training ML models, both supervised and unsupervised, using historical transaction data. The objective is to develop a predictive capability to discern the fraudulent nature of incoming transactions.

Additionally, we comprehensively explain the process of deploying the trained models to a REST API to integrate them seamlessly into an established business software framework. This work extensively utilizes a demonstration of the concept by employing an anonymized dataset containing data transactions. The experimental portion of the study used baseline procedures that closely resemble the proposed work (FL-BEPP for FPS) and have already been explored in the associated literature.

Baseline 1: ML techniques (Sovacool, B.K., 2020) (Alam, M.R., 2019) (Islam, M.M., 2020) within the BT context for FD have been extensively employed in training models for healthcare and smart-home applications. Data mining is a computational technique used to automatically categorize, group, and partition data, with the aim of revealing patterns and rules within the data that may suggest noteworthy trends, such as indications of fraudulent behavior.

Baseline 2: The utilization of dynamic ML techniques (Selvaraj, S., 2020) (Anikwe, C.V., 2022) (Abbas, S., 2020) (Nasonov, D., 2018) (Makhdoom, I., 2020) (Yin, C., 2017) is prevalent in training healthcare and smart-home models. The research used conventional ML training models and integrated BT to address several aspects, such as scheduling and energy efficiency inside fog-cloud methodologies.

Baseline 3: The integration of FL with BT for healthcare applications in (Dhasarathan, C., 2023) (Muazu, T., 2023) (Rehman, A., 2022) (Stephanie, V., 2022) (Lakhan, A., 2022) has been utilized for comparison.

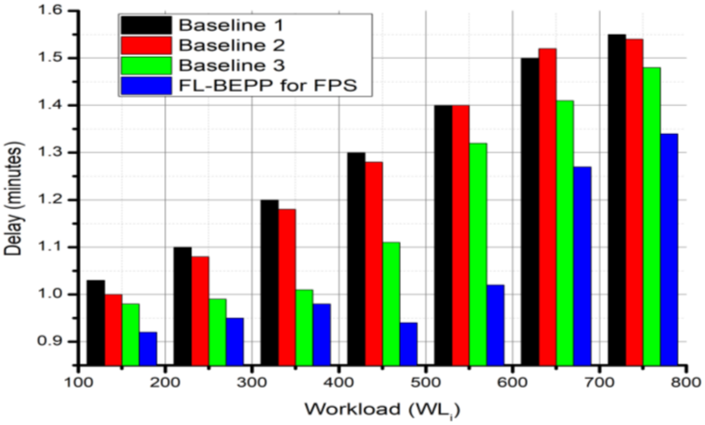

Figure 3: Delay Performance (in Minutes) of Various Methods for Different Workloads

Fig. 3 presents a comparative analysis of the effectiveness of multiple approaches, namely Baseline methods and FL-BEPP for FPS, in managing different workloads. In the case of a workload of 150, the FL-BEPP system demonstrates superior performance compared to the Baseline techniques, exhibiting a delay of 0.92 minutes as opposed to the range of 0.98 to 1.03 minutes. FL-BEPP consistently demonstrates decreased latency compared to the Baseline techniques across all scenarios as the demand intensifies. For example, when the workload is set at 750, FL-BEPP demonstrates a delay of 1.34 minutes, which outperforms the delays recorded in the Baseline techniques, ranging from 1.48 to 1.55 minutes. The findings suggest that FL-BEPP effectively mitigates delays across diverse workloads, highlighting its potential for enhancing fraud protection and security within the IoMT architecture.

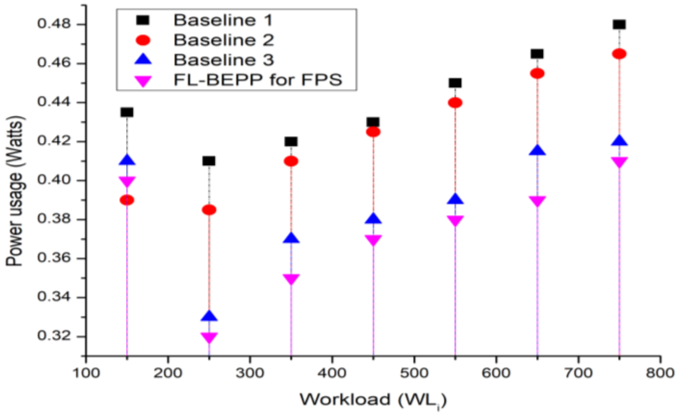

Figure 4: Power Usage (in Watts) of Various Methods for Different Workloads

Fig. 4 compares the power efficiency between Baseline approaches and the proposed FL-BEPP for FPS over varying workloads. When the workload is set at 150, FL-BEPP exhibits power utilization equivalent to the Baseline approaches, with power values ranging from 0.39 to 0.435 Watts. FL-BEPP consistently exhibits reduced power consumption in all circumstances compared to the Baseline techniques as the workload intensifies. For example, when subjected to a workload of 750, FL-BEPP demonstrates a power consumption of 0.41 Watts, surpassing the Baseline techniques ranging from 0.42

to 0.48 Watts. The findings of this study indicate that FL-BEPP demonstrates efficacy in preventing fraud and enhancing security within the IoMT framework. Additionally, it is seen that FL-BEPP exhibits superior power efficiency compared to the Baseline techniques. These outcomes underscore the potential of FL-BEPP in fostering the development of sustainable and energy-efficient healthcare systems.

5 Conclusion

This study presents a novel architecture, Federated Learning and Blockchain-Enabled Privacy-Preserving (FL-BEPP), designed to address the challenges of FPS inside the IoMT framework. The system integrates a variety of dynamic tactics. This study investigates the medical applications that demonstrate rigid limitations, such as time limits, and flexible constraints, such as the use of resources when implemented on distributed fog and cloud nodes. The main aim of the FL-BEPP system is to efficiently identify and ensure the protection of data confidentiality and integrity across several levels, encompassing both local fog nodes and distant cloud environments. The objective mentioned above is accomplished by simultaneously fulfilling time limitations related to healthcare tasks and minimizing power consumption and delay. When the workload is adjusted to 750, FL-BEPP exhibits a delay of 1.34 minutes, surpassing the delays seen in the Baseline methods, which varied between 1.48 and 1.55 minutes. The findings suggest that the proposed FL-BEPP effectively mitigates delays and reduces power usage across diverse workloads, highlighting its potential for enhancing fraud protection and security within the IoMT architecture.

References

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

[2] Alam, M.R., St-Hilaire, M., & Kunz, T. (2019). Peer-to-peer energy trading among smart homes. *Applied energy*, *238*, 1434-1443.

[3] Anikwe, C.V., Nweke, H.F., Ikegwu, A.C., Egwuonwu, C.A., Onu, F.U., Alo, U.R., & Teh, Y.W. (2022). Mobile and wearable sensors for data-driven health monitoring system: State-of-the-art and future prospect. *Expert Systems with Applications*, *202*.

[4] Dhasarathan, C., Hasan, M.K., Islam, S., Abdullah, S., Khapre, S., Singh, D., & Alqahtani, A. (2023). User privacy prevention model using supervised federated learning-based block chain approach for Internet of Medical Things. *CAAI Transactions on Intelligence Technology,* 1-15.

[5] Islam, M.M., Rahaman, A., & Islam, M.R. (2020). Development of smart healthcare monitoring system in IoT environment. *SN computer science*, *1*, 1-11.

[6] Jung, S.W. (2022). Universal Redactable Blockchain. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 13*(4), 81-93.

[7] Lakhan, A., Mohammed, M.A., Nedoma, J., Martinek, R., Tiwari, P., Vidyarthi, A., & Wang, W. (2022). Federated-learning based privacy preservation and fraud-enabled blockchain IoMT system for healthcare. *IEEE journal of biomedical and health informatics*, *27*(2), 664-672.

[8] Makhdoom, I., Zhou, I., Abolhasan, M., Lipman, J., & Ni, W. (2020). PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. *Computers & Security*, *88*, 1-33.

[9] Muazu, T., Yingchi, M., Muhammad, A.U., Ibrahim, M., Samuel, O., & Tiwari, P. (2023). IoMT: A Medical Resource Management System Using Edge Empowered Blockchain Federated Learning. *IEEE Transactions on Network and Service Management,* 1-18.

[10] Nasonov, D., Visheratin, A.A., & Boukhanovsky, A. (2018). Blockchain-based transaction integrity in distributed big data marketplace. *In Computational Science–ICCS: 18th International Conference, Wuxi, China, Proceedings, Part I 18*, 569-577. Springer International Publishing.

[11] Prasad, V.K., Bhattacharya, P., Maru, D., Tanwar, S., Verma, A., Singh, A., & Raboaca, M.S. (2022). Federated learning for the internet-of-medical-things: A survey. *Mathematics*, *11*(1), 1-47.

[12] Ray, P.P., Dash, D., & Kumar, N. (2020). Sensors for Internet of medical things: State-of-the-art, security and privacy issues, challenges and future directions. *Computer Communications*, *160*, 111-131.

[13] Rehman, A., Abbas, S., Khan, M.A., Ghazal, T.M., Adnan, K.M., & Mosavi, A. (2022). A secure healthcare 5.0 system based on blockchain technology entangled with federated learning technique. *Computers in Biology and Medicine*, *150*.

[14] Selvaraj, S., & Sundaravaradhan, S. (2020). Challenges and opportunities in IoT healthcare systems: a systematic review. *SN Applied Sciences*, *2*(1).

[15] Sezer, B.B., Turkmen, H., & Nuriyev, U. (2023). PPFchain: A novel framework privacy-preserving blockchain-based federated learning method for sensor networks. *Internet of Things*, *22*.

[16] Sovacool, B.K., & Del Rio, D.D.F. (2020). Smart home technologies in Europe: A critical review of concepts, benefits, risks and policies. *Renewable and sustainable energy reviews*, *120*, 1-20.

[17] Stephanie, V., Khalil, I., Atiquzzaman, M., & Yi, X. (2022). Trustworthy privacy-preserving hierarchical ensemble and federated learning in healthcare 4.0 with blockchain. *IEEE Transactions on Industrial Informatics,* 1-10.

[18] Yin, C., Xi, J., Sun, R., & Wang, J. (2017). Location privacy protection based on differential privacy strategy for big data in industrial Internet of things. *IEEE Transactions on Industrial Informatics*, *14*(8), 3628-3636.

Authors Biography

Dr. Sindhusaranya Balraj, currently working as an Assistant Professor in Department of Computer science and Engineering, Sona College of Technology, Salem. I have completed my Ph.D. (Full-time) in Anna University, Chennai. My research area is Medical Image Processing. I Completed M. Tech (Information Technology) in K.S.R College of Technology with 8.63 CGPA in the year of 2012. I did B. Tech (Information Technology) in Government College of Technology, Coimbatore with 7.57 CGPA in the year of 2010. I have published my research paper in 3 International Journal & presented paper in 6 International and 2 National conferences.

Yamini R received a Doctoral degree from Bharathiar University, India in 2018. Her research includes Energy Aware Computing, Green Algorithms, AI and Machine learning. Her expertise in these fields has enabled her to bring a unique perspective to her teaching, helping students to develop the skills and knowledge needed to succeed in today's technology-driven world.

Dr.M.A.P. Manimekalai working as an Assistant Professor in the Department of Electronics and Communication Engineering at Karunya Institute of Technology and Sciences, Coimbatore. She graduated in Engineering at Alagappa Chettiar College of Engineering and Technology, Karaikudi, Tamil Nadu, India. She secured Master of Engineering in Applied Electronics at V.L.B. Janakiammal College of Engineering &Technology, Coimbatore, Tamil nadu, India. She secured Ph.D., in Information and Communication Engineering, Anna University, Chennai, Tamil Nadu, India. She is in teaching profession for more than 16 years. She has presented more than 25 papers in National and International Journals, Conference and Symposiums. His main area of interest includes Image/Signal processing, Artificial Intelligence and Machine learning.

Dr. K. Geetha holds a Ph. D degree in Information and Communication Engineering from Anna University, Chennai and M.E degree in Computer Science and Engineering from K. S. Rangasamy College of technology, affiliated to Anna University of Technology Coimbatore, Tamil Nadu, India in 2010. She is currently working as a Professor in the Department of Computer Science and Engineering, Excel Engineering College. She has 13.2 years of teaching experience. She has published 27 international journals and presented three papers in the national and international Conferences. She is an active member of ISTE, IEI. Her Research interests includes Ad hoc Networks, Network Security, Cloud Computing.