International Journal of Business and Applied Social Science

E-ISSN: 2469-6501
VOL: 10, ISSUE: 5
May/2024
DOI: http://dx.doi.org/10.33642/ijbass.v10n5p2

A Conceptual Swarm Intelligence Framework for Deriving a Global Healthcare Machine Learning Model

Dr. Sergio Davalos
Milgard School of Business
University of Washington Tacoma
Email: sergiod@uw.edu
USA

ABSTRACT

The analysis of healthcare data is increasingly challenging due to the exponential growth in data volume and the diversity of data formats available. This is compounded by the necessity for patient confidentiality and security. Traditional healthcare systems, often localized, face significant barriers to the goal of achieving efficient information use that limits the use of advanced machine learning. We examine methodologies for deriving a global machine learning (ML) model. We examine the role of federated learning (FL) and swarm learning (SL) in enhancing privacy, security, and interoperability in healthcare data and model management for the development of scalable, collaborative model training. Utilizing cloud computing and Internet of Things (IoT) technologies as the ecosystem for machine learning can result in comprehensively addressing current limitations in healthcare informatics. We present an architecture for the development of a global model that incorporates the FL and SL incorporating a Swarm Intelligence communication layer.

KEYWORDS: Swarm intelligence, IoT, healthcare, architecture, blockchain

1. Introduction

The healthcare industry is grappling with the management of patient data due to the exponential increase in volume and diversity, while also addressing the need for strict confidentiality and data security (Kechadi,2016). Mukhtar (2020) further emphasizes the challenge of extracting meaningful value from this data and highlights the use of machine learning and data mining techniques to mine useful knowledge. These studies collectively underscore the urgent need for innovative methodologies and systems to manage and analyze healthcare data, while also ensuring its quality, privacy, and security.

Additionally, hospitals are at the forefront of healthcare service delivery and constantly, encounter hurdles in efficiently managing and securely sharing patient data, not only within their systems but also in partnership with other healthcare providers and, in some cases, research institutions. These challenges are also compounded by the need to maintain and defend patient privacy and provide confidentiality-enforced healthcare in light of the increasing threat of cyber-attacks and data breaches. These can pose serious risks to maintaining patient privacy and the integrity of healthcare data and healthcare systems.

Furthermore, existing healthcare data management systems typically exist and operate in silos leading to inefficiencies and barriers to the seamless exchange of information. Ideally, a healthcare-based data warehousing system can be of great use in providing rigorous, quantitative information to decision-makers, and faces. However, such a system and related systems encounter challenges in maintaining data quality, privacy, and security (Bouguettaya, 2001). This leads to a lack of interoperability and data sharing which can hamper the potential use of advanced analytical and data mining techniques, such as optimization, forecasting, and machine learning. While hospitals can derive benefits from extracting meaningful insights from local data using machine learning for data mining to predict outcomes or even prescribe appropriate actions to take, the limited sharing of data limits the possible benefits.

At the same time, these capabilities can significantly improve patient care and health outcomes. While hospitals and other healthcare providers can benefit from the sharing of data and analysis, the competing need to maintain privacy and confidentiality requires an information systems solution that can accommodate the two competing objectives. To address these competing objectives, innovative methodologies, and tools are needed to manage and analyze the data, while also addressing ethical and privacy concerns (Kechadi, 2016; Mukhtar, 2020).

One potential solution that has been introduced for this is Federated Learning. Federated learning (FL) is a solution that incorporates a collaborative machine learning approach and, most importantly, does not require the direct exchange of data between the “siloed” (local) data units such as hospitals. The data remains protected at its source. This approach is designed to address privacy concerns while maintaining regulatory compliance since the individual collaborative partner’s (such as hospitals) data remains local and is not shared outside of the local boundaries. The basic algorithm for FL is based on generating machine learning models at the local level using local data and only the model parameters, such as weights for a neural network model, for each locally derived model are shared. In this framework, only model updates (parameters) are shared across the network of collaborating partners at each iteration of the development of the local model. Additionally, in this framework, there is a designated aggregator component (server) whose role is to aggregate (combine) the local model parameters from each of the local units to produce a global model. The resulting parameters are then shared with all the local units to update all the local models with the global model. The process continues until a stopping point is reached such as desired level of performance and a fixed number of interactions.

International Journal of Business and Applied Social Science

E-ISSN: 2469-6501
VOL: 10, ISSUE: 5
May/2024
DOI: http://dx.doi.org/10.33642/ijbass.v10n5p2

FL allows the training of a shared global model while keeping sensitive data in local institutions (Xu, 2021) and maintains data privacy and availability by sharing knowledge rather than raw data (Loftus, 2022; Antunes, 2022; (Pfitzner, 2021). To further enhance privacy, a privacy-preserving federated learning model has been proposed, which uses feature selection and differential privacy to protect sensitive data (Islam, 2022; Kourtellis 2020). Federated Learning (FL) has been successfully applied in healthcare, with potential applications in COVID-19, brain tumor segmentation, mammograms, sleep quality prediction, and smart healthcare systems (Moon 2023). However, FL is not without its challenges, including vulnerability to attacks (Mammen 2021). To address these challenges, FL can be combined with other technologies such as homomorphic encryption and blockchain (Fotohi 2022). Despite these challenges, FL has the potential to revolutionize healthcare informatics by preserving data privacy and improving patient quality of life (Patel 2022).

Additionally, the implementation of federated learning in healthcare faces other challenges, including data heterogeneity, system scalability, and ensuring the integrity and security of the distributed, machine learning process as well as assuring the reliability and accuracy of the resulting models (Patel 2022). Blockchain technology offers a potential solution to these challenges by providing a secure, immutable, and decentralized framework for managing transactions and data exchanges. When integrated with cloud computing, blockchain can further enhance the scalability and efficiency of healthcare data management systems, offering a robust infrastructure for implementing federated learning models.

The integration of blockchain with cloud computing in healthcare systems can significantly enhance scalability and efficiency. Esposito (2018) and Khatoon (2020) both highlight the security and privacy benefits of using blockchain in this regard. Khatoon (2020) specifically proposed a blockchain-based smart contract system for healthcare management. Prokofieva (2019) and Shahnaz (2019) further emphasize the potential applications of blockchain in healthcare, including information dissemination and electronic health records, and discuss the challenges and solutions for implementing blockchain in these areas. Vyas (2019) and Vazirani (2019) discuss the convergence of blockchain and machine learning, and the feasibility of using blockchain for efficient health care, respectively. Rifi (2017) and Zubaydi (2019) emphasize the benefits of blockchain in addressing challenges such as privacy, scalability, and interoperability in eHealth data access management. These studies collectively suggest that the use of blockchain and cloud computing can provide a robust, resilient, scalable, and well-protected infrastructure for implementing federated learning in the development of machine learning models for healthcare applications.

Developing and training clinically useful machine learning (ML) models in the healthcare setting requires addressing the need for sharing patient-related data with a central repository (Chen, et. al, 2021; Howard, et. al, 2021). Also, such data sharing, especially across different countries, can face legal and logistical obstacles. Data sharing between institutions may require patients to forfeit their rights to data privacy and data control. While this problem has been addressed using (centralized) federated learning (FL), (McMahan, et. al, 2017; Lu, et. al, 2022), the need for a central coordinator that manages the learning progress based on all trained models can be seen as a fundamental limitation on the use of centralized federated learning.

Recently, this limitation of FL has been addressed by a new group of decentralized learning technologies, including block-chain FL (li, 2021 and Swarm Learning (SL) (Warnat-Herresthal, 2021). Swarm learning, a decentralized machine learning approach, has shown promise in improving prediction performance and generalizability without centralizing control over the final model. In SL, ML models are trained locally, and models are combined centrally without requiring central coordination by using blockchain-based coordination between peers. This removes the centralization of FL and raises all contributors to the same level. In the context of healthcare data analysis, SL results in equal sharing of the training of multi-centric ML models and provides incentives for organizations to collaborate without having to concentrate data, models, or model management in one place. This level of collaboration among several parties can potentially generate more powerful and more reliable ML systems. Ultimately, SL could improve the quality, robustness, and resilience of ML in healthcare systems (Warnat-Herresthal, 2021).

Swarm Learning (SL) thus offers a decentralized, confidential, and privacy-preserving approach to machine learning in healthcare (Warnat-Herresthal 2021, 2020). Saldanha (2021, 2022) demonstrated its effectiveness in predicting molecular alterations in cancer histopathology, while Warnat-Herresthal (2021, 2022) applied it to disease classification, including COVID-19, tuberculosis, and leukemia. These studies highlight the potential of swarm learning as a substitute for centralized data collection and federated learning. However, the privacy and security aspects of swarm learning need further exploration.

Additional developments show that Swarm Learning (SL) can be combined with distributed machine learning based on standardized AI engines and a permissioned blockchain to securely onboard members, and elected leaders, and merge model parameters (Becker 2022, Vyas 2019, Zekiye 2023). This combination addresses data privacy concerns and enables the secure sharing of medical records (Stephanie 2023). It is worth noting that, Salim (2022) proposes a Machine Learning based Blockchain architecture for secure healthcare systems which can be integrated with Swarm Learning.

While Swarm Learning provides a very workable solution, Swarm Intelligence, a nature-based computing approach, has also shown much promise. Swarm Intelligence algorithms have been successfully applied in healthcare for

International Journal of Business and Applied Social Science

E-ISSN: 2469-6501
VOL: 10, ISSUE: 5
May/2024
DOI: http://dx.doi.org/10.33642/ijbass.v10n5p2

disease diagnosis and treatment (Nayar 2019). In addition, swarm intelligence, based on the Internet of Things, can significantly enhance the efficiency and accuracy of data analysis in healthcare. Nayar (2019) and Ramaswamy (2019) both highlight the potential of swarm intelligence in healthcare data mining, particularly in disease prognosis and clinical decision support. The integration of swarm intelligence with the Internet of Things can further enhance the robustness, flexibility, and scalability of health data management, as proposed by Samuel (2015), Puri (2021), Yoo (2021), Chi (2021), and Deepa (2022). These studies emphasize the importance of security, privacy, and analytics in healthcare data management, and the potential of IoT-based health big data processing and machine learning algorithms in improving efficiency and transparency. Krishnan (2015) also underscores the need for efficient clinical data analysis, which can be achieved through the use of swarm intelligence and IoT.

In light of these developments, this research aims to provide the design of a novel system architecture that leverages the strengths of blockchain technology, cloud computing, and swarm intelligence while incorporating the promises of swarm learning and federated learning. The proposed architecture seeks to address the critical challenges in healthcare data management, including data security, privacy, interoperability, and the efficient utilization of machine learning techniques. By focusing on the specific needs and challenges faced by hospitals, this study aims to contribute a scalable, secure, and privacy-preserving framework that can effectively the way healthcare data is managed, shared, and utilized for the betterment of patient care and health services.

2. Background and Current Technologies

In this section, we review the background concepts and methodologies applicable in developing machine learning solutions in a healthcare setting with local autonomous units such as hospitals or similar healthcare facilities. We review the underlying technologies and discuss the specific needs and challenges in a healthcare setting. A critical need in this regard is to maintain confidentiality and security in data management. We provide introductory overviews of federated learning, blockchain, swarm learning, cloud computing, and swarm intelligence. These are the key components and mechanisms for providing innovative solutions for conducting machine learning on decentralized data.

2.1 Federated Learning

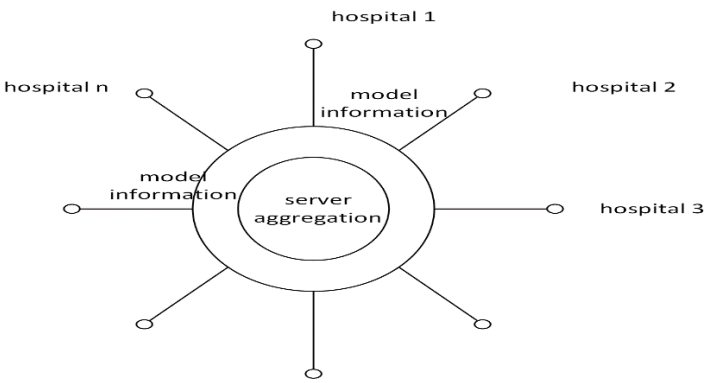
Federated Learning (FL) is an innovative machine learning technique that allows multiple decentralized edge devices or servers to collaboratively learn a shared prediction model while keeping all the training data on the device, without exchanging them (Nguyen 2021; Antunes 2022; Taha 2023). This method addresses various privacy, security, and data locality issues associated with traditional centralized machine-learning approaches. This framework should also support collaborative model training, as seen in Federated Learning (Shiranthika, 2023). To address the challenges of large and diverse datasets, Federated Learning has been proposed as a distributed ML approach (Tedeschini, 2022).

Federated learning(FL) in healthcare is defined as a distributed machine learning approach that allows the training of models on data from multiple sources without sharing the raw data. This is particularly important in healthcare for a variety of reasons such as individual sources do not want to expose their data, there is the sensitive nature of patient data, and the need to utilize as much available data as possible. In this regard, FL has been applied in various healthcare domains, including health data management, remote health monitoring, medical imaging, and COVID-19 (Moon 2023). FL has been identified as having the potential to revolutionize healthcare (Islam, 2022). A detailed discussion of its architecture, privacy mechanisms, and advantages follows.

2.1.1 Typical Federated Learning Components.

In federated learning, data flow is minimal, and at no point is raw data exposed outside of its local setting. The primary data transferred are the parameter updates (e.g., neural network weights or gradients). This significantly reduces the risk of data leakage. The typical system components (Nguyen 2021; Antunes 2022; Taha 2023) are: 1) local units called clients: These are devices or nodes that participate in the federated learning process, each holding their local data unseen by others, 2) aggregators called central server: A server coordinates the learning process, initiates model training rounds, aggregates the updated models from clients, and computes a global model update, 3) communication network: A robust network infrastructure is used to facilitate efficient and secure exchanges between the server and clients. Figure 1 depicts the typical organization of a Federated Learning network.

Figure 1: Federated Learning configuration



International Journal of Business and Applied Social Science

E-ISSN: 2469-6501
VOL: 10, ISSUE: 5
May/2024
DOI: http://dx.doi.org/10.33642/ijbass.v10n5p2

The typical operations in FL are: 1) initialization: The central server initializes a global model and distributes it to selected clients (this is necessary as local units can initiate their model), 2) local model training: Each client trains the model locally using its local, private data (it is also possible to include the use of a shared data set), 3) local updates: After training, clients send their model updates (not the data itself) to the central server. These updates typically consist of weights, gradients, or similar parameters that are typically improved during training, 4) aggregation: The central server aggregates these updates using algorithms such as averaging to update the global model, 5) iteration: The improved global model is sent back to the clients, and the process repeats until the model performance converges or meets a predefined threshold.

FL provides key privacy and security mechanisms FL (Nguyen 2021; Antunes 2022; Taha 2023) such as 1) Data Localization: Since the data remains on the client's device and only model updates are shared, the risk of private data being exposed during transmission is minimized, 2) Secure Aggregation: Protocols such as Secure Multi-party Computation (SMPC) or Homomorphic Encryption (HE) can be used during the aggregation phase to ensure that the server can compute the necessary model updates without actually seeing individual updates, enhancing privacy, 3) Differential Privacy: It has been noted that it may be possible to discern identifying information about clients. One approach to address this is to introduce controlled noise to the model updates sent by the clients to further mask the contributions of individuals. This technique helps in providing a mathematical guarantee of privacy, 4) Robust Communication Protocols: End-to-end encryption can also be used for the sharing of data between the clients and the central server. This can protect against eavesdropping and tampering.

2.1.2 Federated Learning Advantages.

FL has several key advantages over the centralized Approach (Nguyen 2021; Antunes 2022; Taha 2023) including:

- **Enhanced Privacy**: The most significant advantage is enhanced privacy as raw data never leaves the device, reducing the risk of personal data breaches.
- **Scalability**: Federated learning can effectively scale to a large number of participants without the need for massive central data storage and processing capabilities.
- **Reduced Latency**: Local data processing on local devices can significantly reduce the latency involved in making predictions, as the data does not need to be sent over a network to a central server.
- **Utilization of Non-IID Data**: Traditional centralized models often require IID (Independent and Identically Distributed) data for optimal performance. Federated learning, however, can handle non-IID and unbalanced data effectively, as it learns from a multitude of diverse local data distributions.
- **Compliance with Regulations**: By keeping data localized, federated learning naturally supports compliance with strict data privacy regulations like GDPR, which may be more challenging for centralized learning systems.

Thus, federated learning offers a promising alternative to traditional centralized machine learning, especially in scenarios where data privacy is paramount. Its architecture is designed to maximize data privacy while still benefiting from collaborative, decentralized learning, thus providing an optimal solution for developing challenges.

2.2 Blockchain technology

Blockchain technology can be defined as a decentralized digital ledger system that provides a secure and transparent way to record and share information across a network of users. In the context of healthcare, blockchain technology can be applied to enhance data security, integrity, and accessibility while ensuring compliance with privacy regulations. Blockchain technology provides a secure and trustworthy platform for information sharing (Liu 2020), ensuring the integrity and interoperability of electronic health records (Jabbar 2020), and enhancing the transparency and security of medical data (Yuan 2021).

Blockchain in healthcare can facilitate the creation of immutable records of medical data, which can include patient health records, treatment protocols, and pharmaceutical supply chain data. Each block in the chain contains a timestamp and a link to the previous block, creating a chronological and unalterable chain of data entries. This characteristic is particularly useful in healthcare for ensuring the authenticity and non-repudiation of medical records and transactions. Blockchain can also address challenges in health care, such as data sharing and interoperability issues, by creating a mechanism to link personal records and stimulate data sharing (Velmovitsky 2021). Furthermore, it can provide a secure and scalable data-sharing solution (Lokhande 2019), and enable secure healthcare systems by using its decentralized nature (Swetha 2020). Overall, blockchain technology has the potential to improve data integrity and security in healthcare, making it a promising solution for the industry (Brodersen 2016, Baskar 2021). The decentralized nature of blockchain allows multiple stakeholders, including healthcare providers, patients, and even third-party payers to access and contribute to a shared, secure database without requiring a centralized control point. In general, this could potentially streamline processes such as the verification of medical credentials, patient consent management, and the secure transfer of patient medical records across providers. By leveraging blockchain technology, the healthcare sector can significantly reduce fraud, enhance patient safety through more reliable health data, and improve the efficiency of administrative processes.

2.2.1 Federated Learning with Blockchain

The integration of blockchain into federated learning frameworks has been explored extensively, with a focus on enhancing data privacy, security, and reliability. Dai (2023) and Ma (2020) both highlight the potential of blockchain in mitigating privacy information leakage and ensuring the reliability of model parameters. Li (2022) and Li (2021) further discuss the structural design and platform of blockchain-based federated learning, with

International Journal of Business and Applied Social Science
E-ISSN: 2469-6501
VOL: 10, ISSUE: 5
May/2024
DOI: http://dx.doi.org/10.33642/ijbass.v10n5p2

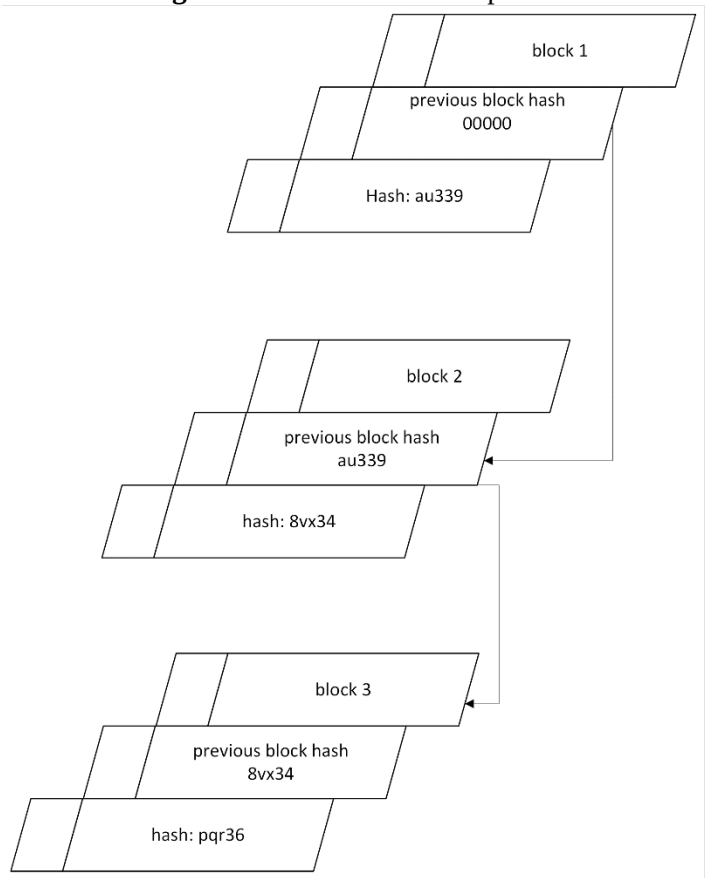
a specific focus on security and privacy mechanisms. Wu (2022) and Lu (2021) propose robust and secure blockchain-based frameworks for federated learning. Wu (2022) and Kasyap (2021) also emphasize the prevention of cybersecurity poisoning attacks. Lu (2021) addresses the security of local parameters and varying resources. Lastly, Li (2020) and Li (2021) introduce decentralized federated learning frameworks that incorporate the notion of committee consensus, leveraging blockchain for global model storage and local model update exchange. These studies collectively underscore the potential of blockchain in addressing the challenges of federated learning, particularly in the areas of privacy, security, and reliability.

The integration of blockchain into federated learning frameworks offers several benefits such as enhanced data privacy protection, incentivized data sharing, and improved verification accountability (Dai2023;Elayan, 2021). However, this integration also presents challenges that include the need for costly computational resources which can limit the participation of resource-constrained local units such as small healthcare facilities or providers (Moore 2023). Blockchain can meet these challenges by providing a decentralized, immutable, and transparent mechanism for securing and verifying data in federated learning environments (Li 2021).

The integration of blockchain and federated learning can facilitate the secure sharing of medical records (Zekiye, 2023). In the context of health professions education, decentralized clinical training programs have been proposed to address the need for healthcare in resource-poor settings (Govender, 2018). Lastly, a decentralized optimization framework has been developed for predictive modeling from federated Electronic Health Records (Brisimi, 2018).

Various architectures and applications of blockchain-based federated learning have been proposed with a focus on addressing the limitations of traditional federated learning which can include single-point failure and lack of motivation (Hou 2021). The use of blockchain in federated learning can also improve performance and enable the development of secure distributed machine learning systems (Li 2022). Decentralized federated learning facilitated by blockchain can further enhance transparency and privacy protection (Bhatia 2022). A multi-layer decentralized framework for robust federated learning, incorporating blockchain, has been proposed to address security issues and prevent central server failure (Wu 2022). Despite these advancements, further research is still needed to address the challenges discussed for successful blockchain-based federated learning (Wang 2021). Figure 2 provides an overview of the Blockchain development.

Figure 2: Blockchain development



2.3 Cloud computing

These diverse components for the development of machine learning models require a strong, reliable infrastructure platform. Cloud computing is a viable solution in this regard. Cloud computing can play a crucial role in healthcare data storage, processing, and accessibility. It can be used in the implementation of health systems such as "Health Care as a Service" (Nur, 2012), and support the processing and storage of

International Journal of Business and Applied Social Science

E-ISSN: 2469-6501
VOL: 10, ISSUE: 5
May/2024
DOI: http://dx.doi.org/10.33642/ijbass.v10n5p2

medical data, particularly in medical imaging (Kagadis, 2013). The applications of cloud computing in health systems include telemedicine, medical imaging, and clinical and hospital information systems (Moghaddasi, 2016). Cloud computing also facilitates real-time data collection and exchange (Aziz, 2016), and its use in healthcare can improve service delivery for patients (Wang, 2013).

However, there are significant concerns about data security and privacy (Tahir, 2020; Calabrese, 2015). To address security and privacy challenges, a novel data protection model has been proposed (Chen, 2011) for cloud platforms. Cloud platforms play a crucial role in supporting complex computations and large-scale data analysis in the field of machine learning and data mining (Marozzo, 2012; Talia, 2015; Pop, 2016; Ren, 2016). These platforms can be used for the introduction of highly complex and sophisticated methods and applications. These platforms provide the necessary infrastructure for developing and executing distributed data analytics applications as well as for integrating data mining methods (Marozzo, 2012; Talia, 2015; Pop, 2016; Ren, 2016). They can also be used for high-performance cloud data mining algorithms and the implementation of scalable knowledge discovery services (Marozzo, 2012; Talia, 2015; Pop, 2016; Ren, 2016). Additionally, cloud platforms have been used for the development of distributed and Software-as-a-Service (SaaS) solutions for machine learning and data mining (Pop, 2016).

2.4 Machine Learning and Data Mining in Healthcare

Machine learning and data mining have become critical tools in healthcare, transforming the way patient data is analyzed and utilized for diagnosis, treatment planning, and outcome prediction (Shailaja, et. al, 2018). Some of the key techniques used are supervised learning, unsupervised learning, deep learning, and associative rule mining. Supervised learning involves training a model on a labeled dataset, where the outcomes are known. This method is frequently used in healthcare for tasks such as diagnostic imaging and disease prediction. Unsupervised learning finds hidden patterns or intrinsic structures from data without the need for labeled outcomes. It's useful in patient segmentation using clustering algorithms. Deep learning, a subset of machine learning involving neural networks with many layers, is profoundly impacting healthcare with highly computational and computationally heavy applications like imaging analysis and drug discovery. Association Rule Mining identifies interesting relations between variables in large databases such as predicting drug interactions and risk factor identification. While integrating these techniques, healthcare faces challenges such as data privacy, varying data quality, and the need for interpretable models. Ensuring data security and addressing ethical concerns are as crucial as the technological advancements themselves. By harnessing these machine learning and data mining techniques, healthcare providers can offer more precise, efficient, and predictive healthcare solutions, ultimately improving patient outcomes and care delivery.

2.5 IoT and Healthcare

The use of IoT in healthcare is a growing area of interest, with a focus on real-time monitoring and data management (Balakrishnan 2021; Rani 2021). This is further enhanced by the integration of AI, which can predict diseases and provide personalized care (Yamini 2020; Mahalakshmi 2019). Collaborative machine learning distributed across IoT devices (simple ones such as edge nodes or complex ones such as computing platforms) through the use of cloud servers can provide not only data analytics insights but also real-time insights (Farahani 2019; Sharma 2020). Cloud computing is, thus, a key component in enabling the processing and analysis of the vast amounts of data collected in the IoT ecosystem (Kandhukuri 2017; Padmavathi 2016).

2.6 Swarm Learning

As discussed earlier, Federated learning has gained significant attention due to its ability to train models across multiple edge devices without sharing data (Li 2019, Gafni 2021). However, it is challenged in terms of data variability, model variability, and tracking performance (Rizk 2020). To address these challenges, researchers have proposed various optimization methods such as multi-objective evolutionary algorithms (Zhu 2018). Despite these efforts, federated learning still lags behind centralized learning in terms of performance (Nilsson 2018). Swarm learning has been proposed as a potential solution to these challenges. The basis of SL is a large number of agents working together to solve a problem. SL has been shown to outperform federated learning in terms of convergence and privacy (Asad 2021).

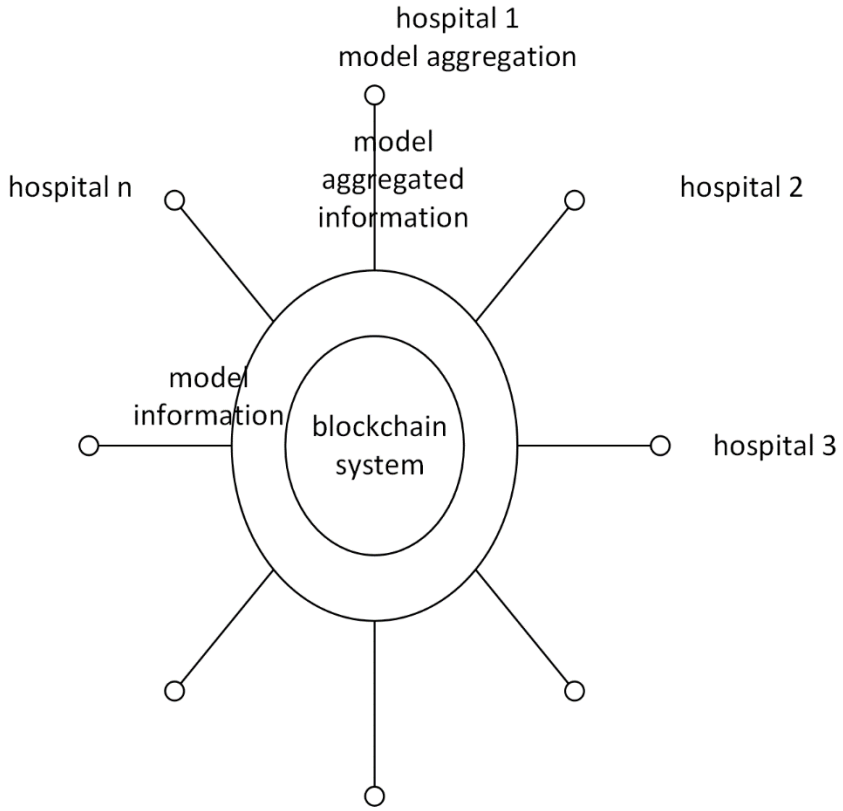
Swarm learning, a decentralized approach to machine learning, offers significant privacy and security benefits by sharing model learnings rather than raw data (Mishra 2023). This approach has been successfully applied in various domains, including autonomous driving (Mishra 2023), drones (Albalawi 2019), and robotics (Prorok 2016). It has also been used in data mining to balance data utility and knowledge privacy (Kalyani 2018), and in privacy-preserving association rule mining (Mandapati 2013, Krishnamoorthy 2017). Furthermore, swarm learning has been combined with differential privacy to protect the broad Data-Information-Knowledge-Wisdom landscape (Li 2021).

SL addresses the challenges of data privacy and safety in healthcare (Becker 2022, Warnat-Herresthal 2021). It has been successfully applied in disease diagnosis and treatment, including the development of disease classifiers (Warnat-Herresthal 2020, Nayar 2019). The integration of Swarm Learning with data mining has also shown promise in healthcare applications (Nayar 2019). Furthermore, Swarm Learning has been used to consolidate knowledge from multi-center non-IID data for medical image segmentation, demonstrating superior performance (Gao 2022). The potential of Swarm Learning in solving healthcare problems continues to be explored (Abdelaziz 2019). However, it is important to note that while swarm learning can improve privacy, it is not immune to security threats, such as data poisoning and adversarial attacks (Gosselin 2022).

International Journal of Business and Applied Social Science
E-ISSN: 2469-6501
VOL: 10, ISSUE: 5
May/2024
DOI: http://dx.doi.org/10.33642/ijbass.v10n5p2

SL eliminates the central server by sharing the parameters with a Swarm network. SL generates local models using local data at the local sites (called Swarm edge nodes). SL utilizes blockchain technology where each node has been pre-authorized which is necessary to execute transactions (new data). Adding new nodes is dynamic utilizing appropriate authorization measures to recognize network nodes. Nodes are added via a formal process including a blockchain smart contract, the model structure, and steps to perform local model training. When defined conditions for synchronization occur, model parameters are exchanged via a Swarm application programming interface (API). The parameters are merged like federated learning to create an updated model with updated parameter settings. The process then starts again with new models generated based on the shared parameters. The blockchain design provides security measures to support data sovereignty, security, and confidentiality. Figure 3 provides an overview of the SL configuration. In architecture, it is similar to federated learning. A key difference is that blockchain technology is used to handle the communication between the local units. Also, a local unit is randomly identified as the aggregator which is Hospital 1 in this figure.

Figure 3: Swarm Learning configuration



2.7 Swarm intelligence

Swarm intelligence (SI) is a field of artificial intelligence that is inspired by the collective behavior of social animals, such as ants, bees, birds, and fish (Kennedy, 2006). This field studies and applies the ways these animals coordinate among themselves and solve complex problems without central control or a single leader. The concept of swarm intelligence arises from biological studies, particularly entomology and ethology, where the focus is on how seemingly simple individuals can perform complex tasks as a group. This behavior is typically observed in colonies of ants, swarms of bees, flocks of birds, and schools of fish.

Swarm intelligence, particularly particle swarm optimization (PSO), has been effectively used in developing machine learning models. Blamah (2013) and Khajenejad (2006) both enhanced PSO by incorporating learning capabilities and Q-learning, respectively, into the particle agents. Winklerová (2013) proposed a Maturity Model to assess the collective intelligence of the swarm, while Notsu (2009) and Rodriguez (2004, 2009) focused on improving learning efficiency and problem-solving capabilities through social space segmentation and distributed learning algorithms. Sousa (2004) further demonstrated the suitability of PSO for data mining and classification tasks. These studies collectively highlight the potential of swarm intelligence, particularly PSO, in developing machine learning models, with each particle acting as a local agent.

The SI systems are characterized by self-organization and decentralized decision-making processes (Dorigo, 2007): Self organization is a process where a structure or pattern appears in a system without a central authority or external element imposing it. The rules followed by individuals are based on local, and often simple, interactions. These are based on using positive feedback which is the enhancement or amplification of actions taken by the group, such as the trail reinforcement mechanism seen in ants finding food and negative feedback to

International Journal of Business and Applied Social Science

E-ISSN: 2469-6501
VOL: 10, ISSUE: 5
May/2024
DOI: http://dx.doi.org/10.33642/ijbass.v10n5p2

maintain system stability, preventing the overexploitation of resources and reducing the impact of overly rapid positive feedback. Additionally, random, probabilistic behavior is incorporated where random actions by individuals can help explore unknown areas and avoid rigid patterns, contributing to flexibility and adaptation. Also, frequent interactions among individuals, which are typically simple (like ants leaving pheromone trails), lead to the emergence of complex group behavior.

There are several advantages from using Swarm Intelligence. One is robustness the decentralized nature of swarm intelligence allows systems to continue functioning even if some individuals fail. Another is flexibility Systems can quickly adapt to changes in the environment or in the task without needing reprogramming or human intervention. A third is scalability in that the principles and systems can be applied to small-scale operations as well as to larger, more complex tasks without significant redesign.

However, there two key challenges involved in implementing SI (Liu, 2000). One is control and predictability since managing and predicting the behavior of decentralized, self-organizing systems can be challenging, particularly under varying environmental conditions. Another is complexity since SI typically involves developing mathematical models that accurately describe swarm behavior. This remains a complex task and thereby limiting theoretical understanding and practical implementation.

Swarm intelligence extends its application to various domains, including healthcare, particularly in decentralized data mining (Nayar, 2019). This application leverages the self-organizing and robust characteristics of swarm principles to enhance data analysis and decision-making processes in medical environments. Swarm intelligence contributes to solving decentralized data mining challenges in healthcare: 1) Decentralized data management where swarm intelligence algorithms, such as those inspired by ant colony optimization, can efficiently manage and mine this decentralized data by optimizing data retrieval and integration processes without the need for a centralized database. 2) feature selection and optimization where swarm algorithms like Particle Swarm Optimization (PSO) are used to select optimal subsets of features that contribute to accurate disease diagnosis or treatment outcomes. This is particularly crucial in genomics and personalized medicine, where patient-specific data varieties are vast. 3) predictive analytics where swarm intelligence can enhance predictive models in healthcare by optimizing them to handle diverse and voluminous data. 4) parallel processing where the decentralized nature of swarm intelligence also allows for the parallel processing of data, thereby speeding up the analytics and ensuring timely decision-making in clinical settings. 5) collaborative diagnostics can be achieved by simulating the collaborative behavior seen in natural swarms, swarm intelligence where multiple algorithms or agents work together to diagnose diseases based on symptoms presented across different patient data points. 6) resource allocation where swarm intelligence algorithms can be applied to optimize the allocation of limited healthcare resources, such as hospital beds, medical staff, and critical medical supplies, particularly in pandemic situations or areas with limited infrastructure

2.8 Swarm Intelligence and IoT in Healthcare

Swarm intelligence seamlessly integrates with the Internet of Things (IoT) framework to revolutionize decentralized data mining in healthcare (Alizadehsani, 2023). This combination harnesses the power of distributed devices and the collaborative decision-making traits of swarm intelligence to optimize healthcare data analysis and management. The IoT framework enhanced with swarm intelligence can addresses healthcare challenges in several key ways: 1) data collection and aggregation where the individual local devices or units can continually collect health-related data from patient's part of the IoT ecosystem and generate vast amounts of data regarding vital signs, physical activity, and environmental conditions. 2) Swarm intelligence algorithms can coordinate the activities of these devices, ensuring that data collection is optimized and relevant data points are prioritized for transmission and analysis. This process mimics natural swarms where individuals adjust their roles based on the needs of the group. 3) Incorporating swarm intelligence into the IoT framework allows for edge computing (local unit) capabilities where data can be processed locally on IoT devices rather than being sent to a central server reducing latency, enhances response times, and maintains data privacy. 4) Decentralized decision making can occur when IoT devices equipped with swarm intelligence can make decentralized decisions. For instance, if a patient's data indicates a potential health issue, the system can autonomously decide to alert medical personnel or adjust the monitoring parameters. 5) Scalability and adaptability can be achieved. Swarm intelligence provides a scalable approach as more devices are added the swarm algorithms can efficiently integrate and manage these new nodes without the need for significant restructuring. Adaptability is achieved to meet the challenge that healthcare environments are dynamic. Swarm intelligence enables IoT frameworks to adapt to changing conditions.

Two key outcomes result from utilizing swarm intelligence: 1) predictive maintenance and operational efficiency 2) enhanced data security. Predictive maintenance occurs when swarm intelligence is used to predict device failures or maintenance needs by analyzing operational data across the swarm of devices, thus preventing downtime and ensuring consistent data quality. Resource optimization is achieved by using swarm intelligence algorithms to optimize the use of computational and communication resources across IoT devices to achieve overall system efficiency. Enhanced data security is gained through the decentralized nature of swarm intelligence, combined with the IoT framework, enhances data security. By distributing data processing and storage across multiple devices, the system reduces the vulnerability associated with central data repositories. Also swarm algorithms can dynamically adjust security measures

International Journal of Business and Applied Social Science
E-ISSN: 2469-6501
VOL: 10, ISSUE: 5
May/2024
DOI: http://dx.doi.org/10.33642/ijbass.v10n5p2

based on detected threats or vulnerabilities, much like a swarm changing its configuration to protect itself from predators.

Swarm intelligence and IoT are increasingly being used in healthcare to improve patient care and optimize healthcare systems. El-Shafeiy (2020) and Roshanzamir (2022) both highlight the potential of swarm intelligence in the Internet of Medical Things (IoMT) for data analysis and management, which can aid in real-time decision-making and remote patient monitoring. Nayar (2019) and Alizadehsani (2023) further discuss the application of swarm intelligence in disease prognosis, diagnosis, and treatment, as well as in addressing optimization problems in IoMT. The integration of AI with IoT in healthcare, as explored by Yamini (2020), Mahalakshmi (2019), and Abualsaud (2022), further enhances the potential of these technologies in predicting diseases, monitoring vital signs, and automating medical decisions. Elango (2023) also emphasizes the role of IoT in remote health monitoring, particularly through smart wearable devices. These studies collectively demonstrate the significant potential of swarm intelligence and IoT in transforming healthcare delivery and management.

The integration of swarm intelligence with the IoT framework in healthcare not only maximizes the utility of distributed data and devices but also brings forth improvements in system responsiveness, patient-specific care, and operational security. This approach is particularly vital in crafting resilient healthcare systems that can thrive in the face of diverse and evolving challenges.

3. Requirements for decentralized learning in healthcare

In this section, we discuss the requirements for a decentralized health care system that uses machine learning by local agents to derive a global model. The requirements are identified at the operational level as well as at the overall system behavior. We then discuss how existing methodologies and technologies can be used components for a global modeling system.

3.1 System Requirements

The basic requirements for decentralized learning in healthcare are based on the assumption a computational ecosystem is in place that provides that a healthcare to a diverse population in a variety of settings. The requirements are based on the need for providing a solution *for decentralized AI systems which accommodates inherently decentralized data structures and data privacy and security regulations in medicine.* The basic requirements are of four areas: 1) data privacy and security, 2) decentralization, 3) performance and 4) ecosystem.

Data and data privacy and security. Data privacy and security are a key factor in developing a system that has local units or components. The system needs to provide a high-level data security that includes patient, practitioner privacy information as well safeguarding data at all levels: access, storage, location, and integrity. There are several key aspects to this:

- *Data is maintained at the local level and is not shared between the local components to maintain a high level of privacy.*
- *The system has the ability to handle large and small data sets.*
- *Exchange of raw data among the local units is not required. This is a basic requirement.*

Decentralization of model development. The main focus of this system is to address the generation and development of machine learning models when the data is decentralized and not shared. Each local unit generates and develops a model. The requirements will need to address:

- *Local data modeling and local autonomy.*
- *A global system is made up of local units (agents). The global system is derived from the interaction between the local units.*
- *Machine learning model parameters are shared but not the data used.*
- *Guarantee secure, transparent and fair onboarding of decentralized (local) units of the system without the need for a central controller.*

System Performance. In order for the system to be effective, several aspects of system performance need to be considered. One is the modeling computational load for each local unit. Another is the minimization of communication among the system components or units. A third is that the system is scalable and adaptive. These can be determined to be:

- *Computational load at the units is adequate and sustainable. Information from local units is aggregated or combined of the local and aggregation can be adaptive to allow for aggregation methods that utilize local unit performance such as accuracy.*
- *A global model meets a baseline level of performance.*
- *Communication via network linkages is minimized which results in reducing data traffic and unit to unit communication. System performance can be impacted if there is a high level of network communication.*
- *The system can increase capacity as needed and local units can come and go.*

Ecosystem environment. A strong ecosystem environment protects the machine learning models from attacks. Since the system utilizes communication between the local components, the sharing of the machine learning model information is vulnerable to cyber-attacks during these times. In addition, we utilize an explainable architecture where the configuration of the interacting components is understandable from an external perspective. The system can be implemented in current and evolving computing environments such as cloud computing**.** Overall the system is reliable, trustworthy, and resilient in an environment that can impact privacy, performance, and system integrity.

4. System Architecture

We have identified the background information related to providing a computational solution for machine learning (ML)

International Journal of Business and Applied Social Science
E-ISSN: 2469-6501
VOL: 10, ISSUE: 5
May/2024
DOI: http://dx.doi.org/10.33642/ijbass.v10n5p2

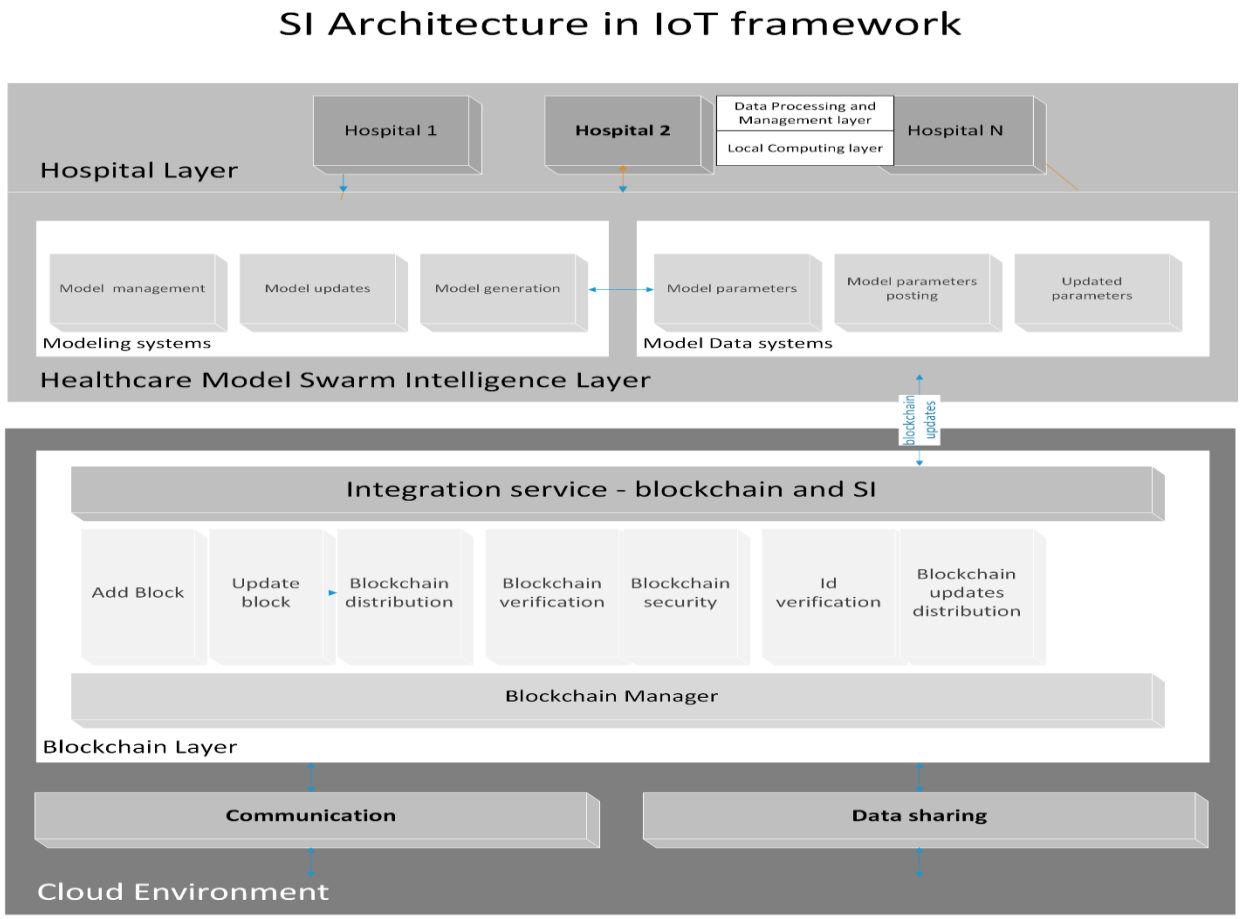
system that functions in a decentralized solution for the development of a global machine learning model and we have identified the key system requirements for such a system in a healthcare environment. In this section, we will discuss a system architecture that meets the system requirements presented in Section 3. The system architecture is based on a swarm intelligence framework utilizing communication and information integration mechanisms used in particle swarm optimization.

4.1 Internet of Things (IoT) framework

The Internet of Things (IoT) framework provides an abstract scaffolding that lends itself for implementing a swarm intelligence based architecture. IoT typically involves a network of interconnected devices that collect, transmit, and process data to enable intelligent decision-making across various environments and sectors. The integration of distributed intelligence within this framework addresses system efficiency and responsiveness.

A cloud environment is the underlying infrastructure for this system. A cloud environment provides a platform neutral environment and can provide scalability of system operations as well as a high level of security. The cloud environment incorporates a blockchain system which is used to transmit model information from one part to other parts for further processing or action. This is achieved through various communication protocols and network solutions such as Wi-Fi, Bluetooth, cellular networks, and Low-Power Wide-Area Networks (LPWAN). In distributed intelligence, this is crucial for enabling devices to share insights and collaborate on decisions without central oversight. Figure 4 provides the conceptual model for the architecture.

Figure 4: Swarm Intelligence System Architecture



4.2 Distributed swarm intelligence for health care

There are five layers involved in the architecture for utilizing distributed swarm intelligence to satisfy the system requirements identified in section 3.

The first layer is the hospital layer which is based on the IoT framework and involves developing local computing units to address the business needs of the hospital. At this level local data can be gathered in real-time data, stored, and processed. In a distributed intelligence setup, these devices are capable of processing data locally, allowing for immediate responses to changes without needing to communicate with a central server.

The second layer is data processing and management. Traditionally, IoT systems rely on cloud computing for data processing; however, with distributed intelligence, much of the processing occurs at the edge of the network. Edge computing devices process data locally, reducing latency and bandwidth usage. This localized processing capability allows for quicker decision-making and can operate independently of central systems, which is advantageous for real-time applications such as autonomous vehicles or industrial automation.

The third layer is the local computing layer. This layer includes the user interfaces and business applications that utilize the processed data to perform specific tasks and deliver services.

International Journal of Business and Applied Social Science

E-ISSN: 2469-6501
VOL: 10, ISSUE: 5
May/2024
DOI: http://dx.doi.org/10.33642/ijbass.v10n5p2

In the context of distributed intelligence, applications can adapt to data inputs more dynamically and operate in a semi-autonomous manner. For example, a smart home system might automatically adjust heating and lighting based on occupancy and user preferences learned over time.

The fourth layer is the Healthcare Model Swarm Intelligence Layer. Distributed intelligence leverages advanced analytics and machine learning algorithms at various points in the IoT framework. These algorithms are deployed both in the cloud and on edge devices. They enable devices to learn from data patterns, predict future events, and make decisions independently. This capability is key to optimizing operations, enhancing user experiences, and managing resources efficiently.

The fifth layer is the Blockchain Layer. With increased data processing at the device and edge levels, security becomes a paramount concern. The distributed nature of intelligence requires robust encryption, secure data transmission protocols, and continuous security updates to protect against vulnerabilities. In figure 3, the key function of the blockchain layer are identified and are based on the common blockchain components. Incorporated within the blockchain layer is the service for the integration of blockchain mechanisms and the swarm intelligence layer.

4.3 Emergence of collective intelligence.

4.3.1 Communication

The key aspect of the system is how the local computing units communicate with each other and how the developing local machine learning models are integrated. Based on the Particle Swarm Optimization algorithm each local unit (agent) is capable and able to share is current information. How this is accomplished depends on the nature of the system component: biological versus artificial. It also depends on the nature of the information such as behavioral or information sharing. In this system, we focus on the sharing of the local model information with the members of the swarm. The swarm includes all the local computing units in this case. So, it is necessary that the information from all units is incorporated.

4.3.2 Aggregation of information

Each local unit uses the blockchain layer access the combined information from the local units. The units communicate with the blockchain either to request a connection or to provide information. The blockchain mechanism then provides the necessary data after verification of the local unit's access to the blockchain information. In this configuration, the method for aggregation is based on the choice of the system architect. The basic methods for aggregation are averaging of model information and optimization by selecting the model with the best results and sharing that.

4.3.3 Adaptive system performance and use

The blockchain enables the system to add or remove local computing units. The resulting system performance is based on the remaining units. The system architect can determine the frequency with which local units interact with the blockchain. However, the system should not make changes that result in a lower level of performance. Additionally, it is possible to weight the information from a local unit based on accuracy or other performance measures.

In a practical scenario, consider a smart city with IoT-enabled traffic management systems. Traffic sensors collect data on vehicle flow, and instead of sending all data back to a central system, local processors analyze this data to adjust traffic signals in real time to optimize flow. Simultaneously, some data is sent to central systems for long-term traffic planning and coordination with other city services.

By integrating distributed intelligence, IoT frameworks can enhance responsiveness, reduce dependence on central systems, and enable more personalized and context-aware services. This decentralized approach also helps in scaling the system efficiently as the number of connected devices grows.

Integrating swarm intelligence into decentralized data mining in healthcare not only enhances the efficiency and accuracy of data analysis but also ensures robustness, flexibility, and scalability in managing health data. These benefits are particularly important in improving patient outcomes and operational efficiency in the increasingly complex and data-driven landscape of modern healthcare.

5. CONCLUSION

This study highlights the challenges in healthcare data management, primarily driven by the escalating complexity and volume of data, alongside critical needs for privacy and security. By integrating basic concepts of advanced methodologies like federated learning (FL) and swarm learning (SL) with blockchain technology, cloud computing, and the Internet of Things (IoT) base on a Swarm Intelligence framework, we propose a robust solution to these challenges. Federated learning enhances data privacy by enabling machine learning across multiple sites without sharing raw data, while swarm learning decentralizes the learning process further, eliminating the need for a central coordinator. Blockchain integration ensures the integrity and security of data exchanges within these frameworks, thus enhancing trust and compliance with regulatory standards. Furthermore, the synergy between cloud computing and IoT facilitates scalable and efficient data processing and management, essential for handling the growing data demands of modern healthcare systems.

The proposed system architecture leverages the strengths of these technologies to deliver a scalable, secure, and privacy-preserving framework that could significantly improve the management, sharing, and utilization of healthcare data. This, in turn, promises to enhance patient care and operational efficiency across healthcare settings. Future research should focus on refining these integrative models, addressing potential technological and implementation challenges, and evaluating their effectiveness in real-world healthcare environments. Through continuous innovation and collaboration, the goal of achieving a transformative impact on healthcare informatics, thereby improving the quality of life and healthcare outcomes for patients globally, appears increasingly attainable.

International Journal of Business and Applied Social Science

E-ISSN: 2469-6501
VOL: 10, ISSUE: 5
May/2024
DOI: http://dx.doi.org/10.33642/ijbass.v10n5p2

The existing literature on blockchain technology, cloud computing, and federated learning in the healthcare sector highlights several key areas for future research. Ermakova (2013) and Stantchev (2014) both emphasize the need for further development and validation of cloud-based applications and platforms, particularly in the context of healthcare. Soltanisehat (2020) and Kassab (2019) underscore the potential of blockchain in healthcare, with a focus on technical aspects and the need for prototype implementations. He (2023) and Agbo (2019) both identify the potential of blockchain and federated learning in overcoming data silos and enhancing data security in healthcare. However, they also highlight the need for further research to evaluate the effectiveness of these technologies. Al-asmari (2021) and Elghoul (2021) both discuss the advantages and challenges of blockchain technology in healthcare, with a focus on security and scalability. These studies collectively underscore the need for further research to address these gaps and to design a comprehensive system architecture for hospitals.

REFERENCES

Albalawi, M., & Song, H. (2019). Data Security and Privacy Issues in Swarms of Drones. *2019 Integrated Communications, Navigation and Surveillance Conference (ICNS)*, 1-11.

Abdelaziz, A., Salama, A.S., & Riad, A.M. (2019). A Swarm Intelligence Model for Enhancing Hea Abouelmehdi, Karim,

Abderrahim Beni Hssane, Hayat Khaloufi and Mostafa Saadi. "Big data security and privacy in healthcare: A Review." EUSPN/ICTH (2017).

Abualsaud, K. (2022). Machine learning algorithms and internet of things for healthcare: A survey. IEEE Internet of Things Magazine, 5(2), 133-139.

Alizadehsani, R., Roshanzamir, M., Izadi, N.H., Gravina, R., Kabir, H.M., Nahavandi, D., Alinejad-Rokny, H., Khosravi, A., Acharya, U.R., Nahavandi, S., & Fortino, G. (2023). Swarm Intelligence in Internet of Medical Things: A Review. Sensors (Basel, Switzerland), 23.

Andrew Hard, Kanishka Rao, Rajiv Mathews, Swaroop Ramaswamy, Françoise Beaufays, Sean Augenstein, Hubert Eichner, Chloé Kiddon, and Daniel Ramage. Federated learning for mobile keyboard prediction. arXiv preprint arXiv:1811.03604, 2018.

Antunes, R.S., André da Costa, C., Küderle, A., Yari, I.A., & Eskofier, B. (2022). Federated Learning for Healthcare: Systematic Review and Architecture Proposal. ACM Transactions on Intelligent Systems and Technology (TIST), 13, 1 - 23.

Asad, M., Moustafa, A., & Ito, T. (2021). Federated Learning Versus Classical Machine Learning: A Convergence Comparison. ArXiv, abs/2107.10976.

Aziz, H. (2016). Cloud Computing and Healthcare Services. Journal of Biosensors and Bioelectronics, 7, 1-4.

Balakrishnan, L., & Krishnaveni (2021). An Internet of Things(IoT) Based Intelligent Framework for Healthcare – A Survey. 2021 3rd International Conference on Signal Processing and Communication (ICPSC), 243-251.

Baskar, S., Ramar, K., & Shanmugasundaram, H. (2021). Data Security in Healthcare Using Blockchain Technology. 2021 International Conference on Decision Aid Sciences and Application (DASA), 354-359.

Blamah, N.V., Adewumi, A.O., Wajiga, G.M., & Baha, B.Y. (2013). An Intelligent Particle Swarm Optimization Model Based on Multi-Agent System.

Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Aguera y Arcas. Communication-efficient learning of deep networks from decentralized data. In Artificial Intelli- gence and Statistics, pages 1273–1282. PMLR, 2017.

Brodersen (2016). Blockchain: Securing a New Health Interoperability Experience.

Bhatia, L., & Samet, S. (2022). Decentralized Federated Learning: A Comprehensive Survey and a New Blockchain-based Data Evaluation Scheme. 2022 Fourth International Conference on Blockchain Computing and Applications (BCCA), 289-296.

Brum, R.C., Drummond, L.M., Castro, M.C., & Teodoro, G. (2021). Towards Optimizing Computational Costs of Federated Learning in Clouds. 2021 International Symposium on Computer Architecture and High Performance Computing Workshops (SBAC-PADW), 35-40.

Calabrese, B., & Cannataro, M. (2015). Cloud Computing in Healthcare and Biomedicine. Scalable Comput. Pract. Exp., 16.

Chen, L., & Hoang, D.B. (2011). Novel Data Protection Model in Healthcare Cloud. 2011 IEEE International Conference on High Performance Computing and Communications, 550-555.

Chen, R. J., Lu, M. Y., Chen, T. Y., Williamson, D. F. K. & Mahmood, F. Synthetic data in machine learning for medicine and healthcare. Nat. Biomed. Eng. 5, 493–497 (2021).

Chi, Y. (2021). Application and Research of Deep Mining of Health Medical Big Data Based on Internet of Things. 2021 3rd International Conference on Artificial Intelligence and Advanced Manufacture.

International Journal of Business and Applied Social Science

E-ISSN: 2469-6501
VOL: 10, ISSUE: 5
May/2024
DOI: http://dx.doi.org/10.33642/ijbass.v10n5p2

Dai, W., Liang, Z., Huang, Y., Jiang, R., Qin, M., & Han, B. (2023). Blockchain combined with Federated Learning technology research. 2023 IEEE 7th Information Technology and Mechatronics Engineering Conference (ITOEC), 7, 1866-1873.

Deepa, S., Sridhar, K.P., Baskar, S., Mythili, K.B., Reethika, A., & Hariharan, P.R. (2022). IoT-enabled smart healthcare data and health monitoring based machine learning algorithms. J. Intell. Fuzzy Syst., 44, 2927-2941.

Dorigo, M., Birattari, M., Garnier, S., Hamann, H., de Oca, M. M., Solnon, C., & Stützle, T. (2007). Swarm intelligence. Scholarpedia, 2(9), 1462.

Duan, Q., Hu, S., Deng, R., & Lu, Z. (2022). Combined Federated and Split Learning in Edge Computing for Ubiquitous Intelligence in Internet of Things: State-of-the-Art and Future Directions. Sensors (Basel, Switzerland), 22.

Elango, S., Manjunath, L., Prasad, D.R., Sheela, T., Ramachandran, G., & Selvaraju, S. (2023). Super Artificial Intelligence Medical Healthcare Services and Smart Wearable System based on IoT for Remote Health Monitoring. 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT), 1180-1186.

El-Shafeiy, E.A., & Abohany, A.A. (2020). A new swarm intelligence framework for the Internet of Medical Things system in healthcare.

Esposito, C., Santis, A.D., Tortora, G., Chang, H., & Choo, K. (2018). Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? IEEE Cloud Computing, 5, 31-37.

Farahani, B.J., Barzegari, M., & Aliee, F.S. (2019). Towards Collaborative Machine Learning Driven Healthcare Internet of Things. Proceedings of the International Conference on Omni-Layer Intelligent Systems.

Fang, C., Guo, Y., Wang, N., & Ju, A. (2020). Highly efficient federated learning with strong privacy preservation in cloud computing. Comput. Secur., 96, 101889.

Fotohi, R., Shams Aliee, F., & Farahani, B. (2022). Federated Learning: Solutions, Challenges, and Promises. 2022 6th Iranian Conference on Advances in Enterprise Architecture (ICAEA), 15-22.

Gafni, T., Shlezinger, N., Cohen, K., Eldar, Y.C., & Poor, H.V. (2021). Federated Learning: A signal processing perspective. IEEE Signal Processing Magazine, 39, 14-41.

Gao, Z., Wu, F., Gao, W., & Zhuang, X. (2022). A New Framework of Swarm Learning Consolidating Knowledge From Multi-Center Non-IID Data for Medical Image Segmentation. IEEE Transactions on Medical Imaging, 42, 2118-2129.

Ghallabi, S., Essalmi, F., Jemni, M., & Kinshuk (2014). Enhanced Federation and Reuse of E-Learning Components Using Cloud Computing. International Conference on Smart Learning Environments.

Gosselin, R., Vieu, L., Loukil, F., & Benoît, A. (2022). Privacy and Security in Federated Learning: A Survey. Applied Sciences.

Hou, D., Zhang, J., Man, K.L., Ma, J., & Peng, Z. (2021). A Systematic Literature Review of Blockchain-based Federated Learning: Architectures, Applications and Issues. 2021 2nd Information Communication Technologies Conference (ICTC), 302-307.

Howard, F. M. et al. The impact of site-specific digital histology signatures on deep learning model accuracy and bias. Nat. Commun. 12, 4423 (2021).

H.S., Foersch, S., Hoffmeister, M., Truhn, D., & Kather, J.N. (2021). Swarm learning for decentralized artificial intelligence in cancer histopathology. Nature Medicine, 28, 1232 - 1239.

Islam, T.U., Ghasemi, R., & Mohammed, N. (2022). Privacy-Preserving Federated Learning Model for Healthcare Data. 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), 0281-0287.

Jabbar, R., Fetais, N., Krichen, M., & Barkaoui, K. (2020). Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity. 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), 310-317.

Kagadis, G.C., Kloukinas, C., Moore, K.L., Philbin, J., Papadimitroulas, P.G., Alexakos, C., Nagy, P.G., Visvikis, D., & Hendee, W.R. (2013). Cloud computing in medical imaging. Medical physics, 40 7, 070901.

Krishnan, P., Jeyabalan, J., Soundarrajan, S., & Jaikumar, A. (2015). EFFICIENT CLINICAL DATA ANALYSIS USING INTERNET OF THINGS.

Kalyani, G., Chandra, ·.M., Rao, S., Janakiramaiah, ·.B., & Chandra, M.V. (2017). Particle Swarm Intelligence and Impact Factor-Based Privacy Preserving Association Rule Mining for Balancing Data Utility and Knowledge Privacy. Arabian Journal for Science and Engineering, 43, 4161 - 4178.

Kandhukuri, A., & Rammohan, B. (2017). Implement Iot -Based Health Care Solutions Based On Cloud Computing. International Journal of Research, 4, 365-372.

Kechadi, Mohand Tahar. “Healthcare Big Data: Challenges and Opportunities.” International Conference on Big Data and Advanced Wireless Technologies (2016).

Khajenejad, M., Afshinmanesh, F., Marandi, A., & Araabi, B.N. (2006). Intelligent Particle Swarm Optimization Using Q-Learning.

International Journal of Business and Applied Social Science

E-ISSN: 2469-6501
VOL: 10, ISSUE: 5
May/2024
DOI: http://dx.doi.org/10.33642/ijbass.v10n5p2

Khatoon, A. (2020). A Blockchain-Based Smart Contract System for Healthcare Management. Electronics.

Kourtellis, N., Katevas, K., & Perino, D. (2020). FLaaS: Federated Learning as a Service. Proceedings of the 1st Workshop on Distributed Machine Learning.

Krishnamoorthy, S., Sadasivam, G.S., Rajalakshmi, M., Kowsalyaa, K., & Dhivya, M. (2017). Privacy Preserving Fuzzy Association Rule Mining in Data Clusters Using Particle Swarm Optimization. Int. J. Intell. Inf. Technol., 13, 1-20.

Li, C., Yuan, Y., & Wang, F. (2021). Blockchain-enabled Federated Learning: A Survey. 2021 IEEE 1st International Conference on Digital Twins and Parallel Intelligence (DTPI), 286-289.

Li, D., Han, D., Weng, T., Zheng, Z., Li, H., Liu, H., Castiglione, A., & Li, K. (2022). Blockchain for federated learning toward secure distributed machine learning systems: a systemic survey. Soft Computing, 26, 4423 - 4440.

Li, T., Sahu, A., Talwalkar, A., & Smith, V. (2019). Federated Learning: Challenges, Methods, and Future Directions. IEEE Signal Processing Magazine, 37, 50-60.

Li, Y., Chen, C., Liu, N., Huang, H., Zheng, Z., & Yan, Q. (2020). A Blockchain-Based Decentralized Federated Learning Framework with Committee Consensus. IEEE Network, 35, 234-241.

Li, Y., Duan, Y., Maamar, Z., Che, H., Spulber, A., & Fuentes, S. (2021). Swarm Differential Privacy for Purpose Driven Data-Information-Knowledge-Wisdom Architecture. ArXiv, abs/2105.04045.

Li, Z., Li, Q., Zhou, Y., Zhong, W., Zhang, G., & Wu, C. (2023). Edge-cloud Collaborative Learning with Federated and Centralized Features. Proceedings of the 46th International ACM SIGIR Conference on Research and Development in Information Retrieval.

Liu, H., Crespo, R.G., & Martínez, O.S. (2020). Enhancing Privacy and Data Security across Healthcare Applications Using Blockchain and Distributed Ledger Concepts. Healthcare, 8.

Liu, L., Zhang, J., Song, S.H., & Letaief, K.B. (2019). Client-Edge-Cloud Hierarchical Federated Learning. ICC 2020 - 2020 IEEE International Conference on Communications (ICC), 1-6.

Liu, Y., & Passino, K. M. (2000). Swarm intelligence: Literature overview. Department of electrical engineering, the Ohio State University.

Loftus, Tyler J., Matthew M. Ruppert, Benjamin Shickel, Tezcan Ozrazgat-Baslanti, Jeremy A. Balch, Philip A. Efron, Gilbert R. Upchurch, Parisa Rashidi, Christopher Tignanelli, Jiang Bian and Azra Bihorac. “Federated learning for preserving data privacy in collaborative healthcare research.” Digital Health 8 (2022): n. pag.

Lokhande, S., Mukadam, S., Chikane, M., & Bhonsle, M. (2019). Enhanced Data Sharing with Blockchain in Healthcare. Lecture Notes in Electrical Engineering.

Lu, M. Y. et al. Federated learning for computational pathology on gigapixel whole slide images. Med. Image Anal. 76, 102298 (2022).

Lu, Y., Huang, X., Zhang, K., Maharjan, S., & Zhang, Y. (2021). Blockchain and Federated Learning for 5G Beyond. IEEE Network, 35, 219-225.

Ma, C., Li, J., Ding, M., Shi, L., Wang, T., Han, Z., & Poor, H.V. (2020). When Federated Learning Meets Blockchain: A New Distributed Learning Paradigm. IEEE Computational Intelligence Magazine, 17, 26-33.

Mahalakshmi, S. (2019). Artificial Intelligence with the Internet of Things on Healthcare systems: A Survey. International Journal of Advanced Trends in Computer Science and Engineering.

Mammen, P.M. (2021). Federated Learning: Opportunities and Challenges. ArXiv, abs/2101.05428

Mandapati, S., Bhogapathi, R.B., & Rao, S. (2013). Swarm Optimization Algorithm for Privacy Preserving in Data Mining.

Marozzo, F., Talia, D., & Trunfio, P. (2012). A Cloud Framework for Big Data Analytics Workflows on Azure. High Performance Computing Workshop.

Matthias Paulik, Matt Seigel, Henry Mason, Dominic Telaar, Joris Kluivers, Rogier van Dalen, Chi Wai Lau, Luke Carlson, Filip Granqvist, Chris Vandevelde, et al. Federated evaluation and tun- ing for on-device personalization: System design & applications. arXiv preprint arXiv:2102.08503, 2021

Mishra, A., Jefferson, O.P., Kapur, P., Kannur, K., Agarwal, P., & Arya, A. (2023). Swarm Learning In Autonomous Driving: A Privacy Preserving Approach. Proceedings of the 2023 15th International Conference on Computer Modeling and Simulation.

Moghaddasi, H., & Tabrizi, A.T. (2016). Applications of Cloud Computing in Health Systems. Global Journal of Health Science, 9, 33.

Moon, S., & Lee, W.H. (2023). Privacy-Preserving Federated Learning in Healthcare. 2023 International Conference on Electronics, Information, and Communication (ICEIC), 1-4.

International Journal of Business and Applied Social Science

E-ISSN: 2469-6501
VOL: 10, ISSUE: 5
May/2024
DOI: http://dx.doi.org/10.33642/ijbass.v10n5p2

Moore, E., Imteaj, A., Rezapour, S., M. Hadi Amini, S.M., Amini, M.H., & Imteaj, F.A. (2023). A Survey on Secure and Private Federated Learning Using Blockchain: Theory and Application in Resource-Constrained Computing. IEEE Internet of Things Journal, 10, 21942-21958.

Mukhtar, Wafaa Faisal and Eltayeb Salih Abuelyaman. "Opportunities and Challenges of Big Data in Healthcare." Data Analytics in Medicine (2020).

Nayar, N.M., Ahuja, S., & Jain, S. (2019). Swarm intelligence and data mining: a review of literature and applications in healthcare. Proceedings of the Third International Conference on Advanced Informatics for Computing Research - ICAICR '19.

Nguyen, D.C., Pham, V.Q., Pathirana, P.N., Ding, M., Seneviratne, A.P., Lin, Z., Dobre, O.A., & Hwang, W.J. (2021). Federated Learning for Smart Healthcare: A Survey. ACM Computing Surveys (CSUR), 55, 1 - 37.

Nilsson, A., Smith, S., Ulm, G., Gustavsson, E., & Jirstrand, M. (2018). A Performance Evaluation of Federated Learning Algorithms. Proceedings of the Second Workshop on Distributed Infrastructures for Deep Learning.

Notsu, A., Honda, K., Ichihashi, H., & Wada, H. (2009). Particle Swarm in State and Action Space for Q-learning.

Nur, F.N., & Moon, N.N. (2012). Health care system based on Cloud Computing.

Padmavathi, B., & Rana, S.T. (2016). Implementation of IOT Based Health Care Solution Based on Cloud Computing. International Journal of Engineering and Computer Science.

Patel, V., Bhattacharya, P., Tanwar, S., Gupta, R., Sharma, G., Bokoro, P.N., & Sharma, R. (2022). Adoption of Federated Learning for Healthcare Informatics: Emerging Applications and Future Directions. IEEE Access, 10, 90792-90826.

Petri, I., Beach, T.H., Zou, M., Montes, J.D., Rana, O.F., & Parashar, M. (2014). Exploring Models and Mechanisms for Exchanging Resources in a Federated Cloud. 2014 IEEE International Conference on Cloud Engineering, 215-224.

Pfitzner, Bjarne, Nico Steckhan and Bert Arnrich. "Federated Learning in a Medical Context: A Systematic Literature Review." ACM Trans. Internet Techn. 21 (2021): 50:1-50:31.

Pop, D. (2016). Machine Learning and Cloud Computing: Survey of Distributed and SaaS Solutions. ArXiv, abs/1603.08767.

Prokofieva, M., & Miah, S.J. (2019). Blockchain in healthcare. Australas. J. Inf. Syst., 23.

Prorok, A., & Kumar, V.R. (2016). A Macroscopic Privacy Model for Heterogeneous Robot Swarms. ANTS Conference.

Puri, V., Kataria, A., & Sharma, V. (2021). Artificial intelligence-powered decentralized framework for Internet of Things in Healthcare 4.0. Transactions on Emerging Telecommunications Technologies.

Ramaswamy, V., & Mukherjee, S. (2019). An effective clinical decision support system using swarm intelligence. The Journal of Supercomputing, 76, 6599 - 6618.

Rani, S., Chauhan, M., Kataria, A., & Khang, A. (2021). IoT Equipped Intelligent Distributed Framework for Smart Healthcare Systems. ArXiv, abs/2110.04997.

Ren, Y., Lv, H., Li, H., Zhou, L., & Wang, L. (2016). Data Mining Based on Cloud-Computing Technology.

Rifi, N., Rachkidi, E.E., Agoulmine, N., & Taher, N.C. (2017). Towards using blockchain technology for eHealth data access management. 2017 Fourth International Conference on Advances in Biomedical Engineering (ICABME), 1-4.

Rizk, E., Vlaski, S., & Sayed, A.H. (2020). Dynamic Federated Learning. 2020 IEEE 21st International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), 1-5.

Rodriguez, A.A., & Reggia, J.A. (2004). Adaptive Problem Solving with Particle Systems.

Rodriguez, A. (2007). Guided self-organizing particle systems for basic problem solving.

Rodriguez, A.A., & Reggia, J.A. (2009). A distributed learning algorithm for particle systems. Integr. Comput. Aided Eng., 16, 1-20.

Roshanzamir, M., Darbandy, M.T., Roshanzamir, M., Alizadehsani, R., Shoeibi, A., & Ahmadian, D. (2022). Swarm Intelligence in Internet of Medical Things. 2022 IEEE 10th Jubilee International Conference on Computational Cybernetics and Cyber-Medical Systems (ICCC), 000371-000376.

Samuel, R.E. (2015). INTERNET OF THINGS-BASED HEALTH MONITORING AND MANAGEMENT DOMAIN-SPECIFIC ARCHITECTURE PATTERN.

Saldanha, O.L., Quirke, P., West, N.P., James, J.A., Loughrey, M.B., Grabsch, H.I., Salto-Tellez, M., Alwers, E., Cifci, D., Ghaffari Laleh, N., Seibel, T., Gray, R., Hutchins, G.G., Brenner, H., van Treeck, M., Yuan, T.W., Brinker, T.J., Chang-Claude, J., Khader, F., Schuppert, A., Luedde, T., Trautwein, C., Muti,

Shahnaz, A., Qamar, U., & Khalid, A. (2019). Using Blockchain for Electronic Health Records. IEEE Access, 7, 147782-147795.

Shailaja, K., Seetharamulu, B., & Jabbar, M. A. (2018, March). Machine learning in healthcare: A review. In *2018 Second international conference on electronics, communication and aerospace technology (ICECA)* (pp. 910-914). IEEE.

International Journal of Business and Applied Social Science

E-ISSN: 2469-6501
VOL: 10, ISSUE: 5
May/2024
DOI: http://dx.doi.org/10.33642/ijbass.v10n5p2

Sharma, H.K., Patni, J.C., Ahlawat, P., & Biswas, S.S. (2020). Sensors Based Smart Healthcare Framework Using Internet Of Things (Iot). International Journal of Scientific & Technology Research, 9, 1228-1234.

Sousa, T.F., Silva, A., & Neves, A. (2004). Particle Swarm based Data Mining Algorithms for classification tasks. Parallel Comput., 30, 767-783.

Swetha, M.S., Pushpa, S.K., Muneshwara, M., & Manjunath, T.N. (2020). Blockchain enabled secure healthcare Systems. 2020 IEEE International Conference on Machine Learning and Applied Network Technologies (ICMLANT), 1-6.

Taha, Z.K., Yaw, C.T., Koh, S.P., Tiong, S.K., Kadirgama, K., Benedict, F., Tan, J., & Balasubramaniam, Y. (2023). A Survey of Federated Learning From Data Perspective in the Healthcare Domain: Challenges, Methods, and Future Directions. IEEE Access, 11, 45711-45735.

Tahir, A., Chen, F., Khan, H.U., Ming, Z., Ahmad, A., Nazir, S., & Shafiq, M. (2020). A Systematic Review on Cloud Storage Mechanisms Concerning e-Healthcare Systems. Sensors (Basel, Switzerland), 20.

Talia, D. (2015). Making knowledge discovery services scalable on clouds for big data mining. 2015 2nd IEEE International Conference on Spatial Data Mining and Geographical Knowledge Services (ICSDM), 1-4.

Tanushree Shenwai. Google AI implements machine learning model that employs federated learning with differential privacy guarantees. MarkTechPost, 2022.

Vazirani, A.A., O'Donoghue, O., Brindley, D., & Meinert, E. (2019). Implementing Blockchains for Efficient Health Care: Systematic Review. Journal of Medical Internet Research, 21.

Velmovitsky, P.E., Bublitz, F.M., Fadrique, L.X., & Morita, P.P. (2020). Blockchain Applications in Health Care and Public Health: Increased Transparency. JMIR Medical Informatics, 9.

Vyas, S., Gupta, M., & Yadav, R.K. (2019). Converging Blockchain and Machine Learning for Healthcare. 2019 Amity International Conference on Artificial Intelligence (AICAI), 709-711.

Wang, Z., & Hu, Q. (2021). Blockchain-based Federated Learning: A Comprehensive Survey. ArXiv, abs/2110.02182.

Wang, L., & Alexander, C.A. (2013). Medical Applications and Healthcare Based on Cloud Computing. International Conference on Cloud Computing.

Warnat-Herresthal, S. et al. Swarm Learning for decentralized and confidential clinical machine learning. Nature 594, 265–270 (2021).

Winklerová, Z. (2013). Maturity of the Particle Swarm as a Metric for Measuring the Collective Intelligence of the Swarm. International Conference on Swarm Intelligence.

Wu, D., Wang, N., Zhang, J., Zhang, Y., Xiang, Y., & Gao, L. (2022). A Blockchain-based Multi-layer Decentralized Framework for Robust Federated Learning. 2022 International Joint Conference on Neural Networks (IJCNN), 1-8.

Xu, Jie, Benjamin Scott Glicksberg, Chang Su, Peter B. Walker, Jiang Bian and Fei Wang. “Federated Learning for Healthcare Informatics.” Journal of Healthcare Informatics Research 5 (2019): 1 - 19.

Yamini, G. (2020). Exploring Internet of Things and Artificial Intelligence for Smart Healthcare Solutions

Yuan, L., Rana, M.E., & Maatouk, Q.A. (2021). Enhancing Medical Data Transparency and Integrity with Blockchain Based Implementation. 2021 Third International Sustainability and Resilience Conference: Climate Change, 279-285.

Yoo, H., Park, R.C., & Chung, K. (2021). IoT-Based Health Big-Data Process Technologies: A Survey. KSII Trans. Internet Inf. Syst., 15, 974-992.

Zhu, H., & Jin, Y. (2018). Multi-Objective Evolutionary Federated Learning. IEEE Transactions on Neural Networks and Learning Systems, 31, 1310-1322.

Zubaydi, H.D., Chong, Y., Ko, K., Hanshi, S.M., & Karuppayah, S. (2019). A Review on the Role of Blockchain Technology in the Healthcare Domain. Electronics.lth Care Services in Smart Cities Applications.