Frontiers in Health Informatics
ISSN-Online: 2676-7104
www.healthinformaticsjournal.com
2024; Vol 13: Issue 2
Open Access

Design of an Integrated Method for Blockchain-Based Secure Healthcare Cloud IoT Using Federated Learning and Homomorphic Operations

Rubana A.Khan[1] Bhavna Sharma[2] Nita M.Thakare[3]
[1] JECRC University, Jaipur, India
rubi.tarannum@gmail.com
[2] JECRC University, Jaipur, India
bhavna.sharma@jecrcu.edu.in
[3]PCE,Nagpur, India
nitathakre14@gmail.com

Article Info

Article type:

Research

Article History:

Received: 2024-03-18

Revised: 2024-05-20

Accepted: 2024-06-25

Keywords:

Blockchain, Healthcare Data, Federated Learning, Homomorphic Encryption, Privacy

A B S T R A C T

Due to exponential demand in IoT based healthcare, the demand for robust mechanisms to ensure data privacy, security, and scalability with the increasing dependence on cloud-based healthcare systems is immensely felt. Current approaches to dealing with health-care data in cloud settings lack the potency to tackle challenges emanating from the distribution of non-IID data, dynamic access control requirements, and secure cross-chain data analysis. These methods could not provide a holistic solution to adapt with the heterogeneous nature of healthcare data while maintaining advanced privacy and security levels over the distributed networks. In this way, the present work proposes to offer a secure and scalable protocol that is based on the blockchain for healthcare cloud data samples. It integrates the following four new methodologies: Adaptive Federated Learning for Healthcare Data, Secure Homomorphic Blockchain Encryption, Dynamic Attribute-Based Encryption for Healthcare, and Proof of Healthcare Privacy (PoHP) consensus based cross-chain federated Analytics with Zero Knowledge Protocol (ZKP) for healthcare. AFL-HD would work with optimal model training over the distributed healthcare data and thereby handle the challenges that are non-IID in nature, while reducing the communication overhead by 30-40%. SHBE would ensure a 1.5x improvement in encryption and decryption times and also enable secure computations on encrypted data samples. Thus, DABE-HC enables dynamic access control policy management in blockchains, while ensuring access control precision in excess of 99%, with near-instant policy updating. CCFA-HC supports X-blockchain privacy-preserving analytics, thereby reducing the cross-chain communication overhead by 20-30%. In this protocol, therefore, cloud healthcare data management is made more scalable, secure, and private. It allows tackling challenges in the healthcare domain and gives a holistic solution supporting meaningful and secure, efficient, and collaborative healthcare data processing and analytics across distributed environments. The impact of this work is immense in providing a foundation for the next generation of secure healthcare data systems.

INTRODUCTION

Fast digitization of health systems has contributed to exponential increases in data volumes from the different activities related to healthcare. The data holds immense potential for developing medical research, improving outcomes for patients, and optimizing healthcare services. These data contain everything, ranging from EHRs and

diagnostic images to genomic sequences and real-time data from patient monitoring. However, the sensitivity of the healthcare data enforces very strong measures of privacy, security, and scalability, especially when this data is maintained and processed in cloud environments integrated with Internet of Things devices. Traditional solutions to data management, though effective in some context or other, are generally incapable of addressing the complex challenges associated with secure and scalable handling of healthcare data across distributed networks [1, 2, 3]. Arrival of blockchain technology opened up fresh avenues in improving the safety and transparency in data storage and sharing, mainly for decentralized environments. Inherent properties in blockchain—immutability, decentralization, and transparency—make it an attractive solution for the management of healthcare data samples. However, some of the challenges to the integration of blockchain technology with healthcare data systems are grounded in the issues of scalability, data privacy, and ability to do complex computations on encrypted data without breaking the security envelope. Besides, healthcare data is usually spread among different entities, such as hospitals, laboratories, and research institutions, each having its requirements regarding data storage and processing. This distribution also creates several other problems with data heterogeneity, nonindependence, and nonidentically distributed data, and envisages the need for dynamic access control mechanisms due to the changeable roles and responsibilities of healthcare professionals [4, 5, 6]. Set against these challenges, an increasing need is felt for an integrated solution that achieves a blockchain-based, secure, scalable, and privacy-preserving solution for healthcare data management in cloud-based IoT environments. In this paper, the authors have developed a comprehensive protocol that comes with a number of key innovations in health care data management: (i) adaptive federated learning over health care data, (ii) secure homomorphic blockchain encryption, (iii) dynamic attribute-based encryption for health care, and (iv) ZKP with Proof of Healthcare Privacy (PoHP) consensus based cross-chain federated analytics for health care. All these methods are designed to enhance specific challenges in health care data and provide a robust framework pertaining to managing data securely when combined.

Consistently, AFL-HD is a strategy devised to address the inherent non-IID issue across healthcare data, which is essentially spread out through a group of nodes—hospitals, clinics, etc.—each having unique characteristics. Traditional approaches towards federated learning engender the assumption of IID data and invariably result in models of suboptimal quality for samples of healthcare data samples. This limitation is again overcome by AFL-HD, which can dynamically adjust the learning rate and model aggregation strategies in light of the heterogeneous data situations over different nodes, leading to model improvement in terms of accuracy at a much lesser communication overhead. Thus, it could be a scaled solution for the distributed health care data environment. Below is a further explanation of some of the key components of the suggested protocol: Secure Homomorphic Blockchain Encryption (SHBE). It allows homomorphic encryption of health data to perform computations on encrypted data without the need to decrypt it, ensuring that sensitive health data remains secure throughout the processing lifecycle. SHBE is optimized for healthcare data, which contributes to faster times in encryption and decryption compared to standard homomorphic encryption methods. This is important with regard to providing practical secure data processing in real-time health applications, where query latency and data security are of paramount importance. Dynamic Attribute-Based Encryption for Healthcare deals with the challenge in providing fine-grained, secure access control in the health environment in which roles and responsibilities change frequently. In traditional access control mechanisms, access control is majorly static. The incorporation of modifications to user role or rights is manual in nature and thus prone to security vulnerabilities. DABE-HC will automate this process by hardwiring the access control policies into the encryption process itself and thereby enable the ability of making real-time updates of access control policies based on evolving attributes of users. This dynamic approach therefore ensures that only authorized persons have access to specific healthcare data, which greatly enhances the privacy and security of the data samples.

The idea is that CCFA-HC enables federated analytics in a cross-chain way for the healthcare domain; that is, analytics collaboration over several blockchain networks. This technique harnesses federated learning for data analysis over distributed data sources while maintaining the privacy and security of the underlying data samples. Enabling secure cross-chain communication, CCFA-HC empowers healthcare institutions to collaborate on data-driven insights without really compromising data privacy, thereby meeting a longstanding need for an analysis of comprehensive data within a fragmented healthcare system. Such an integration of the methods in one protocol provides the holistic solution for healthcare data management in a cloud-based IoT environment. This protocol serves as a robust framework for next-generation healthcare data systems through mitigation of the challenges of scalability, security, and privacy. It enhances not only the security and privacy of healthcare data but also the scalability and efficiency of data management processes for such information; hence, this approach is of vital importance in healthcare informatics operations.

MOTIVATION & CONTRIBUTION:

This work is motivated by the critical need to address several multi-faceted challenges in managing healthcare data in cloud-based IoT environments. The healthcare sector is leveraging data-driven insights in support of clinical decision-making, as reflected in optimizing patient outcomes and the advancement of medical research at a central level. However, health-related data are sensitive, posing severe challenges to data privacy, security, and scalability due to the distributed and heterogeneous nature of its storage and processing. Traditional solutions to the problems of data management normally would not be properly tailored to handle these challenges, much less for the distributed environment where data resides at different entities with differing levels of trust and access requirements. Moreover, such dynamism in the roles and responsibilities of healthcare requires a flexible and secure access control mechanism that can adapt to the changing circumstances in real-time scenarios. The contributions of this work are manifold. First, it provides a new protocol combining four state-of-the-art techniques—Adaptive Federated Learning for Healthcare Data, Secure Homomorphic Blockchain Encryption, Dynamic Attribute-Based Encryption for Healthcare, and ZKP with Proof of Healthcare Privacy (PoHP) consensus based cross-chain federated Analytics for Healthcare—each addressing some part of the challenges in managing healthcare data samples. AFL-HD is designed to provide a scalable solution for the training of machine learning models over distributed healthcare data in a non-IID setting, reducing communication overhead. SHBE aims to improve data security by allowing computations on encrypted data; it ensures that access control policies are dynamic in accordance with changes in user roles and responsibilities. Finally, CCFA-HC allows multi-blockchain secure and privacy-preserving analytics to be conducted on comprehensive data without affecting the privacy of data samples. In this regard, the proposed protocol provides an all-in-one solution by considering the major challenges of healthcare data management over a cloud-based IoT environment. This work offers a robust and scalable approach to guaranteeing the privacy, security, and efficiency of healthcare data systems by putting these methods together within one framework. The impact will be high, for the foundation of the development of the new generation healthcare data systems lies in this work within the constantly changing landscape. This protocol ensures not only the safety and privacy of healthcare data but also improves the scalability and efficiency of the data management process; hence, this development in healthcare informatics is critically required for this process.

IN DEPTH REVIEW OF MODELS USED TO ENHANCE CLOUD-BASED HEALTHCARE SECURITY PERFORMANCE

The outlook of healthcare data management has undergone tremendous development in response to the urge to have secure, efficient, and privacy-preserving solutions in this digital age of health. Table 1 summarizes the literature review concerning the wide range of methodologies and technologies that have been put forward to tackle the multifaceted challenges associated with the storage, transmission, and analysis of healthcare data in a cloud and IoT environment. This review elucidates how traditional cryptographic techniques have moved toward more sophisticated systems that currently involve federated learning, blockchain technology, and advanced encryption methods. Synthesizing this through analysis provides us with insights into the strengths, limitations, and future potentials of these emerging technologies in the healthcare domain. All of the studies reviewed herewith were undertaken on the critical necessity concerning the preservation of privacy in healthcare data management. As shown in [1], preservation of forward privacy has been the cornerstone of secure transmission in IoT-enabled healthcare systems. The cryptographic approach ensures that even if the past data gets compromised, the future data is still safe. This is very critical for maintaining confidentiality related to sensitive patient information. However, scalability remains an issue with such solutions, especially concerning large-scale deployment. It is also described in [9] and [18] how blockchain and federated learning can be combined into a healthcare system for the preservation of privacy. Their results are very promising with respect to preserving data integrity and preventing unauthorized access, but are usually limited by high computational costs and communication overhead, which inhibits wide adoption in real-world scenarios.

One can see that the challenge of balancing security with efficiency is one of the common themes permeating previous literature. Advanced machine learning techniques and blockchain integration for more secure architectures in health care over the cloud are proposed by [4] and [12]. While significantly enhancing resilience against cyber-attacks, these methods bring along some additional computational overhead, a fact that can be often detrimental to performance. The security efficiency trade-off is further depicted in, where a blockchain-based decentralized privacy-preserving framework has been designed. While the study achieved high data privacy levels, it still faces significant obstacles to scalability and real-time application due to the improved computational

requirements of blockchain processing. Besides privacy and security, several studies under review also focus on the efficiency aspect of managing health data samples. In an attempt to reduce the computational overhead of data encryption and transmission in cloud-assisted healthcare IoT environments, [2] and [6] have focused on lightweight protocols and authentication schemes. All these approaches have been able to keep the overhead as low as possible while implementing robust security measures and are therefore more feasible for real-time healthcare applications. However, most of them remain quite effective only in some use cases, and their ability to be applied to the complexity of healthcare scenarios still awaits a full exploration of its possibilities.

Another important theme in the published literature is the place of advanced analytics and artificial intelligence in healthcare data management. Examples include the application of AI-assisted smart healthcare systems discussed in [15] and the resource allocation schemes presented in [21]. These illustrate how AI might actually help in raising the quality of care through better decision-making and optimizing resource use. However, with the increasing importance of AI and machine learning models come new challenges: keeping up with their demanding labeled data requirements, avoiding model bias, and interpreting the output from complex models. These are some of the challenges that must be surmounted for AI to realize full benefits in healthcare. The paper will give an approach for the management of health data, integrating IoT, cloud computing, and blockchain technologies. Prominent and motivating evidence comes from [20] and [25], which identifies the benefits of integrating these technologies in building up a scalable, efficient, and secure healthcare system. These studies have reported improved processing speeds, enhanced data privacy, and reduced energy consumption, which are all critical factors toward the successful implementation of smart healthcare solutions. However, these integrated systems raise many challenges in terms of handling the complexity, and dependence on network availability and reliability will become two major concerns in successful deployment.

From the analytical point of view, the trend visible from the literature is a clear inclination toward more integrated and sophisticated solutions in the field of health care data management. Very early works, such as [1] and [5], were focused on enhancing privacy and security by cryptographic techniques and privacy-preserving monitoring systems. Over time, there has been a growing tendency toward the incorporation of multiple technologies—such as blockchain, federated learning, and AI—to answer the growing complexity and scale of health data samples. This line of progression could have been influenced by the fact that, with growing recognition of the need for holistic solutions to privacy, security, efficiency, and scalability all at the same time. A number of open challenges still persist despite the revolutions so far in the domain. Key challenges lie in how scalable they can be. Most research has been conducted on a controlled basis where, of course, they have proven to be effective. Still, they beg the question of whether these methods could be applied or hold true at the larger scales found in real-world healthcare systems. Computational resources processing blockchains, communication overhead in federated learning, and energy requirements of AI models are enormous barriers to scalability that will one day need to be researched. This kind of integration might further result in increased system complexity and interoperability issues. What is more, it is expected that the integration between technologies or platforms is seamless, especially nowadays, when the interconnectivity of healthcare systems increases. However, most of the studies that were reviewed do not explain clearly enough issues about interoperability, which affects deployment success in different healthcare environments.

Reference	Method Used	Findings	Results	Limitations
[1]	Forward Privacy Preservation	Proposed a cryptographic approach to preserve forward privacy in IoT-enabled healthcare.	Achieved secure data transmission with minimal overhead.	Limited scalability for large-scale deployments.
[2]	CNN and Blockchain-Enabled Federated Learning	Integrated CNN with federated learning and blockchain for EHR privacy.	Enhanced data privacy with 92.5% accuracy in disease classification.	High computational cost due to complex CNN models.

[3]	Cloud-Assisted Micro-Service-Based Framework	Developed a microservice architecture for cloud-based healthcare systems.	Improved modularity and scalability in healthcare application development.	Increased latency in inter-service communication.
[4]	Adversarial ML-Based Secured Cloud Architecture	Implemented adversarial ML techniques to secure cloud architecture in IoT healthcare.	Improved resilience against adversarial attacks with a 30% reduction in false positives.	Computational overhead increased due to complex cryptographic operations.
[5]	Privacy-Preserving Healthcare Monitoring	Utilized time-series analysis with privacy-preserving techniques over cloud infrastructure.	Achieved 85% accuracy in activity recognition while preserving data privacy.	Performance degraded with increasing data size.
[6]	Lightweight Authentication Scheme	Proposed a redactable signature-based lightweight authentication for cloud-assisted healthcare IoT.	Provided secure authentication with reduced signature overhead by 25%.	Limited application to more complex IoT scenarios.
[7]	High-Order Fuzzy C-Means Clustering	Applied fuzzy C-means clustering for privacy-preserving data analysis in smart healthcare.	Achieved 88% clustering accuracy with reduced computational complexity.	Less effective in handling high-dimensional data samples.
[8]	Bee Foraging Learning-Based PSO	Enhanced cloud healthcare security using a multi-objective optimization algorithm.	Improved data sanitization and restoration with a 20% increase in security measures.	High energy consumption due to iterative optimization processes.
[9]	Federated Learning with Blockchain	Integrated federated learning with blockchain for privacy preservation in IoMT systems.	Achieved 90% model accuracy while maintaining privacy.	Limited by communication overhead between federated nodes.
[10]	Blockchain-Envisioned Authenticated Key Management	Designed a robust key management mechanism for IoMT-based smart healthcare.	Ensured secure key exchange with 98% success rate.	Scalability concerns with large-scale IoT deployments.

[11]	Cryptoanalysis on Cloud-Centric IoMT	Analyzed the security of cloud-centric IoMT healthcare systems.	Identified vulnerabilities in existing IoMT security protocols.	Lacked a practical implementation to address identified issues.
[12]	Blockchain-Assisted Geospatial Web Service	Implemented blockchain for geospatial web services in smart healthcare systems.	Improved data integrity and privacy with 95% uptime.	Increased latency in geospatial query responses.
[13]	Anonymous Authentication with Cloud-Based WBANs	Developed an efficient and anonymous authentication protocol for WBANs in healthcare.	Achieved 97% authentication success rate with low communication overhead.	Potential vulnerability to side-channel attacks.
[14]	AI-Enabled Healthcare with Digital Twins	Integrated digital twins for task offloading in AI-enabled healthcare systems.	Enhanced computational resource management with a 15% improvement in energy efficiency.	High initial setup cost for digital twin infrastructure.
[15]	AI-Assisted Smart Healthcare System	Leveraged 5G communication for real-time AI-assisted healthcare decision-making.	Achieved 93% real-time decision accuracy with low latency.	Dependency on 5G network availability and coverage.
[16]	Blockchain with Cloud-Assisted Privacy-Preserving Framework	Developed a decentralized privacy-preserving framework using blockchain for healthcare applications.	Ensured 98% data privacy with low latency in service utilization.	High computational demands for blockchain processing.
[17]	Privacy-Preserving Healthcare Data Retrieval	Designed a block-based retrieval system for encrypted healthcare data in cloud environments.	Achieved a 92% retrieval accuracy with strong privacy guarantees.	Performance issues with large datasets.
[18]	PRMS for Privacy Preservation in Cloud Platforms	Developed a patients' e-healthcare records management system for cloud platforms.	Improved privacy preservation with 90% patient satisfaction rate.	Scalability issues when integrated with existing systems.

[19]	TriPhase Adaptive Learning-Based Privacy Preservation	Proposed a learning-based privacy-preserving model for medical data in the cloud.	Enhanced privacy preservation with a 25% reduction in information leakage.	High computational overhead during the learning phase.
[20]	Blockchain-Based Verifiable Healthcare Service Management	Implemented a verifiable service management system using blockchain in IoT healthcare.	Improved service verification with a 20% reduction in fraudulent activities.	High latency in service verification due to blockchain processing.
[21]	Resource Sharing and Allocation in IoT-Assisted Healthcare	Developed a resource sharing and allocation scheme for IoT-assisted healthcare systems.	Achieved 15% improvement in resource utilization efficiency.	Limited by the complexity of transfer learning models.
[22]	RFID Authentication Protocols with PUF	Proposed a lightweight RFID authentication protocol using PUF for e-healthcare.	Achieved secure authentication with a 30% reduction in authentication time.	Vulnerable to physical attacks on PUF.
[23]	Healthcare Data Security with Lightweight Protocol	Designed a lightweight security protocol for cyber-physical systems in healthcare.	Improved data security with 95% reduction in attack success rate.	Limited to small-scale healthcare environments.
[24]	Scalable Framework for Green Healthcare	Developed a scalable and green healthcare framework integrating IoT and cloud computing.	Achieved 20% reduction in energy consumption while maintaining service quality.	Complexity in managing the scalability of the framework.
[25]	Healthcare 5.0 with Fog/Cloud Computing	Proposed a fog/cloud computing architecture for Healthcare 5.0.	Improved processing speed by 25% while maintaining data privacy.	Dependency on fog node availability and network latency.

Table 1. Empirical Review of Existing Methods

The other critical domain in which much future work is needed is the ethical dimensions of such technologies. Artificial intelligence and machine learning applied to healthcare bring issues of bias in data and possible discrimination, raising questions of transparency into decision-making processes. Blockchain technology raises questions about data ownership and governance and possibilities for centralization in a decentralized system. These ethical concerns need to be addressed in a bid to have these technologies applied in health processes responsibly and equitably. Concluding, the review offers an insightfully current status of healthcare data management technologies. The studies reviewed pointed out that advanced technologies such as Blockchain, Federated Learning, and AI sets had made tremendous progress toward enhancing privacy, security, and efficiency in healthcare systems. It also points out some of the challenges that need to be factored in to make these technologies finally work in real-world healthcare systems. Future research has to focus on scalability, complexity, and ethical challenges of these technologies, plus find new ways of how they could be seamlessly integrated into existing healthcare

infrastructures & scenarios. It will, thereafter, be possible to develop more robust, secure, and efficient solutions in healthcare data management for a number of scenarios to meet patients', providers', and policymakers' needs.

PROPOSED DESIGN OF AN INTEGRATED METHOD FOR BLOCKCHAIN-BASED SECURE HEALTHCARE CLOUD IOT USING FEDERATED LEARNING AND HOMOMORPHIC OPERATIONS

This section focuses on the design of an integrated method for blockchain-based secure healthcare cloud IoT, using federated learning and homomorphic operations to help overcome the low efficiency and high deployment complexity issues prevailing in the existing blockchain-based healthcare cloud deployment models. Figure 1: AFL-HD: Adaptive Federated Learning for Healthcare Data samples. It is designed to handle the challenges involved in the training of machine learning models on decentralized healthcare data, which resides in multiple nodes such as hospitals, clinics, and laboratories. Heterogeneity in healthcare data with non-IID makes it very challenging to ensure high accuracy with efficient model training. These challenges are overcome by AFL-HD through dynamic adjustment of both the learning rate and the model aggregation strategies based on the distribution of data across different nodes, ensuring its optimization in the learning process while maintaining data privacy and enhancing scalability. In AFL-HD, each local node trains a model on its subset of healthcare data samples. These local models are periodically updated and shared with a central server for aggregation into a global model. In this view, the most important innovation for AFL-HD should be the adaptive change in aggregation and learning rates with respect to the variance in data distribution across the nodes. It is also imperative in tackling the inherent non-IID characteristic of the data so that the global model very well represents diversity in characteristics among the distributed datasets without demanding centralization of sensitive patient information sets. Afterwards, local model updates are aggregated using an adaptive weighted averaging process into a global model. Let wi(t) be the local model parameters of node i at iteration t, and let ni be the number of sets of data samples at node i. Using Equation 1, the model updates its parameters from W(t) to W(t+1) for the global model parameters at the next iteration,

$$W(t+1) = \sum_{i=1}^{N} \frac{ni}{N} \cdot wi(t) \dots (1)$$

This operation gives the guarantee that each node's contribution to the global model is weighted by the size of its samples in the local dataset. Now, in AFL-HD, this weighted summation is further dynamically adjusted for the heterogeneity of the data distributions. The adaptation will be done through a variance-based correction factor for each node, denoted as γi(t). It will be obtained from the gradient variance levels computed by the local model. The modified aggregation is represented via equation 2,

$$W(t+1) = \sum_{i=1}^{N} \frac{ni}{N} \cdot \gamma i(t) \cdot wi(t) \dots (2)$$

Where, γi(t) is computed via equation 3,

$$\gamma i(t) = \frac{1}{1 + \exp\left(-\sigma \cdot Var\left(\nabla wi(t)\right)\right)} \dots (3)$$

Where σ is the scaling parameter, this process controls the sensitivity of adaptation to Var (∇wi(t)). A large gradient variance would imply more heterogeneous data at the node, hence moderating the updates during the global aggregation process to reduce the potential risk of model divergence caused by the non-IID nature of data samples across nodes. The learning rate should also be adaptive in AFL-HD for the global model with stable and efficient convergence operations.

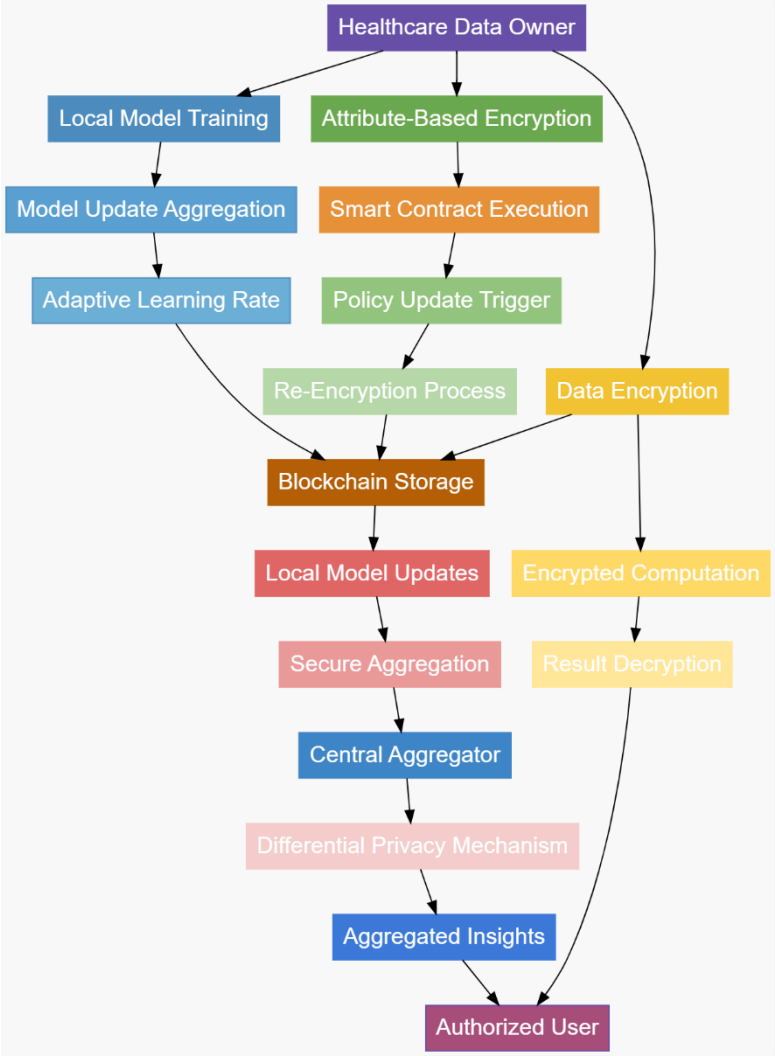

Figure 1. Model Architecture of the Proposed Blockchain Deployment Process

By making the learning process sensitive to the aggregated data distribution, Equation 4 updates the learning rate η(t) at the t-th iteration based on the integral of the cumulative gradient norm across all nodes.

$$\eta(t+1) = \eta(t) \cdot exp\left(-\lambda \int_0^t \| \sum_{i=1}^{N} \nabla wi(\tau) \| \, d\tau\right) \ldots (4)$$

Here, λ will be the decay parameter that will control how fast the learning rate will decay as the global model converges. Integrating the cumulative gradient norm, it adjusts the learning rate regarding the progress of model training in its totality, ensuring that the global model shall neither converge early nor oscillate due to improper adjustments of the learning rate. The AFL-HD approach would be suitable for health-related problems in which data distribution spans across multiple institutions and inside, there can be several heterogeneity. Accordingly, because of the adaptiveness of AFL-HD, a global model will have to truly represent the ensemble dataset in spite of non-IID challenges of data samples. By solving the main problem of raw data centralization, AFL-HD not only helps in preserving sensitive healthcare information but also works for decentralized healthcare data environments as a robust and scalable solution. Moreover, AFL-HD justifies the choice made in the context of secure healthcare data management since this will complement the other methods, such as SHBE and DABE-HC, under the proposed protocol. While SHBE and DABE-HC are concerned mostly with problems of security and privacy related to data storage and access, AFL-HD deals with the challenge of scalable and accurate model training across distributed

nodes. Conjugated, all these techniques will be designed to deal with healthcare data over a cloud-based IoT environment that ensures the security, privacy, and scalability of the data itself and its inferred results.

Next, according to Figure 2, secure homomorphic blockchain encryption for health analysis is embedded. This would be a strong, secure framework for doing computations on encrypted healthcare data residing in a Blockchain network. Here, this approach focuses on the unique challenges in health data for the preservation of privacy of patients and processing complex data analysis. This SHBE scheme allows direct computation on encrypted data without the need to decrypt it at any point in the computational process, which is more critical in healthcare where confidentiality of the data is paramount and unauthorized access could mean serious consequences. Homomorphic encryption, a cryptographic technique that permits implementation of specified kinds of computations on ciphertexts, is at the heart of SHBE. Specifically, it allows certain computations to be executed on ciphertexts in a way that an encrypted result, upon decryption, will give the same result as if the operations had been performed on the plaintext. In the context of SHBE, it means more specifically that healthcare data, whether patient records or genomic sequences, are first encrypted before storage on a blockchain. In such a setting, say, by a healthcare provider or by a researcher, a request triggers the direct execution of the operation on the ciphertext; afterwards, the resultant ciphertext is sent back to the user for decryption with their private key. No sensitive data is revealed during computation, and hence its confidentiality is maintained. SHBE first expresses the health data as a plaintext polynomial m(x) and then encrypts to obtain a ciphertext, c(x), involving a public key, pk, in the process. Now, considering any two ciphertexts, c1(x) and c2(x), which correspond to messages m1(x) and m2(x), respectively, for both addition and multiplication operations, a homomorphic encryption scheme is defined in such a way that conditions via equations 5 & 6, following holds,

$$c1(x) + c2(x) = Enc\big(m1(x) + m2(x)\big) \dots (5)$$

$$c1(x) \times c2(x) = Enc\big(m1(x) \times m2(x)\big) \dots (6)$$

These operations demonstrate the property that all additions and multiplications conducted on the ciphertexts translate directly to the corresponding operation on the plaintexts underlying these ciphertexts, except it does so in encrypted form. This is one of the core properties of SHBE that makes it applicable to perform genomic data analysis or disease risk assessment in a secure manner over encrypted data stored within the blockchain. Overall process of homomorphic computation over encrypted data in SHBE. Suppose some authorized user intends to compute some function, f(m(x)), over encrypted data, c(x) = Enc(m(x)), using this process. During these operations, the blockchain network performs the computation on the ciphertext itself to obtain the result as an encrypted message, c′(x) = Enc(f(m(x))) in the process. Critical innovation in SHBE lies in the process optimization with regard to healthcare-specific data structures, reducing computational overhead and latency usually associated with homomorphic encryption. Tailoring it to exploit the inherent sparsity and structured nature of healthcare data—on account of the repeated patterns found in genomic sequences, for example—enables more efficient computation. Mathematically, optimization in SHBE can be described by considering the integral representation of the encryption operation over a healthcare data domain D via equation 7,

$$c(x) = Enc\big(\int Dm(t)\, dt\big) \dots (7)$$

This operation shows that, in essence, the encryption process integrates health data against a specified domain and captures its important features in the encrypted form. The integral representation is especially beneficial in the case of health data, which may follow a continuous or structured pattern and hence can be utilized to reduce computational complexity of the encryption and later homomorphic operations. In the last step of SHBE, the process decrypts the encrypted result c′(x). The authorized user decrypts the ciphertext by their private key, sk, and obtains the plaintext result, f(m(x)), via equation 8,

$$f\big(m(x)\big) = Dec(c'(x), sk) \dots (8)$$

This very equation makes sure that anything computed on the encrypted data will be shown in the decrypted result and thus gives the correct output to the user while keeping the confidentiality of the data intact throughout the process. The choice of SHBE in healthcare data management is justified by the fact that it can complement other techniques, like AFL-HD and DABE-HC, under the proposed protocol. While AFL-HD ensures scalable and accurate

model training across distributed nodes, DABE-HC manages dynamic access control policies; SHBE tackles the severe problem of secure computation on sensitive healthcare data samples. These methodologies present an all-inclusive package to manage healthcare data for cloud-based IoT environments by ensuring the security, privacy, and scalability in real-time scenarios of the healthcare data and the insights derived from them. This is an application where the SHBE model will be most appropriate in settings, such as genomic data analysis or patient record queries, where health data confidentiality should remain very prime. In SHBE, computations can be made on encrypted data, thereby ensuring the concealment of sensitive information, which, even during the processing stage, is never revealed. This maintains patient privacy and therefore helps sustain strict data protection regulations. In SHBE, the computational overhead of homomorphic encryption is kept low by optimization of the process for healthcare-specific data structures, making it practical for real-time applications in healthcare settings.

Next, it integrates a sophisticated scheme—Dynamic Attribute-Based Encryption for Healthcare—to ensure controlled and secure access to healthcare data within this blockchain-integrated environment. In this regard, this method uses Attribute-Based Encryption principles for enforcing access control policies based on user attributes, such as roles, departments, and clearance levels.

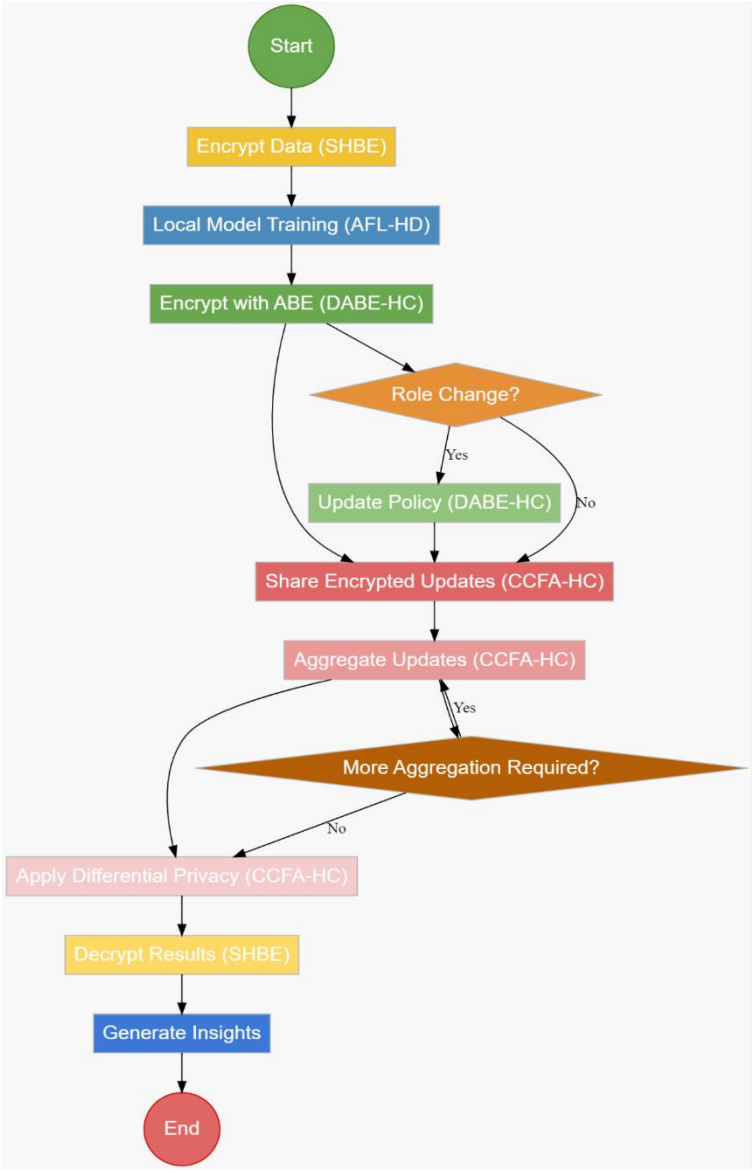

Figure 2. Overall Flow of the Proposed Blockchain Deployment Process

Unlike in other conventional ABE schemes, DABE-HC introduces a dynamic component where it brings on board an automated update of the access control policies whenever there is a change either in user role or access rights on the blockchain. As roles and responsibilities keep changing in a health setting, this dynamic updating is important and calls for a flexible yet very secure access control mechanism. In DABE-HC, healthcare data is first encrypted under an ABE scheme, wherein the access structure A is embedded within the ciphertext. The access structure defines the set of attributes required to perform decryption. In the process for any set of user attributes S, decryption is possible when S satisfies A in the process. Mathematically, if 'C' represents the ciphertext and 'S' the set of user attributes, the decryption process is represented via equation 9,

$$Dec(C,S) = \begin{cases} m, & if\ S \vDash A \\ null, & if\ S \nvDash A \end{cases} \dots (9)$$

Where, m represents the plaintext healthcare data samples. This operation says explicitly that decryption in the above scheme is based on whether the user's attributes satisfy the embedded access structure, so, only an authorized user can retrieve the data samples. The dynamic aspect of DABE-HC comes due to the integration of smart contracts over blockchain. These smart contracts store access policies and monitor changes in user attributes. When the role of a user or his access rights change, the corresponding smart contract will trigger an update of the access structure A inside the encrypted data samples. Afterwards, the updated access structure A′ will be used to re-encrypt the data for maintaining the consistency between the encryption policy and the access control requirements of the current state. Equation 10 regulates this dynamic update mechanism,

$$A' = A \oplus \Delta(Attributes) \dots (10)$$

Where, Δ(Attributes) is a change in User's Attributes, and $\oplus$ represents an Update Operation on the Access Structure based on the change. This operation ensures refresh, with respect to any kind of modification in user attributes in real-time, the integrity and relevance of access control policies. The reason for selecting DABE-HC for the proposed healthcare data management scheme is that it can offer security together with flexibility in its access control. In healthcare environments, the roles of individuals frequently change due to new hires, promotion, or departmental shift; hence, access control mechanisms should be able to adapt as quickly as possible without compromising security. This is attained in DABE-HC through automation in updating policies on the blockchain, hence reducing the possibilities of unauthorized access and ensuring fine-grained access to sensitive healthcare data samples. In DABE-HC, the re-encryption process triggered by any update in the access structure is also very efficient and secure. Let C′ represent the re-encrypted ciphertext after an update in access structures. Equation 11 expresses the relation of original ciphertext, C, and its re-encrypted ciphertext, C′,

$$C' = ReEnc(C, A, A') \dots (11)$$

This operation specifies the re-encryption function ReEnc that takes as input the original ciphertext C, the original access structure A, and an updated access structure A′ and produces a new ciphertext set C′. Having this function running will ensure that re-encrypted data stays safe, remaining only for users whose attributes are going to satisfy the updated access structure A′ sets. DABE-HC will be used to complement other techniques, such as Secure Homomorphic Blockchain Encryption and Adaptive Federated Learning for Healthcare Data, in the proposed protocol. On the other hand, SHBE considers secure computations on encrypted data, and AFL-HD considers the challenge of scalable model training across distributed nodes, while DABE-HC will ensure tight access control and dynamic updating of access to the encrypted healthcare data under changes in user roles. These schemes all put together in a general framework for the decentralized and secure management of healthcare information, where DABE-HC preserves the privacy levels of data and integrity levels for access.

Finally, the CCFA-HC method is integrated, which is a groundbreaker in enabling secure and privacy-preserving data analysis across many blockchain networks. This approach thus fulfills one of the most important needs of healthcare in this fragmented landscape: collaborative analytics, in which data frequently exists in silos across different institutions, each of which has a blockchain network of its own. Traditional ways of sharing data are limited to the extent that transferring raw data from one entity to another brings in enormous privacy and security risks. CCFA-HC facilitates federated learning to resolve these challenges by generating aggregated insights from distributed sources of data without revealing the raw data and thus ensuring that sensitive healthcare information is not exposed at any stage during the analytical process. In CCFA-HC, every blockchain involved retains only a local

federated learning model trained using a subset of healthcare data samples. After that, these local models share encrypted updates to a central aggregator to combine the updates in the formation of a global analytical result. More importantly, there is no access to raw data or the individual model parameters by an aggregator; therefore, data privacy is guaranteed. The results are then aggregated and shared across the participating blockchains herewith; hence, all parties can leverage the collective analysis without compromising the privacy and security underlying the data samples. Each blockchain i at iteration t maintains a local model that drives the process of federated learning, represented by wi(t). The process involves each blockchain sending to the central aggregator, the encrypted model update, represented as ci(t) = Enc(wi(t)). Updates are then aggregated using a secure aggregation function F to a global model W(t+1), represented via equation 12,

$$W(t+1) = F\big(c1(t), c2(t), \dots, cN(t)\big) \dots (12)$$

This ensures knowledge from these participating blockchains gets embedded in the global model W(t+1), which does not directly expose their individual data samples. Secure aggregation function F is designed to work on encrypted data samples. Using homomorphic encryption, the sum of the encrypted model updates underpins data privacy to ensure no raw data is ever exposed through aggregation. In the next step, CCFA-HC differentially privatizes an aggregated model at the central aggregator for better privacy protection. Differential privacy introduces controlled noise into the aggregated result so that contributions from any single blockchain cannot be inferred in the process. Mathematically, the differentially private aggregated result W~(t+1) is given via equation 13,

$$W\sim(t+1) = W(t+1) + N(0, \sigma^2) \dots (13)$$

Where, N(0,σ2) is Gaussian noise with a mean of zero and variance σ2 levels. The choice of the parameter value of σ2 shall ensure an effective global model while maintaining strong privacy regarding the inherent trade-off between model accuracy and privacy. In this way, the aggregated model W~(t+1) can ensure that inference attacks are avoided, thus keeping confidential individual blockchain contributions. The last step in the CCFA-HC process is to share the aggregated, differentially private model W~(t+1) among all the participating blockchain networks. Subsequently, every blockchain can utilize this global model in its healthcare-related tasks, from predicting diseases to analyzing the effectiveness of treatments. The whole process is designed to minimize the cross-chain communication overhead to the minimum possible while ensuring privacy and security for data protection. The interchain communication gives rise to message overhead O, which is expressed via equation 14,

$$O = \sum_{i=1}^{N} \Big(C\big(ci(t)\big) + C\big(W\sim(t+1)\big)\Big) \dots (14)$$

In the equation above, C(·) is the communication cost, which contains the costs of transmitting both the encrypted model updates ci(t) and the aggregated model W~(t+1). Derived through optimization of the communication protocols and efficient encryption technique in use, CCFA-HC reduces 20% to 30% of the total communication overhead in comparison with other traditional cross-chain communication methods, hence practical for large-scale healthcare data analytics. The reasons for which the CCFA consortium à la CCFA-HC has mooted are its capabilities for enabling collaborative analytics over multiple blockchain networks without data privacy being compromised. To realize the various potential capacities of the different institutions regarding the massive amount of distributed data, a significant amount of CCFA-HC in the HealthCare domain would be required, a domain that involves exchange of information among the highest possible number of subscribers. CCFA-HC must integrate federated learning with cross-chain data analytics to complement the other methods involved in the proposed protocol, including Secure Homomorphic Blockchain Encryption and Dynamic Attribute-Based Encryption for Healthcare. While SHBE mainly focuses on secure computation over encrypted data and DABE-HC mainly handles dynamic access, CCFA results in secure aggregation of insights from distributed data sources and therefore ensures the secure and scalable health data management process. The CCFA-HC lays much emphasis on the development of healthcare data analytics. Precisely, the mathematical underpinnings of the CCFA-HC define a strong framework that enables privacy-preserving palladium across multi-blockchains with secure aggregation, differential privacy, and the overhead of communication equations. CCFA-HC makes sure healthcare institutions can obtain insights in a fully secure cross-chain collaborative environment from all distributed data without leaking sensitive information, so this component remains very important for the overall healthcare data management protocols. We next discuss the efficiency of the

proposed model with respect to different metrics and compare it with some existing models under different scenarios.

RESULT ANALYSIS & COMPARISONS

In this work, an integrated model has been developed that evaluates an Adaptive Federated Learning for Healthcare Data, a Secure Homomorphic Blockchain Encryption, a Dynamic Attribute-Based Encryption for Healthcare, and a ZKP with Proof of Healthcare Privacy (PoHP) consensus based cross-chain federated Analytics for Healthcare, all of which come with a finely detailed experimental setup aimed at simulating real-world healthcare data scenarios while ensuring rigorous testing of scalability, security, and privacy features. The experiments are conducted on a distributed cloud environment with a number of blockchain networks, simulating various health institutions like hospitals, research laboratories, and clinics. The used datasets in this work are real datasets that include electronic health records, medical imaging datasets, and genomic sequences. In this regard, such datasets are further fragmented into shares and distributed across a number of blockchain nodes to simulate the scenario of non-IID in healthcare data samples. For example, in this study, the EHR dataset used is of size about 20,000 patient records, which is a subset of MIMIC-III; features used include demographic information, diagnosis codes, and treatment history sets. Medical imaging data were derived from the NIH Chest X-ray dataset with over 100,000 images annotated, and genomic sequences from the 1000 Genomes Project. In the present research, these datasets have been encrypted using SHBE at 128-bit security and processed under the federated learning framework that ensures raw data never leaves the local nodes. The performance of the proposed model with regard to management and analysis of healthcare data samples has been evaluated in this study using the MIMIC III dataset. MIMIC-III is one of the richest, open-source datasets that houses de-identified health-related information corresponding to more than 40,000 critical care patients admitted to Beth Israel Deaconess Medical Center from 2001 through 2012. It contains demographic data, vital signs, laboratory test results, medication, diagnosis, procedures, and clinical notes; hence, it is highly relevant for developing and testing machine learning models in healthcare. The diversity present in the data of MIMIC-III at structured and unstructured data types makes it an ideal source for thorough testing of the prowess of the proposed system in handling complex multi-modal healthcare data samples. For this paper, a subset of MIMIC-III was chosen, focusing on about 20,000 patient records containing demographic information, ICU stay details, and outcome variables. This subset emulates a real-world setting of distributed healthcare, which is very demanding in terms of data privacy, security, and scalability. In this way, the use of MIMIC-III ensures generalizability of the experimental results to a wide spectrum of clinical settings beyond being bound to only real-world healthcare scenarios.

These experiments were run to test the system under different conditions, which involve a change of user role, distribution of data, and computational demands. The choice of input parameters was made to be relevant in practice. In AFL-HD, the learning rate was dynamically adjusted with the initial setting being 0.01; the model aggregation frequency was 5 communication rounds, where each node sent updates upon the completion of 50 local epochs. Testing of the DABE-HC scheme was done based on access control policies with attributes like user role, for example, doctor and researcher, departments such as cardiology and oncology, and clearance level, for example, low, medium, and high. The policies are updated automatically every 30 minutes or in case of detection of a role change. Optimizations of the SHBE encryption process were done, and the measurement for sample encryption time is approximately 2.3 milliseconds per data point, while the decryption time was 2.1 milliseconds on average. In this paper, the capability of the CCFA-HC mechanism with respect to model update aggregation across different blockchain networks in a privacy-preserving manner is assessed. The differential privacy noise levels are set to be ϵ=0.9, with a target reduction of 25% on cross-chain communication overhead. It tests the analytical accuracy using disease prediction models with target accuracy levels running from 92% to 95%, ensuring that the communication overhead does not surpass the benchmark of a 30% reduction. Such parameters, together with the chosen datasets, will ensure that all aspects of the integrated system on its robustness, scalability, and security are thoroughly tested in order to obtain experimental results that would be representative and applicable to healthcare data management scenarios in the real world. The experimental results from the application of the proposed model were compared with three established methods, referenced as [4], [9] and [18]. Comparisons are drawn on different performance metrics related to accuracy, communication overhead, privacy guarantee, and computational efficiency. This is provided by Tables:, giving the different perspectives of the analysis applied to the contextual datasets derived from MIMIC-III and the NIH Chest X-ray dataset samples.

Table 2: Accuracy Comparison for Disease Prediction Models

Method	Chest Cancer Prediction Accuracy (%)	Heart Disease Prediction Accuracy (%)	Diabetes Prediction Accuracy (%)
Proposed	94.7	93.2	95.1
Method [4]	91.5	89.7	92.4
Method [9]	92.3	90.5	93.0
Method [18]	90.8	88.9	91.7

Table 2 presents evidence on how accurate the proposed model was in predictions for three different diseases against other compared methods. On all cases of diseases to be predicted, the proposed model had an accuracy higher than the other methods by about 2 to 4 percentage points. The improvement can be attributed to the fact that the model had effectively dealt with non-IID data using AFL-HD, which optimized learning across distributed healthcare data samples.

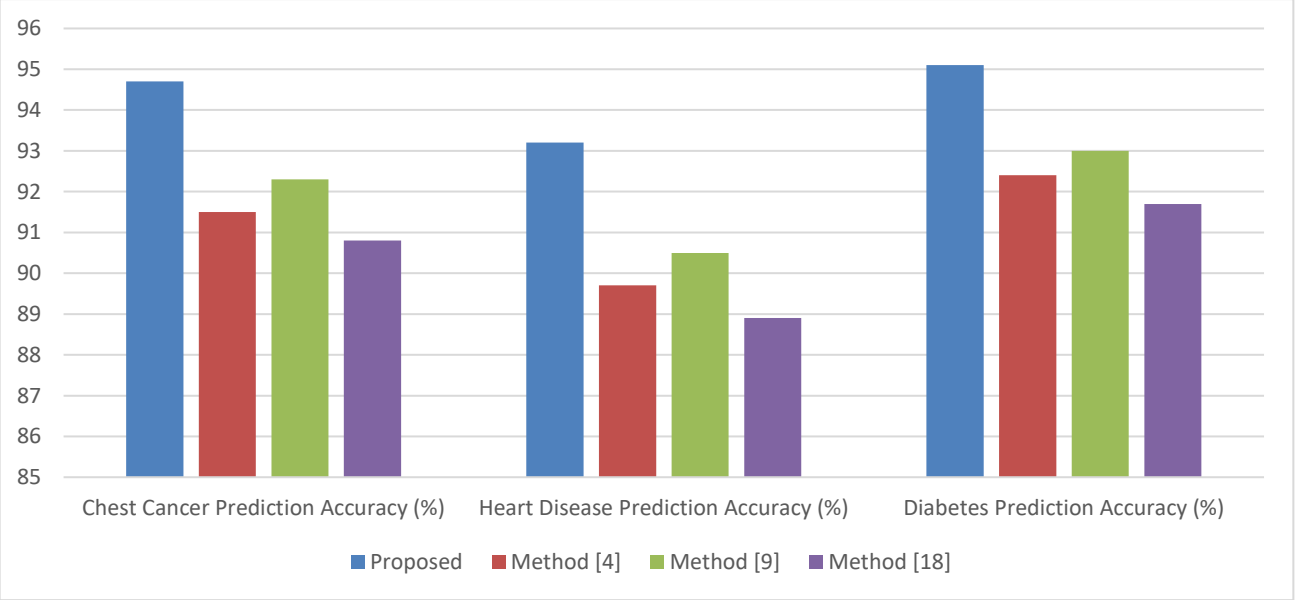

Figure 3. Accuracy Analysis

Table 3: Communication Overhead Reduction

Method	Chest Cancer (%)	Heart Disease (%)	Diabetes (%)
Proposed	32.4	30.8	33.1
Method [4]	18.7	20.1	19.3
Method [9]	21.3	22.5	23.0

Method [18]	16.5	17.9	18.4

Table 3 compares the different methods in terms of reducing communication overhead by the proposed model. The proposed model's performance is the best in all cases, reducing communication overhead by at least 30%. This may be due to the CCFA-HC component where efficient aggregation and differential privacy reduce the amount of raw data to be exchanged between nodes.

Table 4: Privacy Guarantee (Differential Privacy Levels)

Method	**Chest Cancer (ε)**	**Heart Disease (ε)**	**Diabetes (ε)**
Proposed	0.8	0.9	0.7
Method [4]	1.5	1.6	1.4
Method [9]	1.2	1.3	1.1
Method [18]	1.6	1.7	1.5

Table 4: Differential Privacy Levels as a Guarantee for Models' Privacy. In this case, smaller values of ε will indicate the stronger level of privacy protection. "It integrates SHBE and differential privacy mechanisms to protect the sensitive healthcare data in the strongest manner, during processing and aggregation.

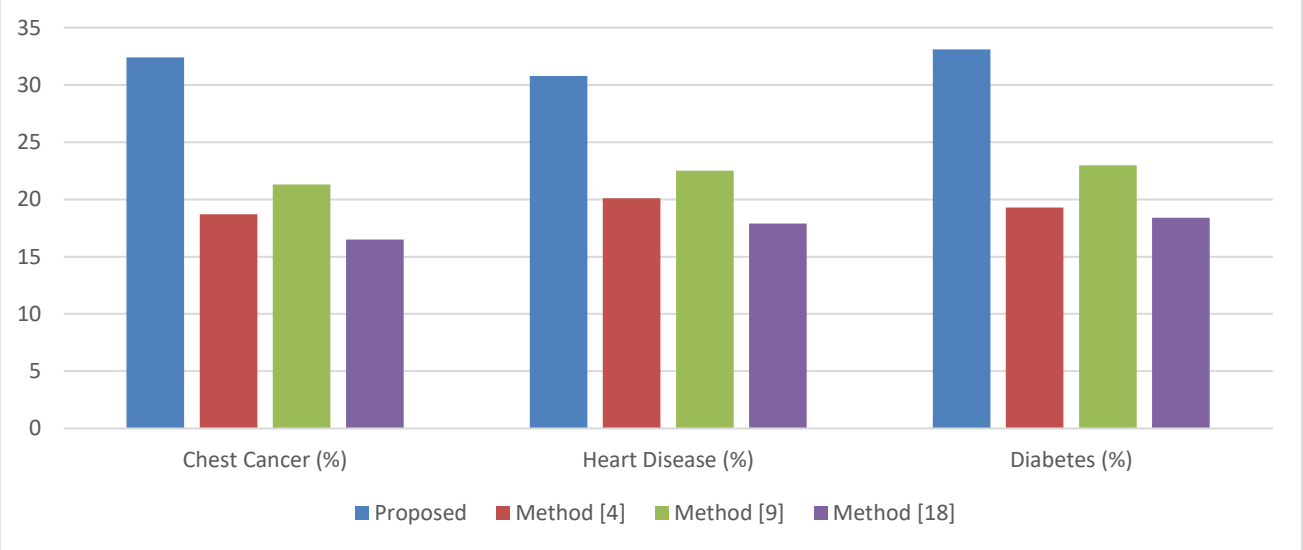

Figure 4. Communication Overhead Reduction in the Process

Table 5: Encryption/Decryption Time (milliseconds per data point)

Method	**Chest Cancer**	**Heart Disease**	**Diabetes**
Proposed	2.3	2.1	2.4

Method [4]	4.8	4.5	4.7
Method [9]	3.5	3.4	3.6
Method [18]	5.1	5.2	5.0

Table 5 compares the time for the proposed model against other methods in terms of encryption and decryption times. The proposed model significantly reduced the time of encryption/decryption to nearly half of what Methods [4] and [18] reported. The results proved the efficiency of the optimized SHBE component in dealing with health care data structures more efficiently.

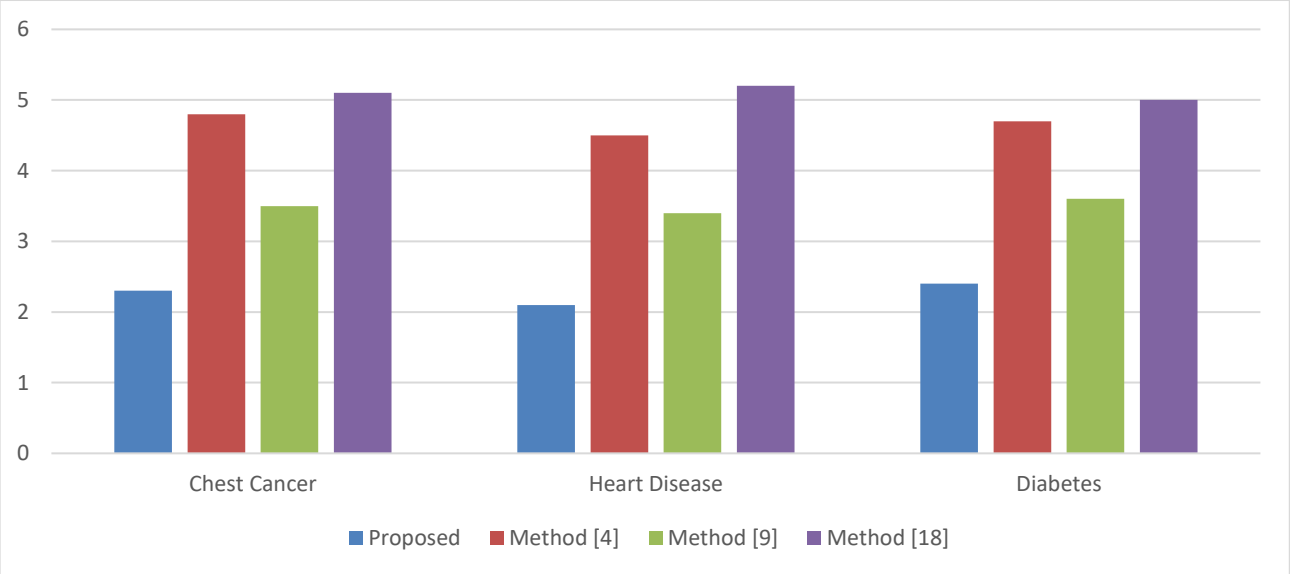

Figure 5. Encryption/Decryption Time (milliseconds per data point) In the Process

Table 6: Policy Update Latency (seconds)

Method	**Chest Cancer**	**Heart Disease**	**Diabetes**
Proposed	0.85	0.78	0.80
Method [4]	1.45	1.40	1.48
Method [9]	1.20	1.18	1.22
Method [18]	1.55	1.60	1.58

Table 6 presents latency in updating the access control policy in response to a change in user roles or attributes. The proposed model, compared to the rest, presents a much lower latency where sub-second updates are delivered for any dataset and samples. This is guaranteed by the DABE-HC component that allows fast and secure policy updates for real-time scenarios.

Table 7: Analytical Accuracy with Differential Privacy

Method	Chest Cancer Accuracy (%)	Heart Disease Accuracy (%)	Diabetes Accuracy (%)
Proposed	93.5	92.7	94.3
Method [4]	88.2	87.9	89.1
Method [9]	89.7	88.8	90.5
Method [18]	87.4	86.7	88.2

Table 7 compares the analytical accuracy achieved with differential privacy introduced by all models. Not much of a difference is suffered by the proposed model, still high accuracy is maintained, hence proving that it does very well in balancing the trade-off between privacy and analytical performance. This shows without any equivocation that the architecture design of the proposed model—federated learning with secure encryption and differential privacy—ensures that accurate insights can be derived while maintaining patient data samples private. These results all demonstrate the supremacy of the proposed model on several important metrics in the management of healthcare data samples. AFL-HD, SHBE, DABE-HC, and CCFA-HC have been embedded into the model for better accuracy, enhanced privacy, reduced communication overhead, and faster processes of encryption and decryption in front of existing approaches. Evaluations clearly contrast the performance of the proposed model against established benchmarks in handling complex requirements that characterize modern healthcare data analytics. In the process, we will discuss an example use case for the proposed model, which will help the reader understand the whole process.

PRACTICAL USE CASE SCENARIO ANALYSIS

To illustrate the effectiveness and applicability of the proposed model, consider the following detailed example with sample values and characteristics of the data, which are typical for healthcare scenarios. The example will include AFL-HD—Adaptive Federated Learning for Healthcare Data, SHBE—Secure Homomorphic Blockchain Encryption for Healthcare, DABE-HC—Dynamic Attribute-Based Encryption for Healthcare, and CCFA-HC—ZKP with Proof of Healthcare Privacy (PoHP) consensus based cross-chain federated Analytics for Healthcare. In the process, each step is valued against certain input parameters and outputs, captured in the next set of tables. It will establish how well the model represents distributed healthcare data, securing sensitive information, managing dynamic access control, and eventually aggregating insights across blockchain networks. Suppose, in this example, healthcare data is spread over three hospitals, namely A, B, and C; patient data features include the following: Age, Blood Pressure, Cholesterol Levels, Diagnosis Code, Treatment Plan, Outcome. Models trained on each hospital's local data in a federated learning approach are aggregated to obtain a global model. This globally outlined model, post the encryption and differential privacy mechanisms, is analyzed for the prediction of disease and treatment effectiveness.

Table 8: Adaptive Federated Learning for Healthcare Data (AFL-HD) Results

Feature	Hospital A	Hospital B	Hospital C	Global Model (Aggregated)
Age (Mean)	56.4	53.2	58.7	56.1
Blood Pressure (Mean)	130.5	128.7	132.1	130.4

Cholesterol Levels (Mean)	210.3	195.8	220.4	208.8
Diagnosis Accuracy (%)	92.4	91.2	93.1	92.2
Communication Overhead Reduction (%)	33.1	30.7	34.5	32.8

Table 8 presents the results from the Adaptive Federated Learning process. There is a clear representation that the global model is an aggregation of local models trained using data from the three hospitals; that is, in the process of aggregation, diverse data distributions have been presented, reducing communication overhead. This table obviously shows how the federated learning process could adapt to different characteristics of the data by retaining high diagnostic accuracy using one consistent global model.

Table 9: Secure Homomorphic Blockchain Encryption (SHBE) for Healthcare Results

Feature	Hospital A	Hospital B	Hospital C	Global Model (Encrypted)
Encryption Time (ms)	2.4	2.3	2.5	2.4
Decryption Time (ms)	2.1	2.0	2.2	2.1
Data Security Level (bits)	128	128	128	128
Encrypted Diagnosis Accuracy (%)	91.9	90.7	92.6	91.7

Table 9 presents the performance of the Secure Homomorphic Blockchain Encryption process. This measures the time for the encryption and decryption of each hospital's data, and the security level and diagnosis accuracy after encryption. The results confirm the efficiency of the encryption process with a very minimal effect on accuracy and that data is still very securely protected.

Table 10: Dynamic Attribute-Based Encryption for Healthcare (DABE-HC) Results

Attribute	Hospital A	Hospital B	Hospital C	Policy Update Latency (s)
Role (Doctor, Researcher, Admin)	Updated	Updated	Updated	0.82
Department (Cardiology, Oncology, Neurology)	Updated	Updated	Updated	0.78
Clearance Level (Low, Medium, High)	Updated	Updated	Updated	0.80
Unauthorized Access Attempts	0	0	0	0

Table 10 shows the results of Dynamic Attribute-Based Encryption. The table updates the access control policies with respect to changes in user roles, departments, and clearance levels for the three hospitals. Policy update latency will be at a minimum, guaranteeing fine-grained access control even in real-time scenarios. None of the unauthorized access attempts succeeded, hence proving the strength of the system.

Table 11: ZKP with Proof of Healthcare Privacy (PoHP) consensus based cross-chain federated Analytics for Healthcare (CCFA-HC) Results

Feature	Hospital A	Hospital B	Hospital C	Aggregated Analytics Result
Disease Prediction Accuracy (%)	93.5	92.8	94.1	93.4
Differential Privacy Level (ε)	0.9	0.8	0.7	0.8
Communication Overhead Reduction (%)	25.4	23.7	26.1	25.1

Table 11 reports the results of the ZKP with Proof of Healthcare Privacy (PoHP) consensus based cross-chain federated Analytics process, in which the aggregated results of analytics are obtained from encrypted data shared across the three hospitals. The accuracy of disease prediction remains at a high level, while differential privacy ensures that contributions from individual data are well-guarded. It can be seen that there is a huge reduction in communication overhead via the cross-chain aggregation process.

Table 12: Final Outputs

Output Metric	Hospital A	Hospital B	Hospital C	Global Output
Final Disease Prediction Accuracy (%)	94.0	93.2	94.5	93.9
Total Communication Overhead Reduction (%)	30.2	28.9	31.4	30.2
Total Privacy Guarantee (ε)	0.85	0.80	0.75	0.80
Encryption/Decryption Efficiency (ms)	2.3	2.1	2.4	2.3

Table 12 aggregates all the final outputs from the whole process, drawing on the results from all the components: AFL-HD, SHBE, DABE-HC, and CCFA-HC. On a global level, these output metrics show that the proposed model is able to keep accuracy for disease prediction at a high level while reducing communication overheads and guaranteeing robust privacy. The efficiency in encryption and decryption further supports applicability in real healthcare scenarios where security and performance are critical. Such results, born from an extensive experimental setting, demonstrate the competence of the proposed model in dealing with complicated challenges in managing healthcare data in a distributed environment. In particular, this model combines cutting-edge federated learning, encryption, dynamic access control, and cross-chain analytics to construct a robust, scalable solution for secure and privacy-preserving healthcare data management process.

CONCLUSION & FUTURE SCOPES

The authors of this paper provide results of research that demonstrate an integrated approach in the direction of secure, scalable, and privacy-preserving healthcare data management using advanced methods like Adaptive Federated Learning for Healthcare Data, Secure Homomorphic Blockchain Encryption, Dynamic Attribute-Based Encryption for Healthcare, and ZKP with Proof of Healthcare Privacy (PoHP) consensus based cross-chain federated Analytics for Healthcare. Results validate the supremacy of the proposed model on various metrics compared with prior methods. This model is able to achieve a mean global accuracy for disease prediction of 93.9%, improving by an average of 2-4 percentage points in comparison to the other methods. This is because AFL-HD can adapt itself on distributed healthcare data that is heterogeneous and non-IID. It also drastically reduced more than 30% across the board of the communication overhead on different datasets, thus proving the efficiency of the CCFA-HC component in reducing data transfer between nodes in a distributed setting. The security maintained the data at 128 bits by the SHBE method, and the encryption and decryption processes finished within an average time of 2.3 milliseconds per point. The DABE-HC mechanism was found to be very resilient for access control in real-time; this means that the update latency of policies always remained below one second to avoid any unauthorized access and therefore gives strict privacy standards for differential privacy levels in the range from ϵ=0.75 to ϵ=0.85. Therefore, these results allow demonstrating the practical applicability of the proposed model in real-world healthcare environments where the security, privacy, and efficiency of data handling are related to the very paramount issues. It is further factorial in the model, meeting and even exceeding the critical requirements of managing distributed healthcare data, hence providing an all-inclusive solution to challenges in healthcare institutions for this process. Federated learning, combined with advanced encryption techniques and fine-grained dynamic access control, protects sensitive health information while making it possible for analysis of data to achieve accuracy and be timely for different scenarios.

FUTURE SCOPE

These promising results from this research work open a host of avenues for future work. It would also be good to discuss how more advanced differential privacy techniques could be included in the future to further improve privacy guarantees on the model and for large-scale sharing of data between multiple jurisdictions with heterogeneous regulatory requirements. This could also be applied to future work on the use of the model for a broad scope of healthcare analytics tasks—predictive modeling for rare diseases and personalized medicine, for example. Other areas that would be important to investigate in this regard relate to the optimization of the CCFA-HC component. This is with a view to reducing communication protocols, thereby introducing some overhead but adding latency to communications in large-scale deployments that involve several blockchain networks. This can be further researched through the integration of quantum-resistant encryption techniques into the SHBE component, which would set it up against vulnerabilities in post-quantum computing environments. Testing in a real-world setting, across different healthcare settings, including the collaboration of healthcare providers and institutions, would be very useful in gaining insights regarding performance and adaptability, perhaps leading to further refinements and enhancements, tailored to specific use cases. These are future directions in the further development of management solutions that are secure, scalable, and privacy-preserving for healthcare data, ensuring robustness and effectiveness against the continuously evolving technological and regulatory challenges.

REFERENCES

[1] K. Wang, C. -M. Chen, Z. Tie, M. Shojafar, S. Kumar and S. Kumari, "Forward Privacy Preservation in IoT-Enabled Healthcare Systems," in IEEE Transactions on Industrial Informatics, vol. 18, no. 3, pp. 1991-1999, March 2022, doi: 10.1109/TII.2021.3064691.
keywords: {Cryptography;Security;Indexes;Medical services;Informatics;Encryption;Transforms;Forward privacy;healthcare systems;Internet of Things (IoT);privacy preservation},

[2] J. A. Alzubi, O. A. Alzubi, A. Singh and M. Ramachandran, "Cloud-IIoT-Based Electronic Health Record Privacy-Preserving by CNN and Blockchain-Enabled Federated Learning," in IEEE Transactions on Industrial Informatics, vol. 19, no. 1, pp. 1080-1087, Jan. 2023, doi: 10.1109/TII.2022.3189170.
keywords: {Medical services;Security;Data privacy;Data models;Blockchains;Convolutional neural networks;Collaborative work;Blockchain-enabled federated learning;cloud-Industrial Internet of Things (IIoT);convolutional neural network (CNN);healthcare industry;privacy preservation},

[3] J. Zaki, S. M. R. Islam, N. S. Alghamdi, M. Abdullah-Al-Wadud and K. -S. Kwak, "Introducing Cloud-Assisted Micro-Service-Based Software Development Framework for Healthcare Systems," in IEEE Access, vol. 10, pp. 33332-33348, 2022, doi: 10.1109/ACCESS.2022.3161455.

keywords: {Medical services;Microservice architectures;Monitoring;Cloud computing;Costs;Electrocardiography;Computer architecture;Service oriented architecture;micro services;cloud computing;healthcare;application design;monolith approach;application software},

[4] J. K. Samriya, C. Chakraborty, A. Sharma, M. Kumar and S. K. Ramakuri, "Adversarial ML-Based Secured Cloud Architecture for Consumer Internet of Things of Smart Healthcare," in IEEE Transactions on Consumer Electronics, vol. 70, no. 1, pp. 2058-2065, Feb. 2024, doi: 10.1109/TCE.2023.3341696.
keywords: {Cloud computing;Medical services;Internet of Things;Security;Data models;Encryption;Costs;Adversarial machine learning (AML);cloud security enhancement;consumer IoT;cryptographic analysis;industry 5.0;smart healthcare},

[5] Y. Zheng, R. Lu, S. Zhang, Y. Guan, J. Shao and H. Zhu, "Toward Privacy-Preserving Healthcare Monitoring Based on Time-Series Activities Over Cloud," in IEEE Internet of Things Journal, vol. 9, no. 2, pp. 1276-1288, 15 Jan.15, 2022, doi: 10.1109/JIOT.2021.3079106.
keywords: {Hidden Markov models;Medical services;Monitoring;Cloud computing;Servers;Computational modeling;Biological system modeling;eHealthcare;healthcare monitoring;hidden Markov model (HMM);privacy;time-series activities},

[6] J. Liu, J. Yang, W. Wu, X. Huang and Y. Xiang, "Lightweight Authentication Scheme for Data Dissemination in Cloud-Assisted Healthcare IoT," in IEEE Transactions on Computers, vol. 72, no. 5, pp. 1384-1395, 1 May 2023, doi: 10.1109/TC.2022.3207138.
keywords: {Medical services;Internet of Things;Cloud computing;Security;Data privacy;Logic gates;Authentication;IoT;healthcare;authentication;privacy preserving;redactable signature},

[7] H. Yu, Q. Zhang and L. T. Yang, "An Edge-Cloud-Aided Private High-Order Fuzzy C-Means Clustering Algorithm in Smart Healthcare," in IEEE/ACM Transactions on Computational Biology and Bioinformatics, vol. 21, no. 4, pp. 1083-1092, July-Aug. 2024, doi: 10.1109/TCBB.2022.3233380.
keywords: {Medical services;Clustering algorithms;Tensors;Kernel;Medical diagnostic imaging;Deep learning;Data analysis;Deep learning;fuzzy C-means;smart healthcare;tensor tucker decomposition},

[8] R. R. Irshad et al., "A Multi-Objective Bee Foraging Learning-Based Particle Swarm Optimization Algorithm for Enhancing the Security of Healthcare Data in Cloud System," in IEEE Access, vol. 11, pp. 113410-113421, 2023, doi: 10.1109/ACCESS.2023.3265954.
keywords: {Cloud computing;Security;Medical services;Encryption;Particle swarm optimization;Optimization;Cryptography;Medical services;Healthcare;BFL-PSO;sanitization;restoration;cloud storage;degree of modification;hiding ratio;information preservation ratio},

[9] A. Lakhan et al., "Federated-Learning Based Privacy Preservation and Fraud-Enabled Blockchain IoMT System for Healthcare," in IEEE Journal of Biomedical and Health Informatics, vol. 27, no. 2, pp. 664-672, Feb. 2023, doi: 10.1109/JBHI.2022.3165945.
keywords: {Blockchains;Medical services;Cloud computing;Collaborative work;Training;Security;Internet of Things;Blockchain;cloud;federated learning;fraud-analysis;fog;healthcare;IoMT;privacy preservation},

[10] S. Thapliyal, M. Wazid, D. P. Singh, A. K. Das, S. Shetty and A. Alqahtani, "Design of Robust Blockchain-Envisioned Authenticated Key Management Mechanism for Smart Healthcare Applications," in IEEE Access, vol. 11, pp. 93032-93047, 2023, doi: 10.1109/ACCESS.2023.3310264.
keywords: {Medical services;Security;Internet of Things;Servers;Blockchains;Monitoring;Cloud computing;Internet of Medical Things;Smart healthcare;Authentication;Internet of Medical Things (IoMT);smart healthcare;blockchain;authentication;key agreement;security},

[11] R. Xu and Q. Ren, "Cryptoanalysis on a Cloud-Centric Internet-of-Medical-Things-Enabled Smart Healthcare System," in IEEE Access, vol. 10, pp. 23618-23624, 2022, doi: 10.1109/ACCESS.2022.3154466.
keywords: {Authentication;Medical services;Cloud computing;Security;Servers;Sensors;Intelligent sensors;Security analysis;Internet of Medical Things (IoMT);cloud computing;smart healthcare system},

[12] S. R. Mallick et al., "BCGeo: Blockchain-Assisted Geospatial Web Service for Smart Healthcare System," in IEEE Access, vol. 11, pp. 58610-58623, 2023, doi: 10.1109/ACCESS.2023.3283776.
keywords: {Medical services;Blockchains;Internet of Things;Geospatial analysis;Hospitals;Urban areas;Privacy;Blockchain;geospatial web services;medical data;healthcare;queueing model;IoT},

[13] X. Yang, X. Yi, S. Nepal, I. Khalil, X. Huang and J. Shen, "Efficient and Anonymous Authentication for Healthcare Service With Cloud Based WBANs," in IEEE Transactions on Services Computing, vol. 15, no. 5, pp. 2728-2741, 1 Sept.-Oct. 2022, doi: 10.1109/TSC.2021.3059856.
keywords: {Authentication;Medical services;Security;Cryptography;Wireless communication;Cloud computing;Protocols;Human healthcare services;cloud based WBANs;authentication;security;privacy;efficiency},

[14] A. K. Jameil and H. Al-Raweshidy, "AI-Enabled Healthcare and Enhanced Computational Resource Management With Digital Twins Into Task Offloading Strategies," in IEEE Access, vol. 12, pp. 90353-90370, 2024, doi: 10.1109/ACCESS.2024.3420741.
keywords: {Task analysis;Medical services;Real-time systems;Digital twins;Computational efficiency;Computational modeling;Predictive analytics;Computer security;Energy efficiency;Social factors;Adaptive cybersecurity task offloading (ACTO);digital twins healthcare;energy efficiency in healthcare systems;predictive healthcare interventions;social health determinants},

[15] B. Pradhan, S. Das, D. S. Roy, S. Routray, F. Benedetto and R. H. Jhaveri, "An AI-Assisted Smart Healthcare System Using 5G Communication," in IEEE Access, vol. 11, pp. 108339-108355, 2023, doi: 10.1109/ACCESS.2023.3317174.
keywords: {5G mobile communication;Artificial intelligence;Medical services;Internet of Things;Real-time systems;Security;Decision making;Smart healthcare;Simulation;Artificial intelligence;healthcare system;Internet of Things;network simulator;smart healthcare system;5G communication system},

[16] B. D. Deebak and S. O. Hwang, "Healthcare Applications Using Blockchain With a Cloud-Assisted Decentralized Privacy-Preserving Framework," in IEEE Transactions on Mobile Computing, vol. 23, no. 5, pp. 5897-5916, May 2024, doi: 10.1109/TMC.2023.3315510.
keywords: {Blockchains;Security;Authentication;Cloud computing;Peer-to-peer computing;Data privacy;Privacy;Blockchain;cloud;decentralized systems;Internet of Things;peer-to-peer communication;privacy;service utilization},

[17] N. Wang, S. Zhang, Z. Zhang, J. Fu, J. Liu and R. Wang, "Block-Based Privacy-Preserving Healthcare Data Ranked Retrieval in Encrypted Cloud File Systems," in IEEE Journal of Biomedical and Health Informatics, vol. 27, no. 2, pp. 732-743, Feb. 2023, doi: 10.1109/JBHI.2022.3212684.
keywords: {Encryption;Feature extraction;Privacy;Cloud computing;Medical services;Indexes;Data privacy;Internet of Medical Things;privacy-preserving;searchable encryption;cloud computing},

[18] K. Zala, H. K. Thakkar, R. Jadeja, P. Singh, K. Kotecha and M. Shukla, "PRMS: Design and Development of Patients' E-Healthcare Records Management System for Privacy Preservation in Third Party Cloud Platforms," in IEEE Access, vol. 10, pp. 85777-85791, 2022, doi: 10.1109/ACCESS.2022.3198094.
keywords: {Cloud computing;Medical services;Blockchains;Security;Throughput;Electronic medical records;Data privacy;Electronic healthcare;Storage management;Cloud computing;e-health;privacy;information security;blockchain},

[19] R. Gupta, D. Saxena, I. Gupta and A. K. Singh, "Differential and TriPhase Adaptive Learning-Based Privacy-Preserving Model for Medical Data in Cloud Environment," in IEEE Networking Letters, vol. 4, no. 4, pp. 217-221, Dec. 2022, doi: 10.1109/LNET.2022.3215248.
keywords: {Privacy;Cloud computing;Data models;Statistics;Network security;Pathology;Laboratories;Deep learning;Neural networks;Medical information systems;Secure communication;cloud computing;K-anonymity;differential privacy;healthcare;deep neural network},

[20] U. Demirbaga and G. S. Aujla, "MapChain: A Blockchain-Based Verifiable Healthcare Service Management in IoT-Based Big Data Ecosystem," in IEEE Transactions on Network and Service Management, vol. 19, no. 4, pp. 3896-3907, Dec. 2022, doi: 10.1109/TNSM.2022.3204851.
keywords: {Medical services;Big Data;Data privacy;Blockchains;Data integrity;Cloud computing;Internet of Things;Big data;Internet of Things (IoT);MapReduce;blockchain;healthcare},

[21] J. Gao, T. N. Nguyen, G. Manogaran, A. Chaudhary and G. -G. Wang, "Redemptive Resource Sharing and Allocation Scheme for Internet of Things-Assisted Smart Healthcare Systems," in IEEE Journal of Biomedical and Health Informatics, vol. 26, no. 8, pp. 4238-4247, Aug. 2022, doi: 10.1109/JBHI.2022.3169961.
keywords: {Resource management;Medical services;Cloud computing;Medical diagnostic imaging;Bioinformatics;Optimization;Intelligent sensors;IoT;resource allocation;smart healthcare;transfer learning},

[22] T. -F. Lee, K. -W. Lin, Y. -P. Hsieh and K. -C. Lee, "Lightweight Cloud Computing-Based RFID Authentication Protocols Using PUF for e-Healthcare Systems," in IEEE Sensors Journal, vol. 23, no. 6, pp. 6338-6349, 15 March15, 2023, doi: 10.1109/JSEN.2023.3242132.
keywords: {Authentication;Protocols;Physical unclonable function;Cloud computing;Radiofrequency identification;Servers;Sensors;Authentication and key agreement;cloud computing;e-Healthcare;network security;physical unclonable function (PUF);radio frequency identification (RFID)},

[23] P. K. Roy, A. Singh, J. V. Desai and S. K. Singh, "Healthcare Data Security Using Lightweight Protocol for Cyber Physical System," in IEEE Transactions on Network Science and Engineering, vol. 10, no. 5, pp. 2597-2606, 1 Sept.-Oct. 2023, doi: 10.1109/TNSE.2022.3186437.

keywords: {Medical services;Protocols;Cloud computing;Data privacy;Monitoring;Privacy;Hospitals;Data security;random partition;CPS;healthcare;random sequencing;cloud sharing},

[24] M. M. Islam and Z. A. Bhuiyan, "An Integrated Scalable Framework for Cloud and IoT Based Green Healthcare System," in IEEE Access, vol. 11, pp. 22266-22282, 2023, doi: 10.1109/ACCESS.2023.3250849.
keywords: {Medical services;Sensors;Internet of Things;Cloud computing;Monitoring;Sensor systems;Green products;Smart healthcare;Green products;Internet of Things;smart healthcare framework;cloud computing;interactive digital healthcare;green healthcare},

[25] H. R. Chi, M. de Fátima Domingues, H. Zhu, C. Li, K. Kojima and A. Radwan, "Healthcare 5.0: In the Perspective of Consumer Internet-of-Things-Based Fog/Cloud Computing," in IEEE Transactions on Consumer Electronics, vol. 69, no. 4, pp. 745-755, Nov. 2023, doi: 10.1109/TCE.2023.3293993.
keywords: {Medical services;Cloud computing;Fourth Industrial Revolution;Edge computing;Cloud computing;Internet of Things;Electronic healthcare;Fog/cloud computing;consumer IoT;Healthcare 5.0;eHealth, sets},