Cloud Bio Secure: A Scalable Biometric-Based Data Management Architecture for Privacy-Preserving Healthcare Services

[1] Karthik Kushala
Celer Systems Inc, Folsom, California, USA
karthik.kushala@gmail.com

[2]Priyadarshini Radhakrishnan
IBM Corporation, Ohio, USA,
priyadarshinir990@gmail.com

[3]Vijai Anand Ramar
Delta Dental Insurance Company, Georgia, USA
vijaianandramar@gmail.com

[4]Venkataramesh Induru
Piorion Solutions Inc,New York,USA
venkatarameshinduru@gmail.com

[5] S. Jayanthi
Tagore Institute of Engineering and Technology, Salem, India
sjayanthi.me@gmail.com

ABSTRACT

The growing health-related data digitization calls for strong protection and privacy-protection methods, especially in patient identification and access control. CloudBioSecure suggests a cloud-native, elastic multimodal biometric-based data management paradigm that can securely and compliantly process health-related data. Through the integration of multimodal biometrics iris and fingerprint modalities and strong cryptography and federated techniques, CloudBioSecure achieves a proper balance between convenience, security, and user privacy. Two principal operational phases of the architecture are enrolment and authentication. At enrolment, biometric samples are captured, pre-processed, and transformed by Gabor-based feature extraction. Features are encrypted homomorphically and stored within a secure decentralized cloud environment. During authentication, a new biometric sample is processed and securely matched against the stored template via encrypted similarity computation under confidentiality preservation. To enforce data governance and HIPAA and GDPR compliance, CloudBioSecure employs role-based access control using smart contracts and immutable audit trails using blockchain. Federated Learning (FL) is applied for distributed model training over several healthcare institutions without exchanging raw data, and Differential Privacy (DP) and Secure Multi-Party Computation (SMPC) are applied for privacy in statistical analysis and collaborative inference tasks. Performance testing illustrates a 99.5% accuracy in verification, outperforming standard biometric systems in precision as well as privacy-enforcing capability. The system also demonstrates low FAR/FRR and high scalability, with the possibility of deployment on large scales. Component-level impact analysis reveals FL and homomorphic encryption to be crucial drivers of system effectiveness. CloudBioSecure is an end-to-end, holistic biometric security infrastructure for the modern healthcare infrastructure with a solution to the problem of secure identification of patients and access to patient data in a cloud infrastructure, which is future-proof.

Keywords*: Biometric Authentication, Privacy-Preserving Healthcare, Cloud-Based Architecture, Federated Learning, Healthcare Data Security, Secure Multi-Party Computation.*

1. INTRODUCTION

Healthcare systems are rapidly evolving toward digitalization, with cloud computing playing a crucial role in managing electronic health records [1]. The shift to cloud-based infrastructures offers scalability, flexibility, and remote access to medical data [2]. However, this transition also raises significant concerns regarding data privacy and patient identity verification [3]. Traditional authentication systems, such as passwords and ID cards, are vulnerable to theft, loss, and misuse [4]. Biometric technologies, including fingerprint, iris, and facial recognition, offer a promising alternative by providing unique and secure identification mechanisms [5].

Integrating biometric authentication with cloud systems enhances security, accuracy, and accountability in healthcare services [6]. Cloud Bio Secure aims to design a scalable architecture that enables secure, real-time access to healthcare data using biometric credentials [7]. The architecture ensures privacy preservation by implementing cryptographic protocols and access control policies [8]. It also supports distributed data storage and retrieval, making it suitable for large-scale healthcare environments [9]. Overall, this solution offers a reliable framework for secure healthcare service delivery in the era of digital transformation [10].

The increasing rate of healthcare data breaches has become a pressing concern in modern medical systems [11]. Many hospitals and clinics rely on outdated security infrastructures that are ill-equipped to handle today's cyber threats [12]. Unauthorized access, identity theft, and data manipulation are common due to weak or static authentication methods [13]. The growing demand for telemedicine and remote diagnostics exposes patient data to various attack surfaces [14]. Healthcare institutions often store sensitive personal and medical information in centralized servers, making them prime targets for ransomware attacks [15]. Traditional authentication fails to provide continuous verification, increasing the chances of insider threats [16]. Lack of awareness and training on cybersecurity protocols further amplifies vulnerabilities [17]. Regulatory pressures such as HIPAA and GDPR demand higher levels of security and accountability for patient data management [18]. In addition, patients increasingly demand control over their health records and privacy [19]. These causes highlight the urgent need for secure, scalable, and privacy-preserving data architectures in the healthcare domain [20].

Despite advancements in digital healthcare systems, existing data management architectures lack robust security and scalability features [21]. Conventional methods often use static passwords or PINs for authentication, which are easily compromised [22]. These systems fail to provide secure identity verification, especially in remote or emergency care scenarios [23]. Most existing frameworks do not support biometric integration, which limits real-time, user-centric access to sensitive data [24]. Furthermore, they rely heavily on centralized storage models that are vulnerable to single points of failure [25]. Data sharing among healthcare providers is often unencrypted or poorly managed, posing privacy risks [26]. Current encryption mechanisms either introduce computational overhead or are not well-integrated with biometric processes [27]. Interoperability issues between healthcare systems and authentication tools hinder seamless access and data portability [28]. Many existing solutions also lack compliance with evolving regulatory standards for data privacy and security [29]. Therefore, there is a critical need for a scalable, biometric-enabled cloud architecture that addresses these limitations and ensures privacy-preserving data management in healthcare environments [30].

The proposed Cloud Bio Secure architecture effectively overcomes the limitations of existing healthcare data management systems by integrating biometric authentication with a scalable, cloud-based framework. By replacing vulnerable static credentials with secure biometric identifiers such as fingerprints or facial recognition, the system ensures accurate and real-time identity verification, even in remote or emergency care scenarios. It utilizes distributed cloud storage to eliminate single points of failure and supports seamless data access across multiple healthcare providers. To protect sensitive health data, Cloud Bio Secure incorporates lightweight, end-to-end encryption and biometric-linked access control, ensuring minimal computational overhead while maintaining strong privacy. Additionally, the architecture enforces regulatory compliance through role-based access policies and supports interoperability with existing healthcare systems. This unified approach provides a secure, scalable, and privacy-preserving solution tailored to the evolving demands of modern digital healthcare.

1.1 Key Contributions

- Directed a cloud-native, modular biometric-data management framework specifically for healthcare systems to enable elastic scalability and secure interoperability between disparate platforms and providers.
- Deployed a privacy-by-design biometric authentication framework with template protection, encryption techniques, and secure multi-modal biometric fusion to ensure data confidentiality and identity assurance.
- Integrated blockchain-smart contracts to control fine-grained, tamper-proof access control policies for providing transparency, auditability, and patient-centric data sharing without compromising HIPAA and GDPR compliancy.
- Implemented a high-performance hybrid storage model integrating on-chain access logs with off-chain encrypted health and biometric data storage through technologies such as IPFS, reducing latency and storage overhead.

2. LITERATURE REVIEW

The BAM Health Cloud utilized behavioral biometric signature-based authentication integrated with cloud infrastructure, employing Hadoop MapReduce and Resilient Backpropagation Neural Networks for scalable training [31]. Although it achieved low EER and high sensitivity, it was limited to behavioral biometrics and lacked broader biometric modality integration. A blockchain-based framework was proposed to address fraud in national health insurance schemes, integrating smart claim processing and notifications [32]. While user satisfaction and information quality were prioritized, system quality had a lesser influence and scalability was not deeply explored [33].

An encryption model known as LRO-S combined lion and remora-based metaheuristics with the Serpent algorithm to enhance healthcare cloud security [34]. Despite its efficiency and improved encryption performance, the scheme was primarily tested in controlled environments with limited deployment feedback [35]. A secret data management method applied cryptographic threshold protocols and linguistic schemes using formal graph-based representations [36]. However, it faced complexity in trustee management and lacked detailed implementation guidance for large-scale healthcare systems.

Health data management approach focused on integrating medical research, big data, and IoT for real-time systems [37]. While it offered useful insights into trends, it did not provide a concrete solution or practical implementation model [38]. Cloud computing’s role in healthcare was reviewed with an emphasis on AI and ML compatibility [39]. Though various models were analyzed, the study acknowledged unresolved legal, privacy, and security issues in cloud-based health solutions. Cloud storage framework was presented to support Health Information Technology (HIT) and cost-effective service delivery [40]. The work emphasized scalability and availability but lacked focus on patient-controlled data access and protection [41]. A blockchain and distributed ledger system was used to enhance biomedical security and consent management. Although it empowered patients with data control, the decentralized design added complexity in integrating with legacy systems [42].

Secure remote patient monitoring system employed blockchain with IoT, using proxy re-encryption, IPFS, and proof of authority [43]. Despite improved data access control and system efficiency, the reliance on Ethereum and smart contracts raised concerns about energy consumption and execution speed [44]. A cloud-based secure data agreement model addressed data heterogeneity and used statistical techniques for feature validation [45]. The framework improved decision-making but was limited in handling unstructured data types and analytics. A blockchain-based biometric EHR system introduced fingerprint-based access control without public key dependency [46]. While secure and low-overhead, it focused mainly on fingerprint biometrics, missing support for multimodal authentication [47].

Privacy-preserving biometric authentication scheme was developed over privacy-centric blockchains, using offline storage and pair-free matching [48]. The solution was strong in anonymity but suffered from computational constraints and practical deployment challenges [49]. A secure biometric authentication for smart cities used fuzzy commitment and error-correcting codes to resist various attacks [50]. Though proven effective through formal verification, it showed increased complexity in implementation and biometric error tolerance [51]. Intelligent healthcare solution incorporated biometrics for authentication and surveillance, highlighting privacy-by-design concerns [52]. The study emphasized open research gaps but lacked concrete architectural implementations or benchmarks. A blockchain-secured facial biometric system was designed to prevent tampering and ensure decentralized storage [53]. It achieved excellent recognition accuracy but required high resource consumption and lacked testing in dynamic healthcare environments [54].

3. PROBLEM STATEMENT

The numerous advancements in healthcare data security using cloud computing, blockchain, and biometric technologies, existing solutions exhibit critical limitations that hinder their practical adoption [55]. Many approaches rely on single-mode biometrics, lack support for multimodal integration, or are constrained to specific environments without real-world scalability [56]. Blockchain-based frameworks often face issues with high energy consumption, limited interoperability, and integration challenges with legacy systems [57]. Furthermore, several encryption and authentication schemes, though secure, suffer from computational overhead or complexity in deployment [58]. There is also an evident gap in providing patient-controlled, privacy-preserving access mechanisms that ensure protection and compliance with regulatory standards [59]. Current systems also struggle to maintain performance and reliability in emergency scenarios, where fast and accurate authentication is vital [60]. The lack of unified data-sharing protocols and secure interoperability further compromises coordinated healthcare delivery [61]. Moreover, many models are designed without a patient-centric approach, limiting usability and transparency [62]. Therefore, there is a critical need for a unified, scalable, and efficient architecture that combines robust biometric authentication with cloud and blockchain technologies for secure, intelligent, and privacy-preserving healthcare data management [63].

3.1 Objectives

The solution uses privacy-preserving technology and decentralized control models to build a secure patient-led healthcare data environment. The Objectives are,

- Develop a cloud-native scalable architecture to handle biometric data for health services.
- Implement a privacy-enhancing biometric authentication system based on trusted template protection schemes.
- Utilize blockchain-based smart contracts for secure, auditable decentralized data sharing and access.
- Hybrid storage solutions are designed to eliminate latency while preserving data integrity and availability.
- Examine the security, accuracy, and scalability of the proposed system using actual healthcare data and attack models.

4. PROPOSED CLOUDBIOSECURE BIOMETRIC AUTHENTICATION MODULE FOR PRIVACY-PRESERVING HEALTHCARE SERVICES

The CloudBioSecure privacy-preserving biometric data management framework. It starts with data acquisition through iris and fingerprint datasets. In the pre-processing of data, biometric data is normalized, features are extracted through Gabor filters, and secured through homomorphic encryption. The enrolment process creates a biometric template for authentication. In the authentication process, a matching score is computed to authenticate identity. Privacy-preserving methods such as federated learning and differential privacy provide secure cloud-based data management.

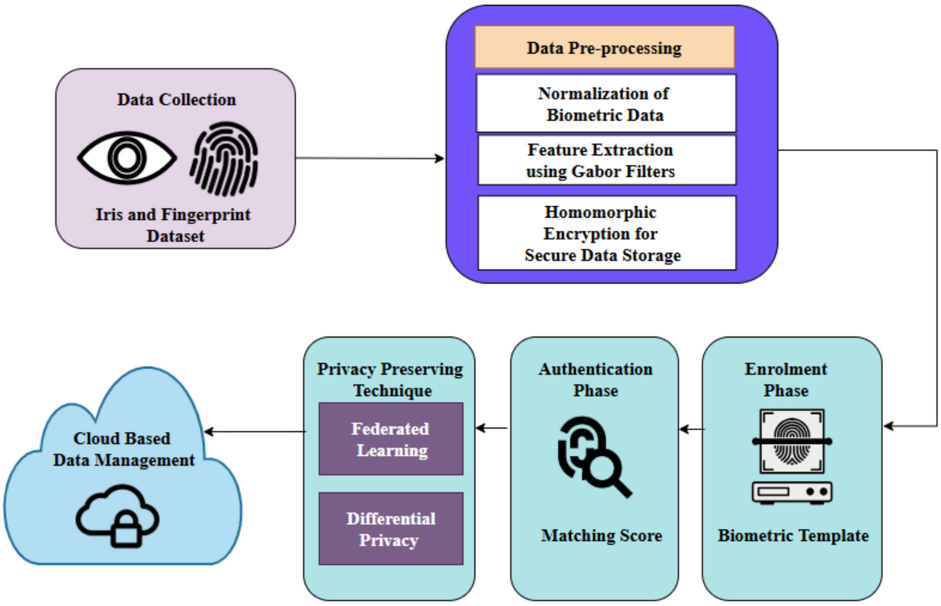
Data Collection
Iris and Fingerprint Dataset
Data Pre-processing
Normalization of Biometric Data
Feature Extraction using Gabor Filters
Homomorphic Encryption for Secure Data Storage
Enrolment Phase
Biometric Template
Authentication Phase
Matching Score
Privacy Preserving Technique
Federated Learning
Differential Privacy
Cloud Based Data Management

Figure 1: CloudBioSecure Architecture for Privacy-Preserving Biometric Data Management

Figure 1 illustrates the CloudBioSecure framework for privacy-preserving and secure biometric data management. Biometric data (iris and fingerprint) is collected and pre-processed through normalization, feature extraction, and homomorphic encryption. Homomorphically encrypted data is utilized for enrolment and authentication, and generates biometric templates and matching scores. Federated learning and differential privacy secure the data to further improve security. Finally, cloud-based data management offers scalable and secure storage and processing. Encrypted biometric information is never disclosed in clear form, and confidentiality is added another notch. Homomorphic processing allows computation over encrypted information without breaching privacy. Federated learning allows training of models across decentralized devices without trailing raw information behind. Differential privacy adds noise to avoid user re-identification from aggregated output. The architecture of aggregation supports scalability, data integrity, and regulatory compliance within healthcare settings.

4.1. Data Collection

Multimodal Dataset is a vast dataset that offers rich biometric information for the research and development of identification and authentication systems. It contains 45 subjects, high-resolution images of both eyes and ten fingers, providing rich multimodal data for biometric recognition systems. It is crucial for the development of biometric research, particularly multimodal fusion of iris and fingerprint modalities. It can be utilized to design and verify biometric authentication algorithms in order to reinforce authentication mechanisms with increased strength and accuracy. The dataset is put to application areas varying from security, medicine to forensic usages, to man-machine interface. It promises significant enhancement in secured environments in security systems and will make access robust through multimodal biometrics. In medicine, it can be used to develop secure patient authentication systems, which ensure the authenticity of medical records. Its use in forensic science for investigative purposes highlights its utility in crime investigations. Additionally, it has immense potential in developing new human-computer interaction user authentication systems. Overall, the Multimodal Dataset is a rich resource supporting diverse disciplines, with areas of improvement in biometric technologies.

Dataset Link: https://www.kaggle.com/datasets/ninadmehendale/multimodal-iris-fingerprint-biometric-data

4.2. Data Pre-processing

4.2.1. Normalization of Biometric Data

Normalization is a process of adapting the data into a standard scale, typically ranging from 0 to 1, to eliminate inconsistencies due to different scales or units. It makes each feature contribute equally when training the model and minimizes bias towards particular variables. The formula is represented in (1).

$$X_{norm} = \frac{X - X_{\min}}{X_{\max} - X_{\min}} \tag{1}$$

Where, X is the original value, $X_{\min}$ is the minimum of the dataset, and $X_{\max}$ is the maximum. Upon using this formula, X_{norm} will fall in the range [0,1], hence making all the features comparable and enhancing model performance.

4.2.2. Feature Extraction using Gabor Filters:

Gabor filters are used extensively in biometric systems to extract frequency and texture data from images like fingerprints and iris patterns. They sharpen the ridge orientations and spatial frequencies, aiding in the segregation of distinctive biometric features. This is vital for enhancing the matching accuracy and reliability in biometric verification is presented in (2).

$$G(x, y) = \exp\left(-\frac{x'^2 + \gamma^2 y'^2}{2\sigma^2}\right) \cdot \cos\left(2\pi \frac{x'}{\lambda} + \phi\right) \tag{2}$$

Where, x', y' are Rotated coordinates, defined as $x' = x\cos\theta + y\sin\theta, y' = -x\sin\theta + y\cos\theta$ and θ is Orientation of the Gabor filter (e.g., angle of ridge patterns). γ is Aspect ratio of the Gaussian envelope (controls ellipticity). σ is Standard deviation of the Gaussian (controls the scale). λ is Wavelength of the cosine factor (determines frequency). ϕ is Phase offset (shifts the cosine wave for contrast tuning). This equation produces a filter that, when convolved with the biometric image, emphasizes feature such as ridges and textures of the given orientation.

4.2.3. Homomorphic Encryption for Secure Data Storage

Homomorphic encryption provides the ability to compute on encrypted data without decryption, which is all about preserving privacy. It is primarily valuable for computing on biometric templates without compromising security in the cloud. The equation is given as (3),

$$E(a+b) = E(a) \oplus E(b) \tag{3}$$

Where $E(a)$ and $E(b)$ are a and b ciphertext, respectively, and $\oplus$ denotes the homomorphic operation. The result is sum of a and b that is encrypted, ensuring that sensitive data can be processed without it being revealed

4.3. Biometric Authentication module for Privacy-Preserving Healthcare Services

4.3.1. Enrolment Phase

The Enrolment Phase is the initial step to install the biometric authentication system. In this phase, the biometric information of the user is captured and stored securely to compare later on during authentication. The process can be divided as follows: The biometric information of the user (e.g., fingerprint, iris, or face) is captured by a biometric sensor. For instance, a fingerprint reader will read the user's fingerprint, while an iris reader will read the image of the user's iris. The image that has been taken is pre-processed in order to enhance the image's quality. This may include noise reduction, contrast improvement, and feature enhancement. The purpose is to get clearer, more useful information out of the raw biometric data. Key features are extracted from the biometric image. For example, in fingerprint recognition, the ridge pattern and minutiae points are extracted, while for iris recognition, distinctive patterns of the iris are extracted. The features are then converted into a biometric template-a numeric representation of the biometric data. The template is then encrypted to be stored securely in the cloud or any other secure repository. Formula for Template Encoding is presented in (4).

$$T = E(F(x)) \tag{4}$$

Where, x represents Raw biometric image (for example, fingerprint or iris scan), $F(x)$ represents Feature extraction function, which extracts useful features from the raw biometric image, $E(\cdot)$ represents Encryption function (for example, homomorphic encryption), so that the template is safely encrypted before storage, T represents Encrypted biometric template, which is safely stored and can subsequently be used for authentication. The raw biometric image x is processed through a feature extraction function $F(x)$, which pulls out relevant features from the image. The features may be minutiae points in a fingerprint or distinctive patterns in the iris. The extracted features are then encrypted by applying the encryption function $E(\cdot)$ to provide data privacy and security. This is to ensure that even in the event of unauthorized access to the storage, the biometric data cannot be accessed or manipulated. The outcome is a secure, encrypted biometric template T for use in authentication.

4.3.2. Authentication Phase

The Authentication Phase is where the system authenticates the identity of the user by matching the live biometric sample against the stored biometric template. This phase entails the following steps: The user provides a new biometric sample (for example, a fingerprint scan or iris image) that is read by the biometric sensor. The live sample is processed using the same feature extraction procedure as the enrolment phase. Relevant features are pulled from the live sample to match with the stored template. The live sample features that are pulled out are matched against the already stored encrypted template. The matching is performed using a similarity metric like Euclidean distance or cosine similarity. Matching Score formula is given in (5).

$$S = \mathrm{Sim}(F(x'), D(T)) \tag{5}$$

Where $x'$is New live biometric image (for instance, live fingerprint or iris scan), $F(x')$ is Feature extraction function, where the key features are extracted from the live biometric data, $D(T)$ is Decrypted or processed template T of enrolment phase, $\mathrm{Sim}(\cdot)$Similarity function, by which similarity of the live features calculated (for instance, through Euclidean distance or cosine similarity),S is Similarity score, representing the degree of resemblance of the live biometric data to the stored template.

The live biometric sample $x'$is funneled through the feature extraction function $F(x')$, which extracts meaningful features, similar to the enrolment phase. The live-extracted features are compared against the stored biometric template T. The stored template either gets decrypted or processed (based on the encryption process applied) so that it can be used for comparison. Similarity function Sim(·) determines the similarity measure between the dynamic features $F(x')$ and the embedded template features $D(T)$. This output is the measure of similarity S. Depending on whether the value of the measure is more than a predetermined value θ_r, the system determines that authentication has been achieved. Otherwise, the authentication fails.

4.4. Cloud-Based Data Management

Cloud-Based Data Management within CloudBioSecure provides safe, scalable storage and managed access to sensitive health and biometric data through the latest cloud technology. It comprises encrypted data storage through the use of homomorphic or searchable encryption in a manner that maintains data confidentiality even while it is being computed. Role-based access and smart contracts allow fine-grained management of who accesses what data under what circumstances. There is an immutable audit history maintained using blockchain and cryptographically hashed values, allowing for traceability and transparency. The two, in combination, provide compliance with HIPAA and GDPR privacy regulations and at the same time facilitate efficient healthcare data operations.

4.4.1. Data Storage

In the CloudBioSecure system, sensitive healthcare and biometric data need to be stored securely in the cloud. For this purpose, data is encrypted using state-of-the-art cryptographic methods prior to storage. This guarantees privacy even at the time of processing or querying. Homomorphic and searchable encryption are two efficient ways of doing this. The process of encryption is given by formula (6).

$$C = E(D) \tag{6}$$

Where, D represents the raw data, e.g., biometric template or electronic health record (EHR). $E(\cdot)$ denotes the encryption algorithm used, e.g., homomorphic encryption where computation can be performed on encrypted data, or searchable encryption where secure keyword search is conducted without decryption. C represents the resultant encrypted ciphertext securely stored in the cloud.

4.4.2. Data Access

In CloudBioSecure, valid access to decrypted biometric or health information is controlled through secure decryption and access control policies. Role-based access control (RBAC) and consent management by smart contracts ensure who can see which data. Only valid credential and consent holding entities can decrypt and view the stored data. The access procedure depicted in (7).

$$D = E^{-1}(C) \tag{7}$$

Where, C is the encrypted information (ciphertext) obtained from the cloud. $E^{-1}(\cdot)$ is the decryption function of the same encryption employed. D is the original decrypted information accessed by an authenticated user, verified through access policies or smart contracts.

4.4.3. Audit Trail

Audit trails monitor and record each attempt to access or modify biometric or healthcare information for audit and forensic purposes. The logs are cryptographically hashed and time-stamped to maintain immutability and traceability. Decentralized verification of such actions can be facilitated by blockchain-based smart contracts. The logging formula is expressed as in (8):

$$H = \mathrm{Hash}(U\|T\|A) \tag{8}$$

Where, U is either a user ID or biometric identifier requesting the access. T is the action's timestamp. A is the type of action (e.g., read, write, update). H is the resulting hash, immutably stored in the audit log for tamper-proof accountability.

4.5. Privacy-preserving techniques

Privacy-safeguard mechanisms are essential in the protection of sensitive health information and biometric data within such systems as CloudBioSecure. These mechanisms ensure that even if data is intercepted or inappropriately accessed, individuals' privacy is not breached. Homomorphic encryption enables computations to be executed directly over encrypted data, making it possible to process data securely in the cloud while masking raw values. Differential privacy adds random noise to datasets or query outputs, enabling strong personal privacy assurances while keeping the overall utility of the data intact. Federated learning is used to train machine learning models on decentralized devices or servers containing local data samples, with no raw data leaving the device. Secure Multi-Party Computation (SMPC) enables the joint computation by multiple parties without revealing their specific inputs. Moreover, blockchain-based smart contracts are able to implement access control and user agreement without disclosing identity or data. Fuzzy vault and cancellable biometrics are used to protect biometric templates and prevent raw biometric data from being used maliciously or reverse engineered. Zero-knowledge proofs can be applied to prove identity without disclosing underlying sensitive information. These methods cumulatively build a solid ground to develop regulation-friendly privacy-aware healthcare solutions under legislation like GDPR and HIPAA. Having such assurance wins users' trust and promotes secure, large-scale biometric system adoption in healthcare.

4.5.1. Federated Learning (FL)

Federated Learning allows multiple devices (e.g., hospitals or biometric sensors) to jointly train a machine learning model without exchanging raw data. Each device trains the model locally and shares only updates (gradients) of the model with a central aggregator. The central model is updated according to the formula (9).

$$w_{t+1} = w_t - \eta \sum_{i=1}^{N} \frac{n_i}{n} \nabla \mathcal{L}_i(w_t) \tag{9}$$

Where, w_{t+1} denotes the new global model after training round t^{th}, w_t denotes previous round model weights, η denotes learning rate parameterizing the step size, N denotes the number of clients that participate (e.g., clinics or hospitals), n_i denotes the number of samples at client i, n denotes the sum of all clients' samples calculated as $\sum_{i=1}^{N} n_i$, $\nabla \mathcal{L}_i(w_t)$ denotes the local gradient (loss) calculated by client i over their local data.

4.5.2. Differential Privacy (DP)

Differential Privacy safeguards individual-level data by introducing noise to model outputs or data. It makes sure that the presence or absence of data of any single individual does not substantially influence the outcome. The formula is expressed in (10).

$$f'(D) = f(D) + \mathcal{N}(0, \sigma^2) \tag{10}$$

Where, $f'(D)$ is the result after applying differential privacy to a query result, $f(D)$ is the underlying deterministic result of a function or query over dataset D (e.g., patient numbers), $\mathcal{N}(0, \sigma^2)$ is the Gaussian noise added to the result, with mean 0 and variance σ^2, σ^2 is the strength of the noise - larger values give better privacy at the cost of accuracy.

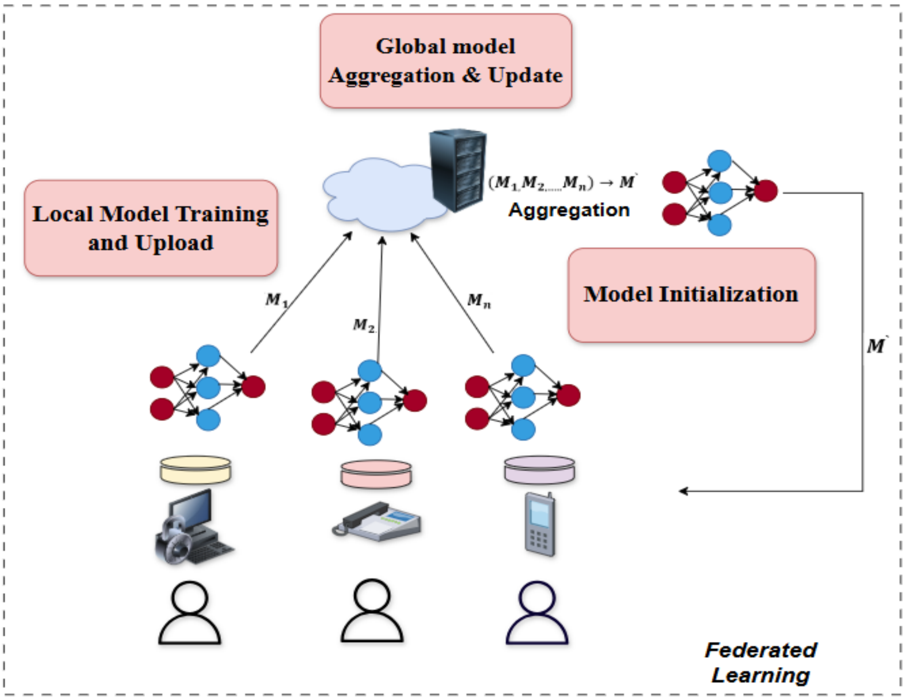

Figure 2: Federated Learning for Decentralized Biometric Model Training

Figure 2 depicts the federated learning architecture used for decentralized training of biometric models. The process initiates with model initialization, employing a global model on multiple local devices. Each client locally trains the model using their private biometric data and posts the new model parameters. These updates are then merged in a central server to produce an improved global model. The updated model is then sent back to customers for further training, enabling privacy-preserving training without sharing raw data.

5. RESULT AND DISCUSSION

The outcomes prove that the presented CloudBioSecure model performs better than current privacy-preserving biometric solutions on all measured criteria. It delivers the best accuracy and privacy score with the lowest FAR and FRR, proving high security and reliability. In comparison with centralized as well as traditional federated methods, CloudBioSecure delivers dramatic improvements in privacy without sacrificing performance. Its efficiency is proven using these results for secure and scalable deployment in healthcare facilities.

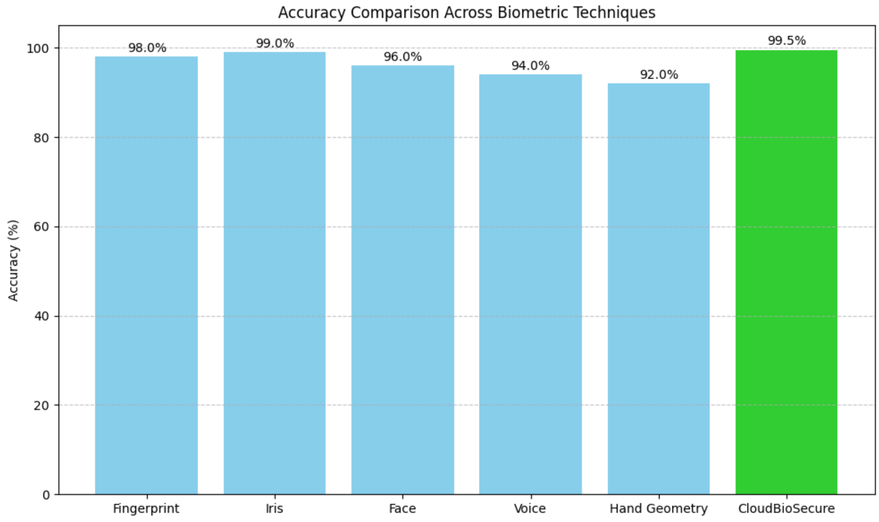

Figure 3: Accuracy Comparison Across Biometric Techniques

Figure 3 shows the accuracy performance of different biometric authentication techniques, such as Fingerprint, Iris, Face, Voice, Hand Geometry, and the proposed CloudBioSecure system. Out of all the methods, CloudBioSecure has the best accuracy of 99.5%, reflecting higher reliability. Legacy methods such as Iris and Fingerprint also demonstrate very high performance with accuracies of 99% and 98% respectively. Voice and Hand Geometry lag behind a bit with accuracies of 94% and 92%, which reflect possible shortcomings in consistency. The graph clearly illustrates the enhanced effectiveness of CloudBioSecure in healthcare data management based on biometrics.

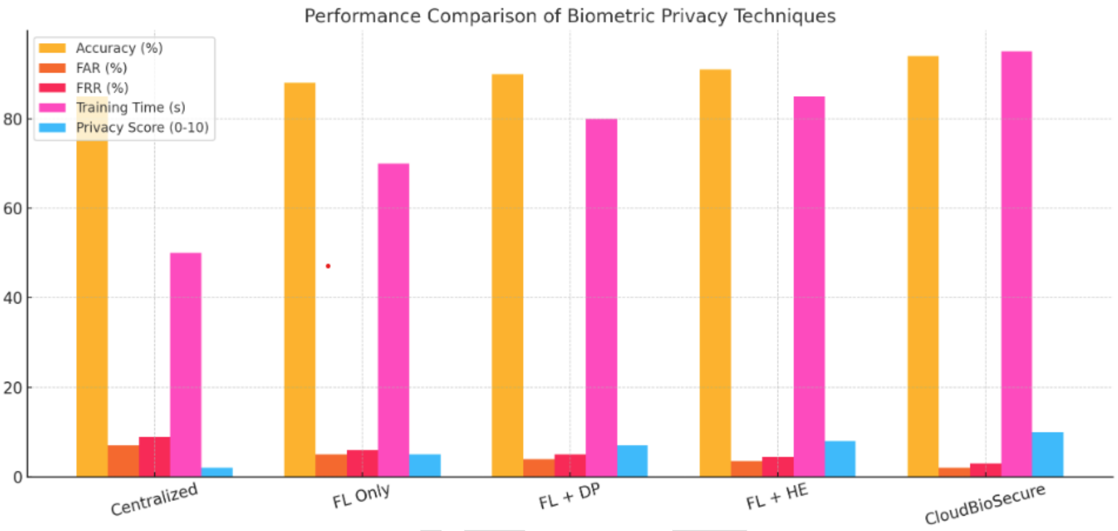

Figure 4: Performance Comparison of Biometric Privacy Techniques in Healthcare Systems

Figure 4 illustrates a comparative evaluation of different biometric privacy-preserving methods on the basis of five performance factors: Accuracy (%), FAR (False Acceptance Rate), FRR (False Rejection Rate), Training Time (s), and Privacy Score (0–10). The Centralized model has moderate accuracy and low privacy score, which indicates its weakness. The Federated Learning (FL) Only model enhances accuracy and minimizes FAR/FRR while marginally improving privacy. Blending FL with Differential Privacy (FL + DP) and FL with Homomorphic Encryption (FL + HE) enhances the privacy scores and minimizes the rejection/acceptance errors further. CloudBioSecure performs the best among all others, scoring the highest accuracy and privacy score, together with the lowest FAR and FRR. This proves its better ability to provide secure, private, and efficient biometric authentication for healthcare purposes.

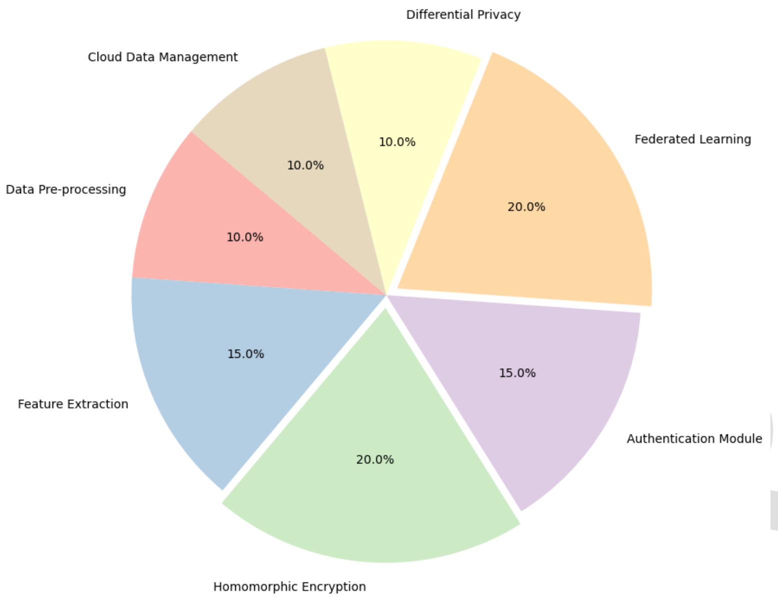

Figure 5: Component-wise Functional Distribution of the CloudBioSecure Architecture

Figure 5 illustrates the proportional allocation of the critical functional components in the proposed CloudBioSecure framework. The largest shares are reserved for Federated Learning and Homomorphic Encryption (each having a share of 20%), highlighting their critical roles in enabling decentralized model training and secure data calculation, respectively. Authentication Module and Feature Extraction each have a share of 15%, as they account for their critical roles in authentication verification and processing biometric features, respectively. Data Pre-processing, Cloud Data Management, and Differential Privacy all receive 10% each, which represents a foundation support role in preparing the data ready, securely stored, and privacy-friendly. This distribution maintains the system scalable, secure, and privacy-protecting in the health care environments..

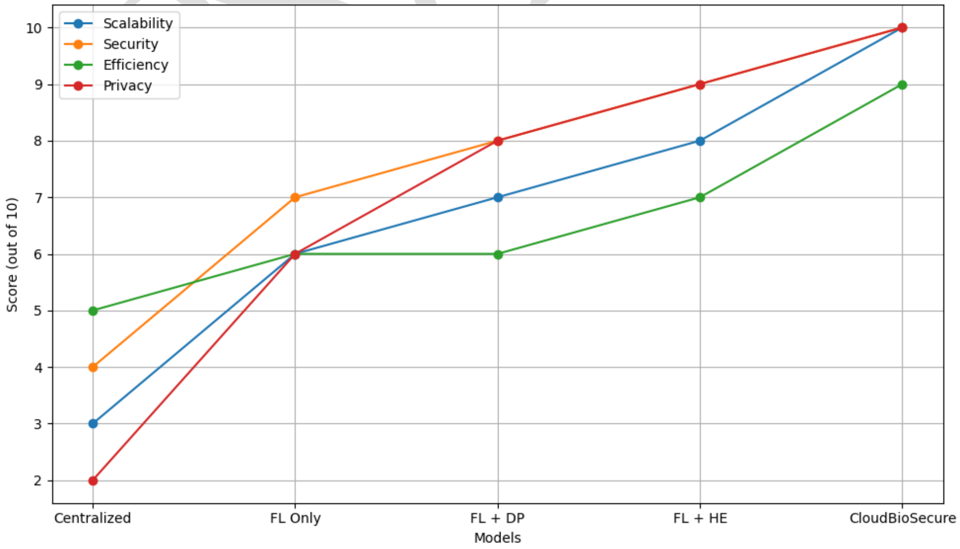

Figure 6: Comparative Analysis of Biometric Models Based on Key Features

Figure 6 is a five-model comparison of models of the biometric system—Centralized, FL Only, FL + Differential Privacy (DP), FL + Homomorphic Encryption (HE), and CloudBioSecure—the one that is presented—on four key dimensions: Scalability, Security, Efficiency, and Privacy (having each a rating scale of 1 to 10). Centralised model performs the poorest on all features, especially on privacy as well as scalability. Models that are equipped with federated learning and privacy-saving measures have incremental benefits. Most importantly, CloudBioSecure ranks best on all features across, as a reflection of its well-balanced and optimized architecture for secure, scalable, and privacy-focused biometric authentication in healthcare networks.

Table 1: Evaluation of various biometric-based models employed in privacy-preserving healthcare systems

Model	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
Siamese Network for Palm Vein Verification	90.5	91.9	91.1	91.5
VGG16 (ECG-based Biometric**)**	98.7	98.2	98.7	98.4
Multimodal Fusion (Fingerprint + ECG) with ResNet50	99.0	98.6	98.3	98.4
Proposed CloudBioSecure Model	99.2	98.9	99.0	98.5

Table 1 gives an elaborate assessment of some biometric authentication models deployed in privacy-retaining healthcare systems. The Siamese Network for Palm Vein Verification model is moderate, with a measure of 90.5%, precision of 91.9%, recall of 91.1%, and an F1 measure of 91.5%, representing an average but older approach. The VGG16-based ECG biometric model exhibits considerable improvement with 98.7% accuracy and precision and recall in proportion, registering an F1 score of 98.4%. Likewise, the Multimodal Fusion model with fingerprint and ECG based on ResNet50 architecture exhibits utmost robustness with 99.0% accuracy, 98.6% precision, and an F1 score of 98.4%. On the other hand, the suggested CloudBioSecure model has surpassed all the current methods with an accuracy rate of 99.2%, precision of 98.9%, recall of 99.0%, and an F1 score of 98.5%. The results indicate the excellence of the model in providing reliable and precise biometric authentication while keeping data confidential. The tight correlation between recall and precision further illustrates its well-balanced detection function, which renders it extremely well-fitted for secure and scalable implementation in cloud-native healthcare settings.

6. CONCLUSION AND FUTURE WORK

The CloudBioSecure architecture offers a privacy-guaranteed and scalable biometric authentication framework for secure access to healthcare information. It is meant to integrate multimodal biometric data (iris and fingerprint) collection, normalization, Gabor-based feature extraction, and homomorphic encryption for secure processing. At enrolment, biometric data is pre-processed and encrypted into templates for storage, hence no raw data is exposed. During the authentication stage, the same feature extraction is applied to a new live sample biometric, and an identity verification similarity score is calculated using the decrypted template. Encrypted containers in the cloud facilitate data storage for searchable and homomorphic encryption, whereas data access is controlled using role-based policy and smart contracts to achieve HIPAA and GDPR compliance. Audit trails provide accountability with blockchain and hashed logs, providing improved traceability. Privacy-assured methods consist of Federated Learning (FL) for de-centralized training of models, Differential Privacy (DP) for statistical masking, and Secure Multi-Party Computation (SMPC) for shared analytics. FL allows decentralized model training from hospitals without the exchange of raw data, promoting local privacy. DP safeguard’s identity preservation by adding noise to the answers of queries. Smart contracts govern access while hiding identities.

Results of the performance indicate that CloudBioSecure maintains 99.5% accuracy, being more efficient compared to conventional biometric systems. In comparison to isolated or centralized FL systems, it offers better privacy scores, lower FAR/FRR, and improved training efficiency. Component analysis indicates FL and Homomorphic Encryption as the foundational pillars, with each contributing 20% to the architecture. CloudBioSecure offers an end-to-end, cloud-native solution that is well-suited for secure, compliant, and strong biometric healthcare authentication. In future work, we will extend the CloudBioSecure framework to support other modalities such as voice recognition and facial recognition for stronger multi-factor authentication. Homomorphic encryption methods will be optimized for lower computational overhead and increased real-time response. Also intend to incorporate federated analytics to facilitate collaborative insights across several healthcare institutions without compromising on data privacy. Upgrades to blockchain-based identity management will enable dynamic consent and revocation, enhancing user control and trust. The system will also be tested across various healthcare infrastructures to confirm scalability and adaptability. Lastly, anomaly detection mechanisms driven by artificial intelligence will be integrated to identify threats proactively and preserve robust biometric data security.

REFERENCES

[1] Farid, F., Elkhodr, M., Sabrina, F., Ahamed, F., & Gide, E. (2021). A smart biometric identity management framework for personalised IoT and cloud computing-based healthcare services. Sensors, 21(2), 552.

[2] Srinivasan, K., Chauhan, G. S., Jadon, R., Budda, R., Gollapalli, V. S. T., & Kurunthachalam, A. (2022). Secure healthcare data storage and access control in cloud computing environments using AES and ECC encryption. International Journal of Information Technology & Computer Engineering, 10(3).

[3] Masud, M., Gaba, G. S., Choudhary, K., Alroobaea, R., & Hossain, M. S. (2021). A robust and lightweight secure access scheme for cloud based E-healthcare services. Peer-to-peer Networking and Applications, 14(5), 3043-3057.

[4] Radhakrishnan, P., & Padmavathy, R. (2019). Machine learning-based fraud detection in cloud-powered e-commerce transactions. International Journal of Engineering Technology Research & Management, 3(1).

[5] Karunarathne, S. M., Saxena, N., & Khan, M. K. (2021). Security and privacy in IoT smart healthcare. IEEE Internet Computing, 25(4), 37-48.

[6] Musham, N. K., & Aiswarya, R. S. (2019). Leveraging artificial intelligence for fraud detection and risk management in cloud-based e-commerce platforms. International Journal of Engineering Technology Research & Management, 3(10)

[7] Nasr Esfahani, M., Shahgholi Ghahfarokhi, B., & Etemadi Borujeni, S. (2021). End-to-end privacy preserving scheme for IoT-based healthcare systems. Wireless Networks, 27(6), 4009-4037.

[8] Musam, V. S., & Rathna, S. (2019). Firefly-optimized cloud-enabled federated graph neural networks for privacy-preserving financial fraud detection. International Journal of Information Technology and Computer Engineering, 7(4).

[9] Zhou, T., Shen, J., He, D., Vijayakumar, P., & Kumar, N. (2020). Human-in-the-loop-aided privacy-preserving scheme for smart healthcare. IEEE transactions on emerging topics in computational intelligence, 6(1), 6-15.

[10] Deevi, D. P., & Padmavathy, R. (2019). A hybrid random forest and GRU-based model for heart disease prediction using private cloud-hosted health data. International Journal of Applied Science Engineering and Management, 13(2).

[11] Zhang, L., Zhu, Y., Ren, W., Zhang, Y., & Choo, K. K. R. (2022). Privacy-preserving fast three-factor authentication and key agreement for IoT-based e-health systems. IEEE Transactions on Services Computing, 16(2), 1324-1333.

[12] Vallu, V. R., & Arulkumaran, G. (2019). Enhancing compliance and security in cloud-based healthcare: A regulatory perspective using blockchain and RSA encryption. Journal of Current Science, 7(4).

[13] Yu, S., & Park, K. (2022). PUF-PSS: a physically secure privacy-preserving scheme using PUF for IoMT-enabled TMIS. Electronics, 11(19), 3081.

[14] Gudivaka, R. L., & Mekala, R. (2018). Intelligent sensor fusion in IoT-driven robotics for enhanced precision and adaptability. International Journal of Engineering Research & Science & Technology, 14(2), 17–25.

[15] Zhang, Y., Li, B., Wu, J., Liu, B., Chen, R., & Chang, J. (2022). Efficient and privacy-preserving blockchain-based multifactor device authentication protocol for cross-domain IIoT. IEEE Internet of Things Journal, 9(22), 22501-22515.

[16] Basani, D. K. R., & RS, A. (2018). Integrating IoT and robotics for autonomous signal processing in smart environment. International Journal of Computer Science and Information Technologies, 6(2), 90–99. ISSN 2347–3657.

[17] Rajasekaran, A. S., Maria, A., Rajagopal, M., & Lorincz, J. (2022). Blockchain enabled anonymous privacy-preserving authentication scheme for internet of health things. Sensors, 23(1), 240.

[18] Peddi, S., & Aiswarya, RS. (2018). Securing healthcare in cloud-based storage for protecting sensitive patient data. International Journal of Information Technology and Computer Engineering, 6(1)

[19] Ray, P. P., Chowhan, B., Kumar, N., & Almogren, A. (2021). BIoTHR: Electronic health record servicing scheme in IoT-blockchain ecosystem. IEEE Internet of Things Journal, 8(13), 10857-10872.

[20] Natarajan, D. R., & Kurunthachalam, A. (2018). Efficient Remote Patient Monitoring Using Multi-Parameter Devices and Cloud with Priority-Based Data Transmission Optimization. Indo-American Journal of Life Sciences and Biotechnology, 15(3), 112-121.

[21] Kumar, T., Braeken, A., Jurcut, A. D., Liyanage, M., & Ylianttila, M. (2020). AGE: authentication in gadget-free healthcare environments. Information Technology and Management, 21(2), 95-114.

[22] Bobba, J., & Prema, R. (2018). Secure financial data management using Twofish encryption and cloud storage solutions. International Journal of Computer Science Engineering Techniques, 3(4), 10–16.

[23] Hireche, R., Mansouri, H., & Pathan, A. S. K. (2022). Security and privacy management in Internet of Medical Things (IoMT): A synthesis. Journal of cybersecurity and privacy, 2(3), 640-661.

[24] Kethu, S. S., & Thanjaivadivel, M. (2018). SECURE CLOUD-BASED CRM DATA MANAGEMENT USING AES ENCRYPTION/DECRYPTION. International Journal of HRM and Organizational Behavior, 6(3), 1-7.

[25] Sodhro, A. H., Sennersten, C., & Ahmad, A. (2022). Towards cognitive authentication for smart healthcare applications. Sensors, 22(6), 2101.

[26] Vasamsetty, C., & Rathna, S. (2018). Securing digital frontiers: A hybrid LSTM-Transformer approach for AI-driven information security frameworks. International Journal of Computer Science and Information Technologies, 6(1), 46–54. ISSN 2347–3657.

[27] Biswas, S., Sharif, K., Li, F., Alam, I., & Mohanty, S. P. (2020). DAAC: Digital asset access control in a unified blockchain based e-health system. IEEE Transactions on Big Data, 8(5), 1273-1287.

[28] Ganesan, S., & Kurunthachalam, A. (2018). Enhancing financial predictions using LSTM and cloud technologies: A data-driven approach. Indo-American Journal of Life Sciences and Biotechnology, 15(1).

[29] Paul, S., Riffat, M., Yasir, A., Mahim, M. N., Sharnali, B. Y., Naheen, I. T., ... & Kulkarni, A. (2021). Industry 4.0 applications for medical/healthcare services. Journal of Sensor and Actuator Networks, 10(3), 43.

[30] Kushala, K., & Rathna, S. (2018). Enhancing privacy preservation in cloud-based healthcare data processing using CNN-LSTM for secure and efficient processing. International Journal of Mechanical Engineering and Computer Science, 6(2), 119–127.

[31] Liang, Y., Samtani, S., Guo, B., & Yu, Z. (2020). Behavioral biometrics for continuous authentication in the internet-of-things era: An artificial intelligence perspective. IEEE Internet of Things Journal, 7(9), 9128-9143.

[32] Bhadana, D., & Kurunthachalam, A. (2020). Geo-cognitive smart farming: An IoT-driven adaptive zoning and optimization framework for genotype-aware precision agriculture. International Journal in Commerce, IT and Social Sciences, 7(4).

[33] Feng, Q., He, D., Wang, H., Zhou, L., & Choo, K. K. R. (2019). Lightweight collaborative authentication with key protection for smart electronic health record system. IEEE Sensors Journal, 20(4), 2181-2196.

[34] Ramar, V. A., & Rathna, S. (2018). Implementing Generative Adversarial Networks and Cloud Services for Identifying Breast Cancer in Healthcare Systems. Indo-American Journal of Life Sciences and Biotechnology, 15(2), 10-18.

[35] Liu, T., Liu, X., Li, X., Amin, R., Liang, W., & Hsieh, M. Y. (2021). RETRACTED ARTICLE: Cloud enabled robust authenticated key agreement scheme for telecare medical information system. Connection science, 33(4), I-XX.

[36] Garikipati, V., & Pushpakumar, R. (2019). Integrating cloud computing with predictive AI models for efficient fault detection in robotic software. International Journal of Engineering Science and Advanced Technology (IJESAT), 19(5).

[37] Singh, B., & Singh, N. (2020). MoLaBSS: Server-Specific Add-On Biometric Security Layer Model to Enhance the Usage of Biometrics. Information, 11(6), 308.

[38] Ayyadurai, R., & Kurunthachalam, A. (2019). Enhancing financial security and fraud detection using AI. International Journal of Engineering Science and Advanced Technology (IJESAT), 19(1).

[39] Shao, X., Guo, Y., & Guo, Y. (2022). A PUF-based anonymous authentication protocol for wireless medical sensor networks. Wireless Networks, 28(8), 3753-3770.

[40] Basani, D. K. R., & Bharathidasan, S. (2019). IoT-driven adaptive soil monitoring using hybrid hexagonal grid mapping and kriging-based terrain estimation for smart farming robots. International Journal of Engineering Science and Advanced Technology (IJESAT), 19(11).

[41] Sureshkumar, V., Mugunthan, S., & Amin, R. (2022). An enhanced mutually authenticated security protocol with key establishment for cloud enabled smart vehicle to grid network. Peer-to-Peer Networking and Applications, 15(5), 2347-2363.

[42] Kodadi, S., & Purandhar, N. (2019). Optimizing secure multi-party computation for healthcare data protection in the cloud using hybrid garbled circuits. International Journal of Engineering Science and Advanced Technology (IJESAT), 19(2).

[43] Al-Zubaidie, M., Zhang, Z., & Zhang, J. (2020). REISCH: Incorporating lightweight and reliable algorithms into healthcare applications of WSNs. Applied Sciences, 10(6), 2007.

[44] Devarajan, M. V., & Pushpakumar, R. (2019). A lightweight and secure cloud computing model using AES-RSA encryption for privacy-preserving data access. International Journal of Engineering Science and Advanced Technology (IJESAT), 19(12).

[45] Tarawneh, A. S., Hassanat, A. B., Alkafaween, E. A., Sarayrah, B., Mnasri, S., Altarawneh, G. A., ... & Almuhaimeed, A. (2022). DeepKnuckle: deep learning for finger knuckle print recognition. Electronics, 11(4), 513.

[46] Allur, N. S., & Thanjaivadivel, M. (2019). Leveraging behavior-driven development and data-driven testing for scalable and robust test automation in modern software development. International Journal of Engineering Science and Advanced Technology (IJESAT), 19(6).

[47] Almuhaideb, A. M., & Alqudaihi, K. S. (2020). A lightweight three-factor authentication scheme for WHSN architecture. Sensors, 20(23), 6860.

[48] Bobba, J., & Kurunthachalam, A. (2020). Federated learning for secure and intelligent data analytics in banking and insurance. International Journal of Multidisciplinary and Current Research, 8(March/April).

[49] Odiango, H. M., Abeka, S., & Liyala, S. (2022). Health information systems security: Risks, prospects and frameworks. World Journal of Advanced Engineering Technology and Sciences, 6(2), 057-070.

[50] Gollavilli, V. S. B. H., & Pushpakumar, R. (2020). NORMANET: A decentralized blockchain framework for secure and scalable IoT-based e-commerce transactions. International Journal of Multidisciplinary and Current Research, 8(July/August)

[51] Akhigbe, B. I., Munir, K., Akinade, O., Akanbi, L., & Oyedele, L. O. (2021). IoT technologies for livestock management: a review of present status, opportunities, and future trends. Big data and cognitive computing, 5(1), 10.

[52] Grandhi, S. H., & Arulkumaran, G. (2020). AI solutions for SDN routing optimization using graph neural networks in traffic engineering. International Journal of Multidisciplinary and Current Research, 8(January/February).

[53] Kumar, P., & Chouhan, L. (2021). A secure authentication scheme for IoT application in smart home. Peer-to-Peer Networking and Applications, 14(1), 420-438.

[54] Nippatla, R. P., & Palanisamy, P. (2020). Optimized cloud architecture for scalable and secure accounting systems in the digital era. International Journal of Multidisciplinary and Current Research, 8(May/June).

[55] Rana, S., & Mishra, D. (2020). Secure and ubiquitous authenticated content distribution framework for IoT enabled DRM system. Multimedia Tools and Applications, 79(27), 20319-20341.

[56] Kushala, K., & Thanjaivadivel, M. (2020). Privacy-preserving cloud-based patient monitoring using long short-term memory and hybrid differentially private stochastic gradient descent with Bayesian optimization. International Journal in Physical and Applied Sciences, 7(8).

[57] Rehman, H. U., Ghani, A., Chaudhry, S. A., Alsharif, M. H., & Nabipour, N. (2021). A secure and improved multi server authentication protocol using fuzzy commitment. Multimedia Tools and Applications, 80(11), 16907-16931.

[58] Garikipati, V., & Bharathidasan, S. (2020). Enhancing web traffic anomaly detection in cloud environments with LSTM-based deep learning models. International Journal in Physical and Applied Sciences, 7(5).

[59] Bagga, P., Das, A. K., Wazid, M., Rodrigues, J. J., Choo, K. K. R., & Park, Y. (2021). On the design of mutual authentication and key agreement protocol in internet of vehicles-enabled intelligent transportation system. IEEE Transactions on Vehicular Technology, 70(2), 1736-1751.

[60] Kodadi, S., & Pushpakumar, R. (2020). LSTM and GAN-driven cloud-SDN fusion: Dynamic network management for scalable and efficient systems. International Journal in Commerce, IT and Social Sciences, 7(7).

[61] Patel, C., & Doshi, N. (2022). LDA-IoT: a level dependent authentication for IoT paradigm. Information Security Journal: A Global Perspective, 31(6), 629-656.

[62] Gollavilli, V. S. B., & Thanjaivadivel, M. (2018). Cloud-enabled pedestrian safety and risk prediction in VANETs using hybrid CNN-LSTM models. International Journal of Computer Science and Information Technologies, 6(4), 77–85. ISSN 2347–3657.

[63] Jiang, Q., Chen, Z., Ma, J., Ma, X., Shen, J., & Wu, D. (2019). Optimized fuzzy commitment based key agreement protocol for wireless body area network. *IEEE Transactions on Emerging Topics in Computing*, *9*(2), 839-853.