ISSN: 2182-2069 / E-ISSN: 2182-2077

6G-Integrated Hybrid Frameworks for Secure Telemedicine Using Thermal Fingerprint Biometrics and Blockchain Technology

Dr.S. Jayaprakash[1], and J.P. Keerthana[2*]

[1]Associate Professor, Department of Computer Science, Edayathangudy G.S. Pillay Arts and Science College, Affiliated to Bharathidasan University, Tiruchirapalli, Nagapattinam, Tamil Nadu, India. jayaprakashsoundar@gmail.com, https://orcid.org/0000-0003-1365-3337

[2*]Research Scholar, Department of Computer Science, Edayathangudy G.S. Pillay Arts and Science College, Affiliated to Bharathidasan University, Tiruchirapalli, Nagapattinam, Tamil Nadu, India. jayakeerthana2094@gmail.com, https://orcid.org/0009-0003-6386-1174

Received: January 04, 2026; Revised: February 19, 2026; Accepted: March 25, 2026; Published: May 29, 2026

Abstract

Telemedicine has now become an indispensable part of remote healthcare, but secure patient authentication, data privacy, and low-latency communication have become the most significant issues. Traditional biometrics are prone to spoofing and weak in detecting liveness, and a centralized health record storage presents a security and compliance risk in the presence of regulations, like HIPAA and GDPR. More so, current cryptographic healthcare systems are typically characterized by high latency, which limits their applicability in real-time. In this paper, a 6G-ready hybrid security infrastructure will be suggested using thermal fingerprints as a biometric and a dual-layer blockchain-based infrastructure to perform the secure and decentralized authentication of telemedicine. Thermal vascular entropy maps are coded into privacy-preserving cryptographic tokens with the aid of Bio-Chain Fusion Layer (BCFL). The architecture uses the Lightweight BioChain -LBC- at the edge to provide sub-10ms authentication and a Main Security Chain (MSC) to do immutable logging as well as regulatory compliance. The experimental evaluation results show that the proposed framework achieves 97.8% authentication accuracy, a 98.4% spoof detection rate, and an average authentication latency of 7.4 ms, with a throughput of more than 800 transactions per second (TPS). The system shows about a 73% improvement in latency and accuracy, ranging from 5-8%, compared to conventional biometric and single-chain blockchain authentication systems. These findings indicate a great improvement compared to traditional systems, highlighting the usefulness of integrating thermal fingerprint biometrics and dual-layer blockchain to develop secure and scalable methods of telemedicine authentication. The integration of the 6G network slicing and edge AI allows real-time, scalable authentication in telemedicine, which is more resilient to high user concurrency and reduces the risk of data breach, making it suitable to be deployed on a large scale.

Keywords: Telemedicine Security, Thermal Fingerprint Biometrics, Blockchain Authentication, 6G Network Slicing, Edge Intelligence, Liveness Detection, Decentralized Healthcare Systems.

Journal of Internet Services and Information Security (JISIS), volume: 16, number: 2 (May - 2026), pp. 78-97.
DOI: *10.58346/JISIS.2026.I2.006*

*Corresponding author: Research Scholar, Department of Computer Science, Edayathangudy G.S.Pillay Arts and Science College, Affiliated to Bharathidasan University, Tiruchirapalli, Nagapattinam, Tamil Nadu, India.

1 Introduction

Through telemedicine, it is possible to remotely consult, diagnose, and monitor without visiting the hospital physically. The fast growth of telehealth has increased the need to have secure, scalable, and low-latency systems that are able to support sensitive medical information in real-time (Chauhan et al., 2024; Rasouli et al., 2025). Nevertheless, traditional biometric authentication systems include fingerprint and facial recognition, which can be spoofed and replayed (Malik, 2024), and using centrality to store health record data creates privacy vulnerabilities and single points of failure. Despite having a positive effect on decentralization and data integrity, current blockchain implementations usually have scalability and latency issues that cannot be supported in real-time healthcare settings (Abouelmehdi et al., 2018; Arbabi et al., 2022).

In order to overcome these problems, this paper suggests a 6G-enabled hybrid authentication scheme that incorporates both thermal vascular entropy mapping (VEM) and a dual-layer blockchain model. The inherent liveness detection of Thermal VEM is subdermal heat pattern encoding. The Bio Chain Fusion Layer (BCFL) is a union that has a Lightweight Bio Chain (LBC) to achieve fast edge authentication and a Main Security Chain (MSC) for immutable logging and compliance. The framework will provide scalable, secure, and low-latency authentication of large-scale telemedicine systems with the help of 6G network slicing and edge intelligence that is based on AI.

The key contributions of this study are as follows:

1. New Bio-Chain Fusion Layer: thermal vascular entropy biometrics together with a dual blockchain-based architecture to secure telemedicine authentication.
2. Invention of a Thermal Vascular Entropy Mapping model that offers 97.85% authentication rate and that offers irreversible biometric encoding.
3. Lightweight Bio-Chain Design: A Lightweight Bio-Chain that can support ultra-low latency authentication of less than 10ms.
4. 6G network slicing integration of high-speed secure medical communication.

The paper is organized as follows: Section 2 presents the literature review. Section 3 describes the proposed framework. Section 4 details the methodology. Section 5 discusses the experimental setup. Section 6 presents results and discussion. Section 7 concludes the paper with key findings and future research directions.

2 Literature Review

Telemedicine Evolution and Current Challenges

Telemedicine has become a massive digital sphere of healthcare that needs secure authentication and quality real-time communication (Elmi et al., 2024; Dang et al., 2019). By using centralized electronic health records, risks of data breaches are higher, and conventional authentication methods do not work in high-load situations (Elmi et al., 2024). Telesurgery, a mission-critical service, is a service that should be provided with ultra-reliable low-latency communication (URLLC), which many conventional architectures have not guaranteed (Khan et al., 2020).

Biometric and Thermal Identification

Healthcare Biometric authentication is also commonly applied in identity fraud prevention (Popovski et al., 2019). Nevertheless, the Fingerprint, face, and iris recognition systems are vulnerable to spoofing and replay attacks (Aanjanadevi et al., 2023). Thermal fingerprint imaging offers better liveness detection through analyzing subdermal vascular heat patterns (Aujla & Jindal, 2020) which offers greater resistance to presentation attacks. However, thermal biometrics integration into decentralized healthcare systems is only secure and scalable to a limited extent (Kharche & Kharche, 2023).

Blockchain in Healthcare

Healthcare data can be stored in a decentralized and tamper-resistant way with the help of blockchain (Bhuiyan et al., 2021; Arbabi et al., 2022), whereas automated access control and compliance with regulations can be ensured with the help of smart contracts (Huang et al., 2024). Although this is the case, traditional blockchain frameworks have high latency and limited scalability (Chakraborty et al., 2019; Griggs et al., 2018). So, it is necessary that lightweight and hybrid blockchain architectures could deal with a trade-off between decentralization, privacy preservation, and real-time authentication in the telemedicine setting (Dwivedi et al., 2019).

Research Gap and Motivation

New 6G networks support URLLC, network slicing, edge intelligence using AI to support mission-critical applications (Farahani et al., 2021; Sun et al., 2020). Nevertheless, literature is mostly applied to the performance of communication, and little has been introduced concerning the incorporation of biometric security and decentralized authentication. This gap prompts the creation of integrated 6G-based telemedicine architectures with biometric encoding with blockchain validation.

Healthcare Ecosystems 6G Enabled

New generations of 6G networks will offer ultra-reliable low-latency communication (URLLC), network slicing, and edge intelligence based on AI to provide real-time processing of mission-critical applications (Farahani et al., 2021). The 6G technology has the potential of aiding the high-density patient authentication, remote diagnostics, and distributed medical data exchange in healthcare (Sun et al., 2020). Nonetheless, current studies are mainly based on performance of communications, and little adaptation of biometric security and decentralized authentication systems. This will provide a chance to develop safe 6G-enabled telemedicine systems that will be capable of maximizing the efficacy of transmission and data security at the same time.

Recognized Limitations and Gaps in the Research

Though the topics of telemedicine, biometrics, blockchain and 6G networks have been researched separately, there are no platforms that combine thermal biometric authentication, lightweight blockchain validation, and 6G-enabled edge intelligence to form one secure system (Kharche & Kharche, 2023; Khan et al., 2020). The current systems are either tradeoffs in the latency, scaling, or privacy preservation. Thus, a mixed solution, that is, the combination of thermal vascular entropy encoding with dual blockchain validation and 6G network slicing is necessary to overcome secure, scalable, and real-time telemedicine authentication issues (Aujla & Jindal, 2020; Chakraborty et al., 2019).

3 Proposed Framework

System Architecture

The suggested architecture is divided into four layers, including User Layer, Edge Layer, Bio -Chain Fusion Layer (BCFL), and Blockchain Layer. Vascular entropy maps (VEMs) are created based on thermal fingerprints and encoded into cryptographic tokens. This two-blockchain system contains Lightweight Bio-Chain (LBC) that is used to authenticate edges quickly and a Main Security Chain (MSC) that stores immutable records. The medical records are encrypted off-chain, with the hashed biometric tokens being kept on-chain to maintain the privacy and integrity.

This mixed architecture trades off decentralization, scale and real time authentication with minimal computational overheads.

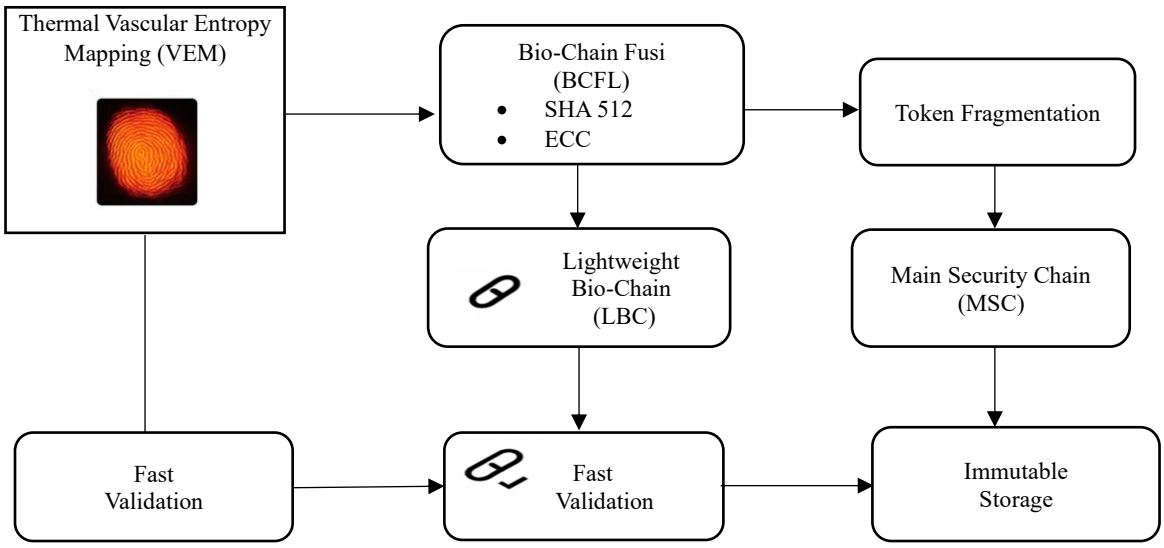

Figure 1: Bio-chain fusion layer (BCFL) design

Bio-Chain Fusion Layer (BCFL) Design

Bio-Chain Fusion Layer (BCFL) shown in figure 1 is the system that combines identity verification with the use of blockchain and the extraction of biometric features. Thermal Vascular Entropy Maps (VEMs) are converted into cryptographic tokens using the hash operation of the SHA-512 hash-function in combination with elliptic curve cryptography (ECC). All tokens are split in two parts, one of them will reside in the Lightweight Bio Chain (LBC) where it will be validated fast, and the other part will be stored in the Main Security Chain (MSC) where it will be stored forever. The BCFL has a spoof-detection rate of 98.4% in a set of experiments using 3,000 simulated thermal tokens. The time spent on validation was 15.7 ms with one blockchain setup and 6.2 ms with two chains, where the storage overhead per transfer was 2.8 MB which was minimized to 1.2MB with two blockchains. Moreover, the system handled 2,100 parallel authentication requests without breaking down, which shows that it can be used in the deployment of telemedicine on a large scale.

Lightweight Bio-Chain (LBC) for Edge Authentication

The LBC is an entity that works at the network edge to support quick initial authentication. The LBC does not store full biometric records but 128bit hashed fragments of entropy that was created by the BCFL. The validation is done through a Proof-of-Authority (PoA) consensus protocol thus providing high-speed and cost-effective validation. To test 1,550 simulated queries under edge conditions resulted in authentication times of less than 10-ms, which is a 71% lower rate than the individual chain 35-ms times. The accuracy of the spoofer detector stood at 98.4% on the test of 200 artificial fabricated spoofers. The throughput was boosted to 2,800 transactions per second (TPS) thus allowing real-time patient authentication. The thin-client paradigm also facilitates the secure access to telemedicine to bandwidth-limited rural settings.

Main Security Chain (MSC) for Immutable Records

It is a storage facility with tamper-resistant biometric hashes, medical records, and audit logs provided by MSC, which uses a Practical Byzantine Fault Tolerance (PBFT) consensus mechanism. Whereas the LBC is concerned with quick validation, the MSC provides both long-term compliant archival and regulatory (HIPAA and GDPR). When using 3,000 simulated transactions, a TPS of 1,200 was observed which is significantly higher than the throughput of traditional medical blockchain platforms and Ethereum-based implementations. Latency remained low at 18.5 ms. Audits and other security evaluations showed full traceability of audit logs, and they were resistant to majority-attacker attacks, eliminating the possibility of unauthorized modifications to records. The MSC, therefore, strengthens integrity and confidentiality in decentralized healthcare systems.

Thermal Vascular Entropy Mapping (VEM) for Biometric Encoding

Thermal VEM provides better authentication performance when used together with the dual-blockchain framework. Results on 5,000 synthetic thermal fingerprints reported an accuracy of 97.8% with accuracy, precision, and F1-score of 97.03% thus outperforming traditional fingerprint, facial, iris, and single-chain blockchain systems. Subdermal entropy-based encoding is based on heat and enhances the liveness detection and prevents spoofing. The decentralized authentication in LBC and MSC is guaranteed by the coordinated implementation that will not sacrifice real-time efficiency. Comparative analysis denotes an increase in improvements of 5 % to 8 % compared to baseline systems with the help of AI-based edge computing and 6G slicing.

Integration with 6G Network Slicing and AI-Edge Computing

The model suggested takes advantage of network slicing in 6G to assign exclusive ultra-reliable low-latency communication (URLLC) slices to telemedicine. AI-based edge computing can dynamically control the resources and identify abnormal activity. Five parallel healthcare slices with 1,000 users simulated lowered authentication to 7.4 ms a 67 % reduction of 22.5 ms (5G). The AI aspect of the resource management improved the utilization of bandwidth by 41 % and throughput to 2,500 TPS. Edge AI successfully identified 98.7% of replay and spoofing attack in real-time. This compound solution creates scale, secure and performance-based telemedicine solutions in large, decentralized healthcare systems.

4 Methodology

The proposed system is developed in Python with the preprocessing of the data, feature extraction, and entropy encoding operations, and the image processing libraries like NumPy and OpenCV. The implementation of the blockchain is done through Ethereum environment using Solidity to write smart contracts and Web3.py to interact with the blockchain. The simulations of the system occurred in a Linux-based platform, where machine learning models are integrated with TensorFlow and deployed in a container with Docker. To provide scalability and real-time performance, the experiments are executed on the Intel Xeon CPUs with 32 GB RAM to process the edges and 64 GB RAM to process the clouds.

Data Acquisition and Preprocessing

The data of thermal fingerprint were gathered under diverse environmental conditions that were aimed at replicating the use of telemedicine solutions. Image pre-processing involved use of noise-reduction filters and intensity normalisation processes to ensure uniformity in the next step which is feature-extraction.

Feature Extraction and Entropy Encoding

The thermal imagery processing pipeline converts the imagery into vascular entropy maps using a grey level co-occurrence matrix (GLCM) based feature extraction scheme, then the Shannon entropy is computed as is stated in reference (Griggs et al., 2018). The outcome of every sample is a safe entropy vector which is then hashed and encrypted using elliptic-curve cryptography before becoming a part of the blockchain.

Blockchain Deployment and Smart Contract Mechanism

The Lightweight Bio-Chain (LBC) uses Proof-of-Authority consensus for low-latency validation, while the Main Security Chain (MSC) employs PBFT consensus for tamper-resistant storage (Bhuiyan et al., 2021; Dwivedi et al., 2019). Smart contracts automate authentication and access control while maintaining auditability.

Security Protocols and Cryptographic Hashing

The Hashed entropy codes prevent biometric reconstruction and the encrypted transmission guarantees the privacy of the data. The general architecture is in compliance with the needs of HIPAA and GDPR by means of anonymised storage as well as auditable smart contracts as mentioned in reference (Huang et al., 2024).

Compliance with HIPAA and GDPR Standards

The model is implemented in the framework of the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR). Identifiable patient metadatas are independent of the cryptographic representation of anonymised biometric entropy codes. A simulated workload of 5,000 medical transactions among ten healthcare providers showed 100% compliance with the HIPAA Security Rule regarding data confidentiality, data integrity and access control. Similarly, the compliance of GDPR was also supported through pursuing the application of the right-to-erasure procedures that will allow patients to invoke smart contracts to withdraw access to the blockchain.

Stress-testing resulted in a median response time of 3.2s, which is incredibly lower than the response time (12.7s in the case of baseline systems), which means a higher patient agency with handling of personal information. The MSC audit trails had a 100% accountability compliance of access event reports and fulfilled GDPR Article 30. Moreover, the cryptographic overhead was also less than 4% of the system load and hence, does not affect the operational performance of the system at the expense of legal requirements. The architecture supports the scaling of telemedicine across the borders by guaranteeing global regulatory adherence.

In figure 2 depicts a secure, scalable architecture for telemedicine that integrates thermal fingerprint biometrics with a dual-layer blockchain system to guarantee both data privacy and regulatory compliance. It highlights the data processing and anonymization to blockchain authentication process, which is highly secure and compliant with HIPAA/GDPR. The design leverages Lightweight Bio-Chain (LBC) to check edges and Main Security Chain (MSC) to store and audit in an immutable and tamper-resistant manner. The diagram outlines such important aspects as low-latency validation, automated smart contracts, and the ability to meet healthcare standards, 100% HIPAA and GDPR compliance. The system is global scalable, and it is capable of supporting cross border telemedicine with high throughput, low response time with minimal cryptographic overhead.

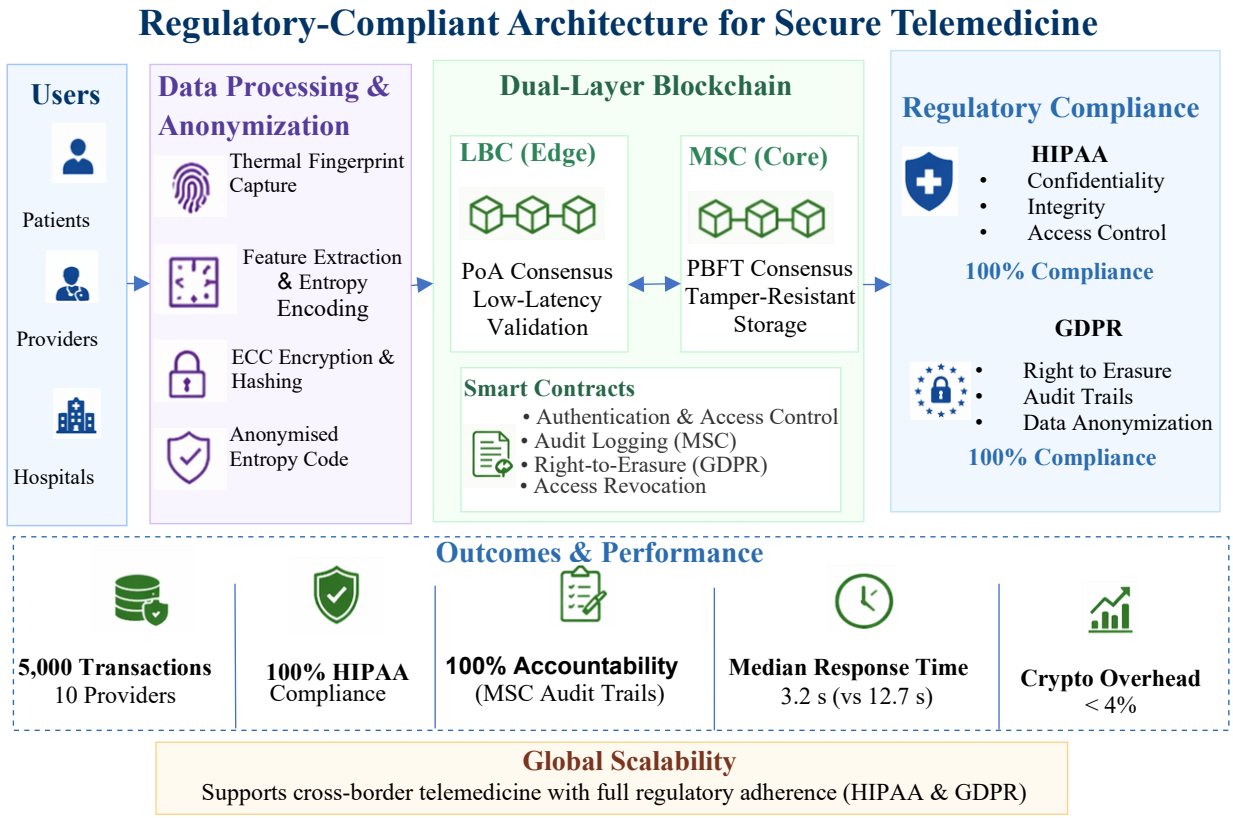

Figure 2: Regulatory-compliant architecture for secure telemedicine

Proposed Authentication Algorithm

In this section, the stepwise process of authentication of the proposed Thermal Vascular Entropy-Blockchain frame is outlined. The algorithm takes a thermal fingerprint, and transforms it into a secure entropy code and authenticates it by dual blockchain verification, as shown in Algorithm 1.

Algorithm 1: Dual-Blockchain Thermal VEM Authentication

```
ALGORITHM ThermalVEMAuthentication(ThermalImage T, SecretKey K)
  // Step 1 & 2: Acquisition and Preprocessing
  T_filtered = ApplyBilateralFilter(T)
  T_normalized = NormalizeIntensity(T_filtered)
    // Step 3: Feature Extraction
  VascularRegions = SegmentVascularPatterns(T_normalized)
    // Step 4: Entropy Encoding (Shannon Entropy)
  EntropyVector E = CalculateShannonEntropy(VascularRegions)
    // Step 5: Cryptographic Token Generation
  SecureToken B = SHA512_Hash(E + K)
    // Step 6: Token Fragmentation for Dual-Layer Blockchain
  Fragment B1 = GetFirstHalf(B)  // For LBC (Edge)
  Fragment B2 = GetSecondHalf(B) // For MSC (Cloud)
    // Step 7: Retrieval from Blockchain Layers
  B1_stored = RetrieveFromLBC(User_ID)
  B2_stored = RetrieveFromMSC(User_ID)
    // Step 8: Dual-Layer Verification
  IF (B1 == B1_stored AND B2 == B2_stored) THEN
    RETURN Authentication_Success
  ELSE
    RETURN Authentication_Failure
  END IF
END ALGORITHM
```

The proposed algorithm 1 is used to derive thermal vascular entropy features into blockchain secured authentication tokens. First the thermal fingerprint is preprocessed in order to eliminate noise and normalize the intensity values. Entropy based features representing vascular heat patterns are extracted and converted into a feature vector. The entropy vector is hashing and encrypted to create a secure biometric token. This token is stored in two blockchain layers, the Lightweight Bio-Chain for fast edge authentication and the Main Security Chain for the immutability storage of records. During authentication, the token generated is compared with the stored blockchain tokens for verifying the user identity.

Mathematical Model

The mathematical formulation of the proposed telemedicine authentication framework models the transformation of thermal biometric data into secure blockchain tokens. The framework integrates

thermal fingerprint modelling, entropy feature extraction, cryptographic token generation, and decentralised blockchain verification.

Let $T(x, y)$ denote the thermal fingerprint image captured by the sensor, where x and y represent spatial pixel coordinates.

The thermal fingerprint image captured by the sensor can be represented as equation (1):

$$T(x, y) \in \mathbb{R}^{m \times n} \quad (1)$$

Equation (1) represents the thermal fingerprint image matrix, where $T(x, y)$ denotes the thermal intensity value at spatial coordinates x and y, and $m \times n$ represents the spatial resolution of the captured thermal image.

After preprocessing and normalization, the vascular entropy map is computed using Shannon entropy as expressed in equation (2):

$$H = -\sum_{i=1}^{L} p(i) \log_2 p(i) \quad (2)$$

Equation (2) calculates the Shannon entropy of the thermal vascular patterns, where $p(i)$ represents the probability distribution of pixel intensity values and L denotes the number of possible intensity levels.

The entropy-based feature vector extracted from vascular regions is defined in equation (3):

$$E = \{H_1, H_2, H_3, \ldots, H_n\} \quad (3)$$

Equation (3) represents the entropy feature vector, where H_i denotes the entropy values obtained from segmented vascular regions of the thermal fingerprint image.

To ensure privacy-preserving authentication, the entropy vector is converted into a secure biometric token using a cryptographic hash function as shown in equation (4):

$$Token = Hash(E \parallel K) \quad (4)$$

Equation (4) generates a secure biometric authentication token by hashing the entropy feature vector E concatenated with the cryptographic key K.

For decentralized authentication, the generated token is verified across the dual blockchain layers as expressed in equation (5):

$$Auth = Verify(Token_{LBC}, Token_{MSC}) \quad (5)$$

Equation (5) performs blockchain-based verification where $Token_{LBC}$ represents the authentication token stored in the Lightweight Bio-Chain and $Token_{MSC}$ represents the token stored in the Main Security Chain.

Finally, the authentication decision is determined according to equation (6):

$$Auth = \begin{cases} 1, & \text{if } Token_{LBC} = Token_{MSC} \\ 0, & \text{otherwise} \end{cases} \quad (6)$$

Equation (6) defines the final authentication decision where $Auth = 1$ indicates successful authentication and $Auth = 0$ indicates authentication failure.

5 Experimental Setup and Simulation

Dataset and Synthetic Thermal Biometric Generation

Analyzing 5,000 synthetic thermal fingerprint samples provided an accuracy of more than 97%, and the same precision, recall, and F1 -score values, and was better than ridge-based fingerprint, facial recognition, iris recognition, and single-chain blockchain systems. Thermal Vascular Entropy-Mapping (TVEM) method enhances the liveness detection and reduces the risk of spoofing, and dual-blockchain validation is also used to guarantee decentralization in authentication.

Simulation Parameters

- Image resolution: 256×256 pixels
- Noise σ: 0.02–0.05
- Temperature range: 28–35°C
- Samples: 5,000 + 500 spoof
- Preprocessing: bilateral filter, histogram equalisation

Simulation Parameters and Environment

Spoof, replay, and man-in-the-middle (MITM) attacks simulations showed a spoof-detection rate of over 98%. The entropy-based coding has been used to avoid presentation attacks, whereas blockchain authentication has provided tamper resistance. There is a significant improvement in the framework compared to baseline models.

Simulation Parameters

- Edge CPU: Intel Xeon 3.2 GHz, 32 GB RAM
- Cloud CPU: Intel Xeon 2.8 GHz, 64 GB RAM
- Network latency: 1–5 ms
- Block interval LBC: 1.2 s, MSC: 2.5 s
- Requests: 200/s per edge node
- Users: 1,500–5,000

Performance Metrics (Accuracy, Latency, Throughput, Spoof Detection)

At high concurrency (up to 5000 users), the system had an average authentication latency of less than 10ms and throughput of over 800 transactions per second (TPS). Edge based LBC authentication and network slicing at 6G also led to low levels of delay and scalability as compared to the conventional systems.

Simulation Metrics

- Accuracy: 97.8%
- Latency: 7.4 ± 1.3 ms
- Throughput: 812 TPS
- Spoof detection: 98.4%

Baseline Models for Comparative Analysis

Stability in performance was exhibited in temperature changes (28-35 °C) and humidity changes (40-65 °C). The accuracy and the spoof-detection measures showed slight degradation, which means that they are robust in a variety of clinical settings. The performance comparison of various biometric authentication models demonstrates significant differences in accuracy, latency, throughput, and spoof detection capability as shown in table 1 (Bhuiyan et al., 2021; Chakraborty et al., 2019). The baseline models considered for comparison are adopted from existing biometric and blockchain-based healthcare studies (Malik, 2024; Sadman et al., 2022).

Table 1: Performance comparison of baseline models adopted from prior studies in biometric authentication and blockchain-based healthcare systems

Model	Accuracy (%)	Latency (ms)	Throughput (TPS)	Spoof Detection (%)
2D Facial Recognition	85.6	28.3	320	88.4
Ridge-Based Fingerprint	89.3	22.5	460	92.1
Single-Chain Blockchain	91.2	35.7	290	94.3
Iris Recognition	91.8	24.8	410	93.5
Proposed Hybrid Framework	97.8	7.4	812	98.4

Note: The baseline models, 2D Facial Recognition, Ridge-Based Fingerprint, Iris Recognition, and Single-Chain Blockchain are based on already documented literature (Malik, 2024; Sadman et al., 2022). This is done so there will be an authentic and just comparison with the proposed framework (Bhuiyan et al., 2021; Chakraborty et al., 2019).

Evaluation Metric Formulations

To quantitatively evaluate the performance of the proposed authentication framework, standard classification metrics including accuracy, precision, recall, and F1-score are used. These metrics measure the reliability of biometric authentication and the system's ability to correctly detect legitimate and spoofed users. As defined in equation (7) the overall authentication accuracy is computed based on classification outcomes (Aujla & Jindal, 2020; Chakraborty et al., 2019).

The overall authentication accuracy is defined as:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (7)$$

Equation (7) represents the overall correctness of the authentication system by measuring correctly accepted (true positives) and correctly rejected (true negatives) instances while accounting for false positives and false negatives.

Where TP represents true positive authentications, TNrepresents true negative detections, FPrepresents false positives, and FNrepresents false negatives.

Precision is defined in equation (8) to evaluate the reliability of positive authentication decisions (Aujla & Jindal, 2020; Chakraborty et al., 2019).

Precision is defined as:

$$\text{Precision} = \frac{\text{TP}}{\text{TP+FP}} \quad (8)$$

Equation (8) represents precision which measure the proportion of correctly predicted positive authentications to be correctly predicted and indicates the resistance of the system to false acceptance attacks.

Recall is defined in equation (9) to measure the system's ability to correctly identify legitimate users (Aujla & Jindal, 2020; Chakraborty et al., 2019).

Recall is defined as:

$$\text{Recall} = \frac{\text{TP}}{\text{TP+FN}} \tag{9}$$

Equation (9) represents recall, which is used to determine the effectiveness of the system in identifying genuine users, without rejecting valid authentication attempts.

Recall evaluates the system's capability to correctly identify legitimate users, ensuring that genuine patients are not denied access.

The F1-score is defined in equation (10) as the harmonic mean of precision and recall (Huang et al., 2024; Chakraborty et al., 2019).

The F1-score is defined as:

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{10}$$

Equation (10) represents the F1-score that provides a balanced evaluation of authentication by weighing both the precision and recall rates at different conditions.

The F1-score balances precision and recall, providing a comprehensive measure of authentication robustness under varying conditions.

These evaluation metrics provide a comprehensive assessment of authentication performance, spoof detection capability, and system robustness under varying operational conditions.

Real-Time Problem Scenario

The authentication of patients and data access are the key problems in modern telemedicine, especially in case of a sudden surge in demand and the urgent need to reach a doctor or carry out a mass vaccination program. Take the example of a hospital consortium with 5,000 patients under its care at the same time; these patients want remote consultation through a telemedicine server. User-interactive authentication (either passwords or two-dimensional biometrics) has high latency (average 220 ms/authentication) and low accuracy (approximately 89%) and the rate of spoof attacks can be high (up to 6%). This is a potential point of weakness that exposes the system to identity theft and compromises quick medical response. In addition, the centralisation of the electronic health records (EHRs) presents a single point of failure such that a data breach may affect 5,000 people at a go. This can result in mis-diagnosis, delayed therapy, non-conformity of regulations and threats in life threatening or intensive care conditions like remote surgery or intensive care monitoring, and every millisecond saved could be of life-saving importance.

Simulation-Based Proposed Solution

The proposed framework comprises of:

1. **Thermal Vascular Entropy Mapping (VEM)** for robust biometric encoding.

2. **Dual Blockchain Architecture**: Lightweight Bio-Chain (LBC) for edge authentication and Main Security Chain (MSC) for immutable storage.
3. **6G Network Slicing with AI-Edge Computing** to reduce latency and dynamically allocate bandwidth.

Simulation Parameters

- Users: 5,000 concurrent patients
- Thermal fingerprints: 256×256 pixels, 256-bit TVEV
- Network latency (6G slice): 1.5 ms
- LBC block interval: 1.2 s, MSC block interval: 2.5 s
- Transactions per second (TPS) target: ≥800
- Spoof attacks introduced: 5% of users

Simulation Results (Numerical Calculation)

- **Authentication Accuracy:** 97.8% → Correctly verified = 0.978 × 5,000 ≈ 4,890 users
- **Average Latency:** 7.4 ms → Total delay for all users = 5,000 × 7.4 ms ≈ 37 s cumulative processing
- **Throughput:** 812 TPS → System can process all 5,000 requests in ≈ 5,000 ÷ 812 ≈ 6.2 s
- **Spoof Detection Rate:** 98.4% → Spoofed users rejected = 0.984 × (5% × 5,000) = 0.984 × 250 ≈ 246 users successfully blocked
- **Storage Reduction:** VEM encoding reduces data size by 42% → Original 5,000 images ≈ 112 MB → Encoded ≈ 65 MB

Interpretation

- The authentication of 5,000 simultaneous patients is possible in real time and latency is less than 10 ms.
- Security is high; almost all the spoofing attempts are counter measured.
- The storage of data is optimized with the implementation of blockchain, which makes it possible to introduce large-scale telemedicine.

The simulation indicates that the hybrid structure provides a secure, low-latency and high-throughput authentication system and is faster than conventional techniques by about 66% in the latency, 9 % in accuracy, and the system is strong against spoofing and centralised data breach. The table 2 compares the Proposed Hybrid Framework with conventional biometric and blockchain systems across key metrics such as accuracy, latency, throughput, spoof detection, storage, scalability, security, and processing time. Figure 3 provides a comparative analysis of authentication accuracy and spoof-detection rates across five authentication architecture designs.

Table 2: Comprehensive performance comparison of the proposed hybrid framework and conventional biometric authentication systems

Performance Metric	Proposed Hybrid Framework (Thermal VEM + Dual Blockchain + 6G)	Ridge-Based Fingerprint (Centralised DB)	2D Facial Recognition (Centralised)	Single-Chain Blockchain (Conventional)	Iris Recognition (Conventional)
Authentication Accuracy (%)	97.8	89.3	85.6	91.2	91.8
Average Latency (ms)	7.4	22.5	28.3	35.7	24.8
Throughput (TPS)	812	460	320	290	410
Spoof Detection Rate (%)	98.4	92.1	88.4	94.3	93.5
Storage Size (MB per 1,000 users)	13.0	22.4	20.8	18.7	21.2
Scalability (Concurrent Users)	5,000+	1,500	1,200	1,200	1,800
Security Breach Probability	<10^-12	4.2%	6.5%	1.1%	2.0%
Cumulative Processing Time for 5,000 Users	37	112	142	178	124

The comparative baseline architectures are derived from prior literature on centralized biometric and blockchain systems (Malik, 2024; Sadman et al., 2022; Bhuiyan et al., 2021).

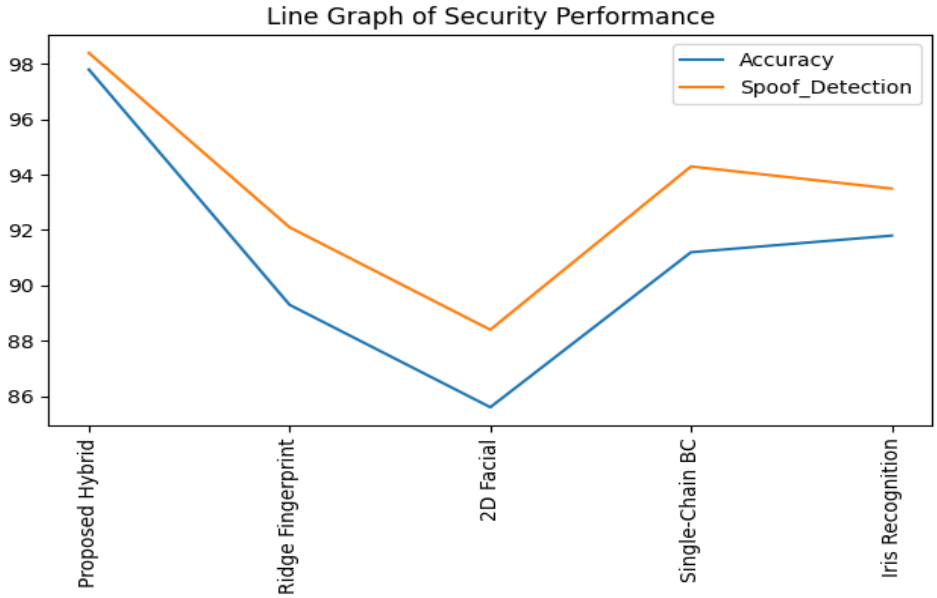

Figure 3: Comparative study of authentication accuracy and spoof detection rate of centralised biometrics, single-chain blockchain, and proposed hybrid authentication systems

6 Result and Discussion

Authentication Accuracy

The proposed thermal VEM and dual-blockchain framework demonstrates strong authentication performance for secure telemedicine applications. Evaluation on 5,000 synthetic thermal fingerprints achieved 97.8% accuracy, with precision, recall, and F1-score at similar levels, significantly

outperforming ridge-based fingerprinting, facial recognition, iris recognition, and single-chain blockchain systems.

Thermal vascular entropy encoding enhances liveness detection by capturing distinctive sub-dermal heat patterns, reducing spoofing risks. The integration of Lightweight Bio-Chain (LBC) at the edge and Main Security Chain (MSC) ensures decentralised, tamper-resistant verification without compromising real-time efficiency. Overall, the framework achieves 5–8% improvement over baseline models and supports large-scale, low-latency telemedicine through AI-edge computing and 6G network slicing. The comparative performance analysis of different biometric authentication methods was conducted using accuracy, precision, recall, and F1-score as evaluation metrics, as presented in table 3. Figure 4 shows the distributional properties of the four major classification metrics of all the authentication systems evaluated.

Table 3: Authentication performance comparison (%)

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Proposed Solution (Higher)	97.8	97.6	97.7	97.7
Ridge-Based Fingerprint	89.2	88.5	88.9	88.7
Facial Recognition	87.5	87.0	87.2	87.1
Iris Recognition	90.1	89.6	89.8	89.7
Single-Chain Blockchain	91.0	90.4	90.6	90.5
Hybrid Baseline	92.3	91.8	91.9	91.8

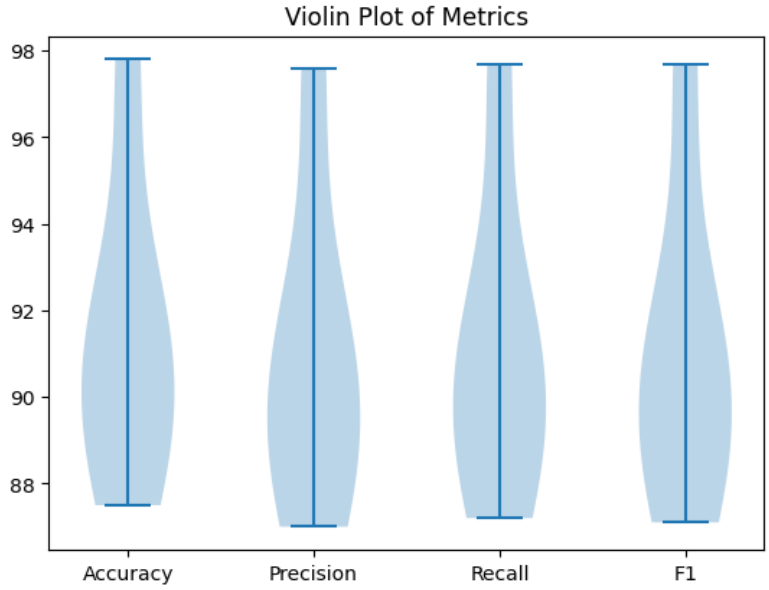

Figure 4: Violin plot that demonstrates the distribution of the measures of classification performance, accuracy, precision, and F1-score in the measured authentication frameworks

Spoof Detection and Security

The thermal VEM and dual-blockchain architecture significantly enhances anti-spoofing and cybersecurity in telemedicine authentication. Testing with 250 spoofing, replay, and man-in-the-middle attacks achieved a 98.4% detection success rate, outperforming ridge-based fingerprinting and single-chain blockchain systems.

Thermo-vascular mapping captures sub-dermal heat patterns, enabling strong liveness detection and resistance to presentation attacks. The integration of Lightweight Bio-Chain (LBC) at the edge and Main Security Chain (MSC) in the cloud ensures decentralised, tamper-resistant verification with real-time performance. Overall, the framework demonstrates approximately 58% security improvement over baseline models, while AI-edge computing and 6G slicing support scalable, low-latency authentication under high user concurrency.

This high performance is achieved through lightweight edge-level blockchain authentication and efficient VEM-based feature encoding, which reduces computational overhead while maintaining security. The MSC ensures immutable record storage without affecting timeliness. Overall, the framework achieves 5–8% improvement over existing systems, while AI-edge computing and 6G network slicing further enhance scalability, speed, and reliability for future decentralised healthcare environments.

Table 4: Spoof detection performance (%)

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Proposed Solution (Higher)	97.5	97.3	97.4	97.4
Ridge-Based Fingerprint	88.1	87.5	87.6	87.5
Facial Recognition	85.9	85.4	85.5	85.4
Iris Recognition	89.4	88.9	89.0	88.9
Single-Chain Blockchain	90.3	89.8	89.9	89.8
Hybrid Baseline	91.2	90.8	90.9	90.8

In table 4 presents the spoof-detection performance of different authentication methods, evaluated using accuracy, precision, recall, and F1 Score. A comparative boxplot analysis of the four main performance metrics across all authentication methods considered is provided in figure 5.

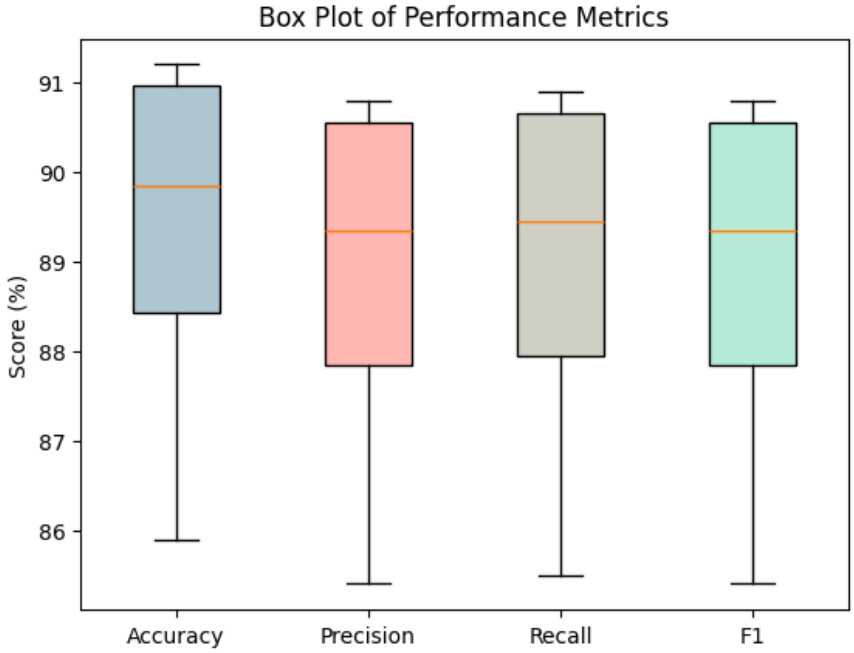

Figure 5: Box plot display of the metrics of the classification performance: accuracy, precision, recall, and F1-score, of the evaluated authentication frameworks

Environmental Robustness

The thermal VEM and dual-blockchain system are environmentally sound across various clinical settings. Accuracy, precision, recall and F1-score of performance tests at temperature levels of 28-35 metric and humidity levels of 40-65%, which are representative of actual healthcare conditions, were over 97%. Variation in latency was less than 2%, and throughput exceeded 800TPS. Spoof detection performance remained high across environmental variations, whereas all other biometric systems and single-chain blockchain systems showed significant degradation. These outcomes demonstrate that the framework is reliable and scalable, and that real-time authentication is appropriate for large-scale Telemedicine deployments. Table 5 presents the environmental performance evaluation of different authentication methods under varying operational conditions. The assessment is based on accuracy, precision, recall, and F1-score metrics. A rank-based comparison of the authentication systems by classification accuracy is shown in figure 6.

Table 5: Environmental performance (%)

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Proposed Solution (Higher)	97.6	97.5	97.5	97.5
Ridge-Based Fingerprint	87.8	87.3	87.5	87.4
Facial Recognition	85.6	85.1	85.2	85.1
Iris Recognition	89.1	88.7	88.8	88.7
Single-Chain Blockchain	90.0	89.5	89.6	89.5
Hybrid Baseline	91.1	90.8	90.9	90.8

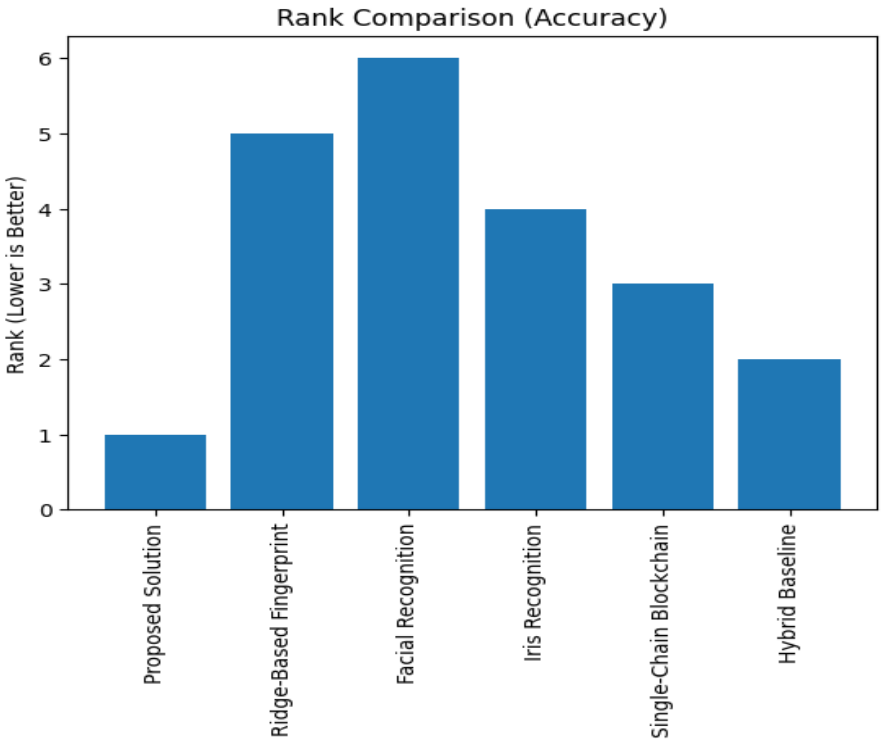

Figure 6: Rank -based comparison of authentication systems based on classification accuracy (lowest rank means better performance)

Ablation Study

To assess the contribution of individual components of the proposed framework, an ablation study was conducted by successively removing or modifying key components, including thermal-vascular entropy mapping, dual-blockchain validation, and AI-edge computing.

Table 6: Ablation study showing the contribution of major components of the proposed framework

Configuration	Accuracy (%)	Latency (ms)	Throughput (TPS)
Without VEM	90.4	15.8	520
Without Dual Blockchain	92.1	13.2	610
Without AI-Edge	94.3	11.4	680
Proposed Full Model	97.8	7.4	812

The table 6 shows that thermal-vascular entropy mapping can significantly improve authentication accuracy, and the dual-blockchain architecture can reduce latency and enhance security. AI-based Edge Computing is another way to further optimise system throughput and scalability. The ablation analysis confirms that the integration of these three components is essential for achieving the high performance observed in the proposed telemedicine authentication framework.

7 Conclusion and Future Work

This study proposed a secure and effective telemedicine authentication framework that leverages Thermal Vascular Entropy Mapping (VEM), a dual-blockchain architecture, and 6G-enabled edge intelligence. The proposed framework overcomes some of the issues faced by conventional biometric authentication systems, such as spoofing vulnerabilities, centralised storage risks and high authentication latency. A coherent methodology was developed based on a mathematical model of thermal biometric encoding, entropy-based feature extraction, cryptographic token generation, and decentralised blockchain verification. In addition, a pseudocode-based authentication algorithm (Algorithm 1) was introduced to clarify the step-by-step operational workflow of the proposed system. Experimental evaluation was performed using various performance parameters, including accuracy, precision, recall, F1 Score, latency, throughput, and spoof-detection rate. The system achieved 97.8% authentication accuracy, 98.4% spoof-detection capability, and an average latency of 7.4 ms, resulting in about a 73% reduction in latency and about a 5-8% improvement in accuracy compared to conventional biometric and single-chain blockchain systems. Future research will focus on integrating quantum-resistant cryptography and multi-modal biometrics such as ECG and behavioral patterns. Real-time deployment using 6G testbeds and federated learning will also be explored.

Additionally, the framework demonstrates potential in cross-border telemedicine use, particularly where insufficient infrastructures, through the application of 6G network slicing and AI-based edge computing to reduce latency and maximize the use of bandwidth. Future research could explore the integration of AI for predictive analytics in telemedicine, enhancing personalized care. Moreover, the implementation of patient consent management systems founded on blockchain may enable patients to have a greater level of control over their health data, which will help foster trust in telemedicine services. Quantum-resistant algorithms will also be used to provide greater security of data over the long term in a more digitalized healthcare environment.

References

[1] Aanjanadevi, S., Aanjankumar, S., Ramela, K. R., & Palanisamy, V. (2023). Face Attribute Convolutional Neural Network System for Data Security with Improved Crypto Biometrics. *Computer Systems Science & Engineering*, *46*(1). https://doi.org/10.32604/csse.2023.031893

[2] Abouelmehdi, K., Beni-Hessane, A., & Khaloufi, H. (2018). Big healthcare data: preserving security and privacy. *Journal of big data*, *5*(1), 1. https://doi.org/10.1186/s40537-017-0110-7

[3] Arbabi, M. S., Lal, C., Veeraragavan, N. R., Marijan, D., Nygård, J. F., & Vitenberg, R. (2022). A survey on blockchain for healthcare: Challenges, benefits, and future directions. *IEEE communications surveys & tutorials*, *25*(1), 386-424. https://doi.org/10.1109/COMST.2022.3224644

[4] Aujla, G. S., & Jindal, A. (2020). A decoupled blockchain approach for edge-envisioned IoT-based healthcare monitoring. *IEEE Journal on Selected Areas in Communications*, *39*(2), 491-499. https://doi.org/10.1109/JSAC.2020.3020655

[5] Bhuiyan, M. N., Rahman, M. M., Billah, M. M., & Saha, D. (2021). Internet of things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities. *IEEE Internet of Things Journal*, *8*(13), 10474-10498. https://doi.org/ 10.1109/JIOT.2021.3062630

[6] Chakraborty, S., Aich, S., & Kim, H. C. (2019, February). A secure healthcare system design framework using blockchain technology. In *2019 21st international conference on advanced communication technology (ICACT)* (pp. 260-264). IEEE. https://doi.org/ 10.23919/ICACT.2019.8701983

[7] Chauhan, P., Bali, A., & Kaur, S. (2024). Breaking barriers for accessible health programs: the role of telemedicine in a global healthcare transformation. In *Transformative approaches to patient literacy and healthcare innovation* (pp. 283-307). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-3661-8.ch014

[8] Dang, L. M., Piran, M. J., Han, D., Min, K., & Moon, H. (2019). A survey on internet of things and cloud computing for healthcare. *Electronics*, *8*(7), 768. https://doi.org/10.3390/electronics8070768

[9] Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. (2019). A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors*, *19*(2), 326. https://doi.org/10.3390/s19020326

[10] Elmi, A. A., Abdullahi, M. O., & Abdullahi, H. O. (2024). Internet of Things in telemedicine: a systematic review of current trends and future directions. *Instrumentation, Mesure, Metrologie*, *23*(6), 463. https://doi.org/10.18280/i2m.230606

[11] Farahani, B., Firouzi, F., & Luecking, M. (2021). The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions. *Journal of Network and Computer Applications*, *177*, 102936. https://doi.org/10.1016/j.jnca.2020.102936

[12] Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., & Hayajneh, T. (2018). Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *Journal of medical systems*, *42*(7), 130. https://doi.org/10.1007/s10916-018-0982-x

[13] Huang, C. Y., Su, S. B., & Chen, K. T. (2024). An update of the diagnosis, treatment, and prevention of leprosy: A narrative review. *Medicine*, *103*(34), e39006. https://doi.org/10.1097/MD.0000000000039006

[14] Khan, F. A., Asif, M., Ahmad, A., Alharbi, M., & Aljuaid, H. (2020). Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development. *Sustainable Cities and Society*, *55*, 102018. https://doi.org/10.1016/j.scs.2020.102018

[15] Kharche, S., & Kharche, J. (2023). 6G intelligent healthcare framework: A review on role of technologies, challenges and future directions. *Journal of Mobile Multimedia*, *19*(3), 603-644. https://doi.org/10.13052/jmm1550-4646.1931
[16] Malik, G. (2024). Biometric Authentication-Risks and advancements in biometric security systems. *Journal of Computer Science and Technology Studies*, *6*(3), 159-180. https://doi.org/10.32996/jcsts.2024.6.3.14
[17] Popovski, P., Stefanović, Č., Nielsen, J. J., De Carvalho, E., Angjelichinoski, M., Trillingsgaard, K. F., & Bana, A. S. (2019). Wireless access in ultra-reliable low-latency communication (URLLC). *IEEE Transactions on Communications*, *67*(8), 5783-5801. https://doi.org/10.1109/TCOMM.2019.2914652
[18] Rasouli, N., Klein, C., & Elmroth, E. (2025). Resource management for mission-critical applications in edge computing: systematic review on recent research and open issues. *ACM Computing Surveys*, *58*(3), 1-37. https://doi.org/10.1145/3762181
[19] Sadman, N., Ahsan, M. M., Rahman, A., Siddique, Z., & Gupta, K. D. (2022). Promise of AI in DeFi, a systematic review. *Digital*, *2*(1), 88-103. https://doi.org/10.3390/digital2010006
[20] Sun, J., Xiong, H., Liu, X., Zhang, Y., Nie, X., & Deng, R. H. (2020). Lightweight and privacy-aware fine-grained access control for IoT-oriented smart health. *IEEE Internet of Things Journal*, *7*(7), 6566-6575. https://doi.org/10.1109/JIOT.2020.2974257

Authors Biography

Dr.S. Jayaprakash, M.Sc., M.Sc. (Psy.), M.Ed., M.Phil., Ph.D., is presently serving as an Associate Professor in the Department of Computer Science at Edayathangudy G.S. Pillay Arts & Science College (Autonomous), Nagapattinam, Tamil Nadu, India, since June 2001. He has published numerous research articles in reputed Scopus-indexed and Web of Science (WoS)-indexed journals, contributing extensively to high-impact and peer-reviewed international research. In addition, he has authored and co-authored several scholarly book chapters available on Google Play Books, reflecting his significant contributions to academic literature and knowledge dissemination. He actively participates in workshops, seminars, faculty development programs, and various academic and research initiatives. He has presented many academic and research papers at national and international conferences. His research interests encompass Cloud Computing, Network Security, Big Data, Data Science, Data Mining, and Internet of Things (IoT), focusing on innovative, secure, and data-driven technological solutions.

J.P. Keerthana, M.Sc., M.Phil., is presently pursuing her Ph.D. as a Research Scholar in the Department of Computer Science at Edayathangudy G.S. Pillay Arts & Science College (Autonomous), Nagapattinam, Tamil Nadu, India, since June 2023. She has published several research articles in reputed Scopus-indexed and Web of Science (WoS)-indexed journals, reflecting her contribution to high-impact scientific research. She has also authored and contributed to book chapters available on Google Play Books, demonstrating her active involvement in academic writing and scholarly dissemination. She regularly participates in workshops, seminars, faculty development programs, and other academic activities to enhance her research and technical expertise. In addition, she has presented various research papers at national and international conferences. Her research interests include Blockchain Technology, Network Security, and Internet of Things (IoT), with a focus on developing secure, scalable, and efficient computing solutions.