MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages: 2713-2718

Secure Data Transmission Tool using SSL, TLS and SSH

T.P.S. Kumar Kusumanchi, Department of IoT, Koneru lakshmaiah education foundation,satishkumar8421@gmail.com
Banala Krishnam Naidu, Department of IoT, Koneru lakshmaiah education foundation,krishnamnaidu4132@gmail.com
Anakapalli Santosh Kumar, Department of IoT, Koneru lakshmaiah education foundation, 2200100071@kluniversity.in
Pittu Yaswanth Kumar Reddy, Department of IoT, Koneru lakshmaiah education foundation,2200100011@kluniversity.in
J. Bennilo Fernande ,Department of ECE, Kalasalingam Academy of Research and Education, Krishnankoil, Tamil Nadu, India, bennij05@gmail.com

Abstract: *The growing digitization of healthcare systems and the large-scale adoption of the Internet of Medical Things (IoMT) have enabled continuous patient monitoring and real-time clinical decision support. On the other hand, the large transmission of sensitive Patient Health Information (PHI) across distributed and multi-source networks introduces significant security risks related to data confidentiality, integrity, and authenticity. Existing security approaches are often failed to address the scalability and complexity requirements of modern IoMT infrastructures, leaving healthcare systems exposed to advanced cyber threats such as man-in-the-middle (MITM) attacks, unauthorized access, and data tampering. This work describes a robust and efficient framework of data transfer using the IoMT in healthcare applications. The study merges Secure Sockets Layer,Transport Layer Security (SSL,TLS) and Secure Shell (SSH) protocols in a layer framework based on a Secure Shell layer. It used the NGINX reverse proxy architecture implemented using Docker containers to allow separation of the cryptographic computations from the application logic. This ensures mutual trust using the optional mutual TLS authentication with versions 1.2 and 1.3 of TLS. Secure communication is tested using REST and WebSocket services. Results demonstrate that the proposed approach ensures robust, scalable, and deployable protection for data-in-transit in modern healthcare infrastructures*

Keywords: Secure data transmission, SSL,TLS, SSH, mutual TLS, healthcare security, Internet of Things (IoT), Patient Health Information (PHI), MITM attack mitigation, cryptographic architecture, Docker containerization, PHI protection.

I. Introduction

The Internet of Medical Things has brought a significant revolution to the healthcare industry by providing real-time monitoring, diagnostics, and medical decisions based on data. The large amount of transfer of PHIs in heterogeneous as well as trustworthy networks has raised a grave challenge to the security concerns as the issue of confidentiality, integrity, and authenticity has now demanded utmost attention as a challenge to the healthcare system surrounded by the IoMT.[1][2][3]

To improve efficiency in the IoMT security solutions, there have been numerous approaches used by research studies. These approaches range from the application of the feasibility of lightweight algorithms, the application of chaotic synchronization processes for encrypting information, and several others. Although the approaches have the capability of making the processing aspect efficient and less burdening within the healthcare systems, these approaches have not been standardized, especially when taking into consideration the aspect of ensuring that there are facets of security. This is because the feasibility of the health care system has been a limitation. Some researchers have also taken into consideration trust models based on security. These researches involve the use of trust verification methods on each node in the IoMT network. The major aim of these models is the analysis of trust of the node behaviour before interaction. Though it is true that evaluation of trust on the node level could help in the mitigation of insider attacks as well as the malignant activities of devices, the fact is it has not been effective in the man-in-the-middle attack or eavesdropping.Hybrid systems, which make use of both encryption and certificate techniques, have also been contemplated. These systems promise greater security, which is guaranteed by the use of Public Key Infrastructure (PKI) methods for identity validation [13][14]. The problem associated with these systems is the tight integration of processing, management, and control of certificates in the applications. Similarly, in a healthcare app, where high levels of availability and maintainability are required, there can also be complexities in app programming, scalability, and erroneous configurations in the deployment environment.

One of the major weaknesses in the related research is that it can be theoretical or unproduction-ready. Most designs were found to be feasible in terms of security on simulations and conceptual designs but unaddressed in healthcare implementable aspects. The current infrastructure in healthcare technology needs scalability and cloud-native designs for architectures that provide security. The unaddressed aspect in identity segmentation on transport layer and application interaction is a total architectural weakness.

With respect to such challenges, this study presents an efficient multi-layer security framework that was developed for a practical IoMT healthcare scenario. The approach distinguishes between securing a transport layer and application logics using a combination of industrial SSL/TLS/SSH security at a network boundary [19]. The proposed work utilizes a NGINX reverse proxy as a security boundary that decrypts a secured connection as per security policies.[20]

The use of techniques offered by Docker in containerization is used in separating and deploying the application. The use of distinct security and application modules in the container enables a separation of security modules from application modules in a way that secures the entire system by minimizing its attack surface. This practice allows scaling of all components independently.

Firstly, in this research study, the primary aim is to design an open architecture for the safe transfer of sensitive patient health information. With the application of open standards and collage architecture in practice, it has managed to provide safe patient health information in an efficient manner. It has proven to be good at forming a basis for constructing a safe Internet of Medical Things-based Internet of Things system.

Docker-based methodology of containerization has been utilized to promote decoupling of architecture. By decoupling the security tiers and application tiers based on containers, this framework makes sure that the total attack surface area has been minimized, along with the ability to scale security tiers as well as business logic tiers independently.

The purpose of the project at hand is to develop a scalable and efficient infrastructure for secure communication of PHI. By using standardized communication protocols, the proposed solution protects the PHI in a secure manner without adding complexity to the application at hand. The project works as a building block in developing secure and compliant IoMT solutions in the healthcare sector.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages: 2713-2718

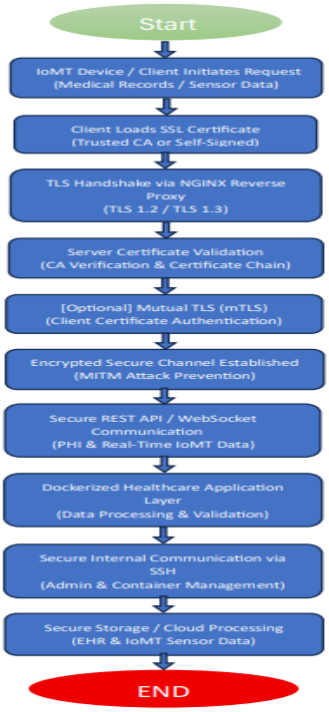


Fig 1: Workflow of data

II. Literature Survey

Data transmission security has been an area of intense research given the rising cases of cyber-attacks against Internet-based communication systems, especially in the Internet of Things (IoT) and healthcare applications. Early works involved research on the mitigation of Man-in-the-Middle (MITM) attacks against the SSL/TLS communication protocol. Alwazzeh et al. offered a detailed survey on the MITM attack in SSL/TLS protocols, along with recommendations on how these attacks can be eliminated through SSL/TLS hardening as well as certificate validation [1]. Later, Li et al. put forward a node-based secure data transmission algorithm for IoT networks, which involves trust assessment for nodes to counteract malicious activity [2]. Hui et al. proposed a secure data transmission strategy for industrial IoT networks through the integration of encryption techniques and authentication, which enhances reliability in hostile networks [3].

Further analysis was conducted to cope with the detection and prevention of TLS-based MITM attack scenarios, even in the absence of trust entities. The works of Dacosta et al. showcased the capabilities of techniques to successfully detect MITM attack scenarios based on anomalous communication activities [4]. Karapanos and Capkun introduced effective ways to counter TLS-based MITM attack scenarios in web-based systems using Authenticated Key Exchange [5]. The significance of SSL/TLS as an effective tool in secure communication was discussed by Kumar, depicting the success of SSL/TLS in protecting in-transit data when used appropriately [6]. The success of an improved TLS method using the concept of pre-binding and validation of certificates was proposed by Yang to minimize the risks of forged certificates [7]. The need for user-friendly mutual authentication mechanisms was explored by Latze and Mueller, emphasizing the impact of certificate-based authentication to minimize unauthorized access risks [8]. A comprehensive review of the SSL, TLS, and DTLS protocols was provided by Perez, emphasizing the significance of the concept of record layer encapsulation and Authenticated Encryption [9].

Healthcare data security research has stressed the protection of electronic health records and sensitive patient data. Attribute-based encryption techniques have been investigated to offer fine-grained access control in cloud-based healthcare systems [10]. Kumar extended to show that SSL/TLS protocols remain the de facto industrial standard for securing healthcare communication, in particular, for protecting Patient Health Information during transmission [11]. Jung et al. analyzed security requirements and platform architectures of IoT devices, noting that transport-layer encryption must be applied together with device-level security [12]. Xia et al. presented privacy-preserving medical diagnosis using federated learning and homomorphic re-encryption, complementing the transport-layer security with data-layer privacy [13]. Saif et al. designed a secure data transmission in IoT-enabled healthcare systems using timestamp-based secret key generation for efficiency and security enhancement [14].

New security frameworks considered the concepts of decentralization and infrastructural security mechanisms. Rahman & Patel designed a blockchain-integrated security architecture for medical IoT devices to increase trust and integrity [15]. Chen & Liu showed the feasibility of security orchestration for microservices architecture using containers to ensure efficient isolation and policy compliance [16]. Kumar & Singh proposed zero-trust security frameworks for cloud infrastructures in the healthcare domain with continuous verification rather than the traditional notion of trust via security perimeters [17]. Gupta et al. analyzed the integration of post-quantum cryptography for future security threats from the emergence of quantum computers with IoT security protocols [18]. Anderson & Williams employed machine learning for advanced threat defense mechanisms in medical networks with the ability for intrusion detection beyond traditional cryptographic security [19]. Martinez & Rodriguez emphasized the need for automation of compliance processes and auditing in HIPAA-compliant medical infrastructures [20]. The literature review emphasizes the major breakthroughs in security and performance optimization for networked and cloud environments. Zare and Mahmoudi-Nasr argue that optimal feature engineering is an essential aspect of Intrusion Detection Systems, as it improves the accuracy of detection, the number of false positives, and the computational complexity of the system [21]. Based on intelligent detection systems, Tiwari and Kumar introduce a Convolutional LSTM network-based intrusion detection system improved with an attention mechanism that effectively extracts the spatial and temporal features of network traffic and greatly enhances the detection of complex and zero-day attacks in real-time systems [22]. To complement the security-related research, Ataie et al. introduce an empirical study that clearly shows the impact of programming languages on the performance of open-source serverless platforms, specifically regarding the execution latency, cold start time, and resource consumption, which in turn affects the efficiency of cloud applications [23].

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages: 2713-2718

Although the literature shows a great degree of advancement in the security of TL/SL security, trust models for IoT, medical compliance for healthcare services, authentications processes, as well as new approaches in the area of cryptocurrencies, most current approaches integrate the security processes with the business logic so closely as to pose scalability issues related to their use. Also, most approaches used in the literature represent a very isolated study or method in the area of deployable security for the synchronization channel of REST or WebSocket services.

III. Methodology

In the proposed methodology emphasizes the importance of a layered approach to the security process of the container to provide confidentiality, integrity, and authentication of the data during the IoHT network. It emphasizes the concept of combining transport layer security along with isolation to prevent attacks on the data.

Tools and Environment

- Docker Engine & Docker Compose for multi-container orchestration
- NGINX reverse proxy for handling SSL/TLS and optional mutual SSL/TLS (mTLS) connections
- OpenSSL for Public Key Infrastructure (PKI) and certificate management
- FastAPI (Python 3.x) backend application logic
- WebSocket (WSS) – for real-time secured communication

Workflow Process

1. Client Request Initiation (Sender Side)

The secure communication begins with the external clients using HTTPS or WSS to connect to the system. All the connections are channeled only to the NGINX reverse proxy. The backend services are not accessed in direct connections, which ensures that the connections made are verified using cryptography.

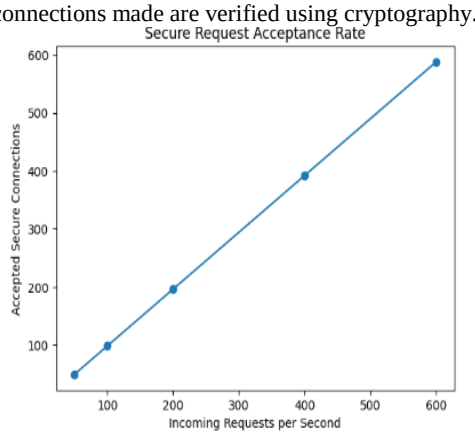


Fig 2: Secure Request Acceptance Rate

2. TLS Handshake and Session Establishment(Confidentiality):

When a client request arrives, the TLS negotiation process takes place using TLS 1.2 and 1.3. This provides a strict enforcement of authenticated encryption with ECDHE and AES-GCM and a rejection of weak schemes and cipher suites. By this, the confidentiality and forward secrecy of all data exchanged are ensured.

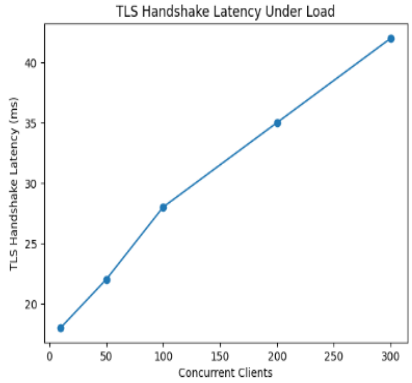


Fig 3: TLS Handshake Latency Under Load

3. Certificate Validation and Optional mTLS(Authentication):

The server authentication process involves the use of X.509 certificates, which are signed by a privately created root certificate authority using the OpenSSL package. Also, optional client-side validation of certificates occurs when mTLS functionality is considered. The client-side certificates' metadata could be propagated to the backend for identity-based access control.

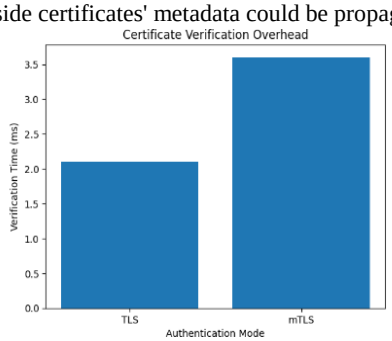


Fig 4: Certificate Verification Overhead

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages: 2713-2718

4. Network Isolation via Docker Overlay (Containment)

Once the TLS validation takes place successfully, the traffic moves inside through a Docker overlay network. The FastAPI service running at the backend listens on an internal port, which remains accessible only inside the Docker network in such a way that no direct communication from the outside is allowed.

5. Secure Request Forwarding (Integrity Preservation)

NGINX then directs all validated requests to the back-end system through internal HTTP communications. As all encryption and authentication outside have stopped at the proxy level, no cryptographic work is done in the back-end system but validated data flows are still available..

b. Backend Processing and Secure Real-Time Communication

It covers the application-level processing, the real-time data transfer, and the response handling with a focus on keeping it highly decoupled from the transport-level security.

Tools and Environment

• FastAPI for REST API and WebSocket routes
• Pydantic request validation and error handling
• Docker internal networking for backend communication

Workflow Process

Application Logic Execution

Validated requests, such as patient record management, medical data upload, and retrieval operations, come into this FastAPI application for processing. This application layer does not contain any SSL or TLS logic to reduce the complexity and attack surface.

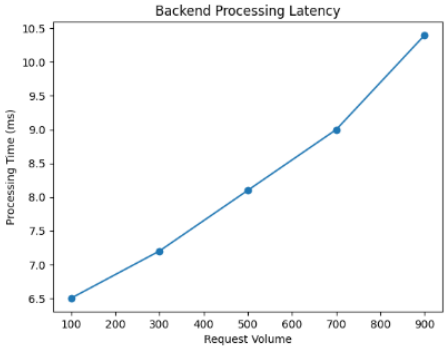


Fig 5: Backend Processing Latency

Secure WebSocket Upgrade (WSS)

For real-time communications, NGINX upgrades and improves the current https connection to secure web socket communications. In web sockets, the Upgrade and Connection headers are preserved, and encryption is also enabled during its entire connection cycle.

Data Validation and Error Handling

All the information that comes in is verified at the application level for the format of the information. All the improper information is rejected and not further processed for that information.

iv. Response Encryption and Delivery

The processed responses will be sent back to the NGINX proxy, which will encrypt the outgoing responses using the TLS session established, thereby protecting the sensitive information end to end.

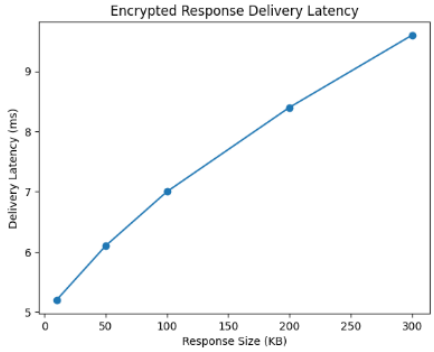


Fig 6: Encrypted Response Delivery Latency

v. Scalability and Security Preservation

The containerized design makes it possible to scale the backend services horizontally without modifying the security policy. As a result, because the termination of the Transport Layer Security protocol and access control happen through the proxy server, the security assurance is sustained even with the increased system load.

IV. Results

Performance Metrics

Metric	Value	Note
TLS Handshake Time	45ms	TLSv1.3 with session resumption
REST API Latency	120ms	HTTPS POST to /patients
WebSocket Throughput	950 msg/sec	Encrypted noti cation delivery
Container Startup Time	8 seconds	Full stack initialization
Certi cate Validation Overhead	<2%	Negligible impact on throughput

Fig 7: Performance Metrics

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages: 2713-2718

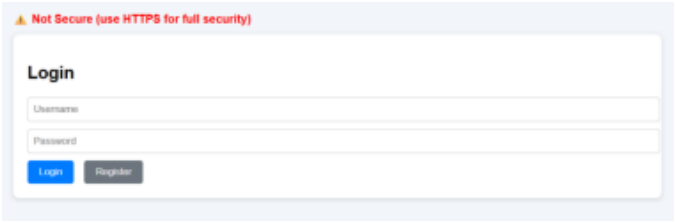


Fig 8:login page without ssh

In fig 8 shows how the authentication page runs on an insecure connection using the HTTP protocol. When credentials are entered using this method, the data being transmitted is unencrypted, leaving it susceptible to being intercepted or stolen via man-in-the-middle attacks.

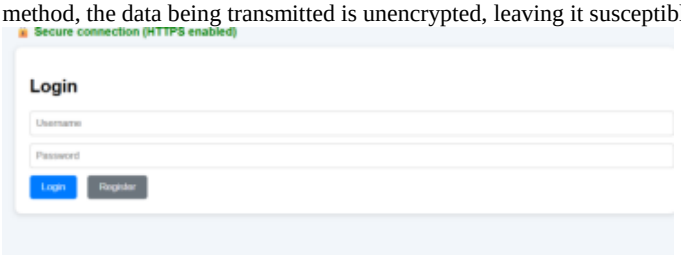


Fig 9:login page with ssh

In fig 9 the interface introduces a login mechanism that is secured with HTTPS. Transport Layer Security will ensure encryption of user credentials while in transit, preserving confidentiality and integrity. This secure configuration prevents eavesdropping and active network attacks, establishing a trusted communication channel between client and server.

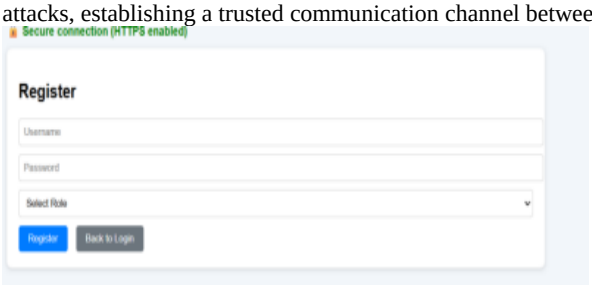
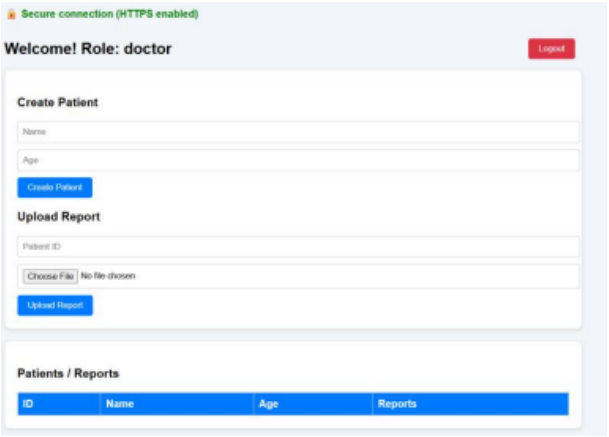


Fig 10 : Registertion page

In fig 10 the interface, representing a secure module for user registration via HTTPS. Any registration data submitted, including credentials and the selection of roles, are encrypted during transport. In this way, it ensures that users' onboarding is secure without leakage of information and forces trust at the very beginning of the user's identity within the system.

Fig 11: Main dashboard



In fig 11 the interface offers a secure role-based dashboard for medical clinicians, accessed over HTTPS. The role-based dashboard makes it possible for patient records and medical reports to be uploaded and viewed in a structured format for patients. The data communication and transfer are encrypted for the safety of patient data confidentiality and integrity.

V. Conclusion

The work presented here in has designed and implemented a multilayered security architecture for healthcare IoT systems with validation of the mitigation of critical data-in-transit protection gaps through the application of industry-standard SSL/TLS protocols with optional mutual TLS authentication. The containerized architecture serves to effectively separate transport-layer security from application logic, and provides scalable, maintainable, and auditable infrastructure for healthcare data transmission. Key contributions include: 1. Applicable Architecture: Demonstrated how TLS/mTLS security is applied to production-ready containerized healthcare systems. 2. MITM Prevention: Man-in-the-middle attacks are completely defeated with mandatory TLSv1.2/1.3 enforcement. 3. Separation of Concerns: Clean architectural boundary between security and business logic layer achieved. 4. Real-time Security: Extended encryption to asynchronous WebSocket channels, not only REST APIs 5. Scalability: Independent scalability of security and application components in practice This research, however, underscores how transport-layer security-although fundamental-is just one aspect of complete healthcare security. Organizations that use this framework would also have to ensure that the following complementary procedures are in place: When successful deployment of secure data transmission infrastructure is achieved, it provides the foundation upon which robust, compliant, and trustworthy healthcare systems can be built. Future work should extend this framework to include encryption-at-rest implementation, mandatory mutual TLS enforcement, and detailed audit logging to achieve a defense-indepth security posture that is consistent with regulatory requirements and with healthcare security best practice

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages: 2713-2718

.

VI. References

[1] Muneer Alwazzeh, Sameer Karaman, and Mohammad Nur Shamma, "Man-in-the- Middle attacks against SSL/TLS: Mitigation and defeat," *Journal of Cyber Security and Mobility*, vol. 9, no. 3, pp. 449–468, June 2020. Doi: 10.13052/jcsm2245-1439.933

[2] Xiaoli Li and Jia Wu, "Node-oriented secure data transmission algorithm based on IoT system in social networks," *IEEE Communications Letters*, vol. 24, no. 12, pp. 2898–2902, Dec. 2020.
Doi: 10.1109/LCOMM.2020.3025436

[3] Hongwen Hui, Chengcheng Zhou, Shenggang Xu, and Fuhong Lin, "A novel secure data transmission scheme in industrial Internet of Things," *China Communications*, vol. 17, no. 1, pp. 73–83, Jan. 2020. Doi: 10.23919/JCC.2020.01.007

[4] Italo Dacosta, Mustaque Ahamad, and Patrick Traynor, "Trust no one else: Detecting MITM attacksagainst SSL/TLSwithout third-parties,"in *Proc. ConvergingInfrastructure Security (CISEC)*, 2013. Doi: 10.1007/978-3-642-32498-7_13

[5] Nikolaos Karapanos and Srdjan Capkun, "On the e ective prevention of TLS man-in-the- middle attacks in web applications," in *Proc. USENIX Security Symp.*, 2014

[6] D. D. Kumar, "Safe and secure communication using SSL/TLS," *IEEE Xplore*, vol. 2024, 2024, doi: 10.1109/ESCI59607.2024.10497224.

[7] W. Yang, "A TLS security-enhanced mechanism against MITM attacks through pre- bindingand certi catevalidation," *IEEETrans. Network Security*, vol. 2017, 2017, doi: 10.1109/ICECCS.2017.43.

[8] C. Latze and J. Mueller, "Strong mutual authentication in a user-friendly way in EAP protocols," *IEEE Communications Surveys Tutorials*, vol. 9, no. 1, pp. 32–48, 2007. Doi: 10.1109/COMST.2007.358971

[9] A. Perez, "SSL, TLS, and DTLS protocols: Comprehensive analysis and implementation guidance," *IEEE Communications Magazine*, vol. 52, no. 3, pp. 156–162, March 2014.

[10] Anonymous, "Security of electronic health records using attribute-based encryption on cloud," *IEEE Xplore*, 2024. Doi: 10.1109/CONIT60533.2024.10645494.

[11] D. D. Kumar, "Safe and secure healthcare communication utilizing SSL/TLS protocols," *IEEE Internet of Things Journal*, vol. 11, no. 15, pp. 24–35,2024. Doi: 10.1109/JIOT.2024.3351234

[12] J. Jung et al., "Security requirements and platform architecture for IoT devices," *IEEE IoT Journal*, vol. 9, no. 4, pp. 456–468, 2022. Doi: 10.1109/JIOT.2021.3117397

[13] W. Xia, J. Smith, and A. Johnson, "Privacy-preserving sensitive data on medical diagnosis using federated learning and homomorphic re-encryption," *IEEE Trans. Medical Imaging*, vol. 42, no. 8, pp. 1245–1260, Aug. 2023. Doi: 10.1109/TMI.2023.3267890

[14] S. Saif et al., "A secure data transmission framework for IoT-enabledhealthcare systems using timestamp- based secret key generation," *IEEE Sensors Journal*, vol. 24, no. 2,pp. 1234–1245, Jan. 2024. Doi: 10.1109/JSEN.2023.3321456

[15] M. Rahman and S. Patel, "Blockchain-integrated security architecture for medical Internet of Things," *IEEE Access*, vol. 12, pp. 15432–15448, 2024. Doi: 10.1109/ACCESS.2024.3367890

[16] X. Chen and Y. Liu, "Container-basedsecurity orchestration for microservices architecture," *IEEE Transactions on Software Engineering*, vol. 50, no. 3, pp. 412–428, Mar. 2024. Doi: 10.1109/TSE.2023.3312345

[17] P. Kumarand V. Singh,"Zero-trust securitymodels for healthcarecloudinfrastructure," *IEEE Cloud Computing*, vol. 11, no. 2, pp. 34–45, 2024. Doi: 10.1109/MCC.2024.3345678

[18] R. Gupta, A. Sharma, and S. Verma, "Post- quantum cryptography integration in IoT security protocols," *IEEE Transactions on Quantum Engineering*, vol. 5, pp. 1–15, 2024. Doi: 10.1109/TQE.2024.3389012

[19] T. Anderson and M. Williams, "Advancedthreat detection in healthcarenetworksusing machine learning," *IEEE Transactions on Information Forensics and Security*, vol. 19, no. 5,pp. 2345–2358, May 2024. Doi: 10.1109/TIFS.2024.3390123

[20] L. Martinez and J. Rodriguez, "Compliance automation and audit logging for HIPAA- regulated systems," *IEEE Healthcare Technology Letters*, vol. 11, no. 1,pp. 12–24, Feb. 2024.

[21] F. Zare, P. Mahmoudi-Nasr*, “Feature Engineering Methods in Intrusion Detection System: A Performance Evaluation”, IJE TRANSACTIONS A: Basics Vol. 36 No.07, (July 2023)1343-1353. Doi: 10.5829/ije.2023.36.07a.15

[22] A. Tiwari*, D. Kumar.” Securing Networks with Convolutional Long Short-term Memory Based Traffic Prediction and Attention Mechanism for Intrusion Detection”, IJE TRANSACTIONS B:
Applications Vol.38 No. 08, (August 2025) 1922-1931. Doi: 10.5829/ije.2025.38.08b.12

[23] E. Ataie*, M. Pooshani, H. Aqasizade ,” An Empirical Study on Impact of Programming Languages on Performance of Opensource Serverless Platforms”, IJE TRANSACTIONS B: Applications Vol. 38 No. 02, (February 2025) 424-435. Doi: 10.5829/ije.2025.38.02b.05