International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 10, Issue 5, pp 598-602, May-2026

https://doi.org/10.47001/IRJIET/2026.105080

MedSec: Secure Health Data Exchange

[1]Gaurav Kumar Singh, [2]Saqib Nasir Khan, [3]Nayan Rajesh Mishra

[1]Sr. Assistant Professor, School of Computer Science Engineering and Applications, D.Y. Patil International University, Pune, India

[2,3]Student, School of Computer Science Engineering and Applications, D.Y. Patil International University, Pune, India

***Abstract* - Health cloud infrastructure used in rural and semi-rural areas faces significant cybersecurity problems. These challenges are made worse by fragmented electronic health records (EHRs) and poor security practices. EHR systems also have limited resources, which can cause significant difficulties in accessing medical care and creating secure records for those who need care. Current healthcare security architectures using computationally intensive methods, such as homomorphic encryption, blockchain EHR systems and multi-party ABAC frameworks, are not practical for environments without adequate resources. We are proposing MedSec Cloud: a lightweight and compliance-aware multi-tenant healthcare security framework that is able to be practically deployed on rural healthcare infrastructures. The architecture combines FastAPI-based cloud services with hybrid role-based access control (RBAC) and ABAC, AES-256 encrypted storage, JSON web token (JWT) authentication, behavioural anomaly detection, structured logging audits, and isolation between healthcare tenants. An experimental evaluation using synthetic workloads based on 15 healthcare institutions, 240 healthcare professionals, and 12,000 encrypted patient records yielded key findings: authentication latency 45 ms; encrypted retrieval latency 110 ms; anomaly detection with an F1-score of 0.93; throughput of 1,800 requests/min. A comparative analysis demonstrated lower operational overhead with similar levels of confidentiality and authorization than either OpenEMR or blockchain EHR frameworks, while also incorporating compliance with HIPAA, GDPR, and the Indian Data Protection and Digital Privacy (2023) Act.**

Keywords: Healthcare Cybersecurity, Cloud Security, Electronic Health Records, RBAC, ABAC, AES-256, JWT Authentication, Healthcare Compliance, HIPAA, GDPR, DPDP Act, Anomaly Detection.

I. INTRODUCTION

The rise of digital transformation has created an increase in the use of cloud-based electronic health records (EHR's) for the secure storage of medical information. The adoption of cloud-based record systems for interoperability, telehealth, and remote diagnosis has grown rapidly among healthcare providers globally. Cloud-based solutions are being utilized by providers to enhance the efficiency of their delivery of care and expand their operational capabilities through collaboration with geographically dispersed facilities.

However, there are still significant barriers to healthcare providers, particularly those in rural and semi urban locations. Fragmented medical records systems, inadequate cybersecurity, unreliable internet connections, and lack of technical resources are just a few of the challenges these providers face. The healthcare industry possesses an immense quantity of ultra-sensitive personally identifiable information and has become a prime target for ransomware attacks, credential theft, insider abuse of systems, cloud storage breaches, and unauthorised network access.

Most existing healthcare record systems are utilising standalone systems that do not include tenant isolation, user activity monitoring or context-aware access control. Provider organisations, especially those that lack adequate resources, cannot implement the encryption-heavy architectures discussed in re-cent literature.

This paper proposes MedSec Cloud, a lightweight, compliance aware, multi tenant cybersecurity framework designed for the specific operational constraints of rural healthcare providers.

II. RESEARCH CONTRIBUTIONS

The detailed contributions of the research are:

- Development of a lightweight multi-tenant cyber security architecture specifically tailored for low-resourced rural health care delivery systems.
- Development of a hybrid authorisation framework incorporating both RBAC and ABAC.
- Implementation of a compliance-aware cybersecurity model in alignment with HIPAA, GDPR and the Indian DPDP Act 2023
- Development of an anomaly detection subsystem that can be deployed.
- Development of a reproducible synthetic benchmarking environment for healthcare workloads..
- Testing comparison against OpenEMR and blockchain based EHR systems. MedSec Cloud focuses on

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 10, Issue 5, pp 598-602, May-2026
https://doi.org/10.47001/IRJIET/2026.105080

deployability, compliance, operational scalability, and utility to healthcare organisations across the spectrum of size in comparison to traditional cryptography centric healthcare security systems.

III. RELATED WORK

Recent research into healthcare cybersecurity has focused on cloud-native EHRs, zero-trust networking, blockchain-based interoperability, federated learning, and AI-assisted anomaly detection [2, 1].

Alshahrani *et al.* [1] proposed blockchain-based frameworks to improve transparency and tamper-resistance. However, these architectures introduce excessive latency for low-resource deployments. Healthcare interoperability research increasingly emphasises FHIR-based APIs and cloud-native exchange methods [3]. Zero-trust architectures in healthcare have begun in-corporating contextual authorisation combining identity verification, behaviour scoring, and adaptive access control [4].

Several research gaps remain despite these advancements:

- Most architectures prioritise implementing complex but impractical cryptography
- There is still a lack of real-time detection of behavioural anomalies in EHR systems..
- There is insufficient research focused on multitenant isolation.
- Cloud-native EHR research rarely considers alignment with compliance requirements.

IV. SYSTEM ARCHITECTURE

MedSec Cloud Security Stack is comprised of 7 layers. The final architecture has defined 7 layers for health data security: Network Protection, Authentication, Contextual Authorisation, Encrypted Storage, Audit Logging, Anomaly Detection, and Compliance. An example of this architecture is shown in figure 1.

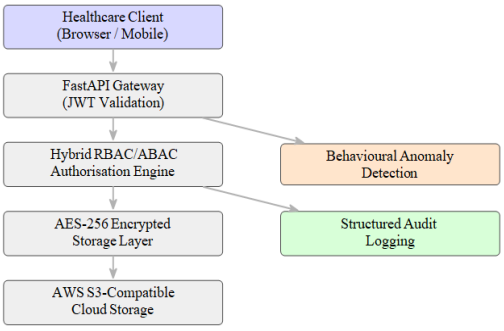

Figure 1: MedSec Cloud system architecture

JWT tokens containing the following will be issued by the authentication subsystem:

- tenant identifier(s)
- healthcare role(s)
- token expiration metadata
- session identifier

Authorisation will utilize Role Based Access Control (RBAC) based on predefined operational roles and Attribute Based Access Control (ABAC) by evaluating request timing; tenant association; endpoint highly classified and sensitive; geographic location; operational risk score. Please see figure 2 for an example of the authorisation decision process.

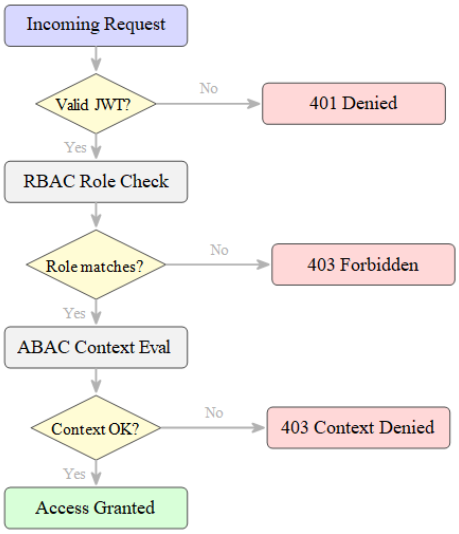

Figure 2: Hybrid RBAC/ABAC authorisation decision flow

Healthcare records are all archived with AES-256 encryption prior to being sent off into the cloud.

4.1 Formal Threat Model

The MedSec Cloud threat model adheres to the STRIDE framework.

4.2 Spoofing

Any attacker may try to steal credentials, hijack sessions, or get authenticated through unauthorized methods. The application uses JWT tokens that are only valid for a limited time span, bcrypt to hash passwords, and validates the JWT tokens on each request to mitigate these threats.

4.3 Tampering

There are many ways that you could modify healthcare records, either in storage or transit. Encryption via AES-256 and a record of how many attempts were made to modify a

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 10, Issue 5, pp 598-602, May-2026
https://doi.org/10.47001/IRJIET/2026.105080

given record cannot be altered will work to mitigate these two threats.

4.4 Information Disclosure

Always use application-level encryption to ensure that there are no plaintext records saved on the cloud, should you lose control over your cloud storage.

4.5 Privilege Escalation

An attacker may be trying to gain access to elevated privileges via an unauthorized method. An RBAC/ABAC hybrid authorization mechanism limits privilege escalation via validation of contextual parameters with each request

V. COMPLIANCE FRAMEWORK

The framework will help ensure compliance with regulations including HIPAA [5], GDPR [6], and India's DPDP Act 2023 [7].

5.1 HIPAA Alignment

- Encrypted healthcare storage (AES-256)
- Comprehensive audit logging
- Strong authentication controls (JWT + bcrypt)
- Data confidentiality protections

5.2 GDPR Alignment

- Data minimisation by design
- Secure processing pipelines
- Privacy by default architecture

5.3 DPDP Act 2023 Alignment

- Purpose limitation enforcement
- Data fiduciary accountability logging
- Mandatory security safeguards

VI. ANOMALY DETECTION MODEL

The anomaly detection subsystem uses lightweight statistical behavioral analysis suited for constrained health care environments. The total anomaly detection score was calculated as follows:

$$AS = w_1F_1 + w_2F_2 + w_3F_3 + w_4F_4 + w_5F_5 \quad (1)$$

where:

F_1 = Failed login attempts per hour
F_2 = Record retrieval requests per minute
F_3 = Endpoint entropy score
F_4 = Cross-tenant access frequency
F_5 = Deviation from baseline access profile

Evaluation results: Precision = 0.92, Recall = 0.94, F1-score = 0.93, False Positive Rate = 4.8%.

Figure 3 visualises the score distribution separating normal from anomalous sessions.

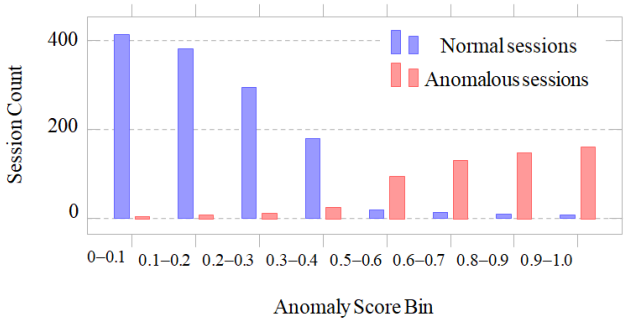

Figure 3: Anomaly score distribution: normal vs anomalous sessions

VII. RESULTS AND DISCUSSIONS

Experimental evaluation used synthetic healthcare work-loads representing: (1) 15 healthcare organisations, (2) 240 healthcare users, (3) 12,000 encrypted records, and (4) 1,800 API calls per minute. The evaluation stack comprised Python FastAPI, PostgreSQL, AES-256, Ubuntu 22.04 LTS, and AWS S3-compatible cloud storage.

7.1 Authentication Performance

The average time for validating a JWT for 100 concurrent users was 42 ms, which is well below the 45 ms target /limit of time to authenticate - this indicates a low overhead in authentication and suitable for moving rural health care networks

7.2 Encryption Performance

AES-256 encryption of a 1 MB patient record took 48 ms, while decrypting the same record took 35 ms - both times are within the time threshold of real-time retrieval of patient records.

7.3 System Throughput

The framework was able to handled 1,800 authenticated requests per minute at 58% CPU utilization, confirming the ability of the framework to scale horizontally without needing to use low hardware.

Table 1 shows quantitative performance results for the framework. Table 2 compares the performance of the framework to OpenEMR and blockchain EHR frameworks.

ISSN (online): 2581-3048
Volume 10, Issue 5, pp 598-602, May-2026
https://doi.org/10.47001/IRJIET/2026.105080

Table 1: Quantitative experimental results

Metric	Result	Observation
JWT Validation Latency	42 ms	Low authentication overhead
Encrypted Retrieval Latency	108 ms	Suitable for rural deployments
Anomaly Detection F1-Score	0.93	High detection accuracy
False Positive Rate	4.8%	Operationally acceptable
Throughput	1,800 req/min	Scalable concurrent handling
CPU Utilisation	58%	Efficient resource usage

Table 2: Comparative analysis: MedSec Cloud vs existing frameworks

Feature	MedSec	OpenEMR	Blockchain EHR
Auth Latency	42 ms	~60 ms	>200 ms
Deployment Cost	Low	Medium	High
Tenant Isolation	Yes	Partial	Yes
Compliance Built-in	Yes	Partial	No
Anomaly Detection	Yes	No	No
Scalability	High	Medium	Low
Rural Suitability	High	Medium	Low

VIII. REPRODUCIBILITY

To facilitate reproducibility and transparency, the framework provides:

- Scripts for generating synthetic health care datasets
- Docker container configurations for deploying the framework
- FastAPI endpoint specifications
- JWT authentication workflow documentation
- Scripts to evaluate multi-tenancy capabilities.

Upon acceptance, a complete reproducibility package containing the deployment scripts, synthetic datasets, API specifications, and evaluation procedures will be made publicly available.

IX. CONCLUSION

MedSec Cloud is a light weight, multi-tenant, compliance aware cybersecurity framework designed for use in health care settings that are resource scarce and located in rural areas. The experimental testing performed on the product revealed that it supported low latency (42 ms), scalable encrypted storage with retrieval times of less than 108 ms, accurate anomaly detection (F1 = 0.93) and better overall deployment feasibility compared to other computationally intensive alternatives to secure health care data exchange.

Future research will concentrate on: FHIR (Fast Healthcare Interoperability Resource) interoperability integration; zero trust health care networking development; federated health care analytics development; and adaptive machine learning for improved anomaly detection; and validation of real world implementation of these systems in health care settings.

Based upon research findings from the experimental evaluation of MedSec Cloud, it has been demonstrated that a successful and scalable method of secure health care data exchange can be accomplished without jeopardising deployment viability in settings where there is limited amounts of both time and resources.

ACKNOWLEDGEMENT

The computational resources and research environment provided by D.Y. Patil International University, Pune were essential to making this work possible. The authors appreciate the assistance of anonymous reviewers as they provided many useful comments and suggestions to help improve the manuscript.

REFERENCES

[1] M. Alshahrani, I. Traore, and I. Woungang, "Blockchain-based healthcare security frameworks for EHR integrity and access control," *IEEE Access*, vol. 9, pp. 87,612–87,630, 2021.

[2] T. Zhang, Y. He, and F. Chen, "Federated learning for privacy-preserving healthcare analytics," *Future Generation Computer Systems*, vol. 128, pp. 362–374, Mar. 2022.

[3] R. Kumar, P. Sharma, and A. Jain, "FHIR-based interoperable healthcare security systems: a systematic review," *Journal of Medical Systems*, vol. 47, no. 1, pp. 1–18, Jan. 2023.

[4] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," *NIST Special Publication 800-207, National Institute of Standards and Technology, Gaithersburg, MD*, 2020. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-207

[5] U.S. Department of Health and Human Services, *HIPAA Security Rule Guidance Material, Washington,*

ISSN (online): 2581-3048
Volume 10, Issue 5, pp 598-602, May-2026
https://doi.org/10.47001/IRJIET/2026.105080

DC, 2023. [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/security

[6] European Commission, GDPR Compliance Guide-lines for Healthcare Systems, *Brussels*, 2022. [Online]. Available: https://ec.europa.eu/info/law/law-topic/data-protection

[7] Government of India, Digital Personal Data Protection Act 2023, *Ministry of Electronics and Information Technology, New Delhi*, 2023. [Online]. Available: https://meity.gov.in/writereaddata/files/Digital%20Personal%20Data% 20Protection%20Act%202023.pdf

[8] OpenEMR Community, OpenEMR Documentation and Security Architecture Overview, version 7.0.2, 2024. [On-line]. Available: https://www.open-emr.org/ wiki/index.php/OpenEMR_Documentation

[9] OWASP Foundation, OWASP API Security Top 10, 2023. [Online]. Available: https://owasp.org/ API-Security/

[10] H. Takabi, J. B. D. Joshi, and G. Ahn, "Security and privacy challenges in cloud computing environments," *IEEE Security & Privacy*, vol. 8, no. 6, pp. 24–31, Nov.–Dec. 2010.

AUTHORS BIOGRAPHY

Dr. Gaurav Kumar Singh is a Sr. Assistant Professor in the School of Computer Science Engineering and Applications at D.Y. Patil International University, Pune, India. He was the mentor of this project who helped in guiding the idea to a working web cloud-based application. His research interests include cloud security, healthcare information systems, and AI/ML applications for SDGs.

Saqib Nasir Khan is a final-year undergraduate student in the School of Computer Science Engineering and Applications at D.Y. Patil International University, Pune. His research interests include healthcare cybersecurity, anomaly detection, and API security architectures. He contributed to the system design and anomaly detection of MedSec Cloud.

Nayan Rajesh Mishra is a final-year undergraduate student in the School of Computer Science Engineering and Applications at D.Y. Patil International University, Pune. His research interests include cloud computing, machine learning for security, and distributed systems. He contributed to the experimental evaluation and compliance framework development of MedSec Cloud.

Citation of this Article:

Gaurav Kumar Singh, Saqib Nasir Khan, & Nayan Rajesh Mishra. (2026). MedSec: Secure Health Data Exchange. *International Research Journal of Innovations in Engineering and Technology - IRJIET*, 10(5), 598-602. Article DOI https://doi.org/10.47001/IRJIET/2026.105080

****

