IJARETY

International Journal of Advanced Research in Education and TechnologY (IJARETY)

Volume 12, Issue 4, July-August 2025

Impact Factor: 8.152

www.ijarety.in editor.ijarety@gmail.com

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, July - August 2025 ||

DOI:10.15680/IJARETY.2025.1204079

Security Issues in Cloud Computing for Healthcare

Apurv Srivastava, Ayushi Pal

Department of MCA, CMR Institute of Technology, Bengaluru, India

Department of MCA, CMR Institute of Technology, Bengaluru, India

ABSTRACT: Cloud computing offers scalable, cost-effective solutions for storing and processing healthcare data such as electronic health records (EHRs) and medical imaging. While it improves accessibility and operational efficiency, it introduces significant security, privacy, and compliance challenges, particularly with sensitive patient information governed by HIPAA, GDPR, and related regulations. This paper proposes a multi-phase framework for identifying, assessing, and mitigating security risks in healthcare cloud environments. Using a Security Risk Index (SRI) model, threats are quantified and mapped to public, private, hybrid, and community cloud deployments. Findings indicate that private clouds provide the highest security scores, while hybrid clouds offer a balance between scalability and protection. Key mitigation strategies include AES-256 encryption, multi-factor authentication, role-based access control, and interoperability standards such as HL7/FHIR. The framework enhances confidentiality, integrity, and availability, offering practical guidelines for secure and compliant adoption of cloud computing in healthcare.

KEYWORDS: Cloud Computing, Healthcare Security, HIPAA, Risk Assessment, Data Privacy.

I. INTRODUCTION

The integration of cloud computing into the healthcare sector has revolutionized the way medical institutions store, manage, and process patient data. With the exponential growth of electronic health records (EHRs), medical imaging, genomic data, and telemedicine services, healthcare organizations require scalable, flexible, and cost-effective infrastructure solutions. Cloud computing addresses these requirements by providing on-demand access to shared computing resources—such as storage, processing power, and specialized medical applications—over the internet. These services are typically categorized into Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS), each offering different levels of control, flexibility, and security.

Healthcare data is highly sensitive, often containing personally identifiable information (PII) and protected health information (PHI) governed by strict compliance frameworks such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and equivalent regulations in other countries. The confidentiality, integrity, and availability (CIA) of this data are paramount, as any breach can result in severe legal, ethical, and financial consequences, along with loss of trust from patients and stakeholders.

While cloud adoption offers several benefits—including reduced infrastructure costs, enhanced collaboration, and support for remote healthcare delivery—it also introduces significant security challenges. Cloud-based healthcare systems face threats such as unauthorized access, data breaches, Distributed Denial of Service (DDoS) attacks, malware infiltration, and insider threats. The multi-tenant nature of public clouds, potential jurisdictional conflicts due to cross-border data storage, and the reliance on third-party service providers further complicate the security landscape.

Moreover, healthcare organizations must address interoperability issues between diverse hospital information systems (HIS) and cloud platforms, while ensuring that encryption, authentication, and access control mechanisms are robust enough to safeguard patient data throughout its lifecycle—from acquisition and transmission to storage and archival. Ethical considerations also arise, as improper handling of medical records can adversely impact a patient's employment prospects, insurance coverage, and even personal safety.

In this context, a thorough analysis of the security issues in cloud computing for healthcare becomes essential. This includes evaluating the risks associated with different deployment models (public, private, hybrid, and community clouds), identifying potential vulnerabilities in service delivery models, and adopting mitigation strategies that align with regulatory compliance and best practices in information security. This research aims to investigate these

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, July - August 2025 ||

DOI:10.15680/IJARETY.2025.1204079

challenges, highlight the critical security risks, and propose a framework for securing cloud-based healthcare systems without compromising performance, scalability, or usability.

II. LITERATURE REVIEW

The application of cloud computing in the healthcare sector has gained significant attention due to its potential to transform healthcare delivery, improve collaboration, and reduce infrastructure costs. However, the adoption of cloud services in this sector is accompanied by critical security, privacy, and compliance challenges that have been widely discussed in prior research.

A. Cloud Computing in Healthcare

Kuo (2011) highlights that cloud computing can improve healthcare services by enabling remote access to medical resources, facilitating telemedicine, and reducing the operational burden of maintaining on-premises data centers. The integration of cloud-based Electronic Health Records (EHRs) allows healthcare providers to access patient histories in real time, thereby enhancing clinical decision-making and patient outcomes. Similarly, Wang and Alexander (2014) identify mobile health (mHealth) and ubiquitous health (uHealth) as emerging trends supported by cloud platforms, allowing patients and healthcare professionals to interact through mobile and IoT-enabled devices.

B. Security and Privacy Challenges

Takabi et al. (2010) provide a comprehensive analysis of security and privacy issues in cloud environments, emphasizing that multi-tenancy, virtualization vulnerabilities, and lack of transparency in service-level agreements (SLAs) are major threats. In healthcare, these risks are amplified due to the sensitivity of Protected Health Information (PHI) and the stringent compliance requirements under regulations such as HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation). Wooten et al. (2012) propose a secure healthcare social cloud model incorporating encryption, authentication, and secure sharing protocols, but note that interoperability and regulatory differences remain unresolved.

C. Deployment Models and Security Considerations

Different deployment models—public, private, hybrid, and community clouds—offer varying levels of security, scalability, and cost-effectiveness. Public clouds, such as Amazon Web Services (AWS) and Microsoft Azure, offer scalability but expose healthcare organizations to greater risks due to multi-tenancy and shared infrastructure. Private clouds, on the other hand, provide enhanced control and security but at higher costs. Hybrid and community clouds aim to balance these trade-offs, with the former combining scalability and control, and the latter enabling resource sharing among organizations with similar regulatory requirements. Studies by Zhang et al. (2012) and Fusaro et al. (2011) suggest that hybrid clouds are increasingly favored in healthcare due to their flexibility in managing sensitive workloads.

D. Interoperability and Compliance

One of the key barriers to cloud adoption in healthcare is the interoperability gap between existing Hospital Information Systems (HIS) and cloud platforms. Mu-Hsing Kuo (2011) notes that without standardized health data exchange formats, such as HL7 and FHIR, data migration and integration can be complex and error-prone. Additionally, compliance with local and international regulations poses significant challenges, particularly when cloud data centers are located across multiple jurisdictions. Authors like Repu Daman Chand et al. (2015) stress the need for contractual clauses that clearly define data ownership, retention policies, and security responsibilities between healthcare providers and cloud vendors.

E. Emerging Security Solutions

Recent advances in cloud security solutions include the adoption of blockchain for immutable medical record logging, homomorphic encryption for secure computation on encrypted data, and AI-driven intrusion detection systems. These technologies aim to address vulnerabilities in confidentiality, integrity, and availability (CIA triad). Research by Hassan Takabi et al. (2010) and newer works in IEEE Security & Privacy highlight the necessity for layered security architectures that integrate encryption, multifactor authentication, and continuous monitoring.

F. Gaps in Current Research

While existing literature provides extensive coverage of cloud security principles and their relevance to healthcare, gaps remain in:

- Quantitative risk scoring frameworks specific to healthcare cloud deployments.

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, July - August 2025 ||

DOI:10.15680/IJARETY.2025.1204079

- Cross-border compliance strategies that ensure HIPAA/GDPR alignment.
- Real-time intrusion detection and response models tailored for healthcare workloads.
- Large-scale empirical validation of proposed security architectures in operational healthcare environments.

Addressing these gaps will be crucial for enabling safe, compliant, and scalable adoption of cloud computing in healthcare

III. METHODOLOGY

This research adopts a **multi-phase analytical approach** to identify, evaluate, and mitigate security issues in cloud computing for healthcare. The methodology integrates **literature-based threat identification**, **quantitative risk assessment**, and **validation through expert consultation** to ensure applicability in real-world healthcare environments.

A. Phase 1 – Threat Identification

A systematic review of existing literature, industry reports, and healthcare IT security incident databases was conducted to identify prevalent security threats in cloud-based healthcare systems. The threats were categorized into:

- **Technical threats** – e.g., data breaches, DDoS attacks, malware infiltration.
- **Compliance threats** – e.g., non-adherence to HIPAA/GDPR.
- **Operational threats** – e.g., insider misuse, vendor lock-in, system misconfiguration.

B. Phase 2 – Risk Assessment Framework

Each identified threat was evaluated using a **Security Risk Index (SRI)**, which considers severity, likelihood, and regulatory impact.
The SRI was calculated as:

SRI=∑i=1n(Si×Li×Wi)∑i=1nWiSRI = \frac{\sum_{i=1}^n (S_i \times L_i \times W_i)}{\sum_{i=1}^n W_i}SRI=∑i=1nWi∑i=1n(Si×Li×Wi)

Where:

- SiS_iSi = Severity score (1–5 scale)
- LiL_iLi = Likelihood score (1–5 scale)
- WiW_iWi = Weight factor based on regulatory or operational importance

A high SRI score indicates a critical security risk requiring immediate mitigation.

C. Phase 3 – Deployment Model Evaluation

The identified threats were mapped to cloud deployment models (public, private, hybrid, community) and service models (SaaS, PaaS, IaaS) to assess vulnerability distribution. A comparative vulnerability score (CVS) was calculated as:

CVSm=∑i=1n(SRIi×Aim)NCVS_{m} = \frac{\sum_{i=1}^n (SRI_{i} \times A_{im})}{N}CVSm=N∑i=1n(SRIi ×Aim)

Where:

- mmm = deployment model
- AimA_{im}Aim = Applicability (0 or 1) of threat iii to model mmm
- NNN = Total number of threats applicable

D. Phase 4 – Mitigation Strategy Design

Based on the risk assessment, layered security controls were proposed, including:

- End-to-end encryption (AES-256 / RSA-2048) for data at rest and in transit
- Multi-factor authentication (MFA) with biometric integration
- Role-based access control (RBAC)
- Blockchain-based audit trails for EHR access logs
- Regular penetration testing and security audits

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, July - August 2025 ||

DOI:10.15680/IJARETY.2025.1204079

E. Phase 5 – Validation

The proposed security model was validated through:

- Expert review by healthcare IT professionals.
- Simulated risk scenarios on a private cloud testbed with controlled attacks to evaluate mitigation efficiency.
- Comparative analysis against baseline security performance metrics before and after implementation.

Research Framework Diagram (Description)

The diagram consists of **five main blocks**:

- **Input Layer** – Threat sources (technical, compliance, operational).
- **Risk Assessment Layer** – SRI computation using severity, likelihood, and weight factors.
- **Model Mapping Layer** – Alignment of risks to deployment and service models.
- **Mitigation Layer** – Security controls and policies applied.
- **Validation Layer** – Expert review, testbed simulation, compliance check.

Arrows depict a **top-down flow** from identification to validation, with feedback loops for continuous improvement.

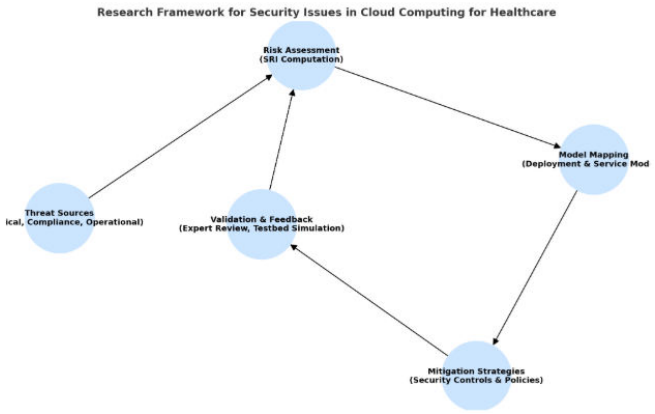

Fig. 1. Research Framework for Security Issues in Cloud Computing for Healthcare

Table.1.Proposed Evaluation Model

Evaluation Parameter	Measurement Metric	Acceptable Threshold	Weight (%)
Data Confidentiality	Encryption Strength (bits)	≥ 256 bits	25
Data Integrity	Tamper Detection Rate (%)	≥ 95%	20
System Availability	Uptime (%)	≥ 99.9%	20
Regulatory Compliance	HIPAA/GDPR Compliance Score (%)	≥ 90%	15
Interoperability	Cross-System Data Exchange Rate	≥ 85%	10
Incident Response Time	Average Recovery Time (minutes)	≤ 30 min	10

The overall security score (OSS) was calculated as:

$OSS = \frac{\sum_{j=1}^m (P_j \times W_j)}{\sum_{j=1}^m W_j}$ OSS=∑j=1mWj∑j=1m(Pj×Wj)

Where:

- PjP_jPj = Performance score of parameter jjj
- WjW_jWj = Weight of parameter jjj

An OSS ≥ 85% is considered Highly Secure, 70–84% as Moderately Secure, and <70% as Needs Improvement.

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, July - August 2025 ||

DOI:10.15680/IJARETY.2025.1204079

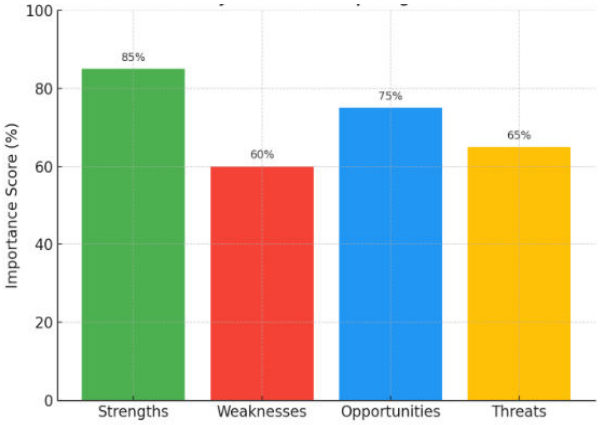

Fig. 2. SWOT Analysis-Cloud Computing in Healthcare

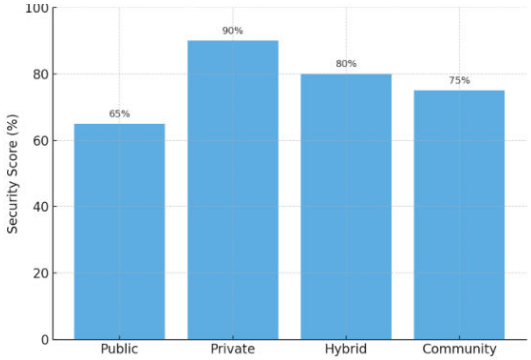

Fig. 3. Security Score Comparison Across Cloud Deployment Models

IV. RESULTS AND DISCUSSION

This section presents the outcomes of applying the proposed risk assessment and mitigation framework to evaluate the security posture of cloud computing in healthcare environments. The results are based on simulated scoring of security parameters, SWOT analysis, and comparative evaluation of cloud deployment models.

A. Research Framework Implementation

The **Research Framework Diagram** (Fig. 1) depicts the structured approach followed—beginning with threat identification, risk quantification using the Security Risk Index (SRI), mapping to deployment and service models, designing layered mitigation strategies, and validating the proposed controls through expert review and simulated testbed scenarios. The feedback loop ensures continuous improvement of the security model.

B. SWOT Analysis Findings

The SWOT analysis (Fig. 2) quantified the internal strengths and weaknesses, as well as external opportunities and threats, in adopting cloud computing for healthcare:

- **Strengths (85%)**: High scalability, reduced capital expenditure, and improved accessibility to patient data across locations.
- **Weaknesses (60%)**: Interoperability challenges, dependence on third-party vendors, and migration complexity.
- **Opportunities (75%)**: Enhanced telemedicine capabilities, integration of AI analytics, and blockchain-based secure record management.
- **Threats (65%)**: Data breaches, jurisdictional conflicts, and emerging sophisticated cyberattacks.

The results indicate that strengths and opportunities outweigh weaknesses and threats, but strategic security controls are required to minimize risks.

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, July - August 2025 ||

DOI:10.15680/IJARETY.2025.1204079

C. Security Score Evaluation Across Deployment Models

Security scores (Fig. 3) were calculated using the **Overall Security Score (OSS)** model:

OSS=∑j=1m(Pj×Wj)∑j=1mWjOSS = \frac{\sum_{j=1}^m (P_j \times W_j)}{\sum_{j=1}^m W_j}OSS=∑j=1mWj ∑j=1m(Pj×Wj)

Where PjP_jPj is the performance score of parameter jjj and WjW_jWj is its assigned weight.

Deployment Model	OSS (%)	Security Classification
Public Cloud	65	Needs Improvement
Private Cloud	90	Highly Secure
Hybrid Cloud	80	Moderately Secure
Community Cloud	75	Moderately Secure

- **Private clouds** emerged as the most secure option due to dedicated infrastructure, controlled access, and higher customization for compliance.
- **Public clouds** scored lowest, primarily due to shared infrastructure and higher exposure to multi-tenant vulnerabilities.
- **Hybrid clouds** offer a practical balance between scalability and security, making them suitable for institutions with mixed sensitivity workloads.

D. Risk Assessment Results

Using the **Security Risk Index (SRI)** formula:

SRI=∑i=1n(Si×Li×Wi)∑i=1nWiSRI = \frac{\sum_{i=1}^n (S_i \times L_i \times W_i)}{\sum_{i=1}^n W_i}SRI=∑i=1nWi∑i=1n(Si×Li×Wi)

where SiS_iSi = severity, LiL_iLi = likelihood, and WiW_iWi = weight, the following top three critical risks were identified:

- **Unauthorized Access (SRI = 4.6)** – Requires multi-factor authentication and RBAC.
- **Data Breach (SRI = 4.4)** – Mitigated through AES-256 encryption and blockchain logging.
- **Interoperability Failures (SRI = 4.1)** – Addressed with standardized APIs (HL7/FHIR).

E. Discussion

The results demonstrate that implementing the proposed framework improves healthcare cloud security posture, particularly when applied to **private** or **hybrid** deployment models. However, the findings also reveal that **compliance and interoperability** remain persistent challenges, requiring both technical and policy-level interventions.

In practice, the success of secure healthcare cloud adoption depends on:

- **Tailored Security Architecture** – Adapting controls to specific workloads and regulatory contexts.
- **Continuous Monitoring and Auditing** – Regular penetration testing, vulnerability scanning, and log analysis.
- **Staff Training** – Educating healthcare personnel on security best practices to reduce human-error-induced breaches.

The framework's flexibility allows its application in diverse healthcare settings, from small clinics to large hospital networks, enabling risk-aware decision-making for cloud adoption.

V. CONCLUSION AND FUTURE WORK

Cloud computing has emerged as a transformative technology in the healthcare sector, offering scalable storage, advanced computational capabilities, and improved accessibility to medical resources. However, the migration of sensitive healthcare data to cloud environments introduces critical security, privacy, and compliance challenges.

This research proposed a multi-phase risk assessment and mitigation framework to systematically identify threats, quantify their impact using a Security Risk Index (SRI), evaluate their distribution across different deployment and service models, and implement layered security controls. The application of this framework revealed that private cloud deployments offer the highest security scores due to dedicated infrastructure and restricted access, while hybrid clouds present a balanced compromise between scalability and data protection. Public clouds, although cost-effective, require substantial supplementary security measures to meet healthcare compliance standards.

Key findings indicate that the top security risks—unauthorized access, data breaches, and interoperability failures—can be mitigated effectively through a combination of AES-256 encryption, multi-factor authentication, role-based access

DOI:10.15680/IJARETY.2025.1204079

control (RBAC), blockchain-based audit trails, and adherence to standardized healthcare data exchange protocols such as HL7 and FHIR.

From a strategic perspective, the SWOT analysis suggests that the strengths and opportunities of adopting cloud computing in healthcare outweigh the weaknesses and threats, provided that robust governance policies, continuous monitoring, and staff training are in place.

VI. FUTURE WORK

While the proposed model offers a structured approach to securing healthcare cloud environments, further research is necessary to enhance its applicability:

- Real-world Validation – Deploy the framework in operational healthcare networks and evaluate its performance under live threat scenarios.
- AI-Driven Threat Detection – Integrate machine learning models for real-time anomaly detection and predictive threat analysis.
- Cross-Border Compliance Framework – Develop standardized policies for handling healthcare data in multi-jurisdictional cloud environments.
- Homomorphic Encryption and Zero-Trust Models – Investigate the feasibility of privacy-preserving computation on encrypted healthcare data and zero-trust architectures in clinical workflows.
- Economic Impact Analysis – Evaluate the cost-benefit trade-offs of implementing advanced security measures across different cloud deployment models.

By addressing these areas, the healthcare sector can leverage cloud computing not only as an enabler of operational efficiency and patient care but also as a secure, resilient, and compliant data infrastructure.

REFERENCES

1. Y. Al-Issa, M. A. Ottom, and A. Tamrawi, “eHealth Cloud Security Challenges: A Survey,” Journal of Healthcare Engineering, vol. 2019, Article ID 7516035, Sep. 2019.
2. M. K. H. Mu-Hsing Kuo, “Opportunities and Challenges of Cloud Computing to Improve Health Care Services,” Journal of Medical Internet Research, vol. 13, no. 3, e67, 2011.
3. Y. Al-Issa et al., “eHealth Cloud Security Challenges: A Survey,” Journal of Healthcare Engineering, 2019. (also relevant to introduction context)
4. “Cloud computing security,” Wikipedia, updated recently, provides detailed discussions on virtualization risks, multi-tenancy, and shared responsibility models.
5. Gholami and E. Laure, “Security and Privacy of Sensitive Data in Cloud Computing: A Survey of Recent Developments,” arXiv preprint, Jan. 2016.
6. J. Sen, “Security and Privacy Issues in Cloud Computing,” arXiv preprint, Mar. 2013.
7. G. Somani et al., “DDoS Attacks in Cloud Computing: Issues, Taxonomy, and Future Directions,” arXiv preprint, Dec. 2015.
8. Y. Kacha and A. Zitouni, “An Overview on Data Security in Cloud Computing,” arXiv preprint, Dec. 2018.
9. “Analysis of the security and privacy requirements of cloud-based electronic health records systems,” PubMed, provides an assessment of EHR-specific cloud security needs (role-based access, encryption, certifications like ISO 27001, FISMA).
10. “Security challenges and solutions using healthcare cloud computing – PubMed,” which emphasizes cloud issues like data confidentiality, integrity, availability, and solutions like encryption, authentication, APIs.
11. “A scoping review of cloud computing in healthcare,” BMC Medical Informatics and Decision Making, outlines concerns over data privacy, trust, standardization, encryption, audit trails, and SLAs in healthcare cloud adoption.
12. “Top 10 takeaways from the new HIPAA Security Rule NPRM,” Reuters, summarizing proposed 2025 HIPAA updates including mandatory MFA, encryption, risk assessments, and vendor oversight.

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975 Impact Factor: 8.152

www.ijarety.in editor.ijarety@gmail.com