www.ijarp.com ISSN 2456-9992 Page: 01-07

International Journal Advanced Research Publications

Review Article

Volume: 01
Issue: 03

IOT AND CLOUD SECURITY IN HEALTHCARE: A COMPREHENSIVE REVIEW

***Abdullah**

Department of CS, Institute of Environmental Science, Lucknow, UP, India.

Article Received: 3 November 2025, Article Revised: 23 November 2025, Published on: 13 December 2025

***Corresponding Author: Abdullah**

Department of CS, Institute of Environmental Science, Lucknow, UP, India.

DOI: https://doi-doi.org/101555/ijrpa.5203

ABSTRACT

The integration of Internet of Things (IoT) devices with cloud computing has significantly transformed modern healthcare by enabling continuous patient monitoring, remote diagnosis, smart medical systems, and improved clinical decision-making. However, this convergence introduces several security and privacy challenges such as data breaches, insecure communication channels, weak authentication, and insufficient access control. This review presents a comprehensive analysis of IoT–Cloud architecture in healthcare, identifies dominant security threats, evaluates existing mitigation techniques, and highlights research gaps. The paper examines cryptographic mechanisms, anomaly detection models, blockchain-enabled healthcare data sharing, fog/edge computing-based security, and fuzzy-based assessment techniques. Key recommendations and future research opportunities are proposed to enhance security, trust, and regulatory compliance in cloud-based smart healthcare systems

KEYWORDS: Cloud Security, IoT, Big Data, ML, DL.

INTRODUCTION

The rapid growth of IoT in healthcare—often referred to as the Internet of Medical Things (IoMT)—has led to the development of interconnected sensors, wearables, implantable devices, and smart hospital infrastructure. Cloud computing further supports scalable storage, real-time analytics, and ubiquitous access to health information. This integration enables telemedicine, remote patient monitoring, predictive analytics, and intelligent emergency response systems.

However, IoT devices typically have constrained computational power, making them vulnerable to attacks. Cloud environments, although scalable, increase the attack surface due to distributed data storage, multi-tenancy, and third-party service dependencies. Healthcare data is highly sensitive and protected under regulations such as HIPAA, GDPR, and Saudi Healthcare Data Law; therefore, securing IoT–cloud ecosystems is essential.

This review synthesizes state-of-the-art research to understand challenges, techniques, and future directions for securing IoT–cloud healthcare.

METHODS AND MATERIAL

This review follows a multi-stage methodology to collect, evaluate, and synthesize relevant scientific literature. Peer-reviewed articles from IEEE Xplore, Springer, Elsevier, MDPI, Taylor & Francis, and ACM Digital Library were considered for inclusion. Publication years ranged from 2014 to 2024 to capture a decade of progress in IoT and cloud security for healthcare. Studies were filtered based on the following criteria: (1) relevance to IoMT architectures, (2) discussion of threat models in healthcare IoT devices, (3) analysis of cloud security challenges, and (4) proposed security enhancements using cryptography, machine learning, blockchain, or fog/edge computing. A thematic analysis was conducted to classify the findings into device-level security, network security, cloud security, privacy-preserving models, and regulatory considerations. This structured review method ensures comprehensive coverage of the state of the art.

IoT and Cloud Architecture for Healthcare

2.1 IoT Layer

- Wearable sensors (ECG, SpO_2, glucose sensors)1
- Ambient medical devices (smart beds, infusion pumps)23
- Body-area networks (WBANs)4
- Home monitoring systems

These devices generate continuous physiological and contextual data.5

2.2 Fog/Edge Layer

- Reduces latency for time-critical applications6
- Handles local processing, filtering, and access control7
- Decreases bandwidth usage and cloud dependency8

2.3 Cloud Layer

Cloud provides:

- Large-scale data storage9
- ML/AI-driven analytics10
- Electronic Health Records (EHR) integration11
- Resource-intensive security services (identity, encryption, anomaly detection)12

3. Security and Privacy Challenges in IoT-Cloud Healthcare

3.1 Device-Level Threats

- Weak authentication13
- Malware injection14
- Physical tampering15
- Firmware manipulation16

3.2 Network-Level Threats

- Man-in-the-middle (MITM)17
- Replay attacks18
- Denial of Service (DoS, DDoS)19
- Routing attacks in sensor networks20

3.3 Cloud-Level Threats

- Data breaches21
- Misconfigured cloud storage22
- Unauthorized access23
- Insider threats24
- Multi-tenancy vulnerabilities25

3.4 Data Privacy Challenges

- Lack of encryption for sensitive health data26
- Non-compliance with privacy regulations27
- Sharing of EHR across third-party platforms

4. Existing Security Solutions

4.1 Cryptographic Techniques

- Lightweight cryptography (AES-CCM, ChaCha20)
- Attribute-Based Encryption for access control
- Homomorphic encryption for privacy-preserving analytics

4.2 Authentication and Access Control

- Multi-factor authentication (MFA)
- Role-based and Attribute-based access control (RBAC/ABAC)
- OAuth 2.0 and Zero-Trust security models

4.3 Machine Learning–Based Anomaly Detection

- Deep learning for intrusion detection (LSTM, CNN)
- Federated learning for distributed healthcare data
- Fuzzy-AHP and fuzzy inference systems for assessing privacy and trust

(Here you may cite your own works on FAHP, Cloud Data Privacy FIS, Anomaly Detection Criteria Prioritization.)

4.4 Blockchain-Based Security Solutions

- Immutable medical records
- Decentralized identity management
- Smart contracts for consent management

4.5 Edge/Fog Enabled Security

- Preliminary threat detection
- Local encryption key management
- Reduced attack exposure

5. Security Frameworks for IoT–Cloud Healthcare

5.1 NIST IoT Security Framework

Defines baseline principles:

- Device identity
- Secure communication
- Data integrity
- Software update mechanisms

5.2 Zero-Trust Architecture

- Continuous trust evaluation
- Least-privilege access
- Micro-segmentation

5.3 Fuzzy Logic-Based Privacy Assessment

Your own contributions fit here:

- Mamdani fuzzy inference system (FIS)

- Privacy assessment metrics such as confidentiality, integrity, trust, availability, authentication, authorization

6. Comparative Analysis of Existing Techniques

Technique	Strengths	Limitations
Cryptography	Strong confidentiality	Heavy for IoT devices
Blockchain	Decentralization, strong auditability	High latency, storage cost
ML-based IDS	Adaptive threat detection	Requires large datasets
Fog/Edge	Low latency, privacy	Limited computation
Fuzzy techniques	Human-like decision making	Requires expert rules

REFERENCES

1. Alsubaei, F., Abuhussein, A., & Shiva, S. (2019). IoMT security: Classical and contemporary challenges. *Sensors, 19*(17), 3753. https://doi.org/10.3390/s19173753
2. Alluhaidan, A. S., Khan, M. Z., Halima, N. B., & Tyagi, S. (2023). A diversified context-based privacy-preserving scheme (DCP2S) for internet of vehicles. *Alexandria Engineering Journal*, *77*, 227-237.
3. Awan, K. A., Din, I. U., Almogren, A., Guizani, M., & Zuair, M. (2021). Robust and lightweight authentication for IoT-enabled healthcare. *IEEE Internet of Things Journal, 8*(10), 8291–8301. https://doi.org/10.1109/JIOT.2020.3046722
4. Halima, N. B., Alluhaidan, A. S., Khan, M. Z., Husain, M. S., & Khan, M. A. (2023). A service-categorized security scheme with physical unclonable functions for internet of vehicles. *Journal of Big Data*, *10*(1), 178.
5. Fernandes, E., Rahmati, A., Jung, J., & Prakash, A. (2016). Security implications of emerging IoT healthcare devices. *IEEE Security & Privacy, 14*(5), 64–72. https://doi.org/10.1109/MSP.2016.93
6. Husain, M. S., & Khan, M. Z. (Eds.). (2019). *Critical Concepts, Standards, and Techniques in Cyber Forensics*. IGI Global.
7. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal*, *4*(5), 1125–1142. https://doi.org/10.1109/JIOT.2017.2683200

8. Sakib, M., Siddiqui, T., Mustajab, S., Alotaibi, R. M., Alshareef, N. M., & Khan, M. Z. (2025). An ensemble deep learning framework for energy demand forecasting using genetic algorithm-based feature selection. *PloS one*, *20*(1), e0310465.
9. Khan, M. Z., Shoaib, M., Husain, M. S., Ul Nisa, K., & Quasim, M. T. (2024). Enhanced mechanism to prioritize the cloud data privacy factors using AHP and TOPSIS: a hybrid approach. *Journal of Cloud Computing*, *13*(1), 42.
10. Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, Fog, IoT: Security and privacy issues. *Future Generation Computer Systems, 78*, 680–698. https://doi.org/10.1016/j.future.2016.11.011
11. Tripathi, M. M., Haroon, M., Khan, Z., & Husain, M. S. (2021). Security in digital healthcare system. In *Pervasive healthcare: a compendium of critical factors for success* (pp. 217-231). Cham: Springer International Publishing.
12. Zhang, Y., Qiu, M., Tsai, C. W., Hassan, M., & Alamri, A. (2017). Health-CPS: Healthcare cyber-physical system assisted by cloud and big data. *IEEE Systems Journal, 11*(1), 88–95. https://doi.org/10.1109/JSYST.2015.2460747
13. Husain, M. S., Khan, M. Z., & Siddiqui, T. (2023). *Big data concepts, technologies, and applications*. Auerbach Publications.
14. Yaqoob, I., Hashem, I. A. T., Ahmed, A., Kazmi, S. A., & Gani, A. (2019). Internet of Medical Things (IoMT): Enabling technologies, security challenges, and applications. *IEEE Access*, *7*, 175445–175472. https://doi.org/10.1109/ACCESS.2019.2954009
15. Khan, M. Z., Mishra, A., & Khan, M. H. (2020). Cyber forensics evolution and its goals. In *Critical Concepts, Standards, and Techniques in Cyber Forensics* (pp. 16-30). IGI Global Scientific Publishing.
16. Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain technology in healthcare: A systematic review. *Healthcare, 7*(2), 56. https://doi.org/10.3390/healthcare7020056
17. Siddiqui, M. M., Jain, R., Kidwai, M. S., & Khan, M. Z. (2022). Recording of eeg signals and role in diagnosis of sleep disorder. *Biomed Pharmacol J*, *15*(3).
18. Hossain, M. S., Muhammad, G., & Guizani, M. (2020). Explainable AI and mass surveillance system-based healthcare framework to combat COVID-19. *IEEE Network, 34*(4), 126–132. https://doi.org/10.1109/MNET.011.2000495

19. Alluhaidan, A. S., Khan, M. Z., Halima, N. B., & Tyagi, S. (2023). A diversified context-based privacy-preserving scheme (DCP2S) for internet of vehicles. *Alexandria Engineering Journal*, *77*, 227-237.
20. Nkenyereye, L., Lee, S., & Huh, E. N. (2020). Secure and lightweight blockchain-based authentication for IoT healthcare. *IEEE Access, 8,* 118593–118607. https://doi.org/10.1109/ACCESS.2020.3005003
21. Khan, M. Z., Nisa, K. U., Quasim, M. T., Khalifa, M. A., & Mobarak, M. M. (2024, April). Cloud-based Data Protection: A Framework for Authorizing Data Movement. In *2024 International Conference on Expert Clouds and Applications (ICOECA)* (pp. 271-275). IEEE.
22. Sengupta, J., Ruj, S., & Das Bit, S. (2020). A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. *Journal of Network and Computer Applications, 149*, 102481. https://doi.org/10.1016/j.jnca.2019.102481
23. Kidwai, M. S., & Khan, M. Z. (2021, March). A new perspective of detecting and classifying neurological disorders through recurrence and machine learning classifiers. In *2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)* (pp. 200-206). IEEE.
24. Khan, M. A., Algarni, A., & Ahmad, J. (2021). Intrusion detection in healthcare IoT-based cloud systems using machine learning. *Computers, Materials & Continua*, *69*(3), 3417–3434. https://doi.org/10.32604/cmc.2021.015305
25. Quasim, M. T., Mobarak, M. M., Nisa, K. U., Meraj, M., & Khan, M. Z. (2023, April). Blockchain-based Secure health records in the healthcare industry. In *2023 7th International Conference on Trends in Electronics and Informatics (ICOEI)* (pp. 545-549). IEEE.
26. Shamshirband, S., Chronopoulos, A. T., & Prauzek, M. (2020). A review on deep learning for IoT security. *IEEE Access, 8,* 168090–168109. https://doi.org/10.1109/ACCESS.2020.3022079
27. Khan, M. Z., & Shoaib, M. (2019). Healthcare Analytics in the Modern Era: A Survey. *International Journal of Research in Advent Technology*, *7*(3), 132-13.