ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed, Open Access Journal
2025, Volume 6 Issue 3
www.ijisea.org

Secure Medical IoT Data Handling in Cloud with Smart Health Insights and Public Verification

Shaik Khudan[1], K. Lakshmana Reddy[2]

[1,2]Department Master of Computer Application(MCA), SVKP & Dr KS Raju Arts & Science College(A), Penugonda, W.G.Dt., A.P India,
khudanshaikoff@gmail.com[1], klreddyin@gmail.com[2]

ABSTRACT

In our increasingly interconnected world, the intersection of healthcare and technology is becoming more pronounced, particularly with the rise of the Internet of Things (IoT) in medical applications. This publication titled "Secure Medical IoT Data Handling in Cloud with Smart Health Insights and Public Verification" presents a compelling exploration of how we can safeguard sensitive health data while harnessing the immense potential of cloud computing to deliver smart health insights. As we delve into this critical topic, it becomes clear that the security and privacy of medical data are paramount. With the proliferation of IoT devices in healthcare settings, there is a pressing need for robust protocols that not only ensure data integrity but also facilitate seamless access for medical professionals and patients alike. The article highlights innovative strategies that leverage cloud technologies to enhance data security while maintaining usability. One of the key takeaways from this work is the emphasis on public verification mechanisms. By integrating transparent verification processes, we can empower patients and stakeholders to trust that their health information is being handled responsibly. This approach fosters a collaborative environment where users can actively engage with their health data, leading to improved health outcomes through informed decision making. Moreover, the fusion of smart health insights derived from IoT data can revolutionize patient care. By analyzing patterns and trends within large datasets, healthcare providers can gain invaluable insights that drive personalized treatment plans and proactive interventions. This not only enhances patient care but also optimizes resource allocation within healthcare systems. In conclusion, the exploration presented in this publication serves as a crucial step towards addressing the dual challenges of data security and patient empowerment in the realm of medical IoT. As we continue to advance technologically, it is imperative that we prioritize ethical considerations and robust security measures to ensure that technology serves as a force for good in healthcare. This article not only raises important questions about our current practices but also initiates a dialogue on how we can move forward responsibly. As we reflect on these findings, let us strive to create a future where technology not only innovates but also safeguards our most personal health information.

Keywords: Internet of Medical Things (IoMT), Cloud Computing, Secure Healthcare Data Management, Public Verifiability, Smart Healthcare, Data Privacy and Security, AES Encryption, RSA Cryptography, Role-Based Access Control (RBAC), Real-Time Health Monitoring, Data Integrity, Privacy-Preserving Authentication.

I. INTRODUCTION

In an era where technology is increasingly interwoven with healthcare, the rise of the Internet of Things (IoT) has transformed the way we collect, analyze, and utilize medical data. The integration of IoT devices in medical settings offers unprecedented opportunities for enhancing patient care and

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed, Open Access Journal
2025, Volume 6 Issue 3
www.ijisea.org

streamlining healthcare processes. However, with these advancements come significant challenges, particularly in ensuring the security and privacy of sensitive health information.

Our project, "Secure Medical IoT Data Handling in Cloud with Smart Health Insights and Public Verification," addresses these challenges head-on. As we delve deeper into the realm of connected medical devices, it becomes imperative to establish robust frameworks that not only protect patient data but also foster trust among users and stakeholders.

The foundation of our approach lies in developing a secure architecture that safeguards medical IoT data stored in the cloud. By employing advanced encryption techniques, we aim to ensure that patient information remains confidential and is accessible only to authorized personnel. Additionally, our focus on public verification mechanisms provides a layer of transparency that empowers patients to take control of their health data.

Moreover, our project seeks to harness smart health insights derived from analyzing real-time data collected from IoT devices. These insights can lead to predictive analytics that not only enhance clinical decision-making but also facilitate personalized medicine tailored to individual patients' needs.

As we embark on this journey, we invite collaboration from healthcare professionals, technology experts, and researchers alike. Together, we can pave the way for a future where secure medical data handling is not just a necessity but a standard practice in the healthcare landscape.

In summary, this project represents a significant step towards bridging the gap between innovative technology and secure healthcare delivery. By prioritizing both security and insightful analytics, we are committed to fostering an ecosystem where patients feel safe and empowered in their health journeys.

II. LITERATURE SURVEY

1. IoMT Security and Privacy Mechanisms
Author: R. H. Khan, M. Salah
Title: IoT Security: Review, Blockchain Solutions, and Open Challenges
This paper presents a comprehensive review of security challenges in IoT, emphasizing medical devices and it discusses blockchain as a promising technology to enhance data integrity and privacy, which aligns with our goal of public verifiability in smart healthcare systems.

2. Cloud-Centric Architectures for Smart Healthcare
Author: S. Sharma, A. Singh
Title:Cloud-Based Healthcare Framework for Real-Time Health Monitoring
The authors propose a cloud-based architecture to support real-time health data collection and analysis from IoMT devices. Their work highlights scalability and data management but lacking in detailed mechanisms for ensuring end-to-end security.

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed, Open Access Journal
2025, Volume 6 Issue 3
www.ijisea.org

3. Lightweight Cryptographic Techniques in IoMT
Author: Y. Zhang, J. Liu
Title:Lightweight Encryption Algorithms for Resource-Constrained IoT Devices
This study explores lightweight encryption schemes suitable for devices with limited computational resources, making it relevant for securing IoMT devices without compromising performance, a key focus in our proposed system.

4. Public Verifiability in Cloud Storage
Author: B. Wang, S. Yu
Title: Public Auditing for Secure Cloud Storage with Efficient Privacy-Preserving Techniques
The authors introduce a public auditing protocol that enables third-party verification of cloud-stored data without exposing sensitive information. Their cryptographic approach inspired our system's public verifiability feature to enhance transparency and trust.

III. METHODOLOGY

The methodology of this project focuses on building a cloud-based smart healthcare system that utilizes Internet of Medical Things (IoMT) devices to monitor patient health data securely and efficiently. The system is designed to collect sensitive health data from wearable or embedded medical devices and transmit it in real-time to a centralized cloud server for analysis, storage, and decision-making. The core objectives are to ensure data confidentiality, integrity, access control, and public verifiability of the data shared between patients, medical professionals, and authorized third parties.

The process begins with IoMT devices collecting real-time data such as heart rate, blood pressure, glucose level, etc. This data is then encrypted at the device or gateway level before transmission. The cloud infrastructure handles secure storage and offers analytical services such as predictive diagnostics or alerts based on threshold breaches. A public verifiability mechanism is integrated using cryptographic proofs, which allows third parties (e.g., auditors or insurance providers) to verify the authenticity of the data without compromising privacy. The system also includes secure login and access management features for doctors and patients using role-based access control (RBAC). All modules communicate through secure REST APIs implemented in Java, ensuring robust integration and encryption over HTTPS.

IV. ALGORITHMS FOR PROPOSED METHODLOGY

To ensure secure transmission, storage, and verifiability of health data, the system employs a hybrid of cryptographic algorithms and authentication techniques. At the data encryption level, AES (Advanced Encryption Standard) is used for encrypting health records locally at the device or gateway before being uploaded to the cloud. AES provides fast and strong symmetric encryption suitable for real-time data processing in resource-constrained devices.

For secure key exchange and identity verification, RSA (Rivest–Shamir–Adleman) is utilized. RSA helps in securely sharing AES session keys between devices and the cloud, ensuring that even if data transmission is intercepted, the data remains unreadable. Furthermore, digital signatures based on RSA

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed, Open Access Journal
2025, Volume 6 Issue 3
www.ijisea.org

or Elliptic Curve Digital Signature Algorithm (ECDSA) are used to enable public verifiability. Each encrypted data block can be signed by the data originator (e.g., IoMT device or medical gateway), where the signature can be verified by third parties without revealing the actual data content.

To prevent unauthorized access, the system uses Role-Based Access Control (RBAC) enforced by Java-based middleware. Users are assigned specific roles (e.g., patient, doctor, admin, auditor), and each role is mapped to permissions on what data they can access or verify. Additionally, SHA-256 hashing is applied to ensure data integrity, enabling both the server and third parties to detect tampering or data loss.

System Architecture

The system architecture follows a three-tier cloud-centric model: IoMT Device Layer, Cloud Processing Layer, and Application & Verifiability Layer.

IoMT Device Layer:

This layer comprises sensors and medical devices deployed at the patient's end. These devices continuously monitor health parameters and send data to a local edge/gateway device. The gateway preprocesses the data, encrypts it using AES, and then encrypts the AES key using the public RSA key of the cloud. Java-based embedded code or Android SDKs are used for device-side development.

Cloud Processing Layer:

The encrypted health data and AES key are transmitted to the cloud, where the server decrypts the AES key using its RSA private key and stores the decrypted data. The cloud also runs predictive models or alert mechanisms for healthcare providers. Data is organized and stored securely in a relational database (e.g., MySQL or PostgreSQL) and protected using authentication tokens and SSL connections. REST APIs, developed in Java (e.g., using Spring Boot), serve as the backbone of this layer.

Application & Verifiability Layer:

The top layer consists of user interfaces (web portals or mobile apps) for patients, doctors, and third-party verifiers. Role-based access is enforced, and public verifiability is enabled using digital signatures and hash-based proofs. Auditors or insurers can verify the source and integrity of medical data without accessing the raw contents. This layer uses cryptographic libraries in Java for signing and verification, and displays real-time dashboards for users.

V. SYSTEM ANALYSIS

The proposed cloud-centric IoMT-enabled smart healthcare system is carefully analyzed to ensure it meets critical requirements for security, efficiency, and scalability. By employing lightweight encryption and authentication methods, the system secures sensitive medical data while accommodating the limited computational capabilities of IoMT devices. The integration of public verifiability through advanced cryptographic techniques enhances trust by enabling patients and third parties to independently verify data integrity without compromising privacy. Leveraging cloud infrastructure provides scalable storage and real-time data processing, ensuring responsiveness even

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed, Open Access Journal
2025, Volume 6 Issue 3
www.ijisea.org

with a growing number of connected devices. Additionally, the system's support for standardized protocols promotes interoperability across diverse medical devices and healthcare platforms. Overall, this analysis demonstrates that the proposed solution effectively balances robust security, high performance, and user trust, addressing key challenges faced by existing healthcare systems.

a. Problem Definition

The increasing adoption of Internet of Medical Things (IoMT) devices in healthcare generates vast amounts of sensitive patient data which requires secure and efficient management. Existing healthcare systems face significant challenges in protecting this data due to the limited computational resources of IoMT devices, which restrict the implementation of strong security protocols. Additionally, most current solutions lack mechanisms for public verifiability, making it difficult for patients and authorized parties to independently confirm the integrity and authenticity of stored medical records.

b. Feasibility Study

Technical Feasibility:

The proposed system leverages existing cloud computing platforms and lightweight cryptographic algorithms, which are mature and widely supported technologies. IoMT devices with sufficient processing capabilities are increasingly available, enabling implementation of efficient encryption and authentication mechanisms. Standardized communication protocols facilitate interoperability among heterogeneous devices. Thus, from a technical standpoint, the system can be developed and deployed using current technology.

Economic Feasibility:

Cloud infrastructure reduces the need for expensive on-premise hardware and maintenance costs, making the system cost-effective for healthcare providers. Lightweight security algorithms minimize power consumption, thereby prolonging device life and reducing replacement costs. The benefits of improved data security, real-time monitoring, and enhanced trust can lead to better patient outcomes and potentially lower healthcare costs, justifying the investment.

Operational Feasibility:

The system is designed to integrate smoothly with existing healthcare workflows, providing userfriendly interfaces for patients, providers, and auditors. Public verifiability increases transparency and trust, facilitating regulatory compliance and user acceptance. Training requirements are manageable, and ongoing support can be streamlined through cloud service providers.

Legal and Ethical Feasibility:

By incorporating privacy-preserving cryptographic techniques, the system aligns with healthcare data protection regulations such as HIPAA and GDPR. Public verifiability is implemented without compromising patient confidentiality, addressing ethical concerns related to data sharing and transparency.

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed, Open Access Journal
2025, Volume 6 Issue 3
www.ijisea.org

VI. RESULTS AND DISCUSSION



Figure 1: Shows All the Screen Shots of the Proposed Methodology

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed, Open Access Journal
2025, Volume 6 Issue 3
www.ijisea.org

VII. CONCLUSION

In this paper, we propose a secure and efficient cloud-centric smart healthcare system that leverages the Internet of Medical Things (IoMT) for real-time health monitoring and data management. To meet the growing demand for scalable and reliable healthcare, the system integrates cloud computing for storage and processing, enabling the handling of large volumes of medical data from IoMT devices. Lightweight security protocols are employed to safeguard sensitive patient information while respecting the resource limitations of medical devices, ensuring reliable and continuous operation. A key contribution of this work is the implementation of public verifiability, allowing patients and authorized parties to independently verify the integrity and authenticity of healthcare data stored in the cloud without compromising privacy. This enhances transparency, trust, and compliance with regulatory standards. Advanced cryptographic techniques further ensure data privacy and provide strong protection against tampering or unauthorized access.

VIII. FUTURE WORK

1. Integration of AI and Machine Learning

Future enhancements will incorporate AI/ML algorithms to enable predictive analytics and personalized care. These technologies will analyze real-time IoMT data to detect early health anomalies and facilitate timely, proactive treatments.

2. Adaptive Lightweight Security Protocols

Implementing dynamic, lightweight security measures will enhance protection based on device capabilities and network conditions, ensuring efficient threat response.

3. Efficient Blockchain and Distributed Ledger Technologies

Integrating lightweight blockchain will ensure data integrity and public verifiability with minimal overhead, enabling secure, real-time healthcare operations.

4. Standardization and Interoperability

Defining universal IoMT standards will enable seamless system integration, boosting adoption and enhancing care coordination.

5. Real-World Deployment and Validation

Clinical pilot trials are essential to validate performance, security, and usability, providing feedback to refine the system for practical healthcare use.

REFERENCES :

[1] R. H. Khan and M. Salah, “IoT Security: Review, Blockchain Solutions, and Open Challenges,” Future Generation Computer Systems, vol. 82, pp. 395–411, 2018.

[2] S. Sharma and A. Singh, “Cloud-Based Healthcare Framework for Real-Time Health Monitoring,” IEEE Access, vol. 7, pp. 101938–101948, 2019.

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed, Open Access Journal
2025, Volume 6 Issue 3
www.ijisea.org

[3] Y. Zhang and J. Liu, "Lightweight Encryption Algorithms for Resource-Constrained IoT Devices," Journal of Network and Computer Applications, vol. 120, pp. 115–129, 2018.
[4] B. Wang and S. Yu, "Public Auditing for Secure Cloud Storage with Efficient Privacy-Preserving Techniques," IEEE Transactions on Cloud Computing, vol. 6, no. 3, pp. 833–846, 2018.

[5] K. Lee and M. Kim, "Blockchain-Based Secure Data Sharing for Smart Healthcare Systems," IEEE Access, vol. 8, pp. 69015–69026, 2020.
[6] A. R. Al-Ali et al., "An Efficient Security Framework for Internet of Medical Things in Smart Cities," IEEE Internet of Things Journal, vol. 7, no. 5, pp. 4423–4432, May 2020.