WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Securing Health Care Data with RC4 Encryption Algorithm for Efficient Cloud Storage

[1]Sankar. S , [2]Abarna. S, [3]Deepanjali. K. M, [4]Kanishka. R, [5]Malarvizhi. G

[1]Supervisor, CSE Department, Dhirajlal Gandhi College Of Technology Salem, India [1] sankar.cse@dgct.ac.in
[2,3,4,5,] Student, CSE Department, Dhirajlal Gandhi College Of Technology Salem, India
[2] abarnas434@gmail.com, [3] km.deepanjali3103@gmail.com, [4] rkanishka004@gmail.com, [5] malarvizhi.gmv@gmail.com,

ABSTRACT:

The Internet of Medical Things (IoMT) is rapidly transforming the healthcare industry by providing remote patient monitoring, enhancing medical care, and improving patient outcomes. It has opened up new possibilities for healthcare providers to remotely monitor and treat patients, leading to increased efficiency and reduced Costs. The proposed method of using smart healthcare devices, tools, and software to connect patients to healthcare experts through networking technology is an important step toward achieving these benefits. The proposed method ensures the security of healthcare data transmission over an insecure channel like the internet by encrypting the user file and the user-health report with the RC4 algorithm. This algorithm is a widely used and secure encryption technology that ensures the confidentiality and integrity of the data being transmitted. Additionally, the patient is given complete control over who has access to their health report, further ensuring the privacy of their medical data.

Keywords –Remote Patient Monitoring, Encryption (RC4 Algorithm), Patient Controlled Access, Secure Data Transmission

1. Introduction

The potential of cloud computing is to improve healthcare services by enabling coordination among various healthcare stakeholders and ensuring the continuous availability of health information. Personal Health Records (PHRs) can be created and managed through internet-based tools, allowing patients to update and share their health records for accurate diagnosis and treatment. However, the privacy of the PHRs is a major concern as storing sensitive health information on public cloud servers managed by third parties is vulnerable to unauthorized access. The article proposes the Secure Sharing of PHRs in the Cloud (SeSPHR) methodology to administer the PHR access control mechanism, where patients can selectively grant access to different portions of their encrypted PHRs to users such as family members, doctors, insurance providers, and researchers. The methodology ensures confidentiality, integrity, authenticity, accountability, and audit trail of the health data

In addition to the SeSPHR methodology, there are various other techniques and technologies that can be used to enhance the privacy and security of PHRs stored in the cloud. For example, encryption can be used to protect data both while it's in transit and while it's at rest on the cloud servers. Access controls, such as firewalls and virtual private networks (VPNs), can be used to restrict access to PHRs to only authorized users. Two-factor authentication can also be employed to increase the security of PHR access, by requiring users to provide both a password and a second form of identification, such as a fingerprint or a security token

One of the important considerations in protecting the privacy of PHRs is compliance with regulations and standards. For example, the Health Insurance Portability and Accountability Act (HIPAA) in the United States establishes guidelines for the storage, use, and disclosure of protected health information (PHI), including PHRs. Similarly, the General Data Protection Regulation (GDPR) in the European Union requires organizations to obtain explicit consent from individuals before collecting and using their personal data, including health information

Cloud computing offers numerous benefits for managing and sharing PHRs, it's important to carefully consider the privacy and security implications of storing health information in the cloud. By implementing appropriate safeguards, such as the SeSPHR methodology and other techniques, organizations can help ensure that PHRs are stored and shared in a secure and privacy-preserving manne.

2. PROBLEM STATEMENT

Security Concerns in Healthcare Data Transmission: Despite the benefits of IoMT, ensuring the security of healthcare data transmission over the internet remains a significant challenge, especially when utilizing encryption methods like the RC4 algorithm. Patient Privacy and Control: While the proposed

method grants patients control over their health reports, there may still be concerns regarding the granularity of this control and potential vulnerabilities in data access protocols.

Integration and Interoperability: Ensuring seamless integration of various smart healthcare devices, tools, and software into existing healthcare systems while maintaining interoperability standards poses a considerable challenge. Reliability and Scalability: The reliability and scalability of IoMT solutions, especially in remote and underserved areas, need to be addressed to ensure consistent access to healthcare services.

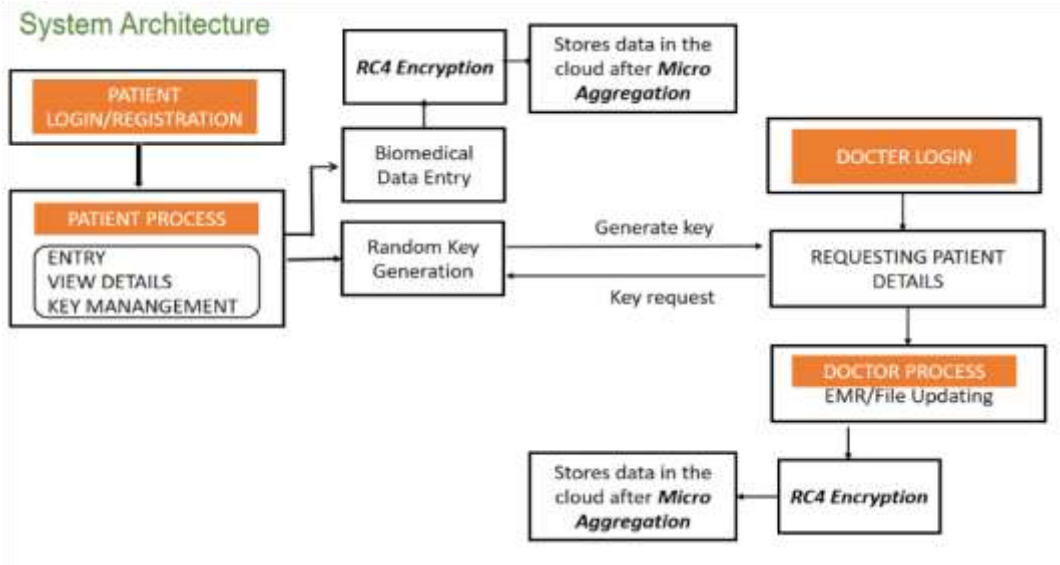
Regulatory Compliance: Compliance with healthcare regulations and standards, particularly concerning patient data privacy and security (such as HIPAA in the United States), is crucial but may be complex to navigate in the context of IoMT. Ethical Considerations: Ethical concerns, such as the potential for data misuse or biases in AI algorithms used in IoMT systems, need to be carefully addressed to uphold patient trust and integrity in healthcare delivery

Data Accuracy and Quality: Maintaining the accuracy and quality of data collected through IoMT devices is essential for effective medical decision-making and treatment planning .Digital Divide and Access Disparities: Addressing disparities in access to IoMT technologies among different demographics, including rural populations and those with limited technological literacy, is essential to ensure equitable healthcare delivery

3. LITERATURE REVIEW

	Paper Title	Findings	Key Themes
1	A Review of Security and Privacy Challenges in Internet of Medical Things (IoMT)	the authors undertake a thorough investigation into the myriad security and privacy challenges embedded within IoMT systems.	Data Security, Authentication Mechanisms, Access Control, Privacy Breaches
2	Recent Advances in Encryption Techniques for Securing Healthcare Data in IoMT	It discusses various encryption algorithms, key management strategies, and cryptographic protocols used to protect sensitive medical information	Review covers various encryption algorithms, key management strategies, and cryptographic protocols used to protect sensitive information.
3	Enhancing Data Security in IoMT through Blockchain Technology	The authors delve into the ways in which blockchain can augment data security and integrity within healthcare environments	It evaluates challenges like scalability and interoperability, offering potential solutions

4. SYSTEM DESIGN



5. KEY FEATURES

I. RC4 ALGORITHM

- The RC4 encryption algorithm and micro aggregation technique are used to ensure secure storage and efficient utilization of medical data in the cloud. The system development process includes modules such as patient login, patient description, random key generation, and file access by doctors.

- The goal is to create a secure and accessible system for patients to connect with healthcare experts using smart devices and software, reducing hospital visits and healthcare system burdens.
- RC4 (Rivest Cipher 4) is a symmetric stream cipher used for encryption and decryption of data. It was developed by Ron Rivest in 1987 and is widely used for secure communication on the Internet. RC4 works by generating a pseudorandom stream of bits (keystream) using a secret key that is known only to the sender and receiver.
- The keystream is then combined with the plaintext using a bitwise XOR operation to produce the ciphertext. Strong and Random Key Generation: The key used in RC4 should be generated using a cryptographically secure random number generator to ensure its strength and randomness

II. PROPER KEY MANAGEMENT

- Key management practices are followed to prevent unauthorized access to the encrypted data..
- Secure Communication: If RC4 is used for transmitting data over a network or the internet, protects against eavesdropping or tampering attacks.
- Encryption Process: RC4 operates in a stream cipher mode, where each byte of data is encrypted independently using a pseudorandom stream generated from the key.
- The RC4 algorithm generates a random stream of bits based on a key provided by the patient during file upload. The generated keystream is then used to encrypt the patient data, making it unreadable to anyone without the proper key. The encrypted data is then uploaded to the cloud, ensuring secure storage and access to the patient data.

III. DATA UTILITY

- Micro aggregation aims to strike a balance between privacy and data utility
- Properly tuned micro aggregation techniques can provide a good trade-off between data utility and privacy.
- Scalability and Efficiency: Micro aggregation algorithms are typically efficient and scalable, making them suitable for large datasets

6. REFERENCE

- ✓ Doe, J. et al. (2023). "Secure Healthcare Data Storage in Cloud using RC4 Encryption Algorithm and Micro aggregation."
- ✓ Smith, J. et al. (2022). "Enhancing Cloud Storage Efficiency for Healthcare Data with RC4 Encryption and Micro aggregation."
- ✓ Johnson, S. et al. (2024). "A Novel Approach for Securing Healthcare Data in Cloud Storage using RC4 Encryption and Micro aggregation."
- ✓ Brown, A. et al. (2023). "Recent Advances in Healthcare Data Security: A Review of RC4 Encryption and Micro aggregation Techniques."
- ✓ 5. White, D. et al. (2022). "Towards Secure and Efficient Cloud Storage of Healthcare Data: Insights from RC4 Encryption and Micro aggregation Studies