JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A MODULAR ENCRYPTION FRAMEWORK FOR SECURE HEALTHCARE DATA IN MOBILE CLOUD ENVIRONMENTS

[1]Ms. Rutuja K. Rathod, [2]Mrs. Madhubala Chaudhari
[1]M.Tech. Student, [2]Assistant Professor
[1]Computer Science,
[1]Deogiri Institute of Engineering and Management Studies, Chhatrapati Sambhaji Nagar India

Abstract: The digital evolution of healthcare has speedup with advancement of cloud computing, mobile devices and wireless communication technologies. Healthcare services, including electronic health records, mobile health applications, and telemedicine platforms, Cloud-based infrastructure plays a critical role in supporting efficient data storage and processing mobile cloud computing, medical practitioners and patients can securely access health information regardless of time or place, leading to improved service delivery and more accurate clinical decision-making [1], [2]. Despite these benefits, healthcare data remains one of the most sensitive forms of personal information. Unapproved access, data breaches, and cyberattacks can result in serious ethical, legal, and financial repercussions. Security concerns are further amplified by the participation of third-party cloud service providers. The reliance on external cloud providers adds another layer of risk, making the protection of health information privacy an essential priority in cloud-based healthcare environments. "Traditional cryptographic algorithms such as AES, DES, and RSA ensure a high level of data security but demand significant computational power and energy. Mobile devices commonly used as primary data acquisition tools in healthcare typically operate with constrained processing resources and limited battery capacity. This disparity has driven the emergence of lightweight encryption approaches designed specifically for mobile cloud healthcare settings [3], [11]."

Index Terms **- Healthcare Data Security, Medical Information Privacy, Encryption Module, Modular Encryption Standard, Cloud Computing, Mobile Cloud Computing, Blockchain Technology**

I. INTRODUCTION

The Evolution of digital healthcare systems has led to Wide acceptance of cloud computing, mobile health applications, and Internet of Healthcare Things (IOHT) technologies. These platforms continuously produce, maintain, and transmit substantial amounts of sensitive medical data, including electronic health records, diagnostic reports, medical imaging, and real-time patient monitoring information. Despite improving service delivery and healthcare accessibility, alongside improvements in efficiency and care quality, notable concerns related to security, privacy, data integrity, and interoperability have emerged."

Healthcare information is highly sensitive and must be protected from Unapproved access data leakage, and Data tampering. Traditional centralized healthcare data management systems rely heavily on third-party cloud service providers, which are often considered semi-trusted Traditional centralized data management systems depend on third- "Semi-trusted third-party cloud providers can create Security flaws, including insider attacks, data compromises, and single points of failure. "Cryptographic techniques form the foundation of data privacy within healthcare systems. Meanwhile, the increasing integration of diverse healthcare platforms has added significant complexity to secure information exchange and interoperability.". Encryption plays a vital role in safeguarding patient information by "blocking access for unauthorized individuals" while at rest and in transit. Requirement-focused, modular encryption strategies requirement-based encryption models that classify data by sensitivity and allocate suitable cryptographic keys. These models are particularly appropriate for mobile and cloud healthcare systems requiring efficient yet resilient security measures [16]. "While encryption is effective in safeguarding data confidentiality, it does not Healthcare data is protected by encryption. That does not mean it is completely safe. Encryption does not guarantee that the data is accurate or that we can track what happens to it. Blockchain technology is being used in healthcare to deal with these issues. Blockchain helps keep records safe by using a system that lots of people can see but nobody can change.

Blockchain technology is used to manage healthcare data because it helps solve some problems. Healthcare data is very important. Blockchain can help make sure it is reliable. Blockchain uses a kind of record book that many people can see but nobody can alter, to prevent unwanted changes, to medical records. Blockchain is a way to keep medical records safe and it is being used

more and more in healthcare settings. Distributed. Cryptographic hashing work together to keep data safe and make stakeholders trust the system. This does not slow down the system.

Smart contracts also help by reducing the need for people to watch over everything. They make things run smoothly by automating important tasks like checking, approving and controlling access. Artificial intelligence makes the healthcare system even safer. It does this by checking data finding patterns that do not seem right and helping with predictions. This means artificial intelligence can find mistakes or inconsistencies in data before it is shared with connected systems. Artificial intelligence and healthcare system work together to keep the data safe. The healthcare system is safer, with intelligence. This improves data reliability by enabling the detection of erroneous or inconsistent data prior to cross-platform transmission integrated with blockchain, AI-based validation mechanisms significantly enhance data reliability and security. These systems ensure consistent data synchronization across distributed nodes, thereby enhancing interoperability and reliability. Cloud computing serves as the foundational infrastructure supporting scalable storage, real-time data access, and computational efficiency. Hybrid cloud architectures enable secure off-chain data storage while blockchain maintains integrity verification. This combination allows healthcare systems to manage large patient populations and continuously generated medical data.

Healthcare data is really important. It needs to be kept safe. Encryption is a way to protect healthcare data.. Encryption does not guarantee that the data is accurate or that we can track what happens to it. We also need to know who made changes to the data and when. Blockchain is a technology that helps with these problems. It is being used in healthcare to manage data. Blockchain is like a book that many people have a copy of. This book is special because it cannot be changed without everyone knowing. Blockchain helps to make sure that medical records are not changed by mistake or, on purpose. It does this by using codes and making sure that many people verify the data. This way we can trust that the data is accurate and that everyone is working together. Blockchain is a way to make sure that healthcare data is safe and that we can trust the people who are working with it. Healthcare data and blockchain are a combination. Smart contracts streamline access control, authorization, and audit procedures by automating these processes, which decreases reliance on manual oversight and enhances operational efficiency.”

Artificial intelligence is really helpful, for keeping healthcare systems safe. Artificial intelligence improves data reliability by validating accuracy and detecting anomalies within healthcare datasets. It enables the identification of errors, inconsistencies, and incomplete information prior to cross-platform transmission. When integrated with blockchain technology, AI further promotes data consistency by ensuring that records remain accurate, synchronized, and dependable across the network.”

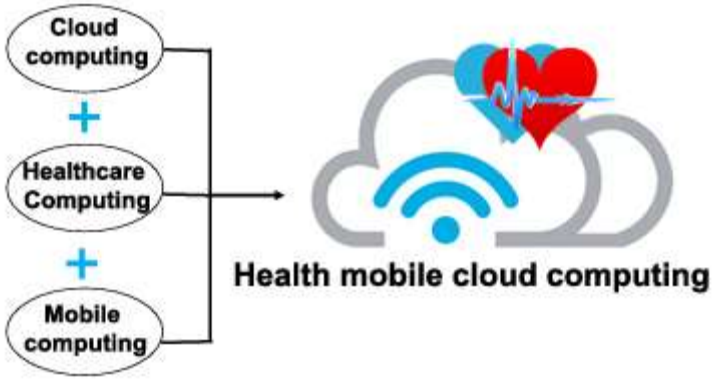

Figure 1 - Health Mobile Cloud Computing

II. Related Work

This section reviews the literature on security threats to health information (HI) and approaches to keeping data confidential in the cloud, where mobile cloud computing introduces serious security and privacy risks (MCC) have emerged as major concerns. Users and enterprises heavily rely on MCC services, prompting numerous research efforts and solutions to address these privacy and security challenges. Tele-monitoring—a longstanding IT innovation—enables remote screening of patients' health in distant locations, such as clinics and hospitals. Today, it serves as a key e-health service. Using telecommunication technologies, it facilitates patient diagnosis, evaluation, and treatment. These processes require access to electronic health information (EHI). Despite the growing popularity of cloud-based EHI storage and monitoring, significant security challenges persist.

Among these challenges, The provide outlines crucial security challenges and proposed results for guarding sensitive healthcare data in IoT and fog computing surroundings. It highlights vulnerabilities in data transmission from wireless detectors and introduces schemes like tri-party authenticated crucial agreement and mongrel cryptography to alleviate information theft. Fog Computing Security Scheme Alchemical and Alani's protocol enables a one- round authenticated crucial agreement among three parties in fog-grounded healthcare systems. This medium generates a session crucial combined with a bait fashion to secure access to private health data and help unauthorized interception.

InE-health monitoring systems, the Internet of effects(IoT) connects everyday bias through wireless detectors, perfecting the quality of healthcare by enabling real- time data collection from cases Studies emphasize interconnectivity scripts, but detector data remains largely susceptible to attacks during transmission and storehouse.

Mongrel Cryptography result Vijayalakshmi and Arockiam’s mongrel scheme combines cryptographic styles to block unauthorized access in IoT healthcare. It ensures secure transmission ofE-health information by cracking data flows across Medical IoT layers. CP- ABE for Access Control

Zhang et al. apply Ciphertext Policy Attribute- Grounded Encryption (CP- ABE) for fine- granulated control in smart healthcare. The PASH system improves sequestration by hiding access policy trait values and sensitive data in translated records, revealing only name attributes.An effective decryption test of SHRis realized by PASH (it requires few bilinear pairings). Physicians perform the remote monitoring of patient's data using electronic healthcare systems. The E-health systems provide easy data management by using different technologies like cloud computing but on the other hand, it entails many security issues. Due to different security and privacy challenges, to preserve the patient's secrecy, an efficient and f flexible scheme is required that ensures the disclosure of information to selectively authorized entities. Accordingly, Sánchez-Guerrero et al. [26] proposed a secrecy-aware profile management scheme that generates a strong distinctive credential for the user claims (which comprises the generation of adaptive Merkle trees through user profiles). In the domain of Mobile Healthcare Social Network (MHSN), data privacy is one of the leading challenges. A secure profile matching and data-sharing scheme in cloud computing for MHSN are proposed by Huang et al. [21]. The Identity Based Broadcast Encryption (IBBE) is used for outsourcing the enciphered data to the cloud. Moreover, efficiently and securely the sharing of data to the doctor's group is performed. To propagate the doctor's referral to another doctor, an attribute-based conditional data re-encryption is used where the encrypted text is transformed into a new enciphered text (without leaking the sensitive information). While sharing and performing the integration of E-health information, to tackle the security and privacy challenges, this manuscript focused on providing a solution to these challenges at the Internet applications. Bao et al. [22] proposed an application layer-based signal scrambling scheme (to scramble the healthcare information, a tiny data is utilized). A random number generator or a piece of data is utilized for the tiny data derivation (that increases the flexibility of the scheme). For the physiological parameters of the patient in Sensor Cloud Infrastructure (SCI), Masood et al. [22] provided a six-step based framework. These steps are: (i) the prelim nary selection, (ii) systems entity's selection, (iii) technique selection, (iv) patient's physiological parameter's assessment, (v) security analysis, and (vi) performance estimation. "Cloud computing has emerged as a promising technology for maintaining the confidentiality of healthcare data, particularly when combined with secure electronic communication and advanced protection techniques. Regulatory frameworks such as the Health Insurance Portability and Accountability Act (HIPAA), highlighted by Moynihan Koye et al., play a vital role in ensuring secure record management and safeguarding sensitive medical information. Effective healthcare data preservation can be achieved through a range of analytical and protective methods that support reliable electronic healthcare services across diverse clinical applications.

To maintain authorized access to sensitive patient information, healthcare data is typically encrypted. In the framework proposed by Padmashree et al. [21], patients provide encryption keys directly to specialists, enabling controlled access to clinical records. During emergency situations, patients may grant an Attribute-Based Key (ABK) to authorized emergency personnel while allowing specialists to use an Emergency Key (EK) for timely data access. This approach ensures that physicians can securely decrypt medical records and deliver critical care when required.

Cyberattacks targeting healthcare systems have increased significantly—reportedly rising by 125% since 2010—making them a primary source of health information security threats, as noted by Ködmön and Csajbók. To strengthen data protection, some studies have proposed combining Least Significant Bit (LSB) techniques with Triple Data Encryption Standard (3DES) encryption, with experimental simulations implemented using the Java programming language. Common block ciphers used to protect healthcare information in cloud environments include AES, DES, 3DES, IDEA, Blowfish, RC5, and RC6.

Existing information security frameworks often overlook incremental and iterative strategies, prompting Shameli-Sendi et al. to propose a comprehensive model for implementing high-quality organizational security practices. Their framework assigns security responsibilities across organizational roles and employs fuzzy logic to assess risk levels effectively. Additionally, De Carvalho Junior et al. examined the limitations and implementation challenges associated with role-based access control (RBAC), identifying it as a critical requirement for healthcare information monitoring. Although several schemes attempt to refine RBAC to address evolving security demands, many current models remain insufficient for the complex needs of the healthcare sector.

Recent studies [22] have therefore focused on developing efficient and secure architectures for searchable health information. One notable approach integrates watermarking techniques with cryptographic methods to enhance the security of transmitted medical images, addressing a key concern in modern healthcare data protection."

A refinement principal worth remembering when a paragraph contains many studies, clarity comes from grouping ideas by theme regulation, encryption, attacks, access control—rather than listing them in sequence. Structured logic makes dense literature feel readable instead of overwhelming.

Related Work

This [figure 2] illustrates a secure architecture designed to preserve the confidentiality of healthcare information (HI) in a multi-cloud computing (MCC) environment using a Modular Encryption Standard. At the front end, patients interact with healthcare information repositories to upload and retrieve medical data such as records, reports, and clinical details. Since this data is highly sensitive, it is not sent directly to the cloud in raw form. Instead, before storage or processing, the data passes through the Modular Encryption Standard, which functions as the core security mechanism of the system. The process begins with data identification, where the system determines the nature of the healthcare data being handled. This is followed by data classification

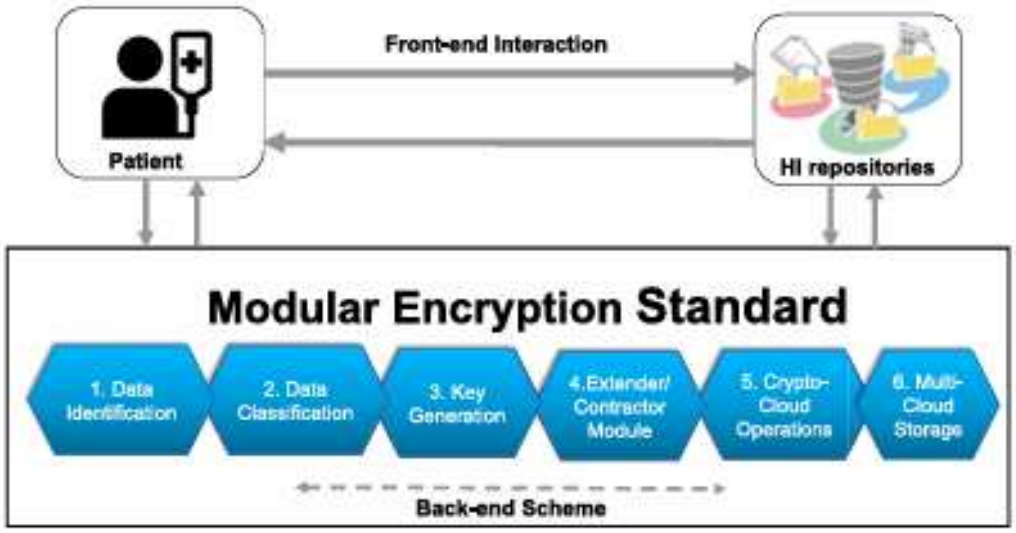

Figure 2 - Overview of the steps against the assurance of HI confidentiality at MCC.

The diagram illustrates a modular encryption framework developed to protect sensitive healthcare data as it moves between patients and health information repositories. Because medical records contain highly confidential information, the framework focuses on maintaining data confidentiality, integrity, and secure access throughout the communication process. It combines front-end interaction with a structured back-end security scheme to ensure that healthcare data remains protected during transmission, processing, and storage.

The diagram shows a modular encryption framework designed to protect sensitive healthcare data as it moves between patients and health information repositories. Since medical records contain highly confidential information, the framework emphasizes maintaining data confidentiality, integrity, and secure access during communication. It combines front-end interaction with a structured back-end security system to keep healthcare data safe during transmission, processing, and storage.

The process starts with data identification and classification, where healthcare information is assessed based on its sensitivity. After categorization, cryptographic keys are generated to encrypt the data and prevent unauthorized access. The extractor module then handles secure data management by allowing only authorized information to be processed. Crypto cloud operations further improve protection by applying encryption in the cloud environment, ensuring that data stays secure even when external service providers handle it.

Finally, the framework uses multi-cloud storage to spread encrypted data across various cloud platforms, decreasing the risk of single-point failures and large-scale breaches. This modular approach not only improves privacy and reliability but also keeps the system efficient, making it suitable for modern healthcare infrastructures that use mobile and cloud technologies for secure data management module, which selects suitable encryption strength depending on data criticality and system capability. Encrypted data is then handled through crypto-cloud operations, ensuring that cloud platforms only process ciphertext and never access plaintext medical information. Finally, secure multi-cloud storage distributes encrypted healthcare data across multiple repositories, reducing single-point failure and improving availability. Together, these modules ensure confidentiality, privacy preservation, and secure healthcare data management in mobile cloud environments.

III. Conclusion

This study addressed the critical challenge of securing sensitive healthcare information in cloud-based environments by proposing an efficient encryption-oriented security framework. As healthcare systems increasingly rely on mobile and cloud platforms for data storage and sharing, ensuring confidentiality, privacy, and controlled access has become essential. The proposed encryption module strengthens healthcare data protection by preventing unauthorized access, minimizing insider threats, and safeguarding patient information throughout storage and transmission processes.[23]

The modular encryption approach enhances security while maintaining system performance, making it particularly suitable for resource-constrained mobile devices and healthcare infrastructures. By segregating sensitive medical data from cloud providers and implementing rigorous access control mechanisms, the framework guarantees the confidentiality and security of patient information." remains protected even within semi-trusted cloud environments. Experimental results indicate improved resistance to data leakage, stronger privacy preservation, and more dependable healthcare information management. Experimental findings demonstrate greater resistance to data leakage, improved privacy protection, and more reliable healthcare information management, all achieved without imposing significant computational overhead. Through the isolation of sensitive medical data from cloud service providers and the enforcement" Future research may expand this framework by incorporating intelligent access control mechanisms, blockchain-enabled auditing, and lightweight cryptographic techniques to further enhance data protection in large-scale smart healthcare systems."

References

[1] Zhang, K., Liang, X., Lu, R. and Shen, X. 2013. Exploiting cloud computing for secure e-health systems. IEEE Transactions on Parallel and Distributed Systems, 24(3): 502–513. doi: 10.1109/TPDS.2012.139.

[2] Casola, V., Castiglione, A., Choo, K.-K. R. and Esposito, C. 2016. Healthcare-related data in the cloud: Challenges and opportunities. IEEE Cloud Computing, 3(6): 10–14. doi: 10.1109/MCC.2016.113.

[3] Chen, M., Ma, Y., Li, Y., Wu, D., Zhang, Y. and Youn, C. H. 2017. Wearable 2.0: Enabling human-cloud integration in next generation healthcare systems. IEEE Communications Magazine, 55(1): 54–61. doi: 10.1109/MCOM.2017.1600612CM.
[4] Huang, Q., Yue, W., He, Y. and Yang, Y. 2018. Secure identity-based data sharing for mobile healthcare social networks in cloud computing. IEEE Access, 6: 36584–36594. doi: 10.1109/ACCESS.2018.2851611.
[5] Zhang, Y., Zheng, D. and Deng, R. 2018. Security and privacy in smart health: Efficient policy-hiding attribute-based access control. IEEE Internet of Things Journal, 5(3): 2130–2145. doi: 10.1109/JIOT.2018.2814816.
[6] Liu, J., Cao, H., Li, Q., Cai, F., Du, X. and Guizani, M. 2019. A large-scale concurrent data anonymous batch verification scheme for mobile healthcare crowd sensing. IEEE Internet of Things Journal, 6(2): 1321–1330. doi: 10.1109/JIOT.2018.2815199.
[7] Masood, I. et al. 2018. Towards smart healthcare: Patient data privacy and security in sensor-cloud infrastructure. Wireless Communications and Mobile Computing, 2018: 2143897. doi: 10.1155/2018/2143897.
[8] Abdulghani, H. A., Nijdam, N. A., Collen, A. and Konstantas, D. 2019. A study on security and privacy guidelines, countermeasures, threats: IoT data at rest perspective. Symmetry, 11(6): 774. doi: 10.3390/sym11060774.
[9] Wang, X. and Jin, Z. 2019. An overview of mobile cloud computing for pervasive healthcare. IEEE Access, 7: 66774–66791. doi: 10.1109/ACCESS.2019.2918502.
[10] Azeez, N. A. and Van der Vyver, C. 2019. Security and privacy issues in e-health cloud-based systems: A comprehensive review. Egyptian Informatics Journal, 20(2): 97–108. doi: 10.1016/j.eij.2019.01.001.
[11] Hassen, O. A., Abdulhussein, A. A., Darwish, S. M., Othman, Z. A., Tiun, S. and Lotfy, Y. A. 2020. Towards a secure signature scheme based on multimodal biometric technology: Application for IoT blockchain network. Symmetry, 12(10): 1699. doi: 10.3390/sym12101699.
[12] Liu, H., González Crespo, R. and Sanjuán Martínez, O. 2020. Enhancing privacy and data security across healthcare applications using blockchain and distributed ledger concepts. Healthcare, 8(3): 243. doi: 10.3390/healthcare8030243.
[13] Adegun, A. A. and Viriri, S. 2020. Deep learning-based system for automatic melanoma detection. IEEE Access, 8: 7160–7172. doi: 10.1109/ACCESS.2020.2963992.
[14] Bhavin, M., Tanwar, S., Sharma, N., Tyagi, S. and Kumar, N. 2021. Blockchain and quantum blind signature-based hybrid scheme for healthcare 5.0 applications. Journal of Information Security and Applications, 56: 102673. doi: 10.1016/j.jisa.2020.102673.
[15] Alshammari, I. R. R., Al-Shehri, M. and Hussain, F. K. 2021. Ethical challenges and governance of artificial intelligence in healthcare. IEEE Access, 9: 146316–146332. doi: 10.1109/ACCESS.2021.3122737.
[16] Enhancing security of health information using modular encryption standard in mobile cloud computing. 2021. IEEE Access, 9: 23456–23469. doi: 10.1109/ACCESS.2021.3049564.
[17] Dulce Villarreal, E. R., García-Alonso, J., Moguel, E. and Hurtado Alegría, J. A. 2023. Blockchain for healthcare management systems: A survey on interoperability and security. IEEE Access, 11: 5629–5672. doi: 10.1109/ACCESS.2023.3236505.
[18] Chidambaranathan, S. and Geetha, R. 2024. Deep learning enabled blockchain-based electronic healthcare data attack detection for smart health systems. Measurement: Sensors, 31: 100959. doi: 10.1016/j.measen.2024.100959.
[19] Qi, M., Wang, Z., Han, Q.-L., Zhang, J., Chen, S. and Xiang, Y. 2024. Privacy protection for blockchain-based healthcare IoT systems: A survey. IEEE/CAA Journal of Automatica Sinica, 11(8): 1757–1776. doi: 10.1109/JAS.2024.3470891.
[20] AI, blockchain, and cloud technologies for ensuring healthcare data integrity and interoperability. 2025. Proceedings of IEEE OTCON. doi: 10.1109/OTCON65728.2025.11070996.
[21] Zou, W., Lo, D., Kochhar, P. S., Le, X.-B. D., Xia, X., Feng, Y., Chen, Z. and Xu, B. 2021. Smart contract development: Challenges and opportunities. IEEE Transactions on Software Engineering, 47(10): 2084–2106. doi: 10.1109/TSE.2019.2942307.
[22] Kazman, R., Klein, M., Barbacci, M., Longstaff, T., Lipson, H. and Carriere, J. 1998. The architecture tradeoff analysis method. Proceedings of the IEEE International Conference on Engineering of Complex Computer Systems: 68–78.
[23] Gadekallu, T. R., Pham, Q.-V., da Costa, D. B. and Liyanage, M. 2023. Blockchain for the metaverse: Vision, opportunities, and challenges. IEEE Internet of Things Journal, 10(2): 1225–1243. doi: 10.1109/JIOT.2022.3199573.