iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** XI **Month of publication:** November 2023

DOI: https://doi.org/10.22214/ijraset.2023.56900

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue XI Nov 2023- Available at www.ijraset.com

Securing Health Data in Mobile Cloud Computing by a Modular Encryption Approach

Sohum Pawar[1], Kunal Pawar[2], Rushikesh Gangatir[3], Shailesh Patil[4], Dr. Khushbu Wanjari[5]
Masters of Computer Applications, Ajeenkya D Y Patil University, Pune, India

Abstract: ***In the dynamic field of healthcare informatics, this research review explores health data security in mobile cloud computing, emphasizing modular encryption standards. In this paper, an exploration of advanced security methodologies within the Mobile Cloud Computing landscape is presented. The study examines three distinct encryption strategies – Symmetric Key Encryption, Public Key Infrastructure, and Homomorphic Encryption – each strategically employing the Modular Encryption Standard. The findings underscore the versatility of these methods in fortifying health information security within mobile environments, providing an understanding of their implementation nuances and comparative advantages. The literature critically assesses protocols, authentication methods, and vulnerabilities in healthcare contexts, extending its analysis to incorporate emerging technologies.***

Keywords: health data security, modular encryption, mobile cloud computing, biometric security, human factors, artificial intelligence, machine learning.

I. INTRODUCTION

Health information security involves safeguarding sensitive medical data from unauthorized access and ensuring its confidentiality, integrity, and availability. This multifaceted concept encompasses protective measures, protocols, and technologies implemented to defend health information against breaches, ensuring the trustworthiness of healthcare data and maintaining privacy standards. In an era marked by rapid technological advancements, the definition of health information security is evolving to address emerging challenges and incorporate innovative solutions. Although frequently used, a universally accepted definition of privacy remains elusive, leading to ongoing philosophical, sociological, and legal discourse privacy is inherently personal subject to individuals' interpretation which encompasses various dimensions such as bodily integrity, freedom from intrusive surveillance, and the right to control personal information. In the realm of health information, the Privacy Rule focuses on its safeguarding, intertwining concepts of privacy, confidentiality, and security.

1) Privacy dictates who access personal information and under what conditions.
2) Confidentiality pertains to intimate relationship information disclosure prevention.
3) Security, encompassing procedural and technical measures, prevents unauthorized access, modification, and dissemination of data.

II. LITERATURE REVIEW

The literature surrounding health data security in mobile cloud computing has undergone a meticulous examination of various facets, providing valuable insights into protocols, authentication methods, and vulnerabilities prevalent in healthcare contexts. This critical assessment serves as a foundation for understanding the evolving challenges and solutions within the dynamic landscape of healthcare informatics.

A. Protocols in Health Data Security

The review delves into established and emerging protocols employed to secure health information in mobile cloud computing environments. Protocols such as HTTPS and Transport Layer Security (TLS) are scrutinized for their efficacy in ensuring encrypted and secure data transmission. Additionally, the literature explores the role of emerging protocols in addressing the evolving threats to health data, offering a comprehensive view of the protocol landscape.

B. Authentication Methods in Healthcare

Authentication methods play a pivotal role in determining access to sensitive health information. The literature comprehensively evaluates traditional methods like username-password combinations and biometric authentication, shedding light on their strengths and vulnerabilities. Moreover, the review extends its scrutiny to novel authentication approaches, such as multi-factor authentication and behavioural biometrics, assessing their potential contributions to enhancing the overall security posture in healthcare contexts.

C. Vulnerabilities in Healthcare Environments

Identifying and mitigating vulnerabilities in healthcare systems is a paramount concern. The literature critically examines the vulnerabilities inherent in mobile cloud computing, ranging from inadequate encryption practices to weaknesses in authentication mechanisms. By elucidating the vulnerabilities, the review provides a groundwork for understanding potential points of exploitation and the need for robust security measures.

D. Incorporation of Emerging Technologies

A noteworthy aspect of the literature review is its commitment to extending the analysis beyond conventional security measures. It delves into emerging technologies poised to revolutionize health data security. Concepts such as blockchain for immutable record-keeping and artificial intelligence for predictive threat detection are explored, emphasizing their potential in mitigating vulnerabilities and enhancing the resilience of healthcare systems.

To meet these evolving demands, leveraging mobile cloud computing (MCC) and employing modular encryption (ME) techniques emerge as instrumental strategies. Cloud computing provides scalable and efficient storage solutions, facilitating seamless access to health data, while modular encryption ensures robust protection against unauthorized access and potential vulnerabilities.

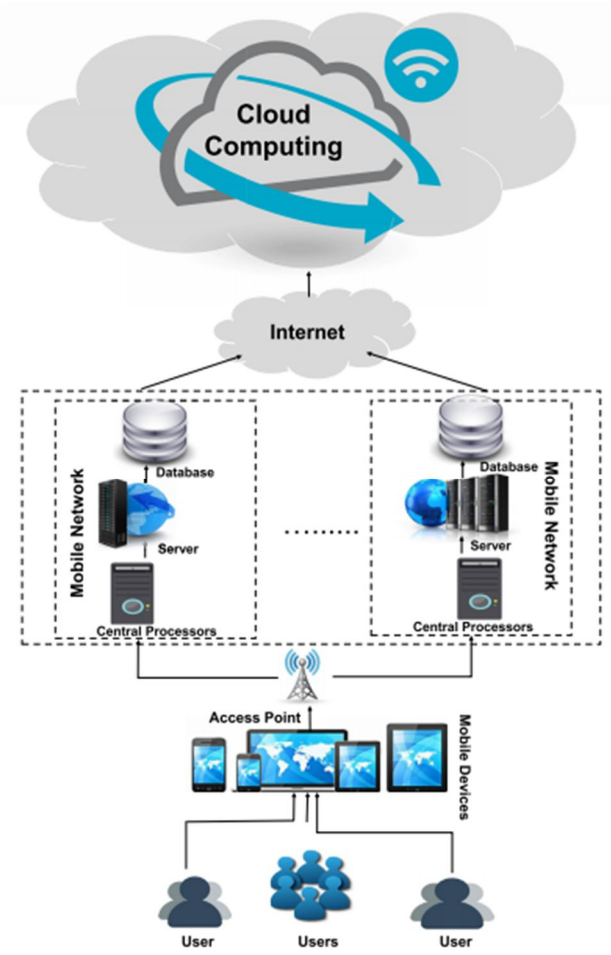


Figure 1. Mobile Cloud Computing.

E. Health Information (HI) Threats

In the domain of Health Information (HI), the landscape is rife with potential threats that demand meticulous attention and strategic safeguards. As the reliance on digital platforms for storing and exchanging health-related information has grown, so have the threats to the security and integrity of this data. This discourse sheds light on various HI threats, each posing a distinct challenge to the integrity and confidentiality of health-related data.

Categories of Health Information Threats:

1) HI-Repudiation

Definition: Inability to acquire HI beyond the trust limit from a designated source.

Mitigation Strategy: Implementation of robust auditing and logging mechanisms to document critical details such as summary, timestamp, and data source. Striving to construct claims without incorporating information sourced from individuals situated on the opposing side of the trust boundary.

2) HI-Tampering

Definition: Involves risks akin to consistent Cross-Site Scripting (CSS) where inputs and outputs of information storage devices are inadequately sanitized.

Mitigation Strategy: Counteracting CSS risks through meticulous validation of inputs and outputs. Vigilance against unauthorized alteration or extraction of information transmitted through secured data flows. Addressing potential tampering by attackers leading to device corruption, with a focus on fortifying defences against log-file-based attacks.

3) HI-Spoofing

Definition: This occurs when an attacker impersonates a legitimate entity, leading to the revelation of sensitive data.

Mitigation Strategy: Adoption of standardized authentication schemes to differentiate between legitimate and fraudulent processes at the destination. Vigilance against attackers spoofing information, ensuring accurate transmission to web servers. Safeguarding against instances where attackers manipulate information before it reaches the device, redirecting it to unintended targets.

4) DDoS Attack

Definition: A Distributed Denial of Service (DDoS) attack targeting servers associated with biosensors poses a significant threat, rendering services unfeasible.

Mitigation Strategy: Strategizing resource management amid potential resource utilization challenges. Recognition of instances were allowing the Operating System to autonomously execute tasks proves effective in coping with the impact of DDoS attacks on user devices.

5) Confidentiality Breach

Definition: This occurs when confidential information entrusted to a cloud service provider by the user is disclosed to unauthorized entities.

Mitigation Strategy: Vigilant enforcement of measures to prevent unauthorized access and disclosure of user information, ensuring strict adherence to consent protocols.

6) HI-Forgery/Eavesdropping

Definition: Involves unauthorized access to and interception of personal data and clinical records during transmission between servers, biosensors, medical frameworks, or user devices.

Mitigation Strategy: Implementation of robust encryption protocols and stringent access controls to thwart unauthorized access and eavesdropping attempts on sensitive health information during data transit.

III. METHODOLOGY

This section focuses on elucidating methodologies integral to securing health information within the domain of Mobile Cloud Computing (MCC) through the application of the Modular Encryption Standard. In the dynamic landscape of MCC, where mobile devices seamlessly interact with cloud resources, safeguarding the confidentiality and integrity of health data is imperative. The incorporation of the Modular Encryption Standard, a cryptographic framework that strategically divides the encryption process into modular components, serves as a foundational element in achieving robust security within this context.

Mobile Cloud Computing optimally integrates cloud resources, facilitating ubiquitous access to health data through mobile devices. The Modular Encryption Standard (MES), characterized by its modularized encryption approach, enhances security by providing a versatile and adaptive cryptographic foundation.

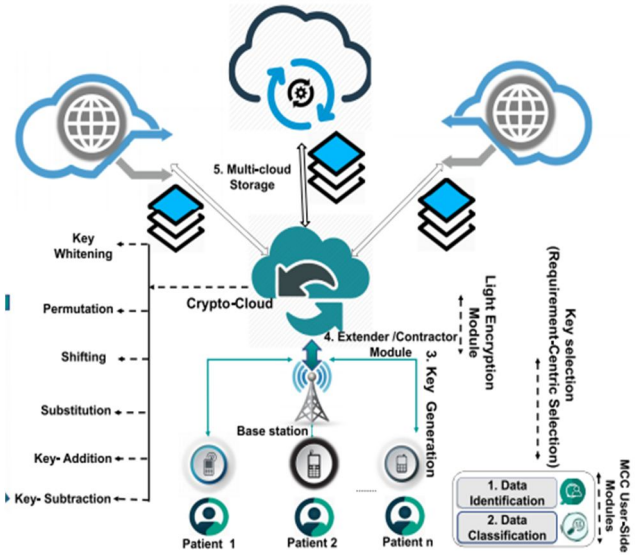


Figure 2. Healthcare monitoring by Modular Encryption Standard (MES) approach.

This methodology section embarks on a comprehensive exploration of three distinctive strategies, each exemplifying the flexibility and effectiveness of modular encryption in fortifying health data within the mobile cloud environment.

A. Symmetric Key Encryption

Symmetric Key Encryption employs a traditional yet robust approach to securing health information within the mobile computing domain. This method utilizes a singular key for both encryption and decryption, ensuring a streamlined and effective data protection paradigm.

The implementation involves the use of symmetric key algorithms, such as the Advanced Encryption Standard (AES), to encrypt health data through a shared secret key. This key is securely exchanged between the mobile device and the cloud server, establishing a secure channel for data transmission.

The advantages of this approach include computational efficiency, attributed to the use of a single shared key, and suitability for managing large volumes of data transmission. However, challenges arise in the form of key distribution and management complexities, particularly in expansive, large-scale environments.

B. Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI) introduces an asymmetrical encryption paradigm, employing a pair of public and private keys to bolster data protection. This methodology heightens security by distinctly separating keys designated for encryption and decryption purposes. In practice, health data is encrypted using the recipient's public key, and only the recipient, possessing the corresponding private key, can decrypt the information. This asymmetric approach contributes to heightened security in scenarios involving data exchange.

The advantages encompass an elevated level of security achieved through the segregation of keys for encryption and decryption, facilitating secure data exchange within dynamic mobile environments. However, challenges arise, including computational overhead attributed to asymmetric key operations and the complexities associated with key management in extensive, large-scale deployments.

C. Homomorphic Encryption

Homomorphic Encryption presents an advanced methodology enabling computations on encrypted data without the necessity for decryption. This innovative approach proves particularly pertinent in scenarios where computations on health data are imperative, and confidentiality must not be compromised. In the implementation of Homomorphic Encryption, health data maintains encryption throughout computations, yielding results without the need for decryption. This method is indispensable in situations requiring secure computation of sensitive health information.

The advantages encompass the capability to conduct secure computations on encrypted data while preserving the confidentiality of the information during the computational process. Nonetheless, challenges include a heightened computational overhead when compared to traditional encryption methods and limitations in supporting specific types of computations. In navigating these methods, this review provides a concise yet comprehensive understanding of the amalgamation of MCC and the MES, offering insights into strategies that fortify the confidentiality and integrity of health information in mobile ecosystems.

IV. CONCLUSION AND DISCUSSION

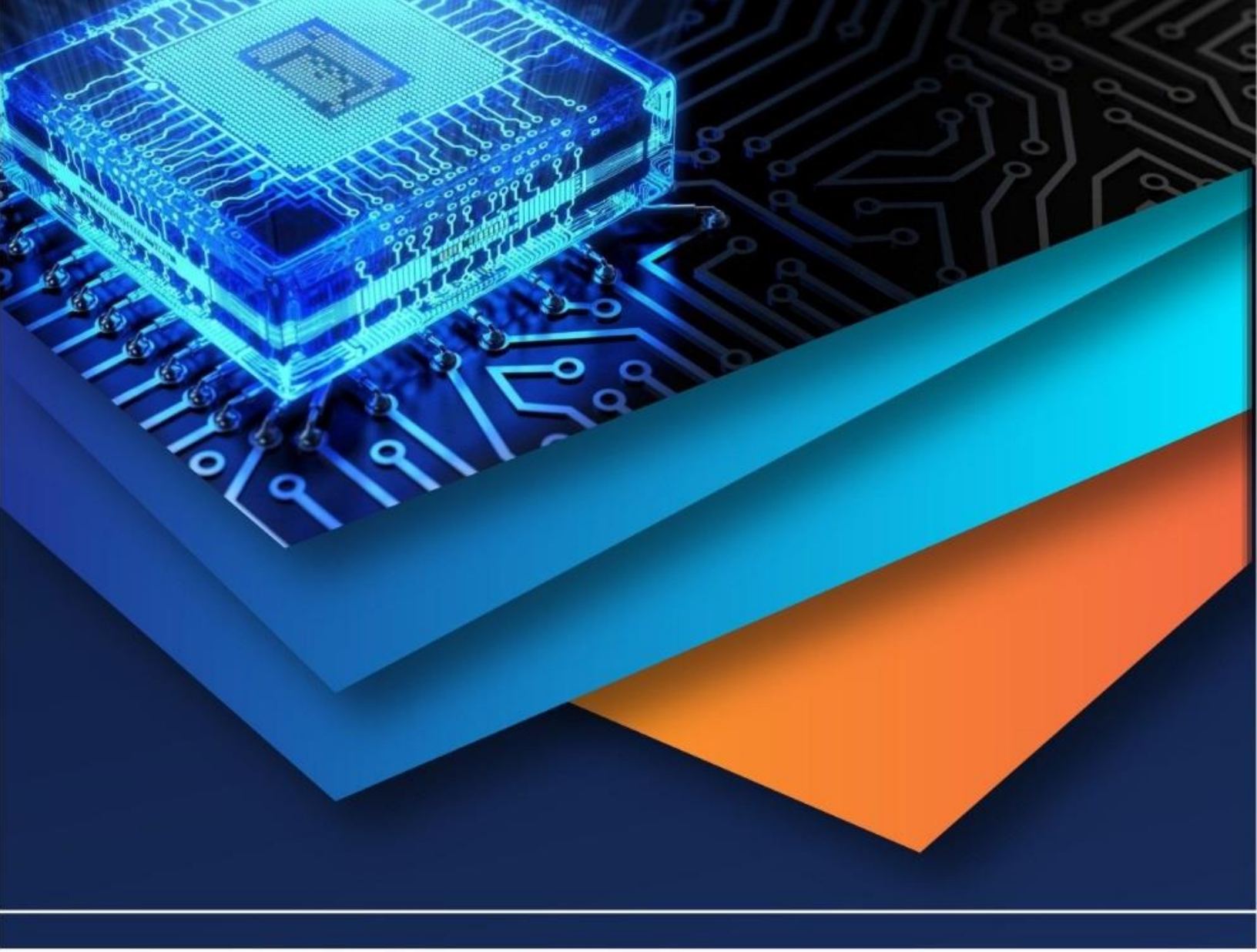
The exploration of modular encryption methodologies within Mobile Cloud Computing not only underscores their significance in fortifying health data security but also illuminates the nuanced advantages and challenges associated with each approach. Symmetric Key Encryption offers computational efficiency, while PKI enhances security through key separation. Homomorphic Encryption introduces an innovative method for secure computations on encrypted data. The integration of these methodologies underscores the importance of a tailored approach to health data security within the mobile cloud environment. As technology continues to advance, the incorporation of artificial intelligence (AI) and machine learning (ML) techniques into health data security protocols emerges as a potential avenue for future exploration. These intelligent systems can proactively identify and mitigate emerging threats, adapting to dynamic healthcare environments. Continuous research and innovation in encryption standards will be pivotal in addressing evolving challenges and ensuring the resilience of health data security in the ever-changing landscape of mobile computing.

V. ACKNOWLEDGMENTS

We extend our deepest appreciation to our mentor Dr. Khushbu Wanjari, for her invaluable insights, expert guidance, and unwavering support throughout the entire research process. Her mentorship has been instrumental in shaping our research endeavours and refining our scholarly pursuits. This research is a collective effort, and you have played a significant role in its realization. Thank you for being an integral part of our academic journey and contributing to the success of this research review paper.

REFERENCES

[1] J. C.-W. Lin, Y. Shao, Y. Djenouri, and U. Yun, ‘‘ASRNN: A recurrent neural network with an attention model for sequence labeling,’’ Knowl.- Based Syst., vol. 212, Jan. 2021, Art. no. 106548.
[2] L. A. Tawalbeh, R. Mehmood, E. Benkhlifa, and H. Song, ‘‘Mobile cloud computing model and big data analysis for healthcare applications,’’ IEEE Access, vol. 4, pp. 6171–6180, 2016.
[3] F. Shiferaw and M. Zolfo, “The role of information communication technology (ICT) towards universal health coverage: the first steps of a telemedicine project in Ethiopia,” Global health action, 5(1), 15638, no. June 2014, pp. 0–8, 2012.
[4] Abd Hamid, N., Ahmad, R. and Selamat, S.R., 2017. Recent Trends in Role Mining Algorithms for Role-Based Access Control: A Systematic Review. World Applied Sciences Journal, 35(7), pp.1054-1058.
[5] M. Sookhak, F. R. Yu, M. K. Khan, Y. Xiang, and R. Buyya, “Attribute based data access control in mobile cloud computing: Taxonomy and open issues,” Futur. Gener. Comput. Syst., vol. 72, pp. 273–287, 2017.
[6] K. Edemacu, H. K. Park, B. Jang, and J. W. Kim, "Privacy arrangement in communitarian ehealth with characteristic based encryption: Survey, difficulties and future bearings," IEEE Access, vol. 7, pp. 89614–89636, 2019.
[7] Kumar, M. S., Ganesh, D., Turukmane, A. V., Batta, U., & Sayyadliyakat, K. K. (2022). Deep Convolution Neural Network Based solution for Detecting Plant Diseases. Journal of Pharmaceutical Negative Results, 464-471.
[8] Y. Al-Issa, M. A. Ottom, and A. Tamrawi, "eHealth cloud security challenges: A review," J. Medical care Eng., vol. 2019, Sep. 2019, Art. no. 7516035.
[9] C. Iwendi, S. Ponnan, R. Munirathinam, K. Srinivasan, and C.- Y. Chang, "A productive and remarkable TF/IDF algorithmic model-based information examination for taking care of utilizations with enormous information streaming," Electronics, vol. 8, no. 11, p. 1331, Nov. 2019.
[10] M. G. Padmashree, S. Khanum, J. S. Arunalatha, and K. R. Venugopal, "SIRLC: Secure data recovery utilizing lightweight cryptography in IoT," in Proc. IEEE Region 10 Conf. (TENCON), Oct. 2019, pp. 269–273.
[11] Raj, Jennifer S. "A novel encryption and decryption of data using mobile cloud computing platform." IRO Journal on Sustainable Wireless Systems 2.3 (2021): 118-122
[12] Lo’ai, A. Tawalbeh, et al. "Mobile cloud computing model and big data analysis for healthcare applications." IEEE Access 4 (2016): 6171-6180.
[13] Q. Huang, W. Yue, Y. He, and Y. Yang, ‘‘Secure identity-based data sharing and profile matching for mobile healthcare social networks in cloud computing,’’ IEEE Access, vol. 6, pp. 36584–36594, 2018.
[14] Y. Zhang, D. Zheng, and R. H. Deng, ‘‘Security and privacy in smart health: Efficient policy-hiding attribute-based access control,’’ IEEE Internet Things J., vol. 5, no. 3, pp. 2130–2145, Jun. 2018.
[15] S. Chenthara, K. Ahmed, H. Wang, and F. Whittaker, ‘‘Security and privacy-preserving challenges of E-health solutions in cloud computing,’’ IEEE Access, vol. 7, pp. 74361–74382, 2019.
[16] A. Algarni, ‘‘A survey and classification of security and privacy research in smart healthcare systems,’’ IEEE Access, vol. 7, pp. 101879–101894, 2019.
[17] A. Alabdulatif, I. Khalil, and V. Mai, ‘‘Protection of electronic health records (EHRs) in cloud,’’ in Proc. 35th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC), Jul. 2013, pp. 4191–4194.
[18] R. Guo, H. Shi, D. Zheng, C. Jing, C. Zhuang, and Z. Wang, ‘‘Flexible and efficient blockchain-based ABE scheme with multi-authority for medical on demand in telemedicine system,’’ IEEE Access, vol. 7, pp. 88012–88025, 2019.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY