iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IV **Month of publication:** April 2023

DOI: https://doi.org/10.22214/ijraset.2023.51056

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 IV Apr 2023- Available at www.ijraset.com

Electronic Health Records Using CP-ABE Access Policy in Blockchain Technology

Mrs. G. V. Leela Kumari[1], P. Jayasree[2], V. Manasa[3], T. Ramya[4], N. Mouni[5], T. Lakshmi Keerthana[6]
[1]*Asst. Professor, M.Tech, Bapatla Women's Engineering College, Bapatla*

Abstract: ***In this paper, we have proposed ciphertext policy attribute based encryption (CP-ABE), which is secured against the attack under the chosen encrypted message attack and indistinguishable under the chosen cipher text attack . On comparing with other schemes, it has the least energy consumption in terms of communication and computation. Based on the proposed CP-ABE, we have implemented a cloud-based internet of medical things enabled smart healthcare system. The healthcare system has achieved secure patients details, and public integrity of patient details stored on the cloud without revealing information to any third entity. Further, we have scrutinized the performance of the proposed health care system in terms of computation energy and communication energy consumption.***
Keywords: Blockchain, Distributed systems, Electronic Health Records, Access Policy

I. INTRODUCTION

The sensor is implanted on or in the patient's body, which collects the patient's Personal Health Information and transmits it to the healthcare provider over a wireless (cellular) network. Any attack on the sensor or unauthorized access to a patient's PHI could result in a life-threatening situation for the patient.

Therefore, the safety and privacy of the patient's PSR on the public network are the main unsolved problems of 's resource limitation challenge. Recently, mobile technology has brought benefits to intelligent healthcare, but the increasing use of data is putting undue pressure on it Mobile phone from network. An interesting solution is device-to-device (D2D) communication, which can work over short distances with the same time/frequency.

Recently, cloud-enabled IoT has potentially served the storage and computation capability for massive IoT data. However, the advantages that cloud leverages to IoT come with the cost of other security risks that have never been noticed in the conventional IoT system. In practice, a cloud is an honest-but-curious entity that follows a correct way to compute and store the massive collected data but curious to access the data inappropriately for an adversarial advantage.

The advantage of using blockchain technology in the electronic-health system is to build a convenient platform that enables an authorized medical entity to diagnose a patient's disease remotely. However, public auditing can provide an effective solution to verify the integrity of stored data remotely.

Since many privacy-preserving schemes [8]– [10] have been discussed, but providing a secure data transmission scheme for cloud-centric IoMT-enabled healthcare is still a challenge. Signature and encryption are two fundamental cryptographic primitives for achieving authenticity and privacy of data, respectively, in a public-key environment. These two essential building-blocks may be composed in several ways, such as sign-then-encrypt, encrypt-then-sign, digital signature with message recovery, and signcryption (authenticated encryption) to ensure authenticity and privacy of data simultaneously. The sign-then-encrypt and encrypt-then-sign schemes have a simple structure, which provides data authentication and privacy with a cost equivalent to the combined cost of signature and encryption schemes. In signature with message recovery scheme, anyone can extract the embedded message without knowing secret information.

Recently, a more efficient solution, signcryption has emerged to design a system that simultaneously achieves privacy and authenticity with a cost significantly smaller than sign-then-encrypt and encrypt-then-sign schemes. Besides, it allows a designated recipient to unsigncrypt and access the message using his secret key.

A. Motivation

The motivation for using electronic health records with attribute based encryption access policy in blockchain technology is to improve data privacy and security, enhanced data sharing, patient control and consent and interoperability. The use of CP-ABE access policy in blockchain technology can provide a secure, efficient and patient-centric approach to managing electronic health records.

B. Objective

The main objective of using electronic health records with attribute-based encryption access policy in blockchain technology is to provide a secure, efficient and patient-centric approach to managing health information.

C. Existing System

In existing system, the state-of-the-art secure and efficient cloud-centric IoMT enabled smart health care system with public verifiability. The system novelty implements an escrow-free identity-based aggregate signcryption (EF-IDASC) scheme to secure data transmission, which is also proposed in this article. The proposed smart healthcare system fetches the medical data from multiple sensors implanted on the patient's body, sign crypts and aggregates them under the proposed EFIDASC scheme, and outsources the data on the medical cloud server via smartphone. The system does not reveal any information about the identity and medical data of the patient.Li et al.present an Identity-based signcryption for low-power devices (sensors) in an online/offline setting that simultaneously fulfills the authentication and confidentiality without authenticating a recipient's public key separately. Omala et al. proposed a lightweight certificate less signcryption (CLSC) scheme for secure data transmission for the WBAN system. Yin et al. give an efficient hybrid signcryption scheme in a certificateless setting for secure communication for WSNs. Unlike scheme, schemes and are resistant to key escrow attack. Zhang et al.discuss a data communication scheme for the e-health system using certificateless generalized signcryption (CLGSC) scheme. Caixue Zhou points out that Zhang et al.'s scheme is susceptible to an insider attack. Thus, the scheme is insecure and vulnerable in terms of data confidentiality. Recently, Zhou has presented an improvised CLGSC scheme for the mobile healthcare system.

In order to reduce the costs of transmission and overhead of verification, Selvi et al. discuss three aggregated signcryption schemes in the identity-based setting, which achieve public verifiability. Wang et al. propose a first identity-based aggregated signcryption scheme using multi-linear mapping in the standard model. Kar proposes a new identity-based aggregated signcryption scheme for low-processor devices. However, schemes are susceptible to the key escrow problem, which is addressed by Eslami et al., followed by presenting an aggregate-signcryption scheme in the certificateless setting. Niu et al. [24] propose a secure transmission scheme for heterogeneous devices, which transmits k messages from k senders in certificateless settings to m recipients in the IBC setting. Kumar et al. propose identity based signcryption scheme for secure peer-to-peer video on demand protocol.

Yang et al. [30] proposed a distributed secure data management with an efficient keyword search system for health IoT. Elhoseny et al. [31] presented a hybrid encryption approach that is built using Rivest, Shamir and Adleman (RSA), and Advance Encryption Standard (AES) algorithms for preserving the diagnostic text data in medical images. From the above discussion, we observed that it is challenged to implement a secure and efficient cloud-centric IoMT-enables smart health care system that achieves public verifiability.

- *Disadvantages:* In the existing work, the system is less effective due to absent of Trust Model Based on Fuzzy Comprehensive Evaluation Method. The system is less security due to Bilinear Diffie-Hellman (BDH) Problem.

D. Proposed System

First, we propose an escrow-free identity-based aggregated signcryption (EF-IDASC) scheme, which addresses the key escrow problem based on the idea given in the existing system.

The system proves that the proposed EF-IDASC scheme is existentially un forgeable under chosen message attack (EUFCMA) and adaptively indistinguishable under the chosen cipher text attack (IND-CCA) in the random oracle model (ROM) and well-known Bilinear Diffie-Hellman Problem (BDHP).

The system compares the proposed EF-IDASC scheme with other related signcryption schemes, in which we show that the proposed scheme consumes the least energy as compared to related schemes. - Then, we propose a secure D2D aggregated-data communication protocol in the cloud-centric IoMT environment for smart health care, that security is based on the proposed EF-IDASC scheme.

Further, we evaluate the energy consumption cost (in mJ) in terms of computation, storage and communication.

The proposed secure healthcare system achieves the patient's anonymity, pubic auditing of the integrity of stored data on the cloud, and mutual authenticity of patient's data with public verifiability.

- *Advantages:* An effective design of system which it ensures that data could not be altered or modifies by any adversary.

The Any forgery or modification in the signcrypted data will be caught by the SD during unsigncryption. Assuming the BDH problem is hard to solve, any malicious attacker cannot modify the original data.

II. LITERATURE SURVEY

Demonstrating that the CLS scheme fails to achieve the claimed security properties by presenting four types of signature forgery attacks. Also proposing a robust certificate less signature scheme to address the aforementioned challenges. RCLS only needs public channels and is proven secure against both public key replacement attacks and malicious but-passive third parties in the standard model.

1) Title: Efficient and Robust Certificate less Signature for Data Crowd sensing in Cloud-assisted Industrial IoT Author: Yinghui Zhang, Robert H. Deng Year: 2019.In this article, they propose an identity-based anonymous authentication and key agreement protocol for WBAN in the cloud- assisted environment, which achieves mutual authentication and user anonymity. In the security analysis, they show that under the well-known computational Diffie Hellman assumption and random oracle model, the proposed IBAAKA scheme is provably secure, as well as achieves the required security properties .
2) Title: A Lightweight Cloud-Assisted Identity-Based Anonymous Authentication and Key Agreement Protocol for Secure Wireless Body Area Network Author: Mahender Kumar; Satish Chand Year: 2020. The hospital for help, patients' details can be monitored remotely, continuously, and in real time, then processed, and transferred to medical data center, such as cloud storage, which greatly increases the efficiency, convenience, and cost performance of healthcare. The amount of data handled by MIoT devices grows exponentially, which means higher exposure of sensitive data. The security and privacy of the data collected from MIoT devices, either during their transmission to a cloud or while stored in a cloud, are major unsolved concerns. Here they focus on the security and privacy requirements related to data flow in MIoT Title: Security and privacy in the medical Internet of Things: A review Author: Wenchang Sun, ZhipingCai Year: 2018.

III. SYSTEM MODEL

A. *Modules*

1) *IOT Devices:* In this module, IOT Device has to register to cloud and logs in, Encrypts and uploads a file to cloud server and also performs the following operations such as Register with department and Specialist and Login and View Profile ,Upload patient details with(pid,pname,paddress,dob,email,cno,age,hospitalname,Disease,bloodgroup,Symptom,attach disease file, attach user image) and encrypt all attribute except pname ,Select patient name details uploaded and Set Access Control permission like by selecting Department and Profession and View all uploaded patient Details with date and Time ,View all Access Control provided details with date and Time.
2) *Medical Cloud Server:* In this module the cloud will authorize both the owner and the user and also performs the following operations such as View all patient details in decrypt mode and View all Access Control Details, View all Transactions and View secret key request and response details with date and Time View No.of same disease in chart, View Patient Rank in chart and View No.Of attackers on patient accessing by wrong secret Key.
3) *KPS:* In this module, the KPS Authority performs the following operations such as Login ,view Owners and authorize and View Users and authorize, List all secret key request details and generate and permit with date and Time and List all attackers Details with date and Time by wrong secret Key with date and Time.
4) *Healthcare Centers:* In this module, the healthcare center user has to register to cloud and log in and performs the following operations such as Register with Department and Profession and Login ,View Profile and Search patient details by content keyword(Display patient files and details if access control is given) and request secret key and List all secret key permitted response from Authority and give download option here only.

B. *Algorithms*

1) *RSA:* **RSA algorithm** is an asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. **Public Key** and **Private Key.** As the name describes that the Public Key is given to everyone.
2) *AES:* Advanced Encryption Standard is a specification for the encryption of electronic data established by the U.S National Institute of Standards and Technology (NIST) in 2001. AES is widely used today as it is a much stronger than DES and triple DES despite being harder to implement.
3) *CP-ABE:* Attribute-based encryption is a generalisation of public-key encryption which enables fine grained access control of encrypted data using authorisation policies. The secret key of a user and the ciphertext are dependent upon attributes In such a system, the decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext.

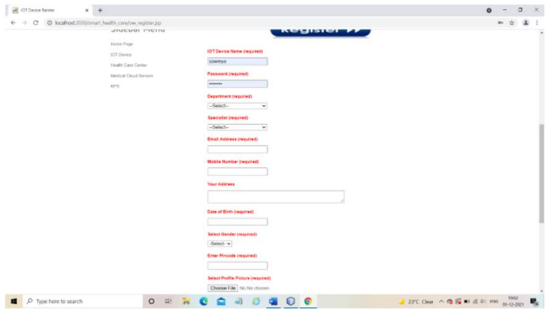
C. Techniques

1) Encryption: Encryption scrambles plain text into a type of secret code that hackers, cybercriminals, and other online snoops can't read, even if they intercept it before it reaches its intended recipients.
2) *Decryption:* Decryption is the process of transforming data that has been unreadable through encryption back to its unencrypted form. In decryption,the system extracts and converts the garbled data and transforms it to texts and images that are easily understandable not only by the reader but also by the system. Decryption may be accomplished manually or automatically. It may also be performed with a set of keys or passwords.

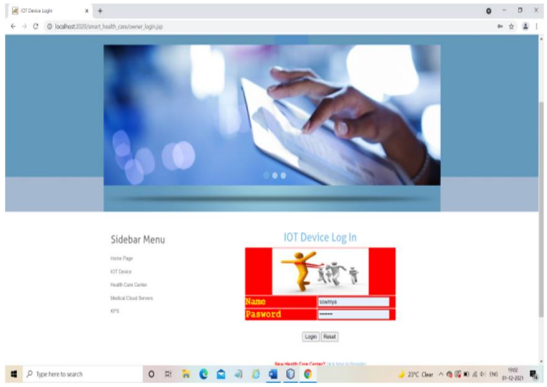
IV. RESULTS AND ANALYSIS

A. Home Page

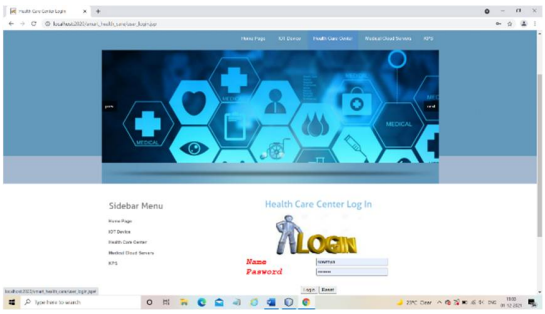
B. User Registration Page



C. IOT Device Login



D. Healthcare Centers Login

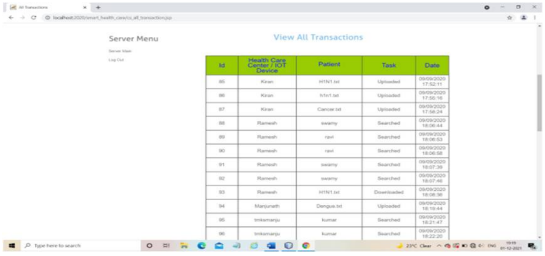


E. Medical Cloud Server Login

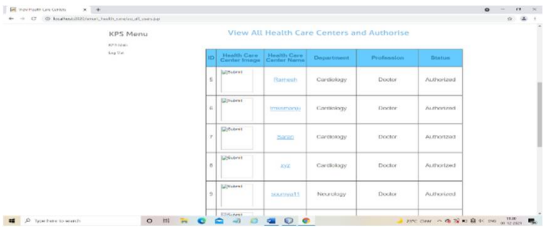
F. View All Patient Details

G. View All Access Control Provided Patient Details

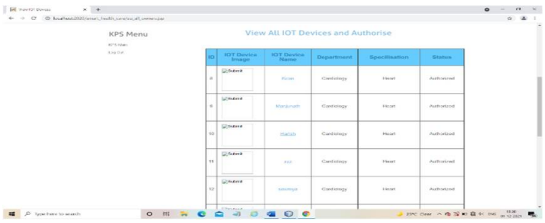
H. view all transactions



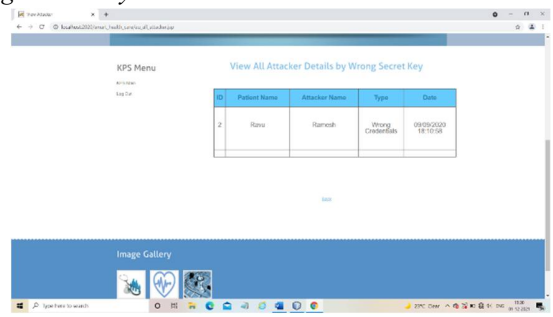
I. View All Healthcare Centers And Authorise



J. View All Iot Devices And Authorise



K. View All Attacker Details By Wrong Secret Key



V. CONCLUSION

In this paper, we have proposed escrow-free identity-based aggregate signcryption (EF-IDASC) scheme, which is secured against the existential forgery attack under the chosen message attack (EUF-CMA) and indistinguishable under the chosen cipher text attack (IND-CCA2). On comparing with other schemes, it has the least energy consumption in terms of communication and computation. Based on the proposed EFIDASC, we have implemented a cloud-centric internet of medical things enabled smart healthcare system. The healthcare system has achieved secure patients PHI within BAN, and outside the BAN, and public integrity of PHI stored on the cloud without revealing information to any third entity. Further, we have scrutinized the performance of the proposed cloud-centric IoMT-based health care system in terms of computation energy and communication energy consumption.

VI. FUTURE WORK

Implementing an Efficient Key-Policy Attribute-Based Encryption by encrypting all attributes and designing attribute-based search technique.

REFERENCES

[1] Y. Zhang, R. Deng, D. Zheng, J. Li, P. Wu, and J. Cao, "Efficient and robust certificateless signature for data IoT," IEEE Trans. Ind. Informatics, 2019.
[2] M. Kumar and S. Chand, "A Lightweight Cloud-Assisted Identity-based Anonymous Authentication and Key Agreement Protocol for secure.Wireless Body Area Network," IEEE Syst. J., vol.Early acce, 2020.
[3] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, "Security and privacy in the medical Internet of Things: A review," Secur. Commun.Networks, vol. 2018, 2018.
[4] A. Zhang, J. Chen, R. Q. Hu, and Y. Qian, "SeDS: Secure data sharing strategy for D2D communication in LTE-Advanced networks," IEEE Trans. Veh. Technol., vol. 65, no. 4, pp. 2659–2672, 2016.
[5] Z. Li, Z. Yang, and S. Xie, "Computing Resource Trading for Edge- Cloud-assisted Internet of Things," IEEE Trans. Ind. Informatics, 2019.
[6] W. Wang, P. Xu, and L. T. Yang, "Secure data collection, storage and access in cloud-assisted IoT," IEEE Cloud Comput., vol. 5, no. 4, pp. 77– 88, 2018.

[7] D. He, S. Zeadally, and L. Wu, "Certificateless public auditing scheme for cloud-assisted wireless body area networks," IEEE Syst. J., vol. 12, no. 1, pp. 64–73, 2015.
[8] V. Sureshkumar, R. Amin, V. R. Vijaykumar, and S. Rajasekar, "Robust secure communication protocol for smart healthcare system with FPGA implementation,"Futur.Gener.Comput.Syst., 2019.
[9] H. Xiong and Z. Qin, "Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks," IEEE Trans. Inf. forensics Secur., vol. 10, no. 7, pp. 1442–1455, 2015.
[10] J. Shen, S. Chang, J. Shen, Q. Liu, and X. Sun, "A lightweight multi-layer authentication protocol for wireless body area networks," Futur.Gener.Comput.Syst., vol. 78, pp. 956–963, 2018.
[11] J. A. Akinyele, M. W. Pagano, M. D. Green, C. U. Lehmann, Z. N. J. Peterson, and A. D. Rubin, "Securing electronic medical records using attribute-based encryption on mobile devices," in Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices, 2011, pp. 75–86.
[12] C. Hu, H. Li, Y. Huo, T. Xiang, and X. Liao, "Secure and efficient data communication protocol for wireless body area networks," IEEE Trans. Multi-Scale Comput.Syst., vol. 2, no. 2, pp. 94–107, 2016.
[13] B. Chandrasekaran, R. Balakrishnan, and Y. Nogami, "Secure Data Communication using File Hierarchy Attribute Based Encryption in Wireless Body Area Networks," 2018.
[14] F. Li, M. K. Khan, K. Alghathbar, and T. Takagi, "Identity-based online/offline signcryption for low power devices," J. Netw. Comput.Appl., vol. 35, no. 1, pp. 340–347, 2012.
[15] A. A. Omala, N. Robert, and F. Li, "A provably-secure transmission scheme for wireless body area networks," J. Med. Syst., vol. 40, no. 11, p. 247, 2016.

BIOGRAPHIES

G.V.Leela Kumari M.Tech,

Asst.Professor,Dept of Computer Science and Engineering,

BEC,Andhra Pradesh,India.

Peddireddy Jayasree[B.Tech],

Student,Dept of Computer Science and Engineering,

BWEC,Andhra Pradesh,India.

Vuyyuru Manasa[B.Tech],

Student,Dept of Computer Science and Engineering,

BWEC,Andhra Pradesh,India.

Thadikonda Ramya[B.Tech],

Student,Dept of Computer Science and Engineering,

BWEC,Andhra Pradesh,India.

Tiyya Lakshmi Keerthana

[B.Tech],

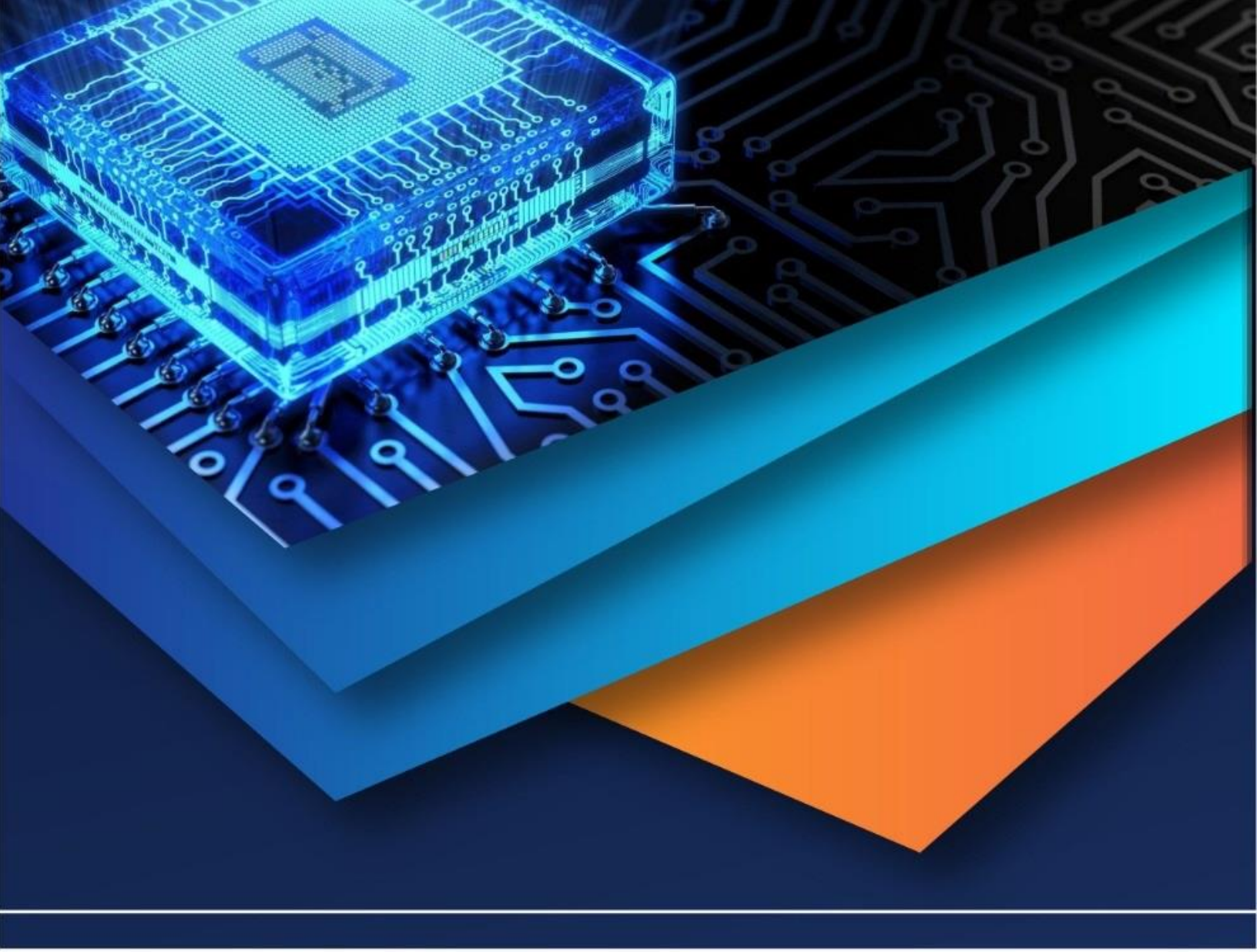
Student,Dept of Computer Science and Engineering,

BWEC,Andhra Pradesh,India.

Nukatoti Mouni[B.Tech],

Student,Dept of Computer Science and Engineering,

BWEC,Andhra Pradesh,India.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY