iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IV **Month of publication:** April 2025

DOI: https://doi.org/10.22214/ijraset.2025.68358

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 13 Issue IV Apr 2025- Available at www.ijraset.com

Secure E-Health Systemwith KED Using Modulo92

Sridevi M[1], Rashmitha R[2], Suchitra G[3], Likhitha B[4]
[1]*Assistant Professor,* [2, 3, 4]*Student, Department of Information Technology, G. Narayanamma Institute of Technology and Science, Hyderabad,India*

Abstract: ***E-wasteIn response to rising cybersecurity challenges, this research proposes the deployment of an e-healthcare system that maintains confidentiality of the patient's medical records. Integration of modern cryptographic DNA with complex encryption methods forms a strong two-tiered security system. This system acts as a robust shield for medical data by preventing unauthorized access to and subsequent breaches of sensitive patient information. With data privacy, confidentiality, and integrity at the forefront, healthcare systems are assured that patients' sensitive information is kept confidential. Such a reliable solution rests in robust security approaches of KED and DNA cryptography, which eradicate access to Patients Health Information (PHI) in a secure e-healthcare System.***

Keywords: Key Encryption and Decryption (KED), Patient Health Information (PHI), DNA cryptography and data confidentiality.

I. INTRODUCTION

The technological advancement known as ‘revolution’ in the health sector comes with its own set of challenges, one of them being the protection of private patient data. Outdated methods, such as old paper records to enter/discharge systems administered through basic computers, are no longer viable due to their inflexible nature, inefficient approach, and vulnerability to cybercrimes. Even modern electronic health records are compromised with gaping holes such as permitting unauthorized hacking access.

To solve this problem, we developed systems aimed at securing patient information. Integrating novel advances in cryptography, including the specialized form of DNAcryptography, protects the information. Our advanced encryption techniques ensure both efficiency and security along with these methods.

Seamless and secure data sharing forms the backbone of our systems. To overcome the problem of fast and secure transfer of patient information, we have employed dynamic encryption techniques and modular arithmetic methods. Also enabling secure communication between patients and doctors through medical centre server while making sure that privacy is maintained and no unauthorized information access is permitted.

.

II. LITERATURE REVIEW

There have been various contributions to the literature review on data privacy and confidentiality

[1] This document focuses on the security of electronic healthcare systems which is very sensitive in nature, especially in relation to safeguarding Patient Health Information (PHI) from prying eyes and cyber-attacks. To support this claim, many methodologies have been proposed based on traditional symmetric and asymmetric encryption methods. While these foundational methods have provided a level of security, advanced hybrid approaches are necessary to counter modern cryptanalysis.

[2] This work focuses on the development of an encryption algorithm based on modulo 37 arithmetic. Primarily, the algorithm was restricted to alphanumeric data by definition, which limited it to two keys. A new study came up with KED algorithm incorporating modulo 69 arithmetic for encryption. This system was shown to have improved protection against brute force and timing attack, thus, facilitating the current research.

[3] This work enhances the KED algorithm by including DNA-based actions as well as AES S - box substitutions. The Advanced Encryption Standard (AES) is an algorithm for symmetric encryption which is still used today. AES is known for its speed and security. Its use in encrypting digital images illustrates the efficiency of AES in protecting vast amounts of data, including PHI. But, like other algorithms, it is vulnerable to differential and linear attack iterations. To make it more secure, we need to add additional security layers.

[4] This paper examines the evolution of the integration of modulo 92 arithmetic with AES and DNA cryptography increases security and operational efficiency. This hybrid approach also talks about not only protecting patient data but also presenting a scalable solution for contemporary e-healthcare settings by resolving fundamental security issues in data transformation and storage.

©IJRASET: All Rights are Reserved

III. PROPOSED SYSTEM AND METHODOLOGY

A. *Proposed System*

We have created a secure e-health system based on KED with Modulo92. This method offers secure encryption of sensitive patient medical information. In this, KED is applied with modulo92 where modulo92 is an arithmetic operation that divides a number by 92 and returns the remainder, which lies between 0 and 91. And this arithmetic operation is also commonly employed for reducing data size and enhancing processing efficiency. Contrary to standard encryption techniques, KED with Modulo92 ensures high-level security and speedy processing as well secure key exchange, protecting information in storage and transit, as well as maintaining confidentiality and integrity of patient health information. It maintains an admirable balance by giving excellent security controls with maximum performance. Thus, its light encryption makes it a good option for e-health applications which must operate with limited resources.

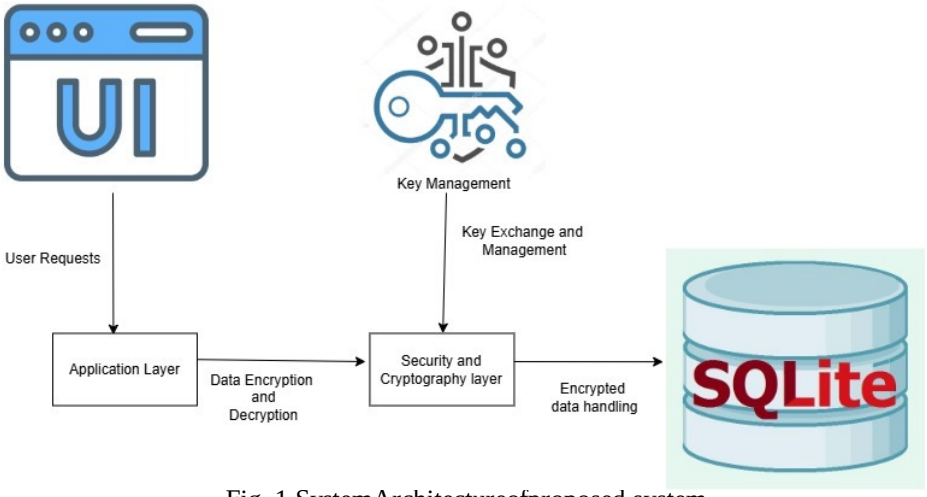


Fig. 1 SystemArchitectureofproposed system

B. *Methodology*

1) *Data Collection*: Patient Health Information (PHI) is gathered from patients and healthcare providers.
2) *Pre-processing:*Data is structured and cleaned to meet encryption requirements.
3) *Encryption:*KED with modulo92 secures pre-processed data for transport and storage also Encrypted data is securely sent between the Medical Centre Server (MCS) and authorised users.
4) *Decryption*:The authorised entity uses a shared symmetric key to securely access PHI.
5) *Validation:* Verify decrypted data integrity to prevent manipulation during transmission.

IV. RESULTS



Fig.2 Login Page of the User

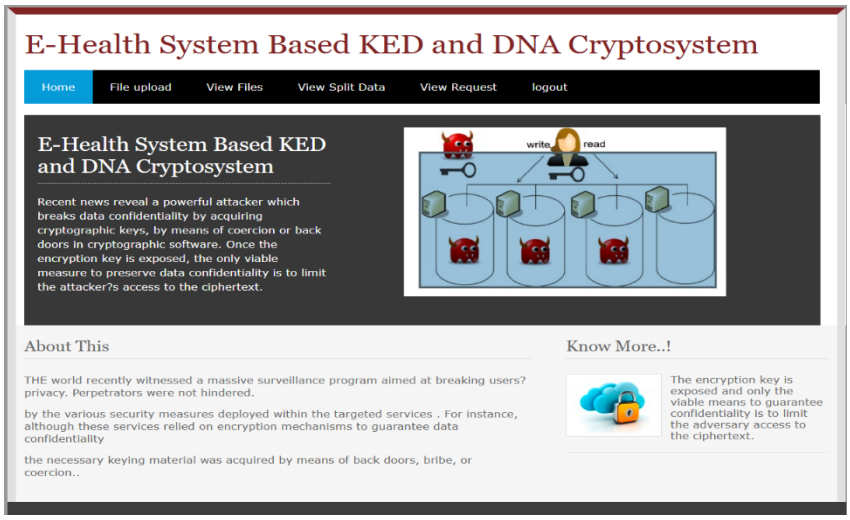


Fig.3 After Patient Login



Fig.4 Patient upload file

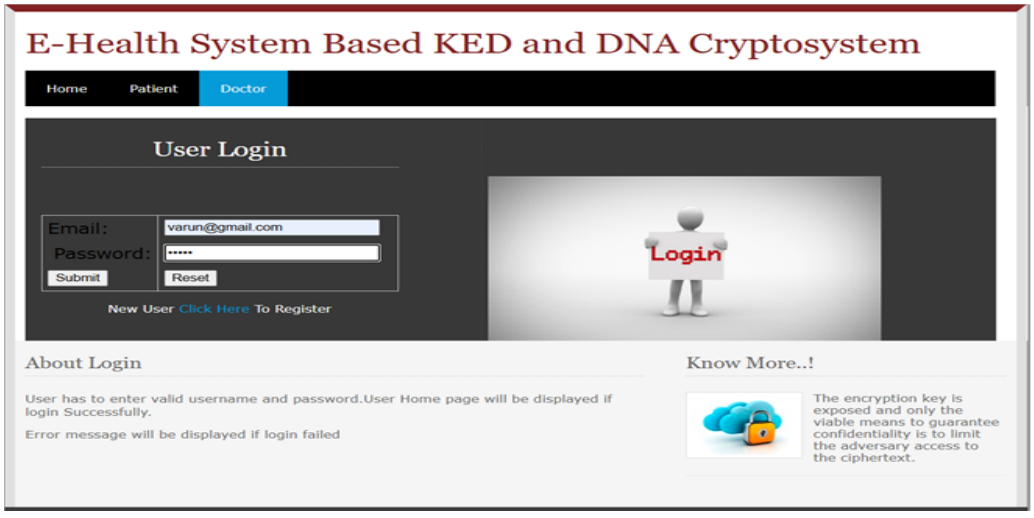


Fig.5 After Doctor Login

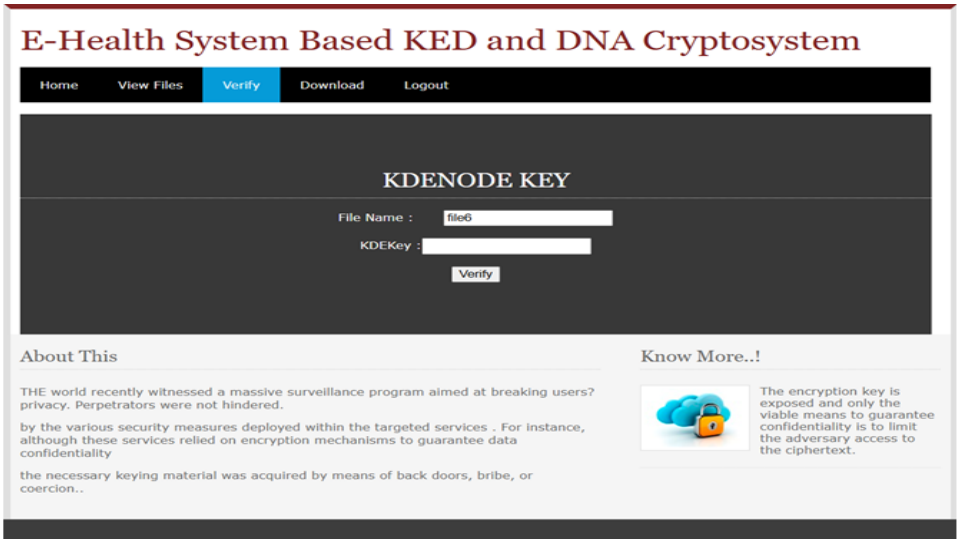


Fig 6. KED key entering page for security



Fig 7. DNA Key entering page for preventing attacks

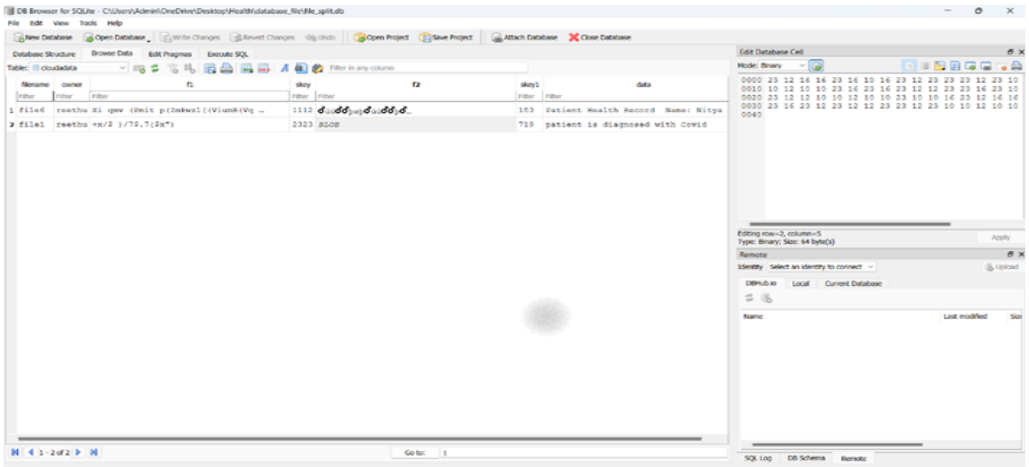


Fig 8. SQLite Database that stores Encrypted data and KED and DNA Keys

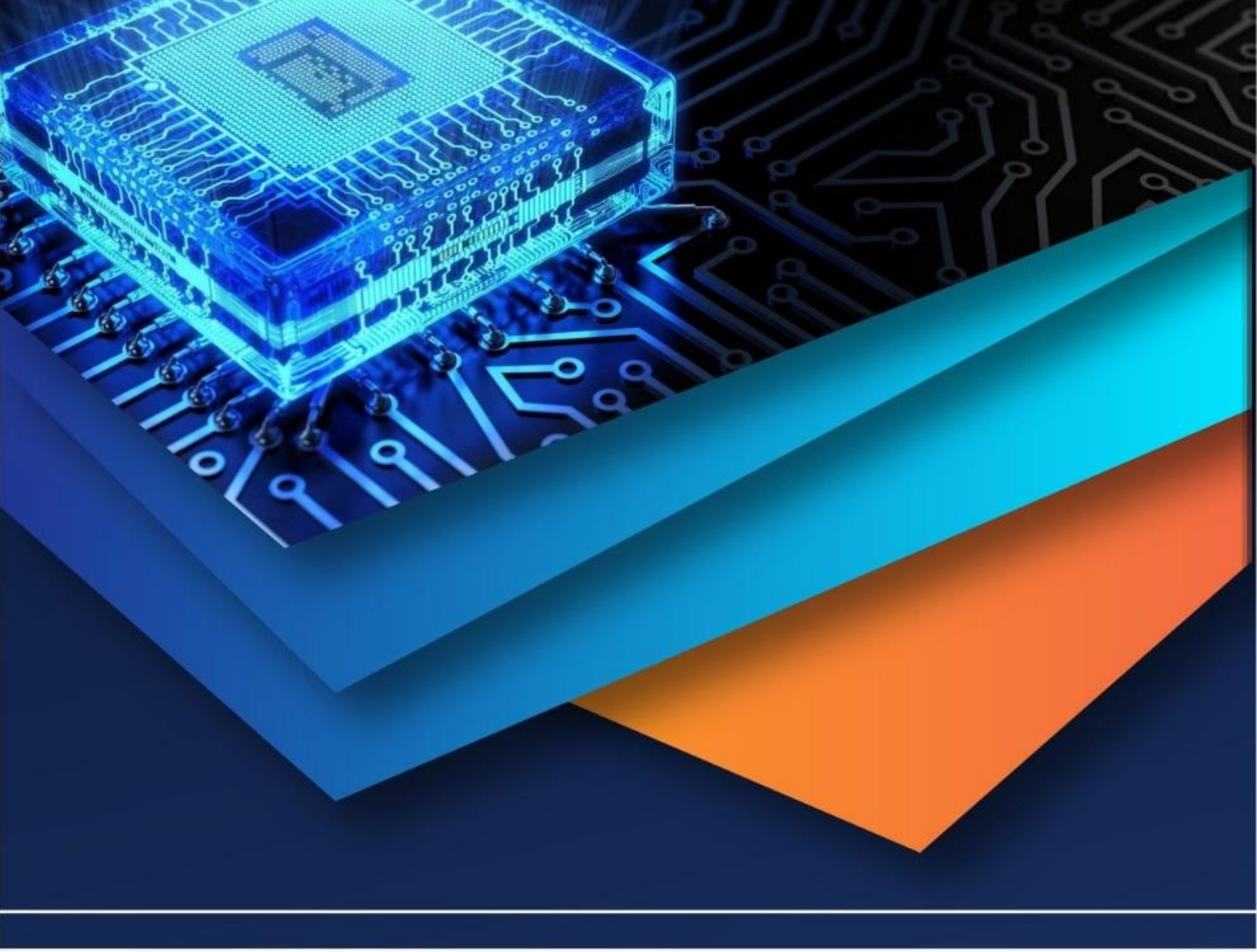
V. CONCLUSIONS

The proposed e-healthcare system seeks to mitigate the challenge of protecting Patient Health Information (PHI) by combining the KED, DNA cryptosystem, alongside the arithmetic of modulo 92. Information Technology is able to minimize risks such as unlawful access and breaches of cyber security, while still maintaining the security, integrity, and authenticity of the data. The system integrates an SQLite database, which permits real-time interaction and decision-making between patients and medical practitioners. It also facilitates smooth seamless interaction between patients and medical practitioners. The system improves user experience and overall effectiveness by minimizing human error and maintains confidentiality. Furthermore, the system will be improved by expanding multi-factor authentication, enhancing scalability, and optimizing the performance of encryption. Its highly adaptable architecture offers strong security and compliance which is suitable for different healthcare environments ranging from small clinics to large institutions.

REFERENCES

[1] J. Warjri and E. George Dharma Prakash Raj, "KED-A Symmetric Key Algorithm forSecured Information Exchange Using Modulo 69," I.J. Computer Network and Information Security, Vol. 10, pp. 37-43, 2013.
[2] Q. Zhang and A. Qunding, "Digital Image Encryption Based on Advanced Encryption Standard (AES) Algorithm," 5th Int. Conf. Instrum. Meas. Comput. Commun. Control, pp.1218–1221, 2015.
[3] Edwin R. Arboleda, Carla Eunice R. Fenomeno, and Joshua Z. Jimenez, "KEDAES Algorithm: Combined Key Encryption Decryption and Advanced Encryption Standard Algorithm," IJAAS, Vol. 8, No. 1, March 2019.
[4] Jie Cui, Liusheng Huang, and Chinchen Chang, "An Improved AES S-box and its Performance Analysis," International Journal of Innovative Computing, Information and Control,May,2011.
[5] G. Jaswanth Varma et al., "Data Security Based on DNA Cryptography Using SBox Encryption," International Journal of Pure and Applied Mathematics, Vol. 115, No. 7, 2017, pp. 429-434.
[6] O. A. Dawood, A. M. S. Rahma, and A. M. J. Abdul Hossen, "New Symmetric Cipher Fast Algorithm of Reversible Operations' Queen (FAROQ) Cipher," International Journal of Computer Networks and Information Security (IJCNIS), Vol. 9, No. 4, pp. 29–36, 2017.
[7] S.Oukili and S. Bri, "High Throughput FPGA Implementation of Data Encryption Standard with Time-Variable Subkeys," International Journal of Electrical and Computer Engineering (IJECE), Vol. 6, No. 1, p. 298, 2016.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)