TITLE: ANALYSIS AND IMPLEMENTATION OF SECURITY ALGORITHM FOR HELATHCARE APPLICATION

ABSTRACT:

The consultation of a patient by a general physician in healthcare system includes the recording of essential medical details and prescription generation. The prescription contains the unique ID and medical notes of a patient to identify him/her and any treatment history for him/her properly. For better data confidentiality and protection, the prescription is encrypted based on Advanced Encryption Standard (AES), which is one of the highly accepted encryption algorithms. The encryption of the prescription further allows it to be sent safely over any department, whether Surgery, Radiology or Pharmacy. Only authorized personnel from each department, holding their respective department specific decryption key, can decrypt and read a prescription. The keys are stored and dispensed safely to prevent unauthorised access to sensitive patient information. This mechanism of encryption ensures that data remains confidential, as access is controlled. Additionally, every new diagnosis procedure or medication added to the treatment of the patient in question is recorded within the database of the hospital. Further data security at rest is given through the use of SHA-256 hashing as a form of cryptographic algorithm to safeguard the data. This combination of AES encryption for data transmission and SHA-256 hashing for storage provides strong protection for patient information, ensuring confidentiality and integrity as it flows through the system and against unauthorized access or data tampering. In Addition we are using FPGA SPART 3 for simulation to see the output in real-time.

Problem Addressed:

The project addresses the issue of unauthorized access to sensitive patient data and the potential for data breaches within healthcare systems. By implementing strong encryption and hashing techniques, patient confidentiality and data integrity are maintained, reducing risks associated with cyber threats.

Differentiation from Similar Solutions:

Unlike traditional healthcare data security systems, this project integrates AES encryption for secure data transmission and SHA-256 hashing for data storage, providing a dual-layer security approach. Additionally, role-based access control and multi-factor authentication ensure that only authorized personnel can access sensitive data, enhancing security beyond conventional encryption methods.

Socio-Economic Importance:

This project plays a crucial role in improving the security and trustworthiness of healthcare systems. By preventing data breaches, it safeguards patient privacy, reducing the risk of identity theft and fraudulent activities. Secure healthcare data management fosters trust among patients, healthcare providers, and regulatory bodies, leading to more efficient healthcare delivery and compliance with data protection laws.

Beneficiaries:

The primary beneficiaries of this project include patients, healthcare providers, hospital administrators, and regulatory authorities. Patients benefit from enhanced privacy and protection of their medical records, while healthcare providers and administrators gain a secure and efficient data management system. Regulatory authorities can ensure compliance with healthcare data protection standards.

Scope of the project:

The project encompasses the secure transmission and storage of patient data across multiple healthcare departments, including Surgery, Radiology, and Pharmacy. It covers the implementation of AES encryption, SHA-256 hashing, role-based access control, and multi-factor authentication to enhance data security. Additionally, regular audits and compliance monitoring ensure the ongoing effectiveness of the security framework.