IJNRD.ORG ISSN : 2456-4184

International Research Journal
IJNRD
Research Through Innovation

INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Hiding Sensitive Medical Data Using Hashing By Third Party Auditor

KS. Arun[1], J. Meganathan[2], S. Naveen[3], M. Nithyaseelan[4], A. Sanjaiy[5]

[1] *Assistant Professor, Cyber Security Department, Mahendra Engineering College, Tamil Nadu, India*
[3-6] *UG Scholar, Cyber Security Department, Mahendra Engineering College, Tamil Nadu, India*

Abstract— **Advancements in data collection, storage, and processing within E-Health systems have significantly elevated the significance and prevalence of data mining in the healthcare sector. Nevertheless, the sensitive nature of the managed and exchanged data introduces a considerable risk of information exposure and disclosure. Consequently, it becomes imperative to obfuscate sensitive relationships through the alteration of shared data. This critical information security concern underscores the necessity of concealing and safeguarding sensitive relationships within shared data. Given that numerous data mining endeavors aimed at uncovering valuable patterns from databases rely on identifying frequent item sets, delving deeper into these sets necessitates the application of Privacy-Preserving Techniques. Addressing complex combinatorial challenges like data distribution problems often involves the utilization of both exact and heuristic algorithms. While exact algorithms are deemed optimal for such scenarios, they encounter scalability limitations, typically suitable for medium-sized instances. Data hashing involves the transformation of input data into a fixed-length character string using a cryptographic hash function, generating a distinct hash value.**

Keywords—cyber security, hashing, securing medical data

I. Introduction

Electronic Health Records (EHRs) are digital versions of patient charts used in clinician offices, clinics, and hospitals. These records contain notes and information collected by and for the clinicians in that particular healthcare setting. EHRs are primarily used by providers for diagnosis and treatment purposes. Compared to traditional paper records, EHRs offer greater value as they enable providers to track patient data over time, identify patients who are due for preventive visits and screenings, monitor patients' health, and ultimately improve the quality of healthcare delivered. Cloud computing has evolved significantly in recent years. Its origins can be traced back to the time when computer systems remotely shared computing resources and applications. Today, cloud computing encompasses a wide range of services and applications delivered over the internet, often accessible through devices that do not require specialized software. Cloud-based communications services allow businesses to integrate communication capabilities into their business applications, such as Enterprise Resource Planning (ERP) and Customer Relationship Management (CRM) systems, extending their functionality and enabling new interactive capabilities. Cryptography is the study of mathematical techniques related to various aspects of information security, including confidentiality, data integrity, entity authentication, and data authentication. Ciphers are the methods used to encrypt data transforming plaintext into ciphertext or cryptograms using mathematical algorithms or functions designed specifically for this purpose called cryptographic hash functions like SHA-256 or RIPEMD-160 which produce fixed length output strings known as hash values/codes that serve as unique fingerprints representing input data making it computationally infeasible even with powerful computers today attempting reverse engineering back original input values due complexity involved within these algorithms/functions themselves.

II. Literature Survey

In a modern medical system, the rapid development of communication technologies, networks, cutting-edge computing techniques, and wireless medical sensors has led to the creation of large-scale Electronic Health Records (EHRs). These EHRs are frequently contracted out and held by third-party Cloud Service Providers (CSPs), which raises legitimate security and privacy concerns regarding cloud services. This is because sensitive data can be exposed to CSPs or unauthorized users during transmission, storage, and sharing. To address these concerns, this study proposes a decentralized hierarchical attribute-based encryption-based anonymous EHR sharing strategy that better protects patient privacy while enabling secure information exchange. The proposed approach utilizes Multiple Attribute Authority (AA) Attribute-Based Encryption (ABE) to enable fine-grained and scalable data access control without creating bottlenecks. A hierarchical access tree is used to encrypt multiple files simultaneously, significantly reducing computational and storage load. Additionally, the proposed disguised access strategy strengthens user privacy protection by adding a Global Identifier (GID) that prevents user collusion attacks. An anonymous key generation mechanism is then implemented to stop multiple AAs from creating a comprehensive profile using the user's GID. Users can perform double verification based on the verification tag and convergent key to ensure the accuracy and integrity of EHRs. The proposed method has been demonstrated to be secure under the Decisional Bilinear Diffie-Hellman assumption while meeting security requirements for key management and privacy preservation in cloud environments through efficiency analysis and experiments conducted on real datasets with varying sizes.

III. SYSEM ANALYSIS

Cloud medical storage offers numerous benefits, such as increased accessibility, scalability, and cost-effectiveness. However, it also presents several challenges and concerns that need to be addressed to ensure the security, privacy, and proper management of sensitive healthcare data. One of the primary concerns with storing medical data in the cloud is ensuring its security and privacy. Any breach or unauthorized access to this data could lead to severe consequences, including legal penalties and loss of trust from patients. Healthcare organizations must comply with various regulatory requirements and standards regarding the storage and handling of medical data. These regulations often require specific security measures and protocols to be in place when using cloud storage solutions. Ensuring compliance with regulations such as HIPAA (Health Insurance Portability and Accountability Act), GDPR (General Data Protection Regulation), PHIPA (Personal Health Information Protection Act) can be challenging and requires ongoing monitoring and updates. When medical data is stored in the cloud, there may be concerns about who owns the data and who has control over it. Healthcare providers must ensure that they retain ownership of their data while having mechanisms in place to control access for third-party vendors or service providers involved in managing their information systems infrastructure through contractual agreements specifying responsibilities around protecting patient confidentiality under applicable laws like HIPAA/HITECH Act which imposes penalties for noncompliance upwards $1 million per violation depending on severity level determined by Office Civil Rights within U S Department Health Human Services OCR). Healthcare organizations may encounter difficulties migrating large amounts sensitive personal health records between different platforms due lack standardization interoperability across various cloud environments used today; however initiatives like FHIR (Fast Healthcare Interoperability Resources) aim address this issue by providing common framework exchange electronic health information securely across disparate systems seamlessly without compromising patient privacy rights protected under law like GDPR/PIPEDA etcetera.. Accessing medical records stored remotely via internet connection can sometimes slower compared accessing locally due network latency bandwidth limitations affecting performance especially when dealing large volumes critical patient information requiring real time analysis decision making capabilities essential deliver timely effective care outcomes desired stakeholders involved process chain including physicians nurses administrators payers etcetera.

IV. FUNCTIONALITIES OF PROPOSED SYSTEM

The proposed remote data integrity auditing scheme for cloud storage services aims to enable secure sharing of sensitive information while maintaining privacy. By encrypting the entire file, users can ensure their data remains private during transmission and storage. However, this approach also prevents others from using the shared files. To address this issue, the paper introduces a Third-Party Auditor (TPA) that can verify the integrity of user data without compromising privacy or introducing additional online burden. The TPA is designed to be secure and efficient, allowing it to audit multiple users simultaneously and efficiently. The proposed system supports privacy-preserving public auditing, which means that even if an attacker gains access to the TPA's records, they will not be able to identify specific user files or their contents. Additionally, performance optimization mechanisms are introduced in the form of parameter selection strategies that minimize computation costs for both clients and service providers. These strategies result in lower overheads compared to non-cooperative approaches currently used in similar systems.

.

Advantages of proposed System:

1. **Enhanced Security Measures:**
   The suggested system integrates cutting-edge security features like advanced encryption, strong access controls, and real-time monitoring tools to safeguard sensitive medical data from unauthorized access, breaches, and cyber threats. This enhances patient privacy and confidentiality significantly.

2. **Improved Compliance:**
   The proposed system streamlines regulatory compliance by integrating requirements directly into its architecture. It includes automated checks, audit trails, and reporting to help healthcare organizations demonstrate adherence to regulations like HIPAA, GDPR, and industry standards effectively.

3. **Interoperability and Data Sharing:**
   The suggested system promotes smooth interoperability and data sharing in healthcare by utilizing standardized data formats, APIs, and interoperability frameworks. This facilitates secure medical record exchange, enhancing care coordination, clinical decisions, and patient outcomes.

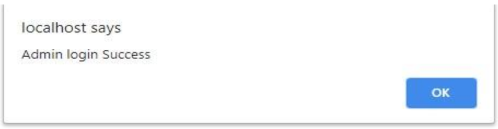
4. **Patient Empowerment:**
   The proposed system empowers patients by giving them control over their medical data. Patient portals, secure messaging, and mobile health apps allow secure access, management, and sharing of records, promoting patient engagement, transparency, and collaboration in healthcare decisions.

V. METHODOLOGY

A. *Methodology of Admin Access*

- The admin, a superuser, accepts and maintains patient data securely on the cloud server.
- Patients can access their details, while the TP (Trusted Person) can access them in emergencies, with admin authorization.

- The admin ensures patient data security and accessibility as needed.

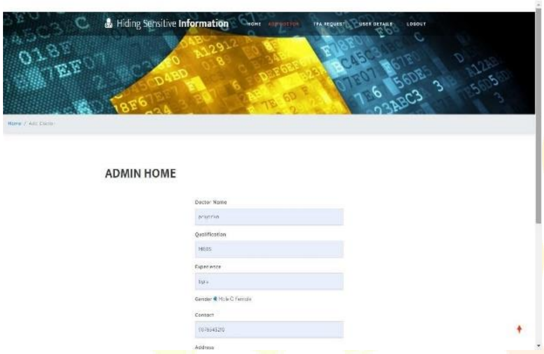

localhost says

Admin login Success

Fig 1 Admin login success

B. *Methodology of Add Doctor*

- The admin will input and store the doctor's personnel information.
- Authentication verification by the admin will also be included for added security and access control.



ADMIN HOME

Doctor Name
priyanka

Qualification
MBBS

Experience
5yrs

Gender ● Male ○ Female

Contact
9876543210

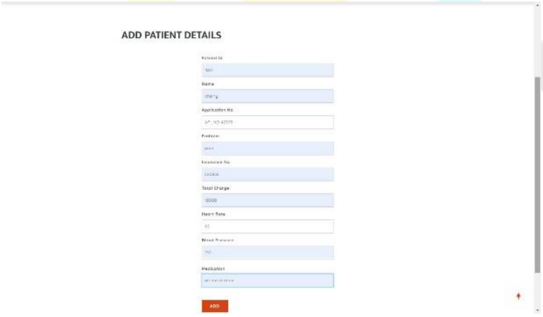
Address

Fig 1.2 Admin Add Doctor

C. *Methodology of Doctor Upload*

The doctor uploads the patient's information to the cloud, first hiding the data before sending the electronic medical records (EMR) reports. These sanitized EMR reports are stored in a database. The patient's medical history is uploaded for their medical care. Hospital doctors treat patients who have been admitted or referred to the hospital, but can include the following:

- By performing surgical procedures.
- By providing general pre- and post-operative care.
- By monitoring and administering medication.
- Here the doctor will upload the necessary details about the patient to the cloud. The cloud stores the data in the EMR.


ADD PATIENT DETAILS

Patient Id
[illegible]

Name
cherry

Application No
AP_NO 42375

Problem
pain

Insurance No
[illegible]

Total Charge
10000

Heart Rate
62

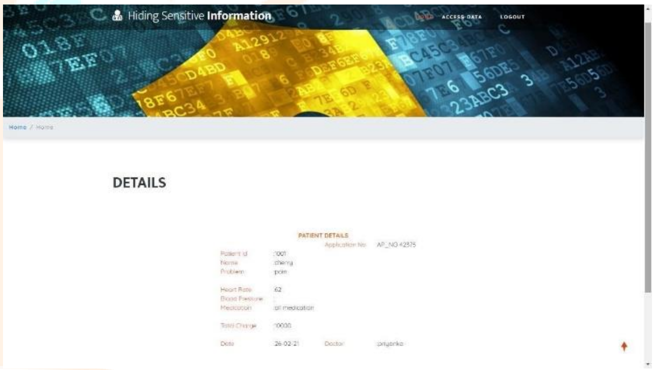
Blood Pressure
[illegible]

Medication
all medication

Fig 1.3 Doctor adds patient details

D. *Methodology of Patient Search*

The Electronic Medical Record (EMR) system enables patients to access their medical records and retrieve encrypted data through a Private Key Generator (PKG). Once decrypted, the data can be utilized anywhere for up to 25 emergencies. Under the Health Insurance Portability and Accountability Act (HIPAA), covered entities must provide patients with access to their medical records, regardless of whether they have paid for services. This emphasis on patient involvement in healthcare is a key aspect of Meaningful Use, which aims to improve patient care by involving patients directly in their care. To achieve this, patients should have timely access to their health information (within 4 business days), an electronic copy of their health information upon request, and a clinical summary for each office visit. These objectives are crucial for Meaningful Use Stage 1. However, some clinicians express concerns about disclosing full chart notes to patients, fearing it may lead to additional time spent explaining the content and potentially increased liability exposure. Despite these concerns, the ability to access patient records in emergency situations is a significant benefit as records are stored on a cloud server and can be accessed whenever needed.



DETAILS

PATIENT DETAILS

Application No AP_NO 42375

Patient Id :1001
Name :cherry
Problem :pain

Heart Rate :62
Blood Pressure :
Medication :all medication

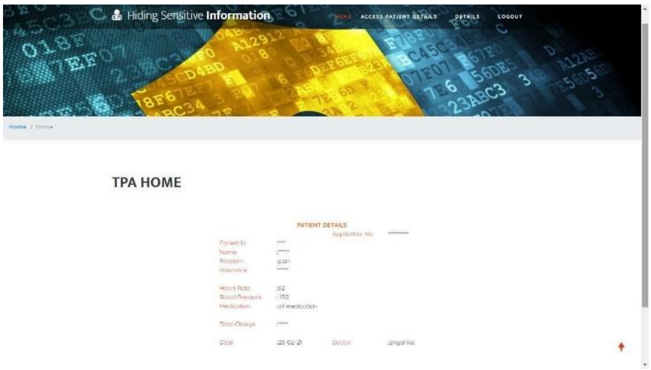
Total Charge :10000

Date 26-02-21 Doctor :priyanka

Fig 1.4 Patient view all the data

E. *Methodology of Sensitive Data hiding*

The proposed system utilizes multiple cloud service provider environments to process data blocks of varying sizes across different locations with identical data copies. These blocks are stored and retrieved based on the storage and computational capabilities of each location. This system addresses the challenge by supporting variable-length block verification. Privacy levels across all cloud providers are evaluated by a trusted authority, assessing security levels and performance of encryption algorithms. The focus lies on concealing specific association rules containing sensitive information on the left-hand side, preventing disclosure of rules with sensitive items. This is achieved by adjusting the database to reduce the confidence of association rules containing sensitive data items. When the confidence falls below a set threshold, the rule is concealed and not disclosed.



TPA HOME

PATIENT DETAILS

Application No ***********

Patient Id :****
Name :*****
Problem :pain
Insurance ******

Heart Rate :62
Blood Pressure : 150
Medication :all medication

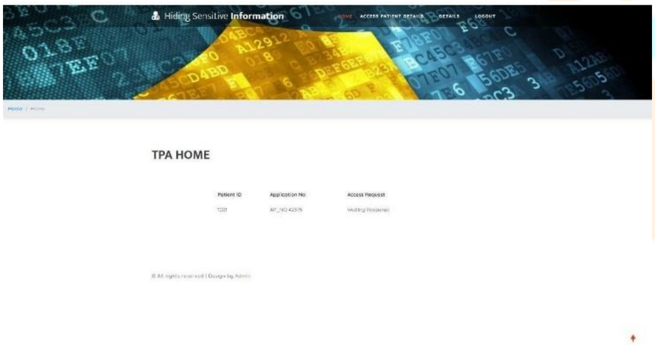
Total Charge :*****

Date :26-02-21 Doctor :priyanka

Fig 1.5 Sensitive Data Hiding

F. Methodology of Emergency TP Access

In case of emergency, an additional login and registration process will be implemented for a Third Party (TP) to access patient details from the cloud, including medication information. The TP will have limited access to the patient's sensitive data, ensuring higher privacy. The patient's ID will be used to retrieve their detailed records from the cloud storage.



TPA HOME

Patient ID	Application No	Access Request
1001	AP_NO 42375	Waiting Response

© All rights reserved | Design by Admin

Fig 1.6 TPA Access

VI. CONCLUSION

An identity-based data hiding scheme with information integrity auditing has been developed to ensure secure cloud storage and facilitate data sharing while protecting sensitive information. The proposed scheme allows files stored in the cloud to be shared and used by others, provided that the sensitive data within the files remains concealed. Additionally, the remote data integrity auditing process is designed to be computationally efficient and easily implementable. Security analysis and experimental results demonstrate that the scheme achieves the desired level of security and efficiency. The project's implementation process has been completed, and it is believed that most of the initially planned system objectives have been met. A trial run of the system has been conducted, and it is producing satisfactory results. The procedures for processing are straightforward and follow a standard order. However, the process of preparing plans may have been overlooked, which could be considered for further enhancement of the application. This work effectively stores and retrieves records from the cloud space database server. The records are encrypted and decrypted as needed to ensure their security.

VII. REFERENCE

1. Pankaj K., Lokesh C., "A secure authentication scheme for IoT applications in the smart home", Peer-to-peer Networking and Applications, vol. 14, pp. 420-438, 2021.
2. Poornima M. C., Mahabaleshwar S. K., "Security and Privacy in IoT: A Survey," Wireless Personal Communications, vol. 115, pp. 1668-1693, 2020.
3. Rajendra P., Harsha D., Chirag M., "Designing an efficient security framework for detecting intrusions in a virtual net of cloud computing", Computers & Security, vol. 85, pp. 402-422, August 2019.
4. Ado Adamou Abba, Olgaegni N., Chafiq T., Ousmane T., Alidou M., Abdelhak M. G., "Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges", Applied Computing and Informatics, pp. 1-23, 2019.
5. "Ahmed Kayed, Suha Omar, "Periodical Key change for cloud mutable security protocol," Microprocessors and Microsystems, vol. 69, pp. 152-158, 2019.
6. Reyhaneh Rezaeinejad, "Comments on a lightweight cloud auditing scheme: Security analysis and improvement," Journal of Network and Computer Applications, vol. 139, pp. 49-56, 2019.
7. Jin L. et al., "Security and privacy in IoT communication," Annals of Telecommunications, vol. 74, pp. 373-374 (Editorial), 2019.
8. Yuqing M., "A Data Security Storage Method for IoT Under Hadoop Cloud Computing Platform," International Journal of Wireless Information Networks, vol. 26, pp. 152-157, 2019.