MEDSECURE

AN ANTI-DATA LEAKAGE SECURITY SYSTEM

Tejeshwini C S[1],Shreya N V[2],Siddraju Saptasagar[3],Shashank P[4],Sara Kousar[5]

[1]*Assistant Professor, Dept. of Information Science & Engineering, VVIET, Karnataka, India*

[2]*Student, Dept. of Information Science & Engineering, VVIET, Karnataka, India*

[3]*Student, Dept. of Information Science & Engineering, VVIET, Karnataka, India*

[4]*Student, Dept. of Information Science & Engineering, VVIET, Karnataka, India*

[5]*Student, Dept. of Information Science & Engineering, VVIET, Karnataka, India*

ABSTRACT

In today's fast-changing healthcare world, it's really important to have a medication recommendation system that's both safe and effective. MedSecure is leading the charge in this shift, using a cutting-edge mix of machine learning and strong encryption to protect patient data while giving personalized medication suggestions. This project covers everything from gathering data to testing the system, all while keeping patient privacy and data security as top priorities.At its heart, MedSecure tackles the big problem of data leaks by using the latest cryptographic methods. By scrambling sensitive patient details and using secure ways for different parties to work together, MedSecure keeps patient data safe and untouched during the recommendation process.

This smart approach not only helps improve treatment results and lift patient care standards but also makes healthcare pros feel confident about how patient data is handled.Old-fashioned medication systems often stumble because they're not great at handling data securely, leaving them open to hacking. MedSecure fixes this by using fancy math tricks to create a super safe line of communication between healthcare pros and the recommendation system. This extra layer of protection not only stops potential data leaks but also makes it easier for doctors to use the system without needing a hospital setup.With MedSecure in place, healthcare folks can move beyond the limits of old-style medication systems, bringing in a new era of patient safety, sticking to meds, and keeping data private. By mixing machine learning and encryption, MedSecure shows the way for how personalized medicine can work securely and effectively, reshaping how decisions are made in healthcare.

Keyword : - *Medsecure, DataSafe Health, Medlock*

1. INTRODUCTION

In healthcare, managing medications is crucial for keeping patients safe, ensuring treatments work well, and lifting overall healthcare quality. Yet, errors in medication and patients not following instructions are big issues. They lead to bad events, higher healthcare costs, and harm to patients. To tackle these problems, using machine learning in medication systems has become a game-changer. Enter MedSecure, a smart medication management system that uses machine learning to transform how medicines are given, watched, and optimized. By using fancy math and analyzing lots of data, MedSecure aims to make patients safer, help them stick to their meds, and give doctors useful info for making decisions.Old-school medication systems often rely on people typing in data by hand, making judgments based on guesswork, and not having all the patient info they need. This can lead to mistakes with meds, bad reactions between drugs, and not choosing the best treatment plans. MedSecure fixes this by using machine learning to sift through heaps of data, spot patterns, and give smart suggestions.With MedSecure, we can step away from the limitations of old systems, bringing in a new era where patients are safer, stick to their meds better, and their data stays private. By using machine learning, MedSecure is reshaping how medications are managed, making it smarter and safer for everyone involved.

2. LITERATURE SURVEY

2.1 IEEE Paper Title: Data Leakage Detection in Healthcare

- Time Of Publication: 2024
- Author: Kishor S Wagah
- Description: Safeguards healthcare data, explores methods like content inspection and intrusion detection, emphasizing privacy-preserving techniques.
- Methodology: Covers content inspection, intrusion detection, and privacy-preserving techniques.
- Limitations: Implementation challenges due to data complexity and privacy standards.

2.2 IEEE Paper Title: Data Breaches Analysis in Healthcare

- Time Of Publication: 2022
- Authors: Chun-Shien Lu, Hong-Yuan Mark Liao
- Description: Conducts a thorough analysis of data breaches in the healthcare sector, categorizing them into internal and external factors and identifying vulnerabilities like poor infrastructure and malware. The study also investigates the increase in breaches from 2009 to 2020 and explores significant ransomware attacks like Trickbot and RYUK, elucidating their impacts on healthcare systems.
- Limitation: The study relies on reported data, which may not capture all breach incidents or provide detailed incident information, potentially limiting the depth of analysis.

2.3 IEEE Paper Title: System for Detecting Data Leakage through Web Browsers

- Time Of Publication:2022
- Author: Jahnavi Reddy
- Description: Proposes a system to detect potential data leakage through web browsers, particularly addressing risks associated with the increasing flow of data through web applications. Traditional defenses like firewalls struggle to prevent web-based leaks without usability impact. The system utilizes a proxy to analyze HTTP traffic at a fine-grained level, categorizing flows and classifying content to identify potential risks.
- Limitation: The effectiveness of the proposed system may be impacted by the complexity of web traffic and the ability to accurately classify content, potentially leading to false positives or missed detections.

2.4 IEEE Paper Title: Investigating Data Breaches in Healthcare

- Time Of Publication:2021
- Author: Adil Hussain She
- Description: Investigates the growing threat of data breaches in healthcare, highlighting vulnerabilities arising from digital transformation. Reveals a surge in breaches and financial losses, emphasizing the need for proactive measures. Analyzing data from 2005 to 2019, the study employs data analysis techniques to reveal trends in healthcare data breaches.
- Limitation: The study's scope may be limited by the availability and accuracy of data from 2005 to 2019, potentially impacting the comprehensiveness of the trends identified

3. SURVEY SUMMARY

In real-time, data breaches pose a significant threat to the healthcare sector, necessitating robust data leakage detection techniques. Emphasizing the importance of safeguarding sensitive healthcare information, methods such as content inspection and privacy-preserving algorithms are highlighted, along with the challenges posed by data complexity and privacy standards. The analysis of insider threats in healthcare data breaches using text mining and visualization techniques reveals vulnerabilities like phishing and malware.

Comprehensive analysis identifies key vulnerabilities and significant ransomware attacks like Trickbot and RYUK. A proposed system to detect data leakage through web browsers analyzes HTTP traffic, noting challenges in accurately classifying content. Research into the rise in healthcare data breaches underscores the need for proactive measures to address vulnerabilities due to digital transformation, despite limitations in data accuracy and availability.

3.1 Drawbacks of The Existing System

- Limited personalization in detection.
- Inflexible detection methods.
- Difficulty in identifying high-risk areas.
- Universal prevention measures.
- False positives and unnecessary alerts.
- Increased resource consumption and costs.

4. METHODOLOGY

This cryptography-based approach protects medical data: classify data by sensitivity, encrypt it at rest and in transit, manage keys securely, monitor access, and keep systems updated. Staff training and data privacy compliance are also essential.

The following are the steps involved in the process:

1. User Registration.

2. Acceptance of Registered user by the admin.

3. User login after acceptance.

4. Data transfer by a user to another user with a secret key.

5. Receiver asking the sender for the secret key to download the data received.

6. Opening of the received data by the receiver using the secret key.

7. If someone tries to open the data without asking for the secret key by guessing the key flag such users as leakers.

8. Admin can block those leakers or if found that they are genuine users then admin can unblock them.

9. The data sent by the sender will have a watermark of the senders name so that the receiver is assured that data is from genuine sender.

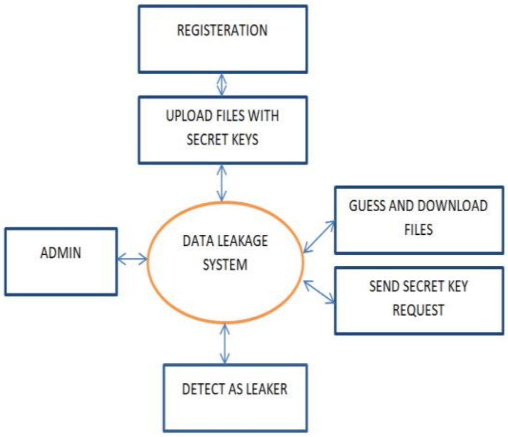


Fig -1: Flow of Proposed System

4.1 WORKFLOW

A sequential diagram for an anti-data leakage system would focus on the message flow and interactions between different components within the system. Here's a representation of a possible scenario:

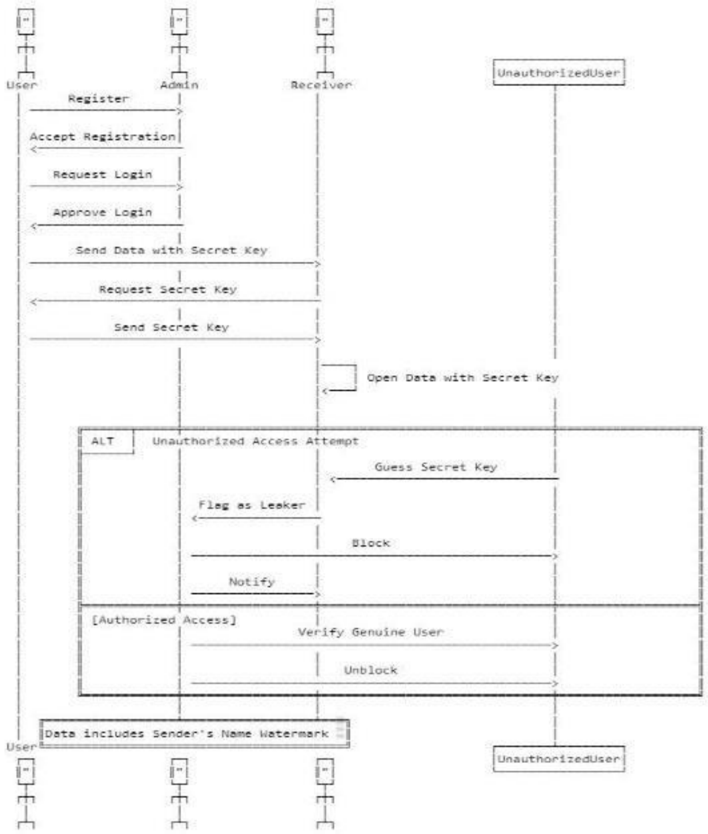


Fig -2: Flow of the Medsecure System

5. RESULT ANALYSIS:

- Personalized Data Protection Recommendations: Tailors data protection strategies to organizational profiles, practices, requirements, and compliance needs.

- Data Interaction Warnings: Identifies and alerts about potential data interaction risks to prevent unauthorized access and breaches.

- Encryption and Access Control Recommendations: Suggests optimal encryption and access controls based on data sensitivity, regulations, and best practices.

- Security Monitoring and Incident Response: Monitors and tracks data access and anomalies in real-time to detect and respond to potential data leaks promptly.

- Compliance Evaluation and Audit Support: Analyzes data handling and security controls for regulatory compliance, identifying gaps and providing remediation actions.

- Predictive Analytics for Data Security: Uses historical data to predict future security risks and effectiveness of security controls, aiding proactive enhancement of data protection.

- Decision Support Tools for Data Governance: Provides policies, procedures, and guidelines for data governance, along with insights into regulations, trends, and best practices.

- Stakeholder Education and Awareness: Offers educational resources and training to enhance stakeholder understanding of data security risks and their roles, fostering a culture of data privacy awareness.

Fig -5.1: UI Page

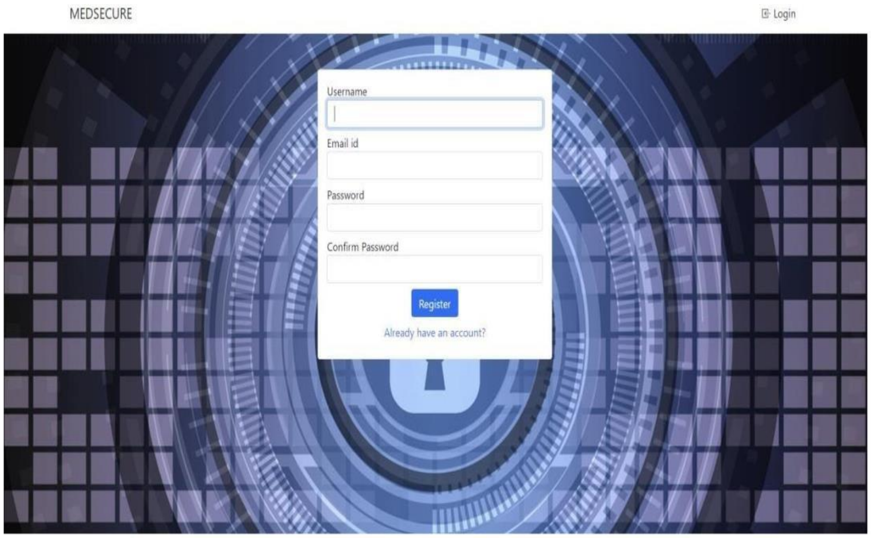
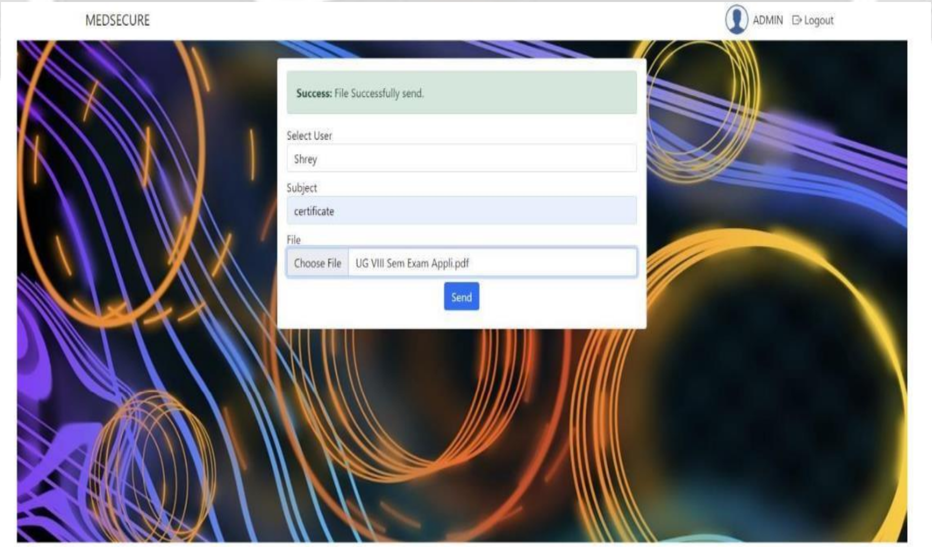


Fig -5.2: login page



Success: File Successfully send.

Select User

Shrey

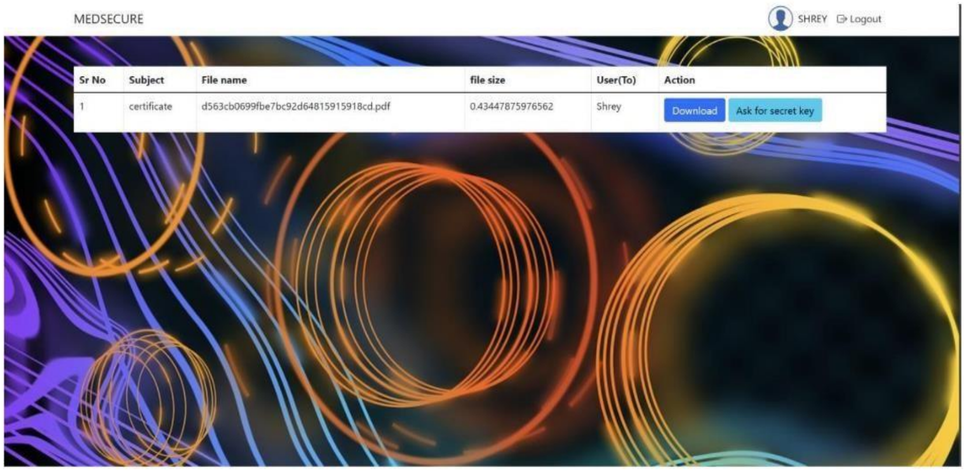
Subject

certificate

File

UG VIII Sem Exam Appli.pdf

Fig -5.3: Send file page



Sr No	Subject	File name	file size	User(To)	Action
1	certificate	d563cb0699fbe7bc92d64815915918cd.pdf	0.43447875976562	Shrey	Download Ask for secret key

Fig -5.4: Download file page

6. CONCLUSIONS

In our project of Data leakage detection, we presented that whenever someone user share files with others there will be a secret key and if someone want to download or access file, they need a secret key which will be request to sender who share this file, after sharing secret key user can download that file, if someone download that file without asking secret key using guess method that will be notified as leakage.

7. REFERENCES

[1]. A Survey on Data Leakage Detection Techniques by Kishor S Wagh (Department of Computer Engineering, All India Shri Shivaji Memorial Society's Institute of Information Technology, Savitribia Phule Pune University, Pune.

[2]. Lee, I. Analysis of Insider Threats in the Healthcare Industry: A Text Mining Approach. School of Computer Sciences, Western Illinois University, Macomb, IL 61455, USA; ilee@wiu.edu Information 2022, 13, 404.

[3]. Data Breaches in Healthcare Security Systems by Jahnavi Reddy, Nelly Elsayed, Zag ElSayed, School of Information Technology, University of Cincinnati, Cincinnati, Ohio, United States

[4]. Healthcare Data Breaches: Insights and Implications by Adil Hussain Seh , Mohammad Zarour Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow