VISVESVARAYA TECHNOLOGICAL UNIVERSITY

Jnana Sangama, Belagavi90018

A PROJECT REPORT

ON

"Securing Pharmaceutical Data Using Homomorphic Encryption"

Submitted in partial fulfillment of
the requirements for the award of the degree of

Bachelor of Engineering
in
Computer Science and Engineering

Submitted by

H M Sukrutha	4MC20CS051
Lohith M Gowda	4MC20CS076
Pratheeksha H S	4MC20CS113
Rakshitha R Ramesh	4MC20CS119

Under the guidance of

B B Neelakantappa

Associate Professor

Department of Computer Science and Engineering

Malnad College of Engineering

Hassan - 573201, Karnataka, India

2021-2022

Malnad College of Engineering

Department of Information Science and Engineering

Hassan - 573201, Karnataka, India

Certificate

This is to certify that project work entitled “Securing Pharmaceutical Data Using Homomorphic Encryption” is a bonafide work carried out by in partial fulfillment

H M Sukrutha	4MC20CS051
Lohith M Gowda	4MC20CS076
Pratheeksha H S	4MC20CS113
Rakshitha R Ramesh	4MC20CS119

for the award of Bachelor of Engineering in Information Science and Engineering of the Visvesvaraya Technological University, Belgavi during the year 2023-2024. It is certified that all corrections/suggestions indicated for Internal Assessment have been incorporated in the report deposited in the departmental library. The project report has been approved as it satisfies the academic requirements in respect of project work prescribed for the Bachelor of Engineering Degree.

Signature of the Guide	Signature of the HOD	Signature of the Principal
B B Neelakantappa	Dr. Geetha Kiran A	Dr. A J Krishnaiah
Associate Professor	Prof. & HOD	Principal
Dept. of CSE, MCE	Dept. of CSE, MCE	MCE

Examiners

Name of the Examiner   Signature of the Examiner

1.

2.

ABSTRACT

Securing pharmaceutical data is of paramount importance due to the sensitive nature of the information involved. Homomorphic encryption presents a promising approach to ensuring data privacy and confidentiality in this domain. Homomorphic encryption enables computations to be performed directly on encrypted data without the need for decryption, thereby preserving data integrity and security throughout processing and analysis.

This project focuses on leveraging homomorphic encryption techniques to secure pharmaceutical data, aiming to safeguard against unauthorized access and breaches while enabling meaningful data analytics. The research explores various aspects of implementing homomorphic encryption within pharmaceutical data environments, including encryption schemes, computational efficiency, and practical applications.

Key objectives include assessing the effectiveness of different homomorphic encryption algorithms in pharmaceutical settings, analyzing the computational overhead associated with encrypted data operations, and evaluating the feasibility of real-time data processing while maintaining security protocols.

By addressing the intersection of data security and pharmaceutical research, this project contributes to advancing secure data management practices within sensitive scientific domains. The outcomes of this study have implications for data privacy regulations, encryption technology development, and secure data analytics in pharmaceutical research and development.

ACKNOWLEDGEMENTS

Salutations to our beloved and highly esteemed institute “Malnad College Of Engineering” for having well qualified staff and labs furnished with necessary equipment.

The successful completion of any task would be incomplete without mentioning the people who have constantly guided and inspired for the project and the report generation.

We avail this opportunity to thank all those people who have helped us in the whole process of completion of this project and the report.

We would like to express our deepest gratitude to our mentor B B Neelakantappa, Department of Computer Science & Engineering for his daily evaluation of the work and for providing us constant encouragement with her unflinching support and valuable guidance throughout this project. We are indebted to him as he has considered us worthy of this project and invested his faith in us. It was a great privilege to work under him. We will take away a lot more than just the technical knowledge from him.

We would also like to place our special thanks to Dr. A J Krishnaiah, Principal, Malnad College Of Engineering for providing the opportunity and the facilities for the completion of our project.

H M Sukrutha
Lohith M Gowda
Pratheeksha H S
Rakshitha R Ramesh

TABLE OF CONTENTS

LIST OF FIGURES

Chapter 1

Introduction

1.1 Introduction to Social Network Analysis

The pharmaceutical industry grapples with safeguarding vast confidential information, including formulas, employee details, and medical records. The imperative to counter cyber threats requires a substantial budget for Information Security Management (ISM), given the potential multi-billion-dollar consequences of attacks. Medical breaches constitute a significant portion of reported data breaches, underscoring the critical need for robust security measures.

Insider threats, often underestimated, pose a greater risk than external hackers, as employees or contractors handle sensitive data. Dealing with malicious insiders, exemplified by the case of Jason Cornish at Shionogi, can be more challenging. Another peril is the production of counterfeit drugs, fueled by the leakage of sensitive information, emphasizing the need for a comprehensive ISM system.

Efficient encryption and restricting insider access help, but Homomorphic Encryption, despite its potential, currently finds no application in pharmaceutical industries. A pioneering initiative aims to employ Homomorphic Encryption in a web application, allowing secure updates of sensitive data, such as tracking medicine components, without involving decryption processes. This innovative approach seeks to enhance data security in the pharmaceutical realm.

1.2 About Project

1.2.1 Problem Statement

- **Cyber Threat Landscape:** The pharmaceutical industry faces a dynamic and evolving cyber threat landscape, necessitating a proactive and adaptive approach to information security.

- **Internal Threats:** Malicious insiders, such as employees or contractors, pose a substantial risk to pharmaceutical data. Addressing the challenge of securing data from within the organization is crucial.

- **Inadequacy of Conventional Encryption:** While traditional encryption methods provide a layer of protection, they may not be sufficient to counter the sophisticated tactics employed by cybercriminals targeting the pharmaceutical sector.

- **Data Integrity and Confidentiality:** Preserving the integrity and confidentiality of sensitive pharmaceutical data during updates and transactions is a paramount concern.

- **User-Friendly Implementation:** The solution must be user-friendly and seamlessly integrate into the daily operations of pharmaceutical companies, ensuring ease of use for employees while maintaining robust security measures.

  By addressing these challenges, our project aims to contribute a novel and effective solution to enhance information security within the pharmaceutical industry through the implementation of Homomorphic Encryption.

1.2.2 Objective

Through our research paper we try to propose a possible application of Homomorphic Encryption in an environment pertaining to Pharmaceutical Companies. Though our proposed idea does not purely incorporate Homomorphic properties in all its functions for example we made use of the AES algorithm to encrypt the textual content and not Paillier algorithm, because the encryption function of the Paillier algorithm makes use of a random prime integer. As a result of which a certain text gets encrypted to different values every time a new entry or updation of data (i.e. Component name and component quantity) is carried out. Also Homomorphic algorithms provide no functionality regarding appending characters to textual data in its encrypted form.

Chapter 2

Literature Survey

M. Nassar et al. [1] presented a research paper explaining the importance of Paillier Algorithm in cloud applications and its implementation. This paper forms the basis of our understanding regarding the Paillier Algorithm and how its Homomorphic properties can be exploited to implement our desired application. The Paillier Algorithm used in our application is designed along the lines of the research carried out in this paper. V. Sidorov and W. K. Ng, wrote a paper on performance Evaluation of Oblivious Data Processing Emulated with Partially Homomorphic Encryption Schemes [2]. There are various Homomorphic Encryption Algorithms available. To decide which one suits our application better, we analyzed the above research paper. The above mentioned paper states that there exist no empirical way of comparing the algorithms and based on one's own application and the type of operations involved, a particular algorithm should be selected. Das, Debasis [3] presented a paper on secured cloud computing using Homomorphic Encryption that highlighted loopholes present in securities of cloud computing. Besides this, it introduced us to the idea of making use of homomorphic algorithms to perform operations on already encrypted data present on cloud which in turn prevents from online security breaches. The paper proposes a scheme and compares the results with existing standards, integrating homomorphic operations with multi-party calculations. Shao et al. [4] presented a paper regarding an efficient way of implementing AES algorithm Since Homomorphic Encryption doesn't allow us to encrypt textual data.

Chapter 3

Project Design

This project aims to design and implement a robust system for securing pharmaceutical data using homomorphic encryption. By leveraging advanced cryptographic techniques, the system ensures the confidentiality and privacy of sensitive information throughout data processing and analysis. The modular architecture facilitates scalability, maintainability, and compliance with data protection regulations in the pharmaceutical domain. This design document outlines the high-level architecture, modules, and interactions necessary to achieve this goal. Homomorphic encryption will enable computations to be performed on encrypted data, ensuring privacy and confidentiality of sensitive pharmaceutical information.

This design document serves as a blueprint for the development and implementation phase, outlining the high-level structure and functionality of each system module.

3.1 Methodology

- The two primary users of our application are Manager and Researcher present in pharmaceutical industries.

- Employees/Researchers perform the work of experimentation while developing medicine, because of which there are frequent changes to the quantities of the components present in the medicines.

- These pieces of information are very confidential and hence should be visible to only authorized people like the manager. The manager holds all the rights like adding/removing employees, watching detailed descriptions of medicines, etc.

- All the keys used for cryptographic operations are stored securely (encrypted form) on the servers adding an extra bit of security to the application.

3.2 Flow Chart

The block diagram shown in Fig. 5.1 is the high level design architecture of Securing Pharmacuetical Data using Homomorphic Encryption.

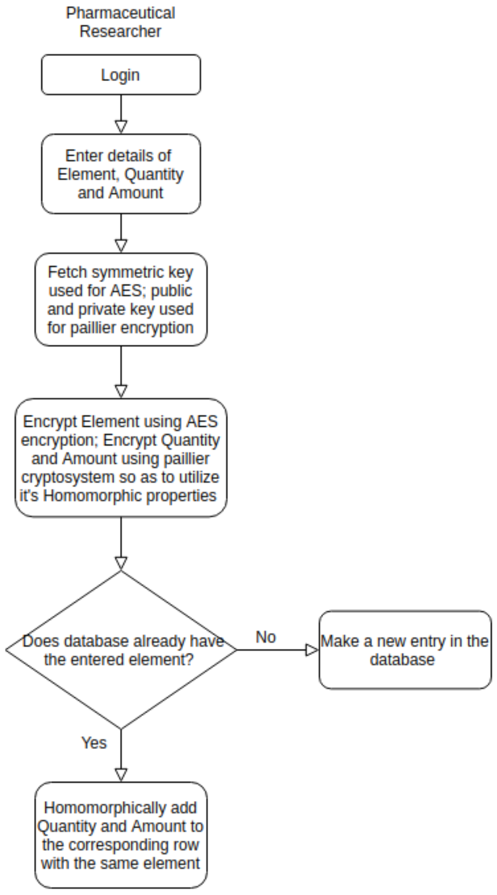

Pharmaceutical Researcher
Login
Enter details of Element, Quantity and Amount
Fetch symmetric key used for AES; public and private key used for paillier encryption
Encrypt Element using AES encryption; Encrypt Quantity and Amount using paillier cryptosystem so as to utilize it's Homomorphic properties
Does database already have the entered element?
No
Make a new entry in the database
Yes
Homomorphically add Quantity and Amount to the corresponding row with the same element

Figure 3.1: High Level Design Overview of Securing pharmaceutical data using Homomorphic Encryption

Chapter 4

Implementation

Implementation We make use of two algorithms to implement our methodology namely, Paillier Cryptosystem and AES algorithm:

- Paillier Cryptosystem Algorithm For our application we make use of the Paillier Cryptosystem algorithm to encrypt the numerical data involved in our web-application that is the cost of component and quantity of the component. Apart from encryption it allows to make manipulations (mostly addition) on the data in its encrypted form homomorphically.

- AES Algorithm AES Algorithm is implemented in our web-application to encrypt the textual data in the system. AES is an encryption standard adopted by the US government and is a symmetric encryption algorithm that uses a single key to encrypt as well as decrypt a particular set of data.

- Key Management on the Server Our application focuses on two users, managers and researchers/employees. In any case the keys need to be stored securely on the servers. There are various ways that we explored and then came to a conclusion of making use of the most suitable one.

Chapter 5

Results

Securing pharmaceutical data using homomorphic encryption yields significant benefits in terms of data privacy, compliance, security, and collaboration. It enables organizations to leverage the power of data analytics while safeguarding sensitive information against unauthorized access and data breaches.

- Data Confidentiality: Homomorphic encryption allows pharmaceutical data to remain encrypted throughout processing and analysis. This ensures that sensitive information, such as patient records, drug formulas, and research data, remains confidential and protected from unauthorized access.
- Secure Data Processing: With homomorphic encryption, computations can be performed directly on encrypted data without decrypting it. This enables secure data processing and analysis while preserving privacy and confidentiality.
- Compliance with Data Regulations: Implementing homomorphic encryption helps pharmaceutical organizations comply with data protection regulations and standards (e.g., GDPR, HIPAA). Encrypted data mitigates the risk of data breaches and ensures adherence to privacy laws.
- Enhanced Data Sharing: Encrypted pharmaceutical data can be securely shared with authorized parties (e.g., researchers, healthcare providers) without compromising confidentiality. This facilitates collaboration and data exchange while maintaining privacy.

- Protection Against Insider Threats: Homomorphic encryption reduces the risk of insider threats by ensuring that even system administrators or service providers cannot access sensitive data in plaintext form without proper authorization.

- Data Integrity: The use of homomorphic encryption techniques helps maintain data integrity by preventing unauthorized modifications to encrypted data. Any tampering or unauthorized access attempts can be detected, ensuring the reliability of pharmaceutical data.

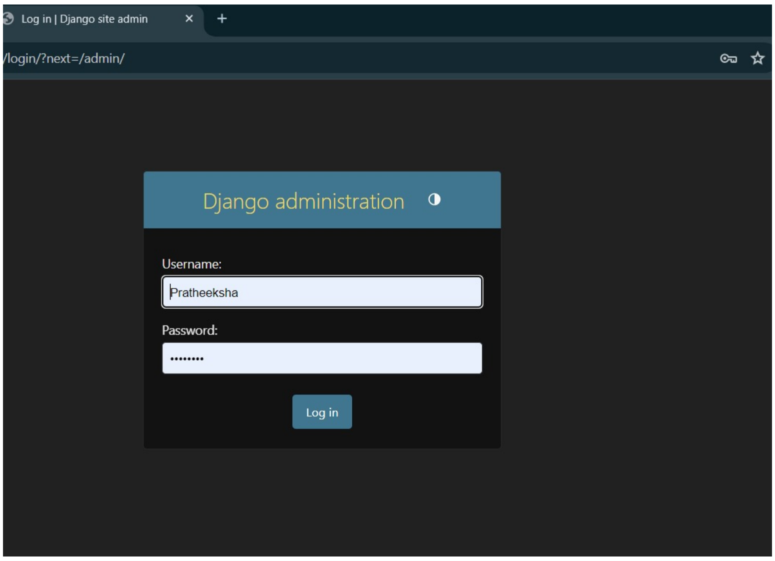
- Scalability and Efficiency: Advances in homomorphic encryption technologies have improved scalability and efficiency, making it feasible to process large volumes of encrypted data with reasonable computational overhead.

- Future-Proof Security: By adopting homomorphic encryption, pharmaceutical organizations future-proof their data security strategies against evolving cyber threats and vulnerabilities.

- Enable Secure Analytics: Encrypted pharmaceutical data can be analyzed securely to derive valuable insights and patterns without exposing sensitive information. This supports data-driven decision-making while protecting patient confidentiality.

- Trust and Reputation: Implementing robust data security measures, including homomorphic encryption, enhances trust and reputation among stakeholders, including patients, healthcare providers, and regulatory bodies.

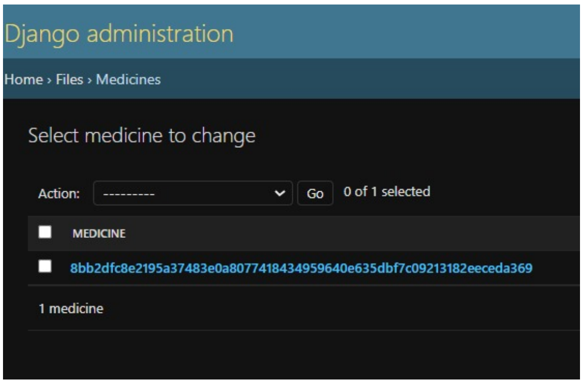
5.1 Screenshots



/login/?next=/admin/

Username: Pratheeksha

Password: ••••••••



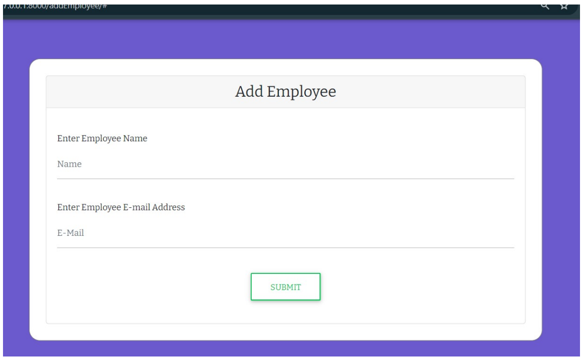
Select medicine to change

Action: ---------

0 of 1 selected

□	MEDICINE
□	8bb2dfc8e2195a37483e0a80774184349596 40e635dbf7c09213182eeceda369

1 medicine



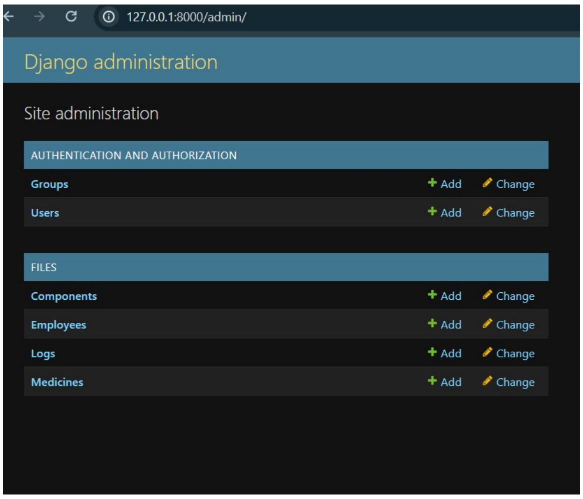
7.0.0.1:8000/addEmployee/#

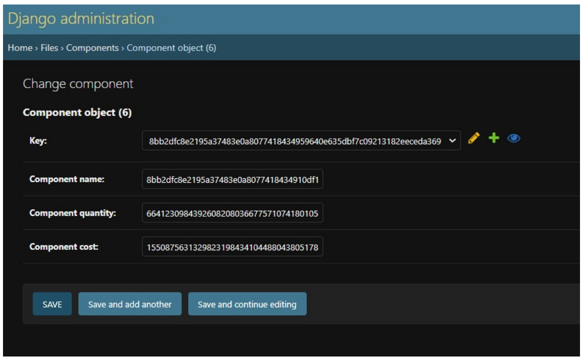
Enter Employee Name

Name

Enter Employee E-mail Address

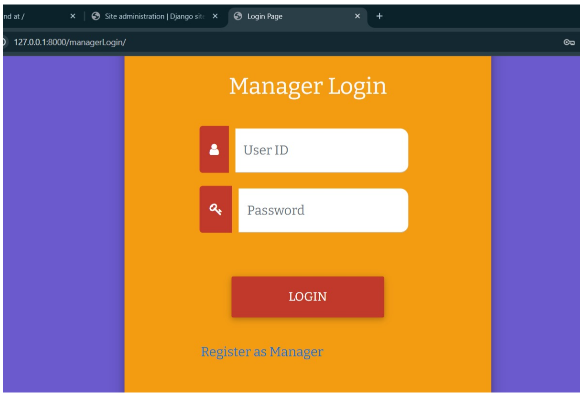
E-Mail

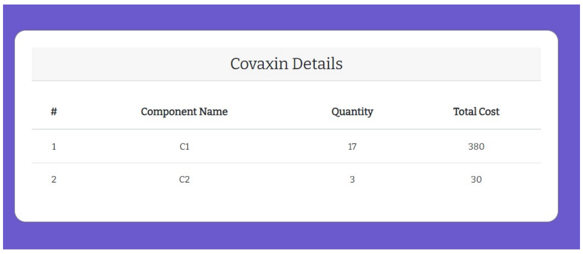



Django administration
Home › Files › Components › Component object (6)
Change component
SAVE
Save and add another
Save and continue editing

Component object (6)

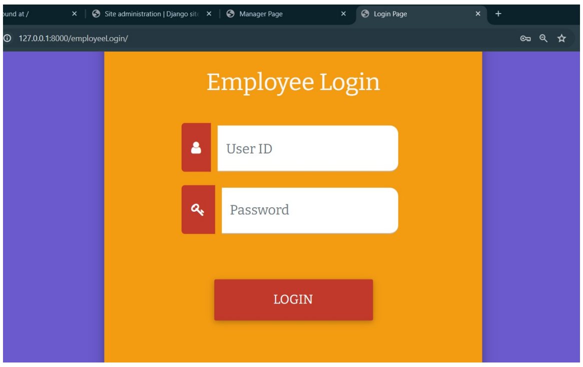
Key:	8bb2dfc8e2195a37483e0a8077418434959640e635dbf7c09213182eeceda369
Component name:	8bb2dfc8e2195a37483e0a8077418434910df1
Component quantity:	6641230984392608208036677571074180105
Component cost:	1550875631329823198434104488043805178





Covaxin Details

#	Component Name	Quantity	Total Cost
1	C1	17	380
2	C2	3	30



Chapter 6

Conclusion

In conclusion, the adoption of homomorphic encryption technology presents a transformative approach to securing pharmaceutical data and addressing critical challenges in data privacy and security within the healthcare industry. The successful integration of homomorphic encryption in securing pharmaceutical data marks a significant advancement in data protection methodologies. This project underscores the importance of leveraging innovative technologies to address complex challenges in healthcare data management while preserving patient confidentiality and regulatory compliance. Moving forward, continued research and implementation of homomorphic encryption will play a pivotal role in shaping the future of secure data analytics and healthcare innovation.

References

[1] Mohamed Nassar, Abdelkarim Erradi, and Qutaibah M. Malluhi. Paillier's encryption: Implementation and cloud applications. In *2015 International Conference on Applied Research in Computer Science and Engineering (ICAR)*. IEEE, 2022.

[2] V. Sidorov and W. K. Ng. Towards performance evaluation of oblivious data processing emulated with partially homomorphic encryption schemes. In *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*, pages 113–115. IEEE, 2021.

[3] Debasis Das. Secure cloud computing algorithm using homomorphic encryption and multi-party computation. In *2018 International Conference on Information Networking (ICOIN)*. IEEE, 2022.

[4] Fei Shao, Zinan Chang, and Yi Zhang. Aes encryption algorithm based on the high-performance computing of gpu. In *2010 Second International Conference on Communication Software and Networks*. IEEE, 2020.