IJERST

International Journal of Engineering Research and Science & Technology

ISSN : 2319-5991

www.ijerst.com

Email: editor@ijerst.com or editor.ijerst@gmail.com

https://doi.org/10.62643/ijerst.2024.v20.i3.pp238-249

ISSN 2319-5991 www.ijerst.com

Vol. 20, Issue 3, 2024

SECURING PHARMACEUTICAL DATA USING HOMOMORPHIC ENCRYPTION

[1] Mr.A.Damodar Rao,[2] M. Vani,[3] M. Neha,[4] N. Spoorthi
[1]Assistant Professor,[234]Students
Department Of CSE
Malla Reddy Engineering College for Women

ABSTRACT:-

In a time when effective data storage and access are essential to the operation of any application, cloud computing emerges as a key area of research in offering limitless storage and effective data access. However, cloud storage comes with a host of drawbacks, the most significant of which are related to user data security. In the current situation, the user is dependent on the third party—the company that provides cloud storage—to take the appropriate precautions to shield its clients' data from unwanted access and to maintain the client-company confidence that no improper handling or misuse of data will occur. The main emphasis of recent cloud computing research has been on developing and implementing cryptographic approaches that provide users control over the privacy of their data kept on cloud servers. One of the cryptographic methods that enables data modification in encrypted form without requiring decryption is homomorphic encryption. Homomorphic encryption may be used to reduce security breaches in the pharmaceutical industry, which is an industry with a high risk of them.

I. INTRODUCTION

The pharmaceutical sector generates a great deal of sensitive and private data in the form of personnel information, medical records, and prescription formulations. The sector must make sure that data is protected against cyberattacks. Cybercriminals have the ability to access or delete pharmaceutical business data, which may have disastrous consequences. For this reason, setting aside enough cash and resources is essential to keeping an effective information security management system. Information security is the process of protecting data from unwanted access, disclosure, or destruction. Cybercriminals' attacks have the potential to damage businesses and consumers billions of dollars. 46 percent [1] of reported data breaches in the US were related to medical or healthcare, according to information obtained from the Identity Theft Resource Center. Some businesses take no security precautions at all because they are unaware that they are under such danger. A danger to the pharmaceutical sector is more likely to come from an insider—an employee or contractor—than from a hacker. Given that they are tasked with handling sensitive firm data, they represent a liability. It's much harder to deal with bitter and hostile insiders than with outsiders. Insiders may undermine the system by intentionally assaulting it, making a mistake that results in unintentional exposure, misusing their record access rights, or gaining unauthorized access to information for financial gain. An example of an insider assault is provided by the Japanese pharmaceutical business Shionogi [1]. Jason Cornish, a former employee, used credentials he received from Shionogi to erase the data of fifteen virtual hosts. The firm was unable to deliver goods, send emails, or process checks as a result of this assault. The anticipated cost of the damage was $800 million. The manufacture of fake medications is a significant risk to the pharmaceutical sector. Deathly outcomes from counterfeit medications include patient fatalities. In contrast to other counterfeit goods like watches or sunglasses, it might be difficult for customers to tell whether they are purchasing a fake medication or not. Lipitor and Epogen are two instances of counterfeit medications. The creation of fake medications may result

https://doi.org/10.62643/ijerst.2024.v20.i3.pp238-249
ISSN 2319-5991 www.ijerst.com
Vol. 20, Issue 3, 2024

from the disclosure of private information about the medication. These causes have made the development of an information security management system by the pharmaceutical business imperative. It is possible to stop hackers from getting unauthorized access to sensitive data by using an effective encryption method. Insiders will only be granted access to information relevant to their department; they will not be granted access to the whole of the data. This will guarantee that information leaks by insiders cannot result in damage. Our investigation revealed that homomorphic encryption has no use at all in the pharmaceutical sector. Our goal is to create a functional system that handles sensitive data in the pharmaceutical industry in a homomorphic manner, taking into account its sensitivity. Our goal is to create a web application that lets workers at a certain pharmaceutical firm change confidential information that is kept on a database server or cloud in a homomorphic manner. Our application's scope is limited to tracking the ingredients used in the creation of a certain medication. Here, the staff member changes the quantity of certain components utilized on a daily basis via the online portal, which has a homomorphic effect on the data contained in the databases, i.e., without requiring any form of decryption on the cloud/database server data.

Problem Statement:

In order to support research, development, and the distribution of life-saving drugs, the pharmaceutical sector in the current day significantly depends on the effective storage, processing, and interchange of sensitive data. The security and privacy of pharmaceutical data are seriously threatened by the expanding threat environment of cyberattacks. A particular area of worry is the susceptibility of pharmaceutical databases to possible breaches, wherein unapproved entry may result in the compromising of confidential data, intellectual property, and even patient information.

Conventional encryption techniques provide some security during data storage and transmission, but they are insufficient for carrying out calculations on encrypted data. Advanced security mechanisms that enable safe computation on sensitive data without compromising its confidentiality are desperately needed in the pharmaceutical industry, where sophisticated data analytics and joint research are critical. Although homomorphic encryption has shown promise, there are still many obstacles to overcome before it can be used to safely and scalably secure pharmaceutical data.

Thus, the issue at hand is the insufficiency of current security protocols to safeguard pharmaceutical data from advanced cyberattacks and the shortcomings of traditional encryption techniques to allow for safe data processing. To protect against unwanted access, guarantee data integrity, and promote a safe atmosphere for cooperative research and innovation in the pharmaceutical sector, a strong framework for homomorphic encryption data security must be developed.

Objectives:

Proposed Objectives:

1. Implement Homomorphic Encryption Scheme:
   - Develop and implement a suitable homomorphic encryption scheme tailored to the unique requirements of pharmaceutical data, ensuring a balance between security and computational efficiency.
2. Secure Data Transmission and Storage:
   - Apply homomorphic encryption techniques to safeguard pharmaceutical data during both transmission and storage, preventing unauthorized access and mitigating the risk of data breaches.
3. Enable Computation on Encrypted Data:
   - Design and implement secure computational protocols that allow for meaningful operations on homomorphically encrypted pharmaceutical data, preserving its confidentiality while facilitating necessary analytical processes.

https://doi.org/10.62643/ijerst.2024.v20.i3.pp238-249
ISSN 2319-5991 www.ijerst.com
Vol. 20, Issue 3, 2024

4. Optimize Performance and Scalability:
- Address performance challenges associated with homomorphic encryption, such as computation overhead, and optimize the system to ensure scalability for large datasets typical in pharmaceutical research and development.

5. Integrate with Existing Systems:
- Develop seamless integration mechanisms to incorporate homomorphic encryption into existing pharmaceutical data management systems, ensuring minimal disruption to workflows while enhancing overall data security.

6. User Authentication and Access Control:
- Implement robust user authentication mechanisms and access control policies to regulate and monitor access to homomorphically encrypted pharmaceutical data, preventing unauthorized individuals from compromising sensitive information.

II. LITERATURE SURVEY

Roberts, Shawn Josette. "The necessity of information security in the vulnerable pharmaceutical industry." Journal of Information Security 5.04 (2014): 147

The pharmaceutical industry is a major annual income generator. The sector is evolving, with a growing reliance on technology to power day-to-day operations. Private and sensitive information, such as financial, personnel, medical, and research records, is generated in large quantities by the pharmaceutical industry. Cybercriminals target the pharmaceutical industry more often because of this. One of the pharmaceutical industry's primary responsibilities to its stakeholders, employees, and customers across the globe is the protection of patient information. Businesses should provide enough resources to develop an information security management system that works. An key component of every pharmaceutical company's infrastructure, information security management is crucial to the industry's success. When hackers harm a company's reputation, it could take a long time to fix. The main contributions of this paper will be to demonstrate the necessity of information security in the pharmaceutical industry, to outline the concerns surrounding information security in the industry, to provide examples of organizations that have helped victims of cybercrime, and to describe the regulations that have been put in place to reduce the frequency and severity of such breaches.

V. Sidorov and W. K. Ng, wrote a paper on performance Evaluation of Oblivious Data Processing Emulated with Partially Homomorphic Encryption Schemes

There are a lot of homomorphic encryption techniques available. For this reason, we reviewed the aforementioned research report to choose the one that was most appropriate for our needs. Since there is currently no practical way to compare algorithms, the aforementioned study suggests that their unique applications and the types of operations involved should be taken into consideration when choosing an algorithm.

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

More and more, studies in cloud-safe outsourcing and privacy-preserving computing are using Paillier's additive homomorphic encryption, along with other cryptographic methods like garbled circuits. For the purpose of this research, we review Paillier's encryption and its applications to secure online voting and privacy-preserving remote computing. Here we present a new version of Paillier's cryptosystem that makes use of Python as an interface language and fast GMP C-routines for mathematical computations.

https://doi.org/10.62643/ijerst.2024.v20.i3.pp238-249
ISSN 2319-5991 www.ijerst.com
Vol. 20, Issue 3, 2024

Das, Debasis. "Secure cloud computing algorithm using homomorphic encryption and multi-party computation." 2018 International Conference on Information Networking (ICOIN). IEEE, 2018.

There are a lot of security concerns about cloud computing since it is a new technology. Encrypting data in untrusted clouds is a possible option. Using the padding concept, it is possible to randomize this data on the cloud, which might lead to increased security. This paper explains how to encrypt user data using an RSA-based hybrid algorithm (HE-RSA) and a padding scheme called Optimal Asymmetric Encryption Padding (OAEP). This allows multiple parties to compute a function on inputs while keeping the data secure and private. To ensure user privacy and security in the cloud, computationally competent clouds use homomorphic encryption (HE) on encrypted data without pre-decryption, and secure multi-party computing (SMPC) is another option. To facilitate encrypted data computations without decryption, our study proposes a method that merges homomorphic encryption with multi-party computing. Our cloud model's cryptographic procedures are compared to the costs of homomorphic encryption and multi-party computing.

Shao, Fei, Zinan Chang, and Yi Zhang. "AES encryption algorithm based on the high performance computing of GPU." 2010 Second International Conference on Communication Software and Networks. IEEE, 2010.

The need for fast encryption cannot be met by the traditional AES method due to its excessively long encryption time. The GPU's high-performance computing capabilities are now the center of attention in the scientific community. This research compares CPUs and GPUs and recommends using the GPUs' high-speed processing capabilities to improve the AES algorithm. Also, the AES encryption method has been finalized; it relies on GPU high-speed processing. The results show that the GPU-based AES encryption algorithm significantly outperforms the CPU-based AES encryption method in terms of computational speed, leading to an improvement in encryption efficiency..

III. SYSTEM ANALYSIS

EXISTING SYSTEM :

Businesses and individuals might lose billions of dollars if cybercriminals launch an assault. Based on data collected from the Identity Theft Resource Center, over half of all reported data breaches in the United States involved healthcare or medical-related entities. Due to a lack of awareness, some companies do not implement any security measures all. Insiders, such as employees or contractors, pose a greater threat to the pharmaceutical industry than hackers. Because they are responsible for dealing with confidential company information, they pose a risk. Dealing with angry and resentful insiders is far more difficult than dealing with outsiders. There are a number of ways in which insiders might compromise the system. These include malicious attacks, accidental disclosure, abuse of record access permissions, and financial gain by illegal access to information. The Shionogi insider attack is exemplified by a Japanese pharmaceutical company [1]. An ex-employee named Jason Cornish deleted fifteen virtual hosts' data using credentials he obtained from Shionogi.

EXISTING SYSTEM DISADVANTAGES:

1.LESS ACCURACY

2. LOW EFFICIENCY

PROPOSED SYSTEM :

Our proposed strategy is to fix the security holes in the pharmaceutical sector. Our software is mostly used by managers and employees in the pharmaceutical sector. Workers and researchers often alter the proportions of chemicals since the process of developing new treatments includes experimentation. This information is very confidential and should only be accessible to authorized

https://doi.org/10.62643/ijerst.2024.v20.i3.pp238-249
ISSN 2319-5991 www.ijerst.com
Vol. 20, Issue 3, 2024

individuals, such the manager. Everything from adding or removing employees to seeing detailed medication information is under the manager's purview. Keeping all of the cryptographic keys encrypted on the servers adds an extra degree of protection to the application. As separate users, let's take a look at the Manager and the Workers' interactions with the system.

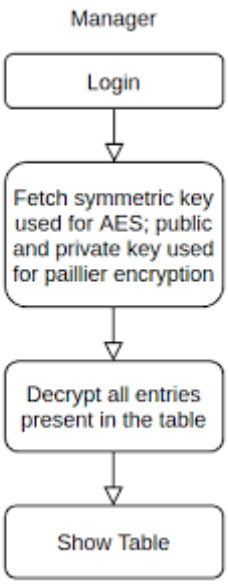
PROPOSED SYSTEM ADVANTAGES:

1.HIGH ACCURACY

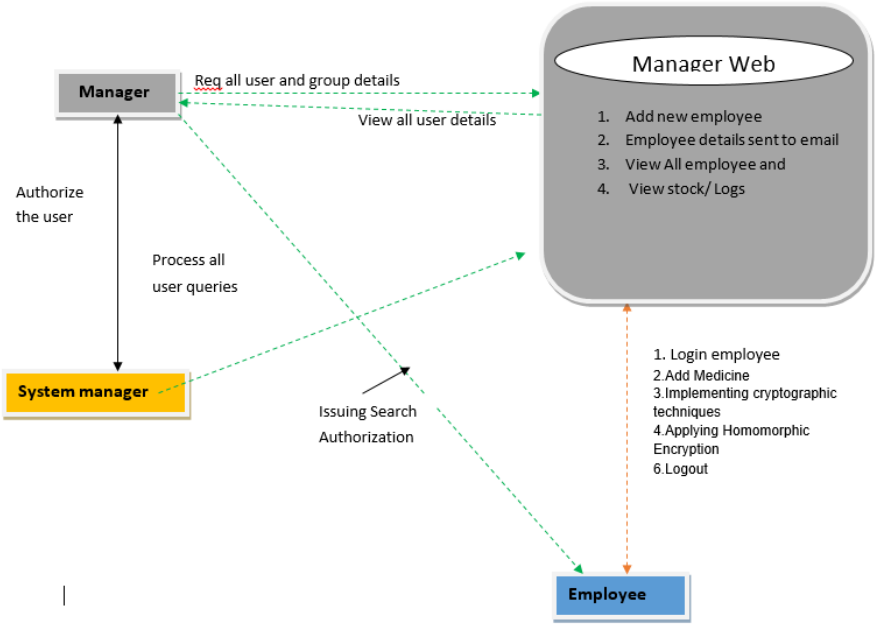
2.HIGH EFFICIENCY

IV. SYSTEM DESIGN

System Architecture



BLOCK DIGARAM



https://doi.org/10.62643/ijerst.2024.v20.i3.pp238-249

ISSN 2319-5991 www.ijerst.com

Vol. 20, Issue 3, 2024

V. SYSTEM IMPLEMENTATION

MODULES:

- User
- System

User

The user is required to enter the retina picture in this module.

System

Image pre-processing, running the CNN algorithm, retinopathy prediction, and accuracy display are all tasks that fall within this module's purview.

VI. SCREEN SHOTS

Nowadays, every business uses some combination of servers and databases connected to the internet to manage their company data. Yet, malicious outside users may breach databases and delete data, and malicious inside employees can steal or misuse the information from time to time. The development of various encryption techniques has allowed for the protection of sensitive data. When data is processed or retrieved, these techniques decrypt it after encrypting it.

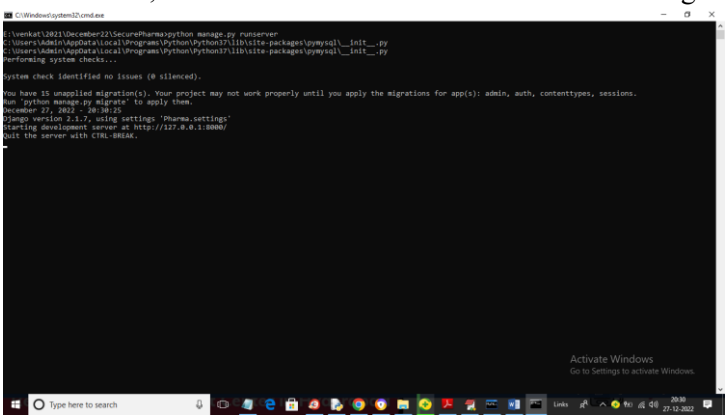
In response, the paper's author proposes homomorphic encryption, a security measure that prevents data leaking and allows processing on encrypted data without decryption. Encryption provides security when stored, but it becomes susceptible to abuse when processed.

The suggested study's author ensures the security of the pharmaceutical database that management and personnel would access. The employee is provided with a username and password once their manager enters their information. They may use these to access the system to input or update the medicine's quantity, price, and other data. If the previously encrypted amount already exists in the database, the new quantity is appended to it when using homomorphic encryption. A new record is then produced for the database. Because employees would not have direct access to the data, it will be protected.

The application may be accessed by the manager with the credentials "admin" and "admin," who can then search through employee and LOG data for various drugs.

To begin the project, open MySQL and create a database using the contents of the DB.txt file.

To launch the Python web server, double-click the "run.bat" file. The following output will be shown.

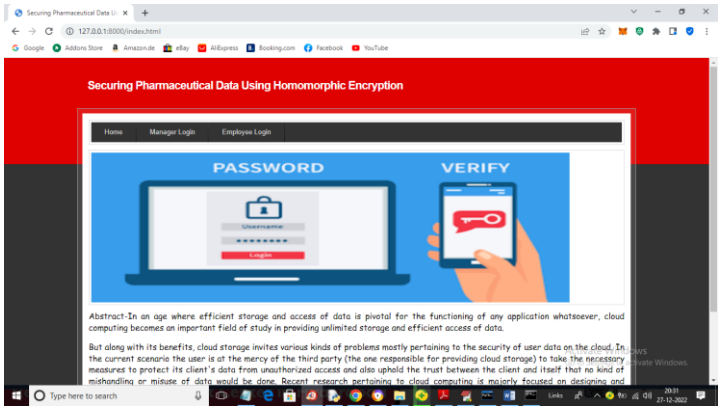


In above screen python web server started and now open browser and enter URL as http://127.0.0.1:8000/index.html and press enter key to get below page

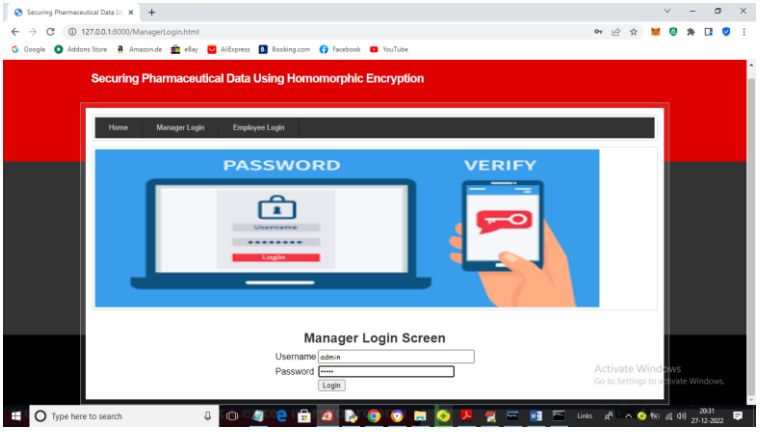
https://doi.org/10.62643/ijerst.2024.v20.i3.pp238-249

ISSN 2319-5991 www.ijerst.com

Vol. 20, Issue 3, 2024



Click on the "Manager Login" link on the top screen to get to the page below.



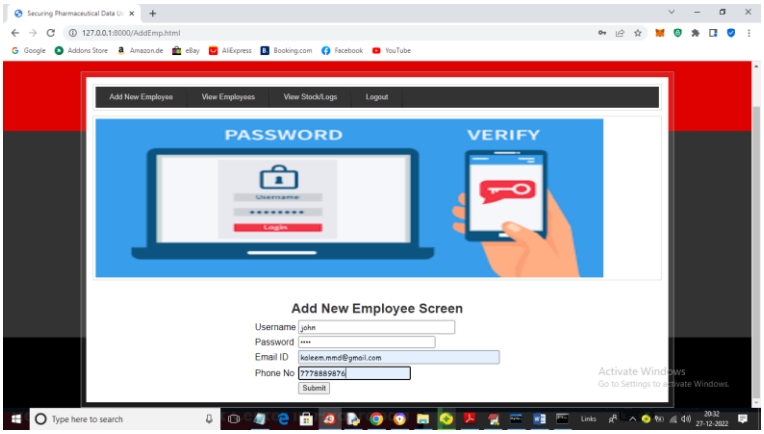
In above screen manager is login and after login will get below page

In above screen click on ‘Add New Employee’ link to get below page

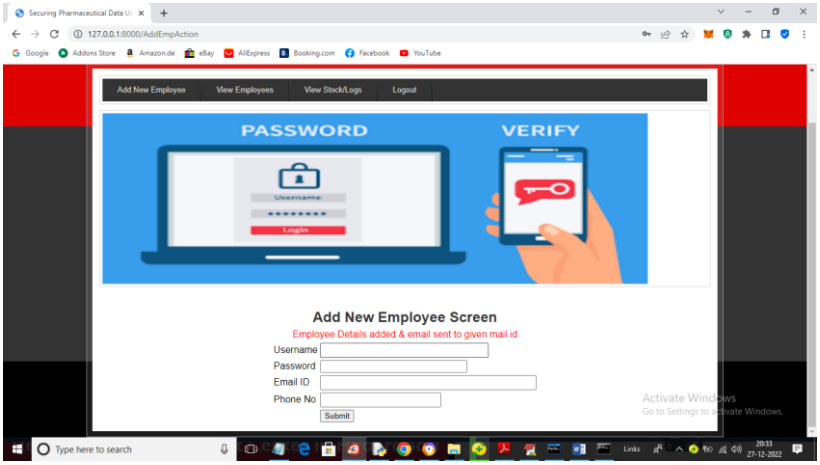
https://doi.org/10.62643/ijerst.2024.v20.i3.pp238-249

ISSN 2319-5991 www.ijerst.com

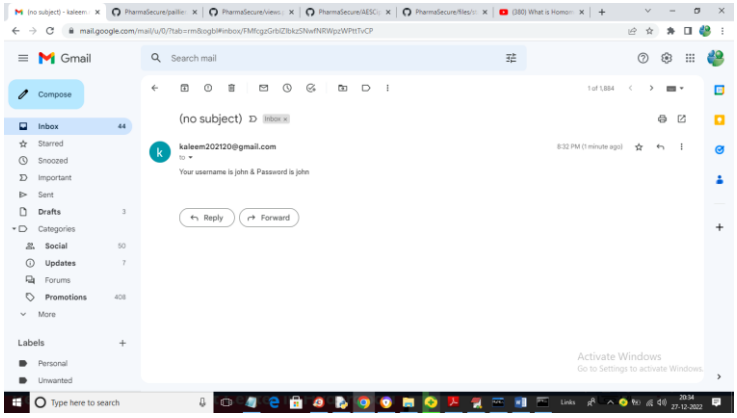
Vol. 20, Issue 3, 2024



In above screen manager adding employee details and give valid email id to receive mails



In above screen employee details added and now we can check mail

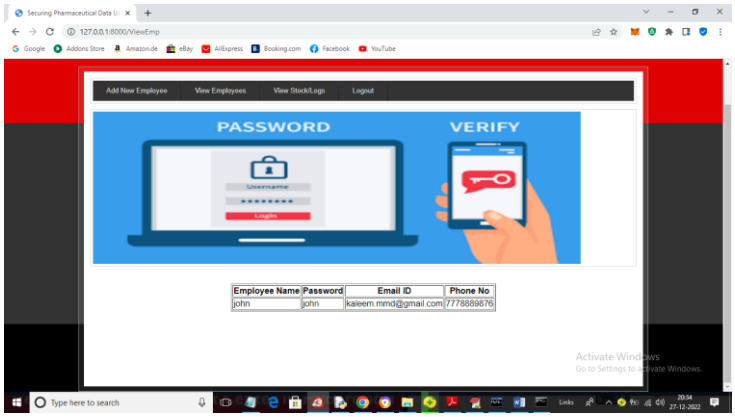


In above screen we got mail for username and password and now manager can click on 'View Employee' link to view details

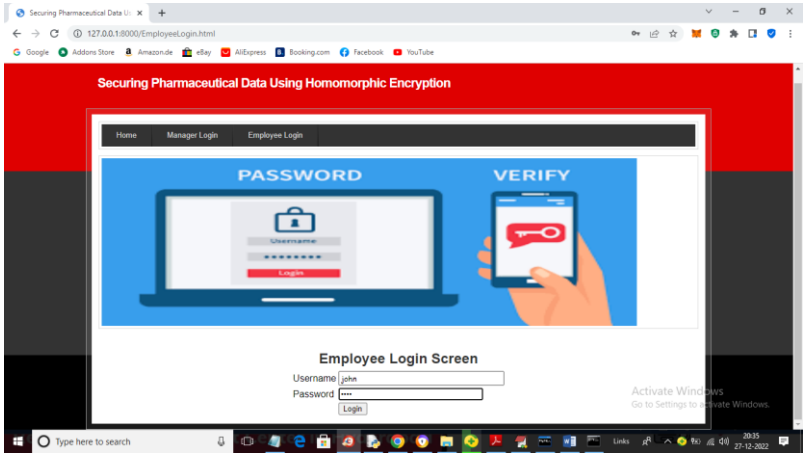
https://doi.org/10.62643/ijerst.2024.v20.i3.pp238-249

ISSN 2319-5991 www.ijerst.com

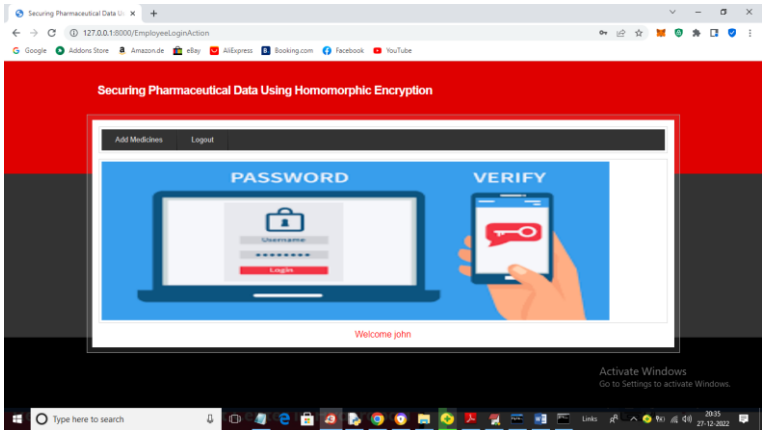
Vol. 20, Issue 3, 2024



In above screen manager can view all employee details and now logout and login as employee to add medicine details



In above screen employee is login and after login will get below page

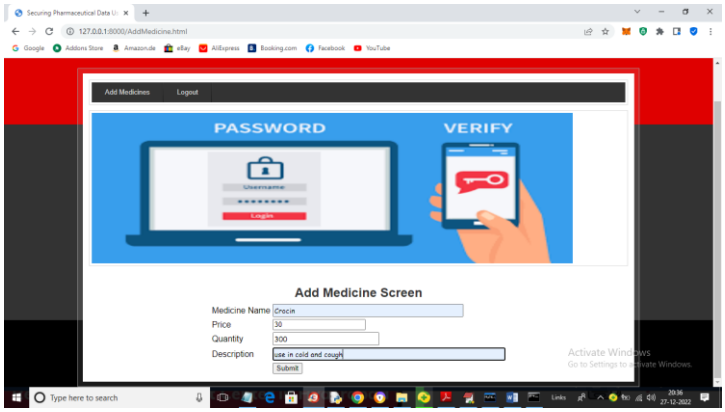


In above page employee can click on 'Add Medicines' link to add medicine details

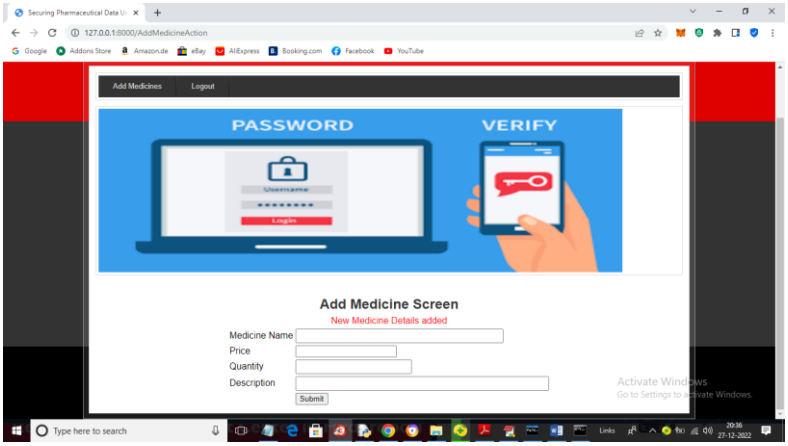
https://doi.org/10.62643/ijerst.2024.v20.i3.pp238-249

ISSN 2319-5991 www.ijerst.com

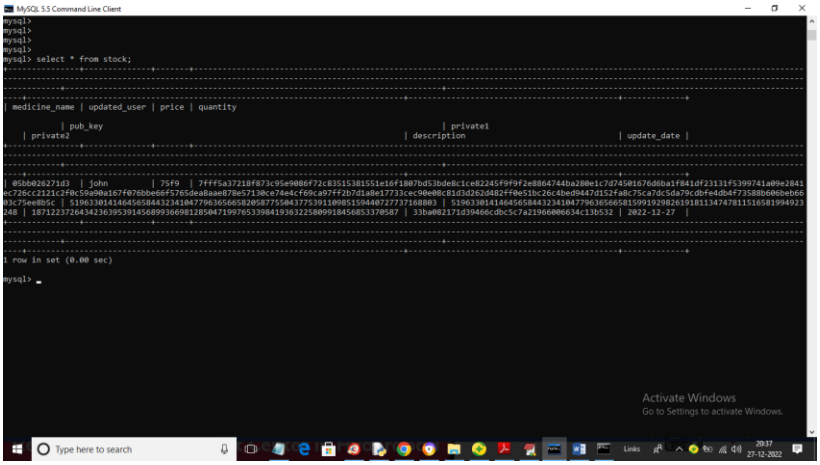
Vol. 20, Issue 3, 2024



In above screen employee adding medicine details and press button to get below page



The information about the drug is shown in the above screen, and by using the same name, you may add more quantities to update their quantities. The database screen below shows that all data is secured.

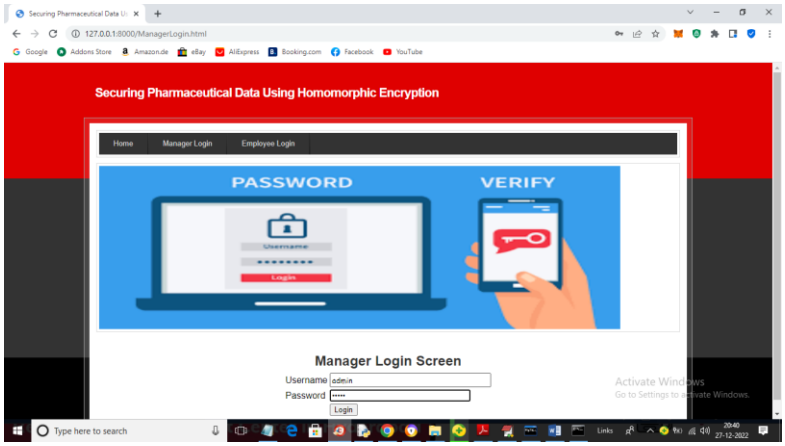


All of the data is shown in an encrypted way on the above screen; no one can read it. Now the manager may log in and see the information of those medications in an unencrypted form.

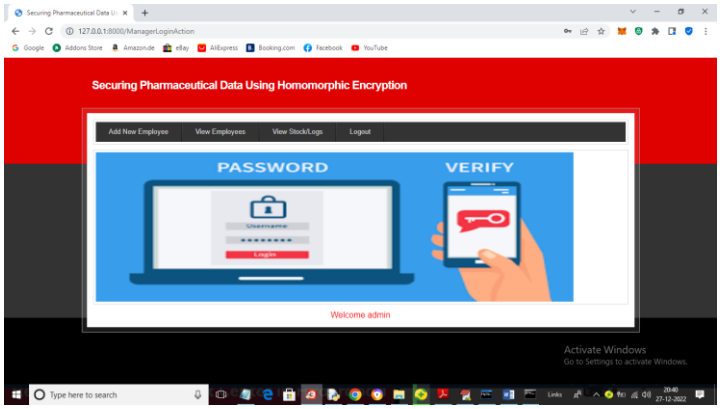
https://doi.org/10.62643/ijerst.2024.v20.i3.pp238-249

ISSN 2319-5991 www.ijerst.com

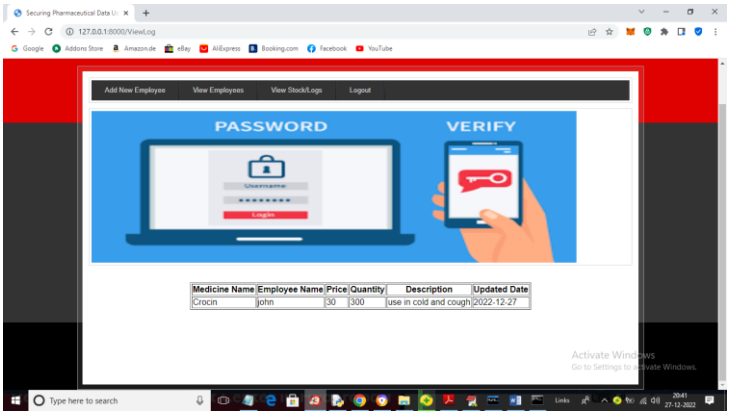
Vol. 20, Issue 3, 2024



In above screen manager is login and after login will get below page



In above screen manager can click on 'View Stock/Log' link to view medicine details in decrypted format



In above screen manager can view all details in decrypted format. Similarly you can add many records and can decrypt and view

VII. CONCLUSION

In a functional prototype, we succeeded in implementing homomorphic operations as envisioned. As was previously said, we created an application that enables staff members of a certain pharmaceutical firm to change confidential information on the server cloud/database without having to first decode any encrypted data that is kept there. Given the significance of keys in executing these homomorphic procedures, it was imperative to safeguard these keys, which were unique for each user gaining access to the program. To do so, we created a secure key generation and storage feature that added an extra

https://doi.org/10.62643/ijerst.2024.v20.i3.pp238-249
ISSN 2319-5991 www.ijerst.com
Vol. 20, Issue 3, 2024

degree of protection to the application by storing the keys in an encrypted state on the server and limiting access to them to unique login credentials.

Future Scope

We try to present a possible use of homomorphic encryption in a pharmaceutical firm scenario in this research work. Our proposed idea does not always rely on homomorphic characteristics, in contrast to the Paillier method's encryption function which employs a randomly chosen prime integer. For example, instead of the Paillier method, we encrypted the text using the AES algorithm. Consequently, a particular text is encrypted to a new value whenever data (such the name and quantity of the component) is updated or inputted. In addition, there is no way to append characters to encrypted text using homomorphic techniques. To resolve these issues, more research may be undertaken. Despite these reservations, we are nonetheless hopeful that our study and the proposed method can pave the way for more investigations in this field.

REFERENCES

1. Roberts, Shawn Josette. "The necessity of information security in the vulnerable pharmaceutical industry." Journal of Information Security 5.04 (2014): 147
2. Homomorphic Encryption: An Overview - https://www.sciencedirect.com/topics/computerscience/homomorphic-encryption.
3. Nassar, Mohamed, Abdelkarim Erradi, and Qutaibah M. Malluhi. "Paillier's encryption: Implementation and cloud applications." 2015 International Conference on Applied Research in Computer Science and Engineering (ICAR). IEEE, 2015..
4. Islam, Naveed, William Puech, and Robert Brouzet. "How to secretly share the treasure map of the captain?." Multimedia on Mobile Devices 2010. Vol. 7542. International Society for Optics and Photonics, 2010.
5. V. Sidorov and W. K. Ng, "Towards Performance Evaluation of Oblivious Data Processing Emulated with Partially Homomorphic Encryption Schemes," 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), New York, NY, 2016, pp. 113-115.
6. Das, Debasis. "Secure cloud computing algorithm using homomorphic encryption and multi-party computation." 2018 International Conference on Information Networking (ICOIN). IEEE, 2018.
7. Shao, Fei, Zinan Chang, and Yi Zhang. "AES encryption algorithm based on the high performance computing of GPU." 2010 Second International Conference on Communication Software and Networks. IEEE, 2010.
8. Where to store a server side encryption key?, https://security.stackexchange.com/questions/12332/where-to-store-a-server-sideencryption-key
9. Liu, Jian-dong, Shu-hong Wang, and You-ming Yu. "TDHA-A One-Way Hash Algorithm Based on Extended Integer Tent Maps with Dynamic Properties." 2008 International Symposium on Electronic Commerce and Security. IEEE, 2008.
10. What is the avalanche effect in cryptography? How can we measure it ?, https://www.researchgate.net/post/What_is_the_avalanche_effect_in_cryptography_How_can_we_measure_it
11. Additive ElGamal encryption algorithm, https://crypto.stackexchange.com/questions/9000/additive-elgamal-encryption-algorithm