ISSN: 2395-7852

International Journal of Advanced Research in Arts, Science, Engineering & Management

Volume 10, Issue 3, May 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 6.551

+91 9940572462 +91 9940572462 ijarasem@gmail.com www.ijarasem.com

International Journal of Advanced Research in Arts, Science, Engineering &Management (IJARASEM)

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 6.551 |Bimonthly, Peer Reviewed & Referred Journal|

| Volume 10, Issue 3, May 2023 |

Cryptographic Representation of Critical Pharmaceutical Data using Pallier Homomorphic and AES Techniques

Mrs. Suma K[1], Ameesha[2], Amogh Puranik[3], Anjani J[4], Ashish U Shetty[5]

Senior Assistant Professor, Mangalore Institute of Technology and Engineering, Moodbidri, Karnataka, India[1]

UG Student, Mangalore Institute of Technology and Engineering, Moodbidri, Karnataka, India[2 -5]

ABSTRACT: The ability to provide infinite storage and effective access to data has become crucial in a time when both are essential for the operation of any application. However, in addition to its advantages, it also presents a number of issues, most of which are related to the security of user data. In the current situation, it is incumbent to the third party to take the appropriate precautions to safeguard its clients' data from unauthorized access and to sustain the confidence between the client and itself that no data processing or misuse would occur. The majority of current storage research is devoted to developing and putting into practise cryptographic methods that let the user be in charge of the privacy of the data that is being stored on the system. The safe system known as Pharma Prudent is designed to protect the priceless pharmaceutical assets stored in the database. One of the cryptographic methods is homomorphic encryption, which enables alteration of data while it is encrypted without the need to decrypt it first. Pharma Prudent uses homomorphic encryption techniques to protect data within the company because the pharmaceutical industry is a sector with a high risk of security breaches and brute-force attacks.

KEYWORDS*:* Cryptographic method**,**Homomorphic encryption**,** Pharmaceutical industry, Security breaches,Brute-force attacks.

I.INTRODUCTION

The pharmaceutical industry generates enormous amounts of sensitive and private data, such as personnel information and drug formulations. The industry must make sure that cybercrime doesn't access their information. By obtaining or erasing the pharmaceutical industry's information, cybercriminals might cause irreparable damage. The pharmaceutical sector is more at risk from an internal contractor or employee than it is from a hacker. They are a liability because they are trusted with the company's private information. Outsiders are considerably easier to handle than hostile and disgruntled insiders. Insiders may harm the system by intentionally assaulting it, misusing their record access rights, accidentally disclosing information, or accessing it for financial gain. These factors have made creating an information security management system for the pharmaceutical business a requirement. With this goal in mind, Pharma Prudent seeks to provide an improved security solution for the organization's pharmaceutical assets. By utilising a powerful encryption technique, it is possible to stop hackers from gaining unauthorised access to important data. Additionally, only the information relevant to their department will be made available to insiders; they will not be given access to the entire database. In this way, it will be impossible for insiders to damage others by leaking knowledge. Our application's focus is on keeping track of the ingredients required to make a certain treatment. Here, the employee updates the amount of specific components used on a daily basis through the web portal, and this information is homomorphically (i.e., without involving any kind of decryption process on the data stored on the cloud/database server) reflected on the data stored in the databases. An encryption algorithm known as a homomorphic encryption algorithm enables mathematical operations to be carried out on encrypted data. This implies that data processing can be delegated to a third party without having to have faith in the security of the data. Therefore, it is impossible to access the original data without the correct decryption key. This method aids in

preventing data breaches within the company. The capacity to process encrypted data has the potential to address a number of significant business issues encountered by businesses in all sectors.

II.LITERATURE REVIEW

Das, Debasispresented 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.

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

Shao et al. presented a paper regarding an efficient way of implementing AES algorithm Since Homomorphic Encryption doesn't allow us to encrypt textual data in accordance with our proposed methodology. Therefore we analyze this paper to gain insight on the working of the AES algorithm which is used in our proposed methodology to encrypt the textual data on the server.

No.	Paper Title	Author Name	Key Points	Remark
1	Secure cloud computing algorithm using homomorphic encryption and multi-party computation.	Das, Debasis	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	It proposes a scheme and compares the results with existingstandards, integrating homomorphic operations with multi-party calculations.
2	Towards Performance Evaluation of Oblivious Data Processing Emulated with Partially Homomorphic Encryption Schemes	V. Sidorov and W. K. Ng	There are various Homomorphic Encryption Algorithms available. To decide which one suits our application better, we analysed the above research paper	It proposes a scheme that there exist no empiricalway of comparing the algorithms and based on one's own application and the type of operations involved , a particular algorithm should be selected.

3	AES encryption algorithm based on the high performance computing of GPU.	Shao, Fei, Zinan Chang, and Yi Zhang.	This paper proposes that AES algorithm is improved by use of GPU's high performance computing capability and compared with that using CPU. And AES encryption algorithm base on high performance computing of GPU is also completed.	Therefore we analyze this paper to gain insight on the working of the AES algorithm which is used in our proposed methodology to encrypt the textual data on the server.

III.METHODOLOGY OF PROPOSED SURVEY

In this project, we aim to improve the security flaws currently existing in the pharmaceutical industries. The Manager head and Employees/Researchers who work in the pharmaceutical sectors are our application's two main users. In the process of creating medicines, employees and researchers conduct experiments, which results in frequent changes to the components' component quantities. Since these pieces of information are very private, only authorised individuals, such as the manager, should have access to them. The manager is in charge of all decisions, including whether to hire or fire people and what specifics go into medications. A further layer of protection is added to the application by the secure storage of all cryptographic keys (in encrypted form) on the servers. Let us analyse how each user namely the Manager and the Employees interact with the system.

The manager of a specific department is in charge of monitoring the development of a specific medicine and the specifics of its components. Every time a manager logs in, the keys needed to access the hidden data are first fetched, and all entries are then decrypted to reveal the information to the management. The flowchart figure 1 displays the actions a manager would take.

The researchers and employees who are in charge of a medicine's real development make up the second group of users of our system. The full facts of the medication shouldn't be disclosed to these individuals because doing so could result in security breaches. The researcher must submit his research's specifics, such as componentquantityand price, to start the process. The programme then begins by determining whether or not the database already has that specific component. If so, the amount and quantity are homomorphically added; otherwise, a new entry is put into the table. The steps outlined in the flowchart figure 2 are then carried out after the necessary keys have been retrieved from the server.

For our application we make use of the Paillier Cryptosystem algorithm to encrypt the numerical data used in our web application, which is the component cost and component quantities. In addition to encryption, it enables homomorphic actions (most often addition) on the data. Our web application uses the AES Algorithm to encrypt the textual data it stores. The US government has selected the symmetric encryption method known as AES, which employs a single key to both encrypt and decrypt a specific set of data. Along with encrypting data, we also use the AES algorithm to protect some files that contain keys important to the operation running in our web application. Our application focuses on two users, managers and researchers/employees. In any case the keys need to be stored securely on the servers. Keeping keys in a specific file and encrypting that file with the user password or an analogous key is one way to store them safely on the server. One of this service's key benefits is giving users greater control when they log in to the system to obtain results. For managers, we utilize their own passwords, whereas for employees, we use the name of the medicine that the manager added for that specific employee. We consider the medicine name's security issues and keep it on the server in encrypted form as a result. With the help of this functionality, the employee is able to alter information about the medicine to which the manager added him.

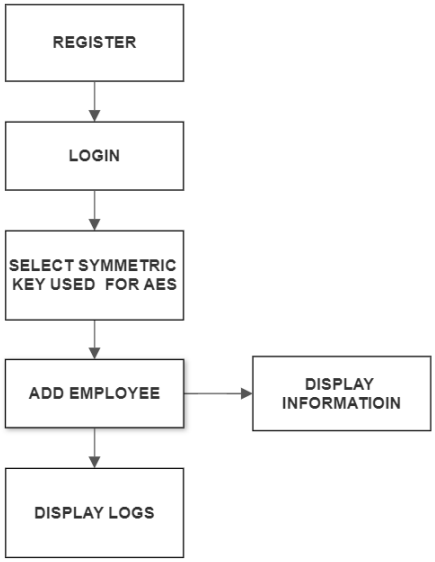

Figure 1: Flowchart of Manager Actions

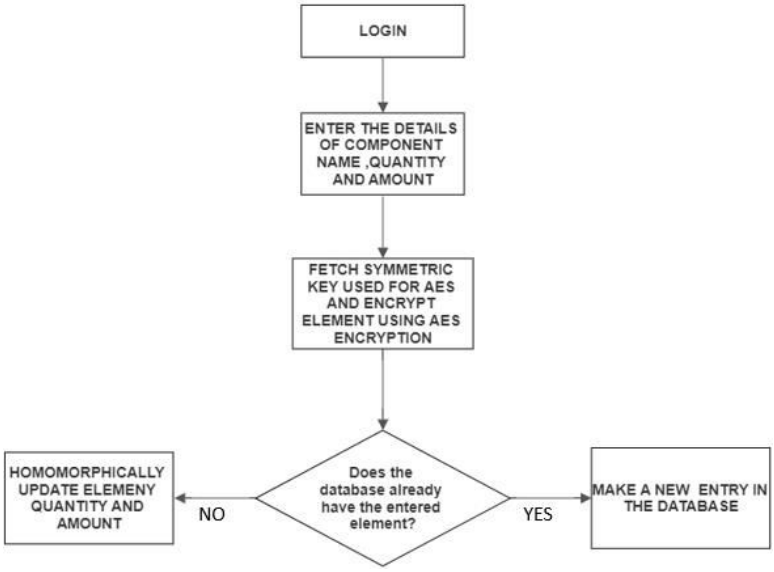

Figure 2: Flowchart of Employee/Researcher Actions

IV.CONCLUSION AND FUTURE WORK

In this paper we have proposed an approach to protect the pharmaceutical organization's predominant asset's data in the cloud/database by using the cryptographic techniques of Advanced Encryption Standard and Paillier homomorphic algorithmic techniques. In order to implement homomorphic operations as planned, we developed an application that enables researchers at a particular pharmaceutical company to update sensitive data on the server database without having to first decrypt any encrypted data that is stored on the cloud or database. It was essential to preserve these keys, which are unique to each person utilising the application, given the importance of keys in carrying out these homomorphic acts. To do this, we developed secure key generation and storage technology that stored the keys on the server in their encrypted form

and was only accessible based on login credentials, which in and of themselves were unique, adding an additional layer of security to the application.

REFERENCES

1. V. Sidorov and W. K. Ng, "Towards Performance Evaluation of Oblivious Data ProcessingEmulated 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.
2. Das, Debasis. "Secure cloud computing algorithm using homomorphic encryption and multiparty computation." 2018 International Conference on Information Networking (ICOIN). IEEE,2018.
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. 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.
5. Homomorphic Encryption: An Overview -https://www.sciencedirect.com/topics/computer-science/homomorphic-encryption.

International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

| Mobile No: +91-9940572462 | Whatsapp: +91-9940572462 | ijarasem@gmail.com |

www.ijarasem.com