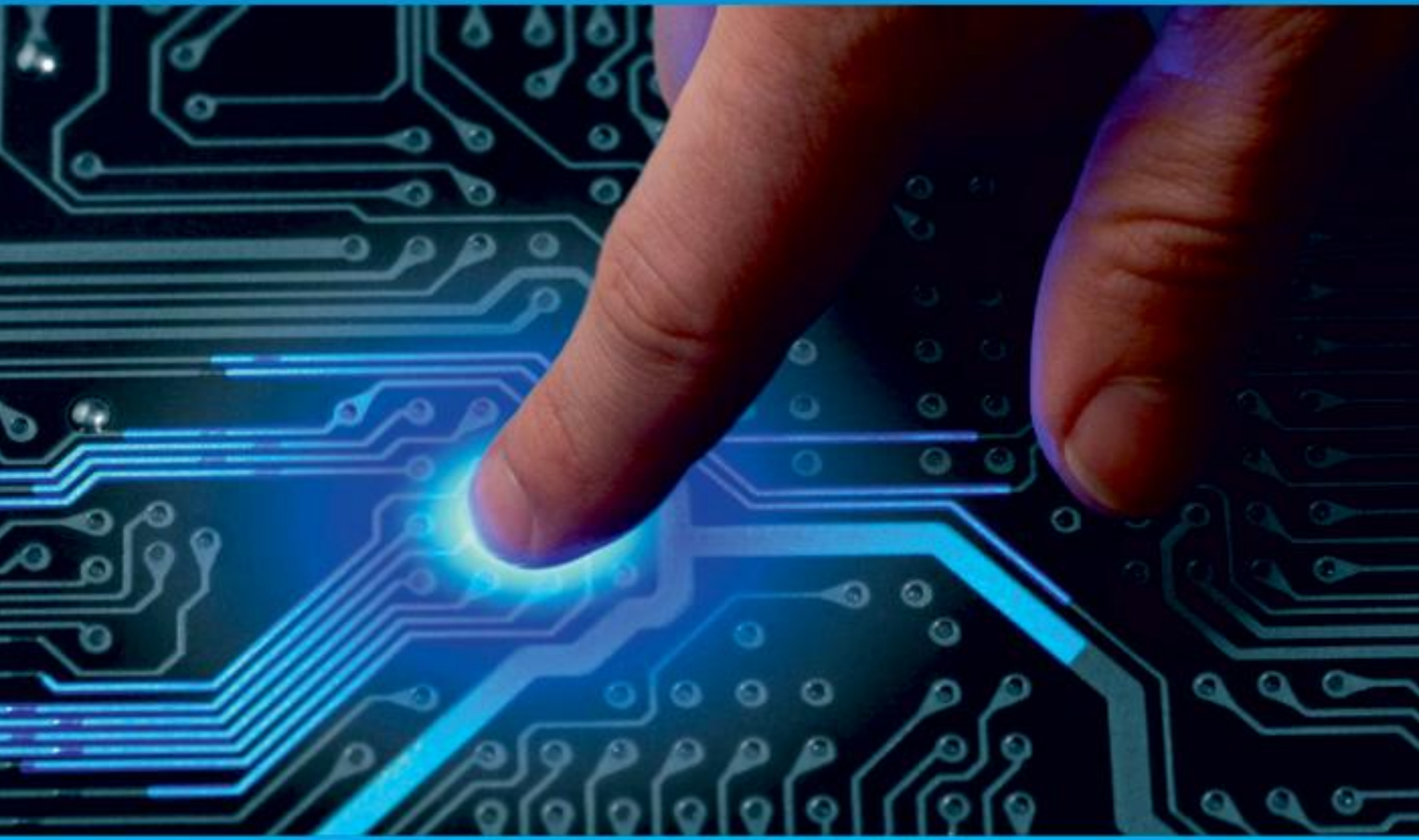
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Special Issue 1, March 2024

1st International Conference on Machine Learning, Optimization and Data Science

Organized by

Department of Computer Science and Engineering, Baderia Global Institute of Engineering and Management, Jabalpur, India

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 || Monthly Peer Reviewed & Refereed Journal |

| "1st International Conference on Machine Learning, Optimization and Data Science"|

Organized by

| Department of Computer Science and Engineering, Baderia Global Institute of Engineering and Management, Jabalpur|

|| Volume 12, Special Issue 1, March 2024 ||

Enhancing Cloud Data Security through the Integration of Machine Learning Model & Homomorphic Encryption Technology

Prof. Pankaj Pali, Prof. Jaya Choubey, Prof. Abhishek Patel

Asst. Professor, Dept. of CSE., Baderia Global College of Engineering and Management, Jabalpur (M.P), India

Asst. Professor, Dept. of CSE., Baderia Global College of Engineering and Management, Jabalpur (M.P), India

Asst. Professor, Dept. of CSE., Baderia Global College of Engineering and Management, Jabalpur (M.P), India

ABSTRACT: In the last decades, Cloud Computing trend has got a boost growth. The main reason behind was establishment of Large & Small Organization of every field. Due to its privileges and flexible nature, numerous organizations adopt it. The main benefit customer get is that they do not have to spend huge amount for the system they want to compute their task, but Cloud provide resources for that like software, hardware, data storage etc. The significant challenge that the Cloud Providers and Customer are facing was security concern towards data which is stored on the third party cloud server. It is the trust of the customer to Providers that their data is safe evens the data accessible or travelling over the internet or over the network which is essential for the honor of the service providers company.

So here we are reviewing a Machine Learning trained Model that can analyze access patterns and data usage frequently. By monitoring these patterns and frequency of data usage, Model predict Security threats and apply a Homomorphic Encryption Technology on the data before transmit over the Network which results the enhancement of the Privacy & Security.

KEYWORDS: Cloud Computing, Security, Homomorphic Encryption, Privacy, Machine Learning.

I. INTRODUCTION

Now days, Cloud Computing Technology is the most rising technology comes in the real world, organizations, users, and other techies are more aware of the superiority of the Cloud Computing offers to their customers. No doubt, Cloud Computing is the next generations system which provides it users everything they need for the computation of their tasks.

Cloud Computing Storage mainly deals with three security issues, Confidentiality, Integrity & Availability. "Confidentiality" means data is confidential to others, no unauthorized access to the data either at Rest or on Network. "Data Integrity" means content of the data should not be breached.

"Availability" means whenever the customer or user wants to access the data, the data should be available to them.

Cloud Storage services are commonly used to store & backup any type of data that are seen accessible, affordable & user friendly. They also make it easier for consumer to share data and synchronized with multiple devices. Certain essential data is saved and handled by systems. The loss or exposure of the priceless data will negatively affect the persons or organizations that control the data. As a result, there is growing need for Cloud data protection [1].

Inspire by the aforementioned above, this review paper focuses on two aspects, first is to keep tracking of the frequently used data on the cloud by using Machine Learning Model and secondly apply extra layer of security to that data using Homomorphic Cryptography technology.

Most of the organizations using traditional encryption method for securing the data on the cloud at rest or at transit. But if they want to analyze or investigate the data they have to either download it (here also data get decrypted) or decrypt it. Here if we go with first approach then the security issue occurs and if we go with second approach then it is time consuming and costly. So here we can understand the value of Homomorphic Encryption. Organizations can share the private data for the evaluation without compromising the security of the data. The data always be in encrypted form andcomputation performs on the encrypted data only.

The Homomorphic Encryption categorized into three categories Partial Homomorphic Encryption, Somewhat

Homomorphic Encryption and Fully Homomorphic Encryption.

- **Partial Homomorphic Encryption (PHE):** only particular mathematical operations can be performed on encrypted values using partially holomorphic encryption (PHE). This suggest that the encrypted data can only be subjected to a single or infinite operations – either addition or multiplication.

- **Somewhat Homomorphic Encryption (SHE):** up to a certain level of complexity, a SHE system can support a single operation (either addition or multiplication), but it can only perform these operations a certain number of times.

- **Fully Homomorphic Encryption (FHE):** FHE helps to preserve data security while preserving accessibility, which is why it has significant potential for balancing functionality and privacy. FHE which is developed fromSHE system, improves the effectiveness of secure multi-party computation by enabling the infinite use of addition and multiplication operations. It is capable of handling arbitrary calculations on your encrypted data, in contrast to other forms of homomorphic encryption. The goal of FHE is to make it possible for people to use encrypted data to carry out useful tasks without needing the encryption key. In particular, there may be application for this idea to improve cloud computing security. FHE gives you a way to access, search and alter your data without giving the cloud provider access, which is useful if you plan to store encrypted data in the cloud but don't want to run the risk of a hacker gaining access to your account.

Application of Fully Homomorphic Encryption: Numerous real-world uses of FHE have already been found by researchers, a few of these are as follows:

- **Securing Data Stored in the Cloud:** by utilizing this method, we can protect the information stored in the cloud without sacrificing the integrity of the data. Calculation or analysis can be done on the data without decrypting it.
- **Enabling Data Analytics in Regulated Industries:** this technique allows data to be shared to outsourced or commercial cloud environment for research and for other purposes while protecting the data privacy.
- **Improving Election Security and Transparency:** Some of the research is going on using the Homomorphic Encryption to conduct Elections more security and transparency.

From all of the above, we can easily identify that now Homomorphic Encryption is more efficient and provide more security to data. Due to its ability of accessing data without decrypt the data make it more suitable for the Cloud Computing technology as there data travels more on the network, and due to cloud storage data always have a chance of vulnerability. So this technique secure the data more with the regular encryption technique.

II. RELATED WORK

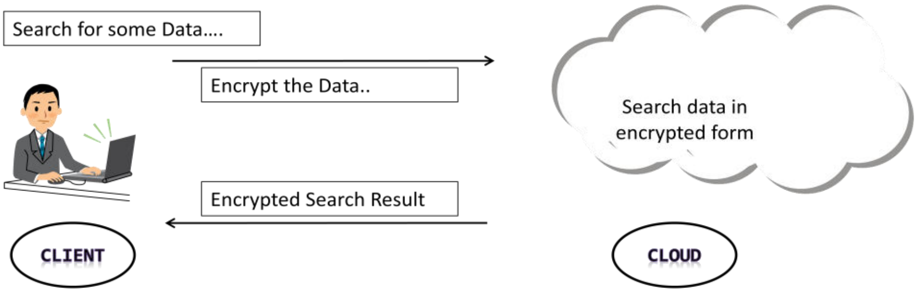
As of the boost evolution of the industrialization, utilization of the cloud is also accelerated. With knowing or without knowing, everyone is using cloud storage services like Drop box, Gmail or MS Office 365. In [2], the author prepared a case study for detailed analysis of the security and privacy challenges faced by the customer or providers considering cloud storage as a service. In above case study, authors discuss the security concerns like data privacy, data security, access control, cyber-attacks & data availability along with performance and reliability. In [3], the authors proposed a model that provides explanation to some safety features of cloud like data security from breaking and protect the data from fake identity user, which can breach the security of cloud data. It lightens the multiple issues and investigates problems face by the cloud computing regarding security and privacy. They provide effective solutions of data security by enhancing the encryption algorithm of data in the cloud. They not only protect the data at rest but also provide scalability of data shared by others.

As we know that the most regular way for provide security to data in the cloud is Encryption. In [4], the author states that providing same security policy is not an ideal way, as not all the data has same sensitivity for the data owner, so they present new method which improves data security in cloud storage. Authors actually combining Machine Learning and Data Classification decision making to classify the data into categories before apply encryption into it. The paper apply suitable encryption algorithm according to their classification, as a result they claim an effective and efficient method with great accuracy, also ensuring sensitivity and integrity of the data at the same time. We all know the benefits of the cloud computing and security & privacy is the main issue with it. As the cloud computing means providing virtual environment like as it was real. Encryption is the main method for the protection of the data in the cloud, the efficiency and speed of encryption techniques differ & level of security is not constant. In [5], the author analyze and understands the above concerns and found out that data classification is the foundation for data security. Here they introduce with data classification based theory, which is based on a set of crucial parameters that are necessary for the security and privacy of the data in a shared network, categorizing the data into low, moderate and high category and secure according to it. In [6], they mention the security services policies for the network, data and infrastructure. They introduced the security not only related to data store on cloud at rest but also different security issues can be taken granted like Network security, User Identity security, Data Storage security, Application security. They provide detailed description about the mentioned securities above.

In [7], the author explore the security issues surrounded by the cloud computing and proposed appropriate solutionto accommodate the problems. They talk about the AES (advanced encryption standard algorithm) encryption in data and how they play an important role in securing the data safe on the cloud. In [8], the author and their team proposed a security algorithm which can protect or provide extra security to the data. According to model proposed in this paper, the data categorized into different groups according to their confidentiality which is mention by the user and provide encryption technique according to that they use different encryption techniques like Secure Hash algorithm (SHA), Advanced Encryption Standard algorithm (AES), Transport Layer security (TLS). These algorithms used to encrypt the data based on the security level mention by the user. In [9], the primary purpose of the author’s presentation of this paper is to provide an overview of the top security flaws and alert the users as well as the developers to the potential threats linked to the data stored on cloud. In [10], the author prevailing the problem associated with cloud computing, that problem is security of data on cloud and suitable implementation of cloud over network. In this, the author implement the data security by accessing the data using Cloud Storage Methodology and use of the encryption technique “RSA algorithm”. According to user, Digital Signature with RSA technique can enhance the security of data over the cloud.

III. PROPOSED WORK

When we store the data on the cloud, the user owns an encryption key to the entire stored data. If the service provider or the any Third party (like in Public Cloud) needs to perform some analytics operations or computations, the client provide the private key to the server (Service Provider) to decrypt data before computations or calculations required, which effect the Privacy, Confidentiality and Security of the data on the Cloud. So Homomorphic Encryption allows a user to decrypt portions of the data block from the cloud, the private data kept secured locked up, but analysis & computation still provide valid result. Like here for Public Cloud this technique comes very effective as the data is shared with others, so by using this data remains encrypted all the time, which enhanced the Data Security (i.e. Confidentiality, Security & Privacy) on the cloud.



Homomorphic Encryption Technique

Homomorphic Encryption can be defined as the process of converting one data set to another while maintaining the connection between the components in both sets. The data in this method is still structured and the mathematical operations yield an equivalent result regardless of the data’s format (either in its Original form or in Encrypted form).
Homormorphic Encryption is mainly categorized into two category :

- Fully Homomorphic Encryption (FHE): allows random computations on encrypted data.
- Partial Homomorphic Encryption (PHE): allows specific computation like addition or multiplication. (two

types of PHE process is mentioned below in Fig. 1 & Fig. 2)

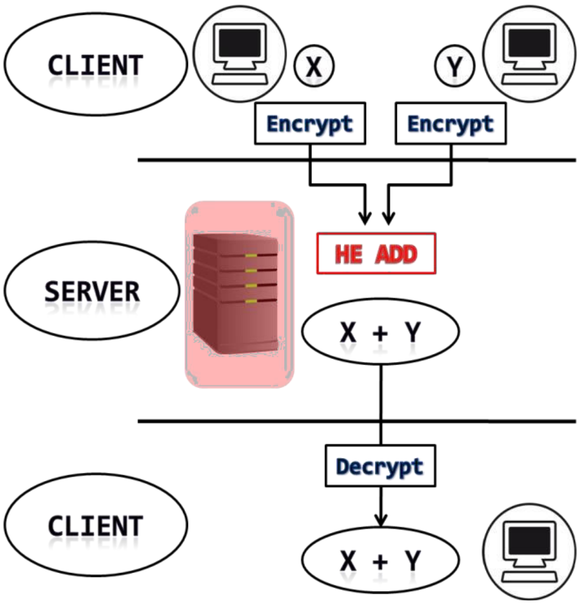


Fig. 1: Additive PHE Process Chart

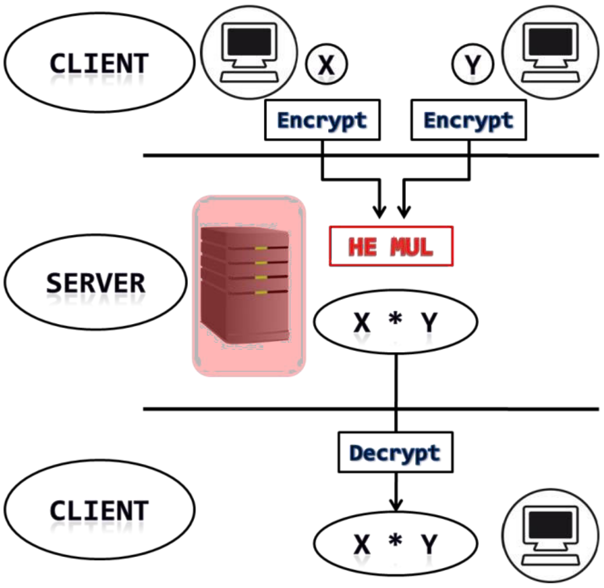


Fig. 2: Multiplicative PHE Process Chart

A Homomorphism is a structure preserving mapping between the algebraic structures.Let us consider a simple function from integers:
f: Z ⌋ Z f(x) = x+x
Above function i.e. f(x) doubles its argument. In this case we have used Multiplication, so it has to satisfy:f(a) ⊗ f(b) = f(a ⊗ b)

Now, Homomorphic Encryption is the encryption that is homomorphic, we can replace above equation with the encrypted data. Let ‘ENC’ denotes Encrypted data, so ENC must satisfied:
ENC(a) ⊗ ENC(b) = ENC(a ⊗ b)

Let the encrypted form of the data is E(x) and we encrypt it with key pair (m, e) then the encrypted data is : $E(x) = x^{e} \mathrm{mod} n$
To prove that above equation is PHE:$E(x1) = x1^{e} \mathrm{mod}\ n$
$E(x2) = x2^{e} \mathrm{mod}\ n$
$\mathbf{E(x1).E(x2) = x1^{e}\ x2^{e}\ mod\ n = (x1x2)^{e} mod\ n = E(x1.x2)}$

IV. Pseudo code

Step 1: The data stored in the cloud get encrypted with the public key Pk and stored in cloud.
Data is D and key is Pk and D’ is the encrypted dataD’∟ D * Pk
Step 2: Suppose a user request for the data D and the frequency of D is cross the benchmark set by the Machine Learning Model, then here our Model works, encrypt D’ using HE
ENC(D’)
Step 3: After encryption it the data (ENC(D’)) is send over to the network.
Step 4: At the client side, the computation checks the data not modified, if the result is matched then, the private key used and decrypt the data at the client side.
Step 6: End

V. Conclusion and Future Work

In the above proposed work, we have created a Machine Learning Model that checks the cloud data which is requested or travels more on the network and after detection this it apply extra security by using Homographic Encryption Algorithm to the data, at the client side the computation checks the result if matched, means data is secure and can be decrypted at the client side. The main problem with this is the Homomorphic Encryption Exception cases like it works on computation addition or multiplication, for large integers number, the computation is so large that it creates problem for getting original data. Secondly our algorithm only considering Integer values for the computation not other values.
The Future work for this is that the computation for the Homomorphic algorithm can be done using Float or Decimal values, which is more secure as compared to Integer values. Secondly upgrade our ML Model for best new Encryption methods to give best performance.

REFERENCES

1. Wu J, Ping L, Ge X, Wang Y, Fu J, ‘Cloud Storage as the Infrastructure of Cloud Computing’, International Conference on Intelligent Computing and Cognitive Informatics (ICICCI), 380-383 June
2. Sajid Habib Gill, MirzaAbdurRazzaq, Muneer Ahmad, Fahad M. Almansour, IkramUlHaq, NZ Jhanjhi, Malik ZaibAlam and MehediMasud, ‘Security and Privacy Aspects of Cloud Computing: A Smart Campus Case Study’, Intelligent Automation & Soft Computing (IASC), 2022
3. Amr M. Sauber, Passent M. El-Kafrawy, Amr F. Shawish, Mohamed A. Amin, and Ismail M. Hagag, ‘A New Secure Model for Data Protection over Cloud Computing’, HindawiComputaional Intelligence and Neuroscience, 2021
4. OussamaArki, AbdelhafidZitouni, MahieddineDjoudi, ‘A Security Method for Cloud Storage Using Data Classification’, International Journal of Grid and High Performance Computing, Sep 2023
5. Kumar Pal Singh, Dr. VinayRishiwal, Prof.(Dr.) Pramod Kumar, ‘Classification of Data to Enhance Data Security in Cloud Computing’, International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), 23-24 February, 2018
6. PriyankaVashisht, ShaliniBhaskar Bajaj, AmanJatain, and AshimaNarang, ‘Cloud Security: Challenges and Future Scope’, International Journal of Innovative Research in Engineering & Management (IJIREM), June 2023
7. N. Suganya, R. Sathiya, G. Ilamurugan, M. Pavithra, and C. Karthikeyan, ‘Enhancing the Reliability of Cloud Data by Implementing AES Algorithm.
8. Lo’aiTawalbeh, Nour S. Darwazeh, Raad S. Al-Qassas, and Fahd AlDosari, ‘A Secure Cloud Computing Model based on Data Classification’ Elsevier B. V., 1877-0509, 2015
9. Ogigau-Neamtiu F. Cloud Computing Security Issues. Journal of Defense Resources Management 2012; 3(2):141-148.
10. Somani U, Lakhani K, Mundra M. Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing. International Conference on Parallel Distributed and Grid Computing (PDGC); 211-216.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

📱 9940 572 462 ☎ 6381 907 438 ✉ ijircce@gmail.com

www.ijircce.com

Scan to save the contact details