International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 05 | May 2020 www.irjet.net p-ISSN: 2395-0072

Secure File Storage on Cloud using Homomorphic Encryption

Prajjwal Thakare[1], Atharva Telang[2], Harshal Sonawane[3], Yogesh Mantri[4], Vidya Gaikwad[5]

[1]-4BE-Dept. of Computer Engineering, VIIT Pune
[5]Assistant Professor- Dept. of Computer Engineering, VIIT Pune

---

Abstract - *Cloud services allow people and businesses to use software package and hardware resources that are provided and managed by cloud suppliers at remote locations. The distance between the client and the physical location of his data creates a barrier as this data can be accessed by a third party and this may affect the privacy of client's data. In this survey paper, we are proposing a system in which two major tasks are carried out. At first, the file will be encrypted before uploading to the cloud. And then while downloading the file, user will need authentication from owner of the file and then only the file will be decrypted.*

Key Words: **Cloud Security, Homomorphic Encryption, Decryption, OAEP.**

1. INTRODUCTION

Now a day's the world is data-centric, hence the big data processing and analysis have become the most important factor for any large establishment and companies. For storing the big-data the many establishments were using the hard drives but this process needed a large amount of storage unit so lack of space is the major issue. To overcome those problems there is a need for an appropriate or more suitable big data infrastructure that supports the storage and processing on a high scale. The 'Cloud Computing' is the proper module to provide convenient, on-demand access to share the computing resources.

We can easily connect to the cloud and access the resources from anywhere. The major risks we face while cloud computing is maintaining the privacy of data. So 'Cloud Security' is the most essential thing while using cloud computing. Many organizations bound by complex regulatory obligations and governance standards are still hesitant to place data or workloads in the public cloud for fear of outages, loss or theft. However, this resistance is fading, as logical isolation has proven reliable, and the addition of data encryption and various identities has improved security within the public cloud. Therefore, many encoding & encryption techniques are used to prevent these breaches & attacks on the cloud with the help of certain cryptographic techniques. For that purpose, we use 'Homomorphic encryption'. In this encryption, while uploading the data on a cloud it is converted into Ciphertext. We can perform all the operations on the Ciphertext it maintains the data integrity. It is a secure technique for encryption. The user's data is encrypted using padding scheme Optimal Asymmetric Encryption Padding (OAEP). Encryption can be done by both ways Symmetric or Asymmetric we use 'Asymmetric Encryption' in this encryption there are different secret keys for encryption & decryption.

While Decryption or Downloading of data for the process of authentication the Unique key generation is carried out every time which is OTP [One Time Password] is sent to the user. Without the user authentication, the file decryption will not be done. By using the Homomorphic Encryption until now we were able to do encryption on Text files but we are introducing the Homomorphic Encryption for the encryption of Images, Videos PDF files and securely storing it on the cloud.

2. LITERATURE SURVEY

2.1Title: Secure Cloud Computing Algorithm Using Homomorphic Encryption and Multi Party Computation.

Author: Debasis Das.

Year: 2018

Description: Proposed a scheme that integrates the multi-party computation with homomorphic encryption to allow calculations of encrypted data without decryption.

2.2 Title: Secure File storage in Cloud Computing using Hybrid Cryptography Algorithm.

Author: Punam V. Maitri, Arune Verma.

Year: 2018

Description: In this paper author have introduced new security mechanism using symmetric key cryptography algorithm and steganography.

2.3 Title: Homomorphic Encryption for Security of Cloud Data.

Author: Mr. Manish M. Potey, Dr. C. A. Dhote, Mr. Deepak H. Sharma.

Year: 2016

Description: This paper focuses on storing data on the cloud in the encrypted format using fully homomorphic encryption.

2.4 Title: A Secure Cloud Computing Architecture Using Homomorphic Encryption.

Author: Kamal Benzekki, Abdeslam El Fergougui, Abdelbaki El Belrhiti El Alaoui.

Year: 2016

Description: Many conventional encryption schemes possess either multiplicative or additive homomorphic property and are currently in use for respective applications.

2.5 Title: A Study of Data Storage Security Issues in Cloud Computing.

Author: Naresh Vurukonda, B.Thirumala Rao.

Year: 2016

Description: This paper gives an overview of the security issues on data storage along with its possible solutions. It also gives a brief description about the encryption techniques and auditing mechanisms.

2.6 Title: Multicloud Stored Encrypted Big Data Secured by Honey Words.

Author: Dr.S.Srinivasan, P.Shanmugavalli.

Year: 2016

Description: This work proposes a multi-cloud environment to securely store big data.

2.7 Title: A review of homomorphic encryption of data in cloud computing

Author: Dr. Amit Chaturvedi, Akanksha Kapoor, Dr. Vikas Kumar.

Year: 2017

Description: In this paper, author reviewed the algorithms proposed for the homomorphic encryption of data in cloud computing.

2.8 Title: Cloud computing system based on wireless sensor network.

Author: Smita Dikondkar, Vidya Gaikwad, Vaishali Mishra.

Year: 2014

Description: This paper focuses integrating the Sensor Networks with Cloud Computing and storing data into cloud.

2.9 Title: ABS-Key.

Author: Gudapati Syam Prasad, V.S. Gaikwad.

Year: 2018

Description: This paper gives an overview of cloud computing security issues, threats and challenges, this paper also described about vulnerability to cloud and their counter measures.

3. SYSTEM ARCHITECTURE

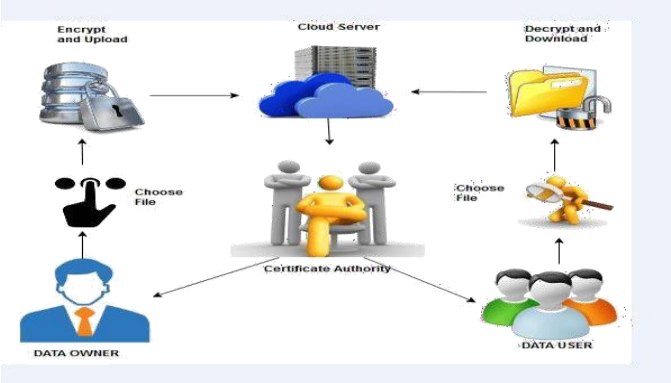

Fig -1: System Architecture

1. At first system architecture explains the process of Encryption & Decryption while Uploading and Downloading the data.
2. While Encryption of data we use certain cryptographic techniques such as OAEP (Optimal Asymmetric Encryption Padding).
3. We use Asymmetric Encryption in Homomorphic Encryption where there are two keys one for encryption and one for decryption.
4. The Data Owner will have a username and password. After selecting a particular file for uploading on cloud, encryption will be done. First the data is converted into ciphertext and then it is defined in a mathematical format.
5. When Data User selects a file from the cloud for downloading, OTP is sent to the Owner. Then the owner will have an authority to give access to the user by sharing the OTP. After successful verification of OTP, the file will be decrypted into ciphertext and then into the original data.

4. ALGORITHM

We are using an Optimal Asymmetric Encryption Padding (OAEP) for padding of the data and then it will be encrypted.

G: Hash Function SHA1 outputting g=160 bits (20 bytes)
H: Hash Function SHA256 outputting h=256 bits (32 bytes)
r: Random seed of 160 bits (same size as of G)
M'=M || 0^(g-len(M))
X=M'⊕G(r) || r ⊕ H(M'⊕G(r))
X=s || t where,
s= M'⊕G(r) and t= r⊕H(s)

Step 1: Select any two prime numbers p and q.
Calculate value for n n = p.q
Calculate value for ϕ(n) ϕ(n) = (p − 1). (q − 1)
Select e such that 1<e< ϕ(n) and e and n are coprime.
Calculate value for d such that,

(d.e) mod ϕ(n)=1

Public key is :(e, n)
Private key is :(d, n)

Step 2: Encryption of message M is $C=X^e \bmod n$

Step 3: Access to the user
An OTP generated using free message API which will be sent to the owner of the file. Owner of the file has to give OTP to the user in order to give access to the file.

When user enters the OTP, after successful verification decryption process starts with the private key.

Step 4: User decrypt the computed data C after successful verification of OTP using private key X= Cd mod n
Parse X as s || t
r ← H(s)⊕t
M' ← s⊕G(r)
Parse M' as M || Z

5. IMPLEMENTATION

For this project we have built a web app which has the following features:

1. We have made a login portal which can be accessed by our email address and password, also if you are new user then you can register in the app through the register here button.

2. When you click on new registration, a registration form is loaded on the app. In this form you have to enter the following details in order to register:
   a. Name
   b. Email Address
   c. Password
   d. Mobile Number
   Also there is a reset button in order to facilitate the resetting of above data if it is wrongly entered.

3. After you login in the login page using our login credentials, the home page has following options in the menu bar:

a. File Uploading – In this tab, you can upload your files to the cloud. It will be homo-morphically encrypted in the database. In this tab, you can specify the scope of your file, either private or public, and upload it to the cloud. You can upload a variety of files types such as txt, pdf, jpg, mp3, mp4, etc
b. My Files – In this tab, you can see the files that you have uploaded until now and download them. Also if the scope of the file is public then you can share the file to other members of the cloud.
c. All Users – This tab is exclusive to the admin of the app. It is used to see all the users of the app. The admin has the control to either activate or deactivate a user.
d. Downloads – This tab is used to download the uploaded files on the server.
e. Logout – It is used to logout of the app.

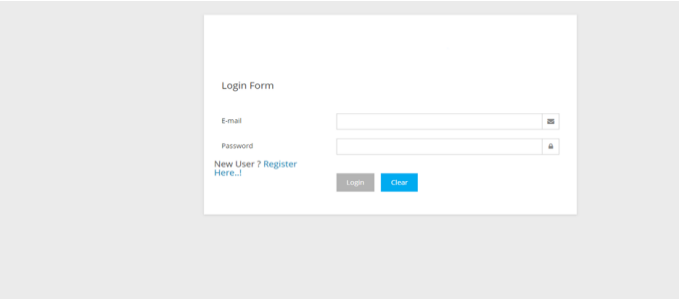

Fig -2: Login Page

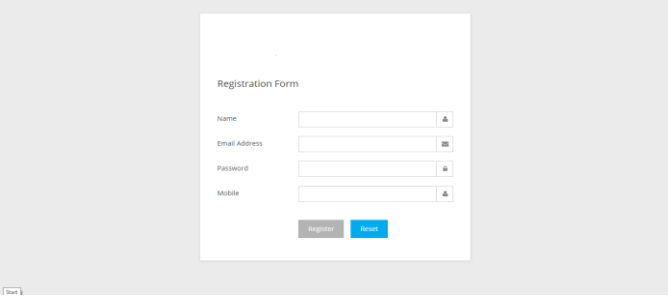

Fig -3: Registration Form

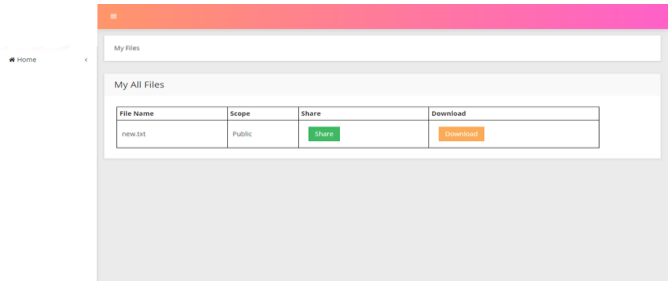

Fig -4: Uploaded File Page

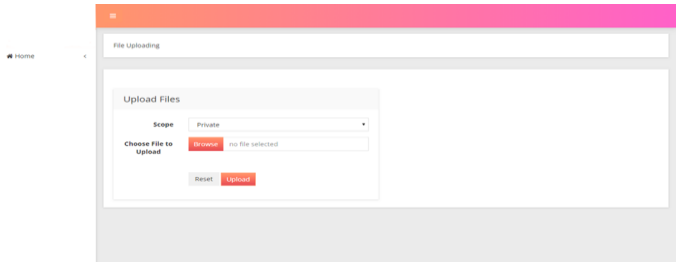

Fig -5: File Upload Page

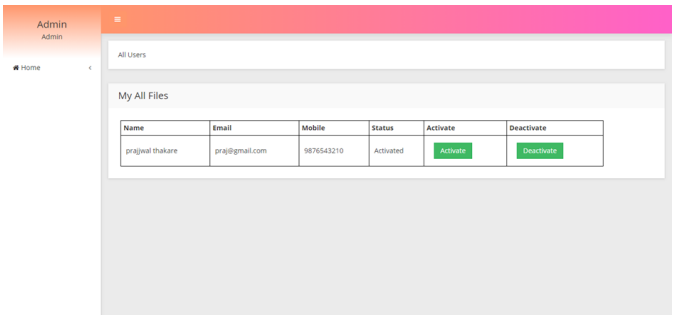

Fig -6: Admin Control Page

6. CONCLUSIONS

The security problems are a big downside for cloud computing development. To preserve the privacy of his knowledge, the owner must encrypt data before being sent to the cloud. By using homomorphic encryption, user can do operations on cypher text without actually knowing the data. And if any user wants to download the file, the owner will have an authority to give him the access to that file, otherwise the file will not be decrypted. And not just text files but image, video, pdf, etc file can be encrypted or decrypted. In this way we can assure the Security of the data uploaded on cloud. For the future purpose we can say that included support for the choice of cloud providers is limited and very basic, but the framework can be extended to support new providers. Further in the current implementation the organizations have to maintain an application at the public clouds that will perform the updation procedure. The framework can be developed in a manner such that the providers can easily integrate it with their platform. Moreover, working with encrypted data is computation intensive and expensive in terms of storage, hence high performance data processing options in the cloud can be applied for better performance. With reference to cryptographic techniques, the proposed approach using newer homomorphic cryptosystems having additive homomorphism, can be explored for performance benefits.

REFERENCES

[1] Benzekki, K., El Fergougui, A., & El Alaoui, A. (2016). A secure cloud computing architecture using homomorphic encryption. International Journal of Advanced Computer Science and Applications, 7(2). doi:10.14569/ijacsa.2016.070241

[2] Chaturvedi, A., Kapoor, A., & Kumar, V. (2017). A review of homomorphic encryption of data in cloud computing. International Journal of Computer Trends and Technology, 43(2), 75-80. doi:10.14445/22312803/ijctt-v43p111

[3] Das, D. (2018). Secure cloud computing algorithm using homomorphic encryption and multi-party computation. 2018 International Conference on Information Networking (ICOIN). doi:10.1109/icoin.2018.8343147

[4] Maitri, P. V., & Verma, A. (2016). Secure file storage in cloud computing using hybrid cryptography algorithm. 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET). doi:10.1109/wispnet.2016.7566416

[5] P.Shanmugavalli, & Dr.S.Srinivasan. (2016, March). Multicloud stored encrypted big data secured by honey words. Retrieved from https://www.ijarbest.com/conference/spcl15/620

[6] Potey, M. M., Dhote, C., & Sharma, D. H. (2016). Homomorphic Encryption for Security of Cloud Data. Procedia Computer Science, 79, 175-181. doi:10.1016/j.procs.2016.03.023

[7] Vurukonda, N., & Rao, B. T. (2016). A study on data storage security issues in cloud computing. Procedia Computer Science, 92, 128-135. doi:10.1016/j.procs.2016.07.335

[8] Gudapati Syam Prasad, V. S. Gaikwad (2018). A Survey on User Awareness of Cloud Security. International Journal of Engineering & Technology, 7(2.32), 131-135. doi:http://dx.doi.org/10.14419/ijet.v7i2.32.15386

BIOGRAPHIES

Mr. Prajjwal Chandrakant Thakare as completed his HSC from Bytco College, Nasik. He is currently persuing BE in Computer Science from VIIT, Pune. He will gradute with bachelor's degree in Computer Science in 2020. He is a member of Computer Socitey of India (CSI). He has work in Cloud Computing as intern at Control Case International Andheri,Mumbai. His research intrests includes Cloud Security, Cyber Security.

Mr.Atharav Pralhad Telang as completed his HSC from Sri Chaitanya Jr college, Hyderabad. He is currently persuing BE in Computer Science from VIIT, Pune. He will gradute with bachelor's degree in Computer Science in 2020. He is a member of Computer Socitey of India (CSI). He has work as Php developer intern at Dream Swarg, Pune.

Mr. Harshal Rajendra Sonawane as completed his HSC from St.Lawrance Jr College,Nasik . He is currently persuing BE in Computer Science from VIIT, Pune. He will gradute with bachelor's degree in Computer Science in 2020. He is a member of Computer Socitey of India (CSI). He has work as Andriod developer intern at Praxis Infotech , Sangli. His research intrests includes Andriod , Data minning.

Mr. Yogesh Ramakant Mantri as completed his HSC from VV Jr. college, Pandarpur. He is currently persuing BE in Computer Science from VIIT, Pune. He will gradute with bachelor's degree in Computer Science in 2020. He is a member of Computer Socitey of India (CSI). He has work as Php developer intern at Fresh gravity Software Baner, Pune. His research intrests includes Data Science and Cyber Security.

Ms. Vidya Gaikwad, has received M.E. in Computer Engineering from Pune University. She is presently working as Assistant Professor at Vishwakarma Institute of Information Technology, since 2009. She is pursuing PhD from Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh in IoT Cloud Security. Her current research interests are: Cloud Security, IoT Security. She has been teaching Computer Organization and Architecture, Cloud Computing, Cyber Security, Computer Networks, Microprocessor.