© 2018 IJSRST | Volume 4 | Issue 8 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Implementing Cryptographic Method for Ensuring Data Security In Cloud Computing Based On Hybrid Cloud

Md Sajid Khan*[1], Dr. Chandra Shekhar Yadav[2], Mayank Deep Khare[2]
M.Tech(CSE)*[1], Professor[2], Asst. Professor[2]
*[1,2]Computer Science & Engineering, Noida Institute of Engineering & Technology, Greater Noida, India

ABSTRACT

In this modern era, Cloud Computing is the most emerging technology in the world, through which people can share resources, services and information among the people using the internet. Information security has been a major issue in cloud computing because the data is stored in different location in the cloud so Data security is the key factors of people's concerns, because cloud computing have been investigated in both academics and industries so data security and privacy are most essential for the future development of cloud computing technology in government, industry, and business. For enhancing the security in cloud computing we have developed the new technology and methodology to secure data in cloud computing, accordingly I have built an application using Cryptographic Algorithms encryption technology to secure & upload data in database, and during upload & retrieve the data they have to use the three level of encryption method to fetch the information.

Keywords: Cloud Computing, Deployment models, Data security, IaaS, PaaS, SaaS, Challenges

I. INTRODUCTION

Cloud computing is Internet based computing technology where virtual shared servers provide software, infrastructure, platform, devices and other resources for hosting customers on a pay as per you-use basis. All information that a digitized system has to offer is provided as a service in the cloud computing model. Users can access these services available on the "Internet cloud" without having any previous know-how on managing the resources involved.

Cloud computing customers do not own the physical infrastructure; rather they rent the usage from a third-party provider. This helps them to save huge financial resources. They consume resources as a service and pay only for resources that they use. Most cloud computing infrastructures consist of services delivered through common centers and built on servers. Sharing resources amongst can improve, as servers are not unnecessarily left idle, which can reduce costs significantly and also increasing the speed of application development.

A few years ago, abstract shapes of cloud were used to denote the internet and cyberspace. Afterwards the cloud has been utilized to represent a more specific idea, with a word Cloud Computing. The expansion and evolution of the electronic services requires continuous improvement in terms of infrastructure. Cloud computing offers a relatively low-cost scalable alternative to in-house infrastructure, both in hardware and software defined the term "Cloud Computing" as a ubiquitous on-demand model for accessing common resources over a network.

Before submitting your final paper, check that the format conforms to this template. Specifically, check the appearance of the title and author block, the appearance of section headings, document margins, column width, column spacing and other features.

II. OBJECTIVE

we introduce the implementation in cloud environment we called "HYBRID Drive". We have implement the **hybriddrive.in** that adding the new facilities in existing cloud application in term of improving the security as well as data storage techniques. Data security and privacy protection are the two main factors of user's concerns about the cloud technology. Though many techniques on the topics in cloud computing have been investigated in both academics and industries, data security and privacy protection are becoming more important for the future development of cloud computing technology in government, industry, and business. Data security and privacy protection issues are relevant to both hardware and software in the cloud architecture.

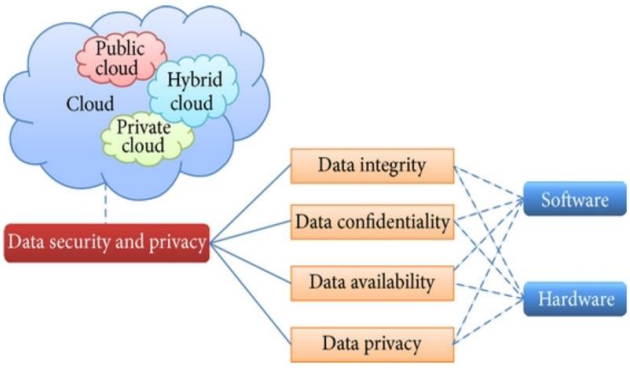

Fig. 1.Organization of data security and privacy in cloud computing.

III. III. EXISTING SYSTEM

Data security in Cloud Computing involves more than data encryption. Requirements for data security depend upon on the three service models SaaS, PaaS, and IaaS.

A. Two states of data normally have threat to its security in clouds; Data at Rest which means the data stored in the cloud and Data in Transit which means data that is moving in and out of the cloud. Confidentiality and Integrity of data is based upon the nature of data protection mechanisms, procedures, and processes.

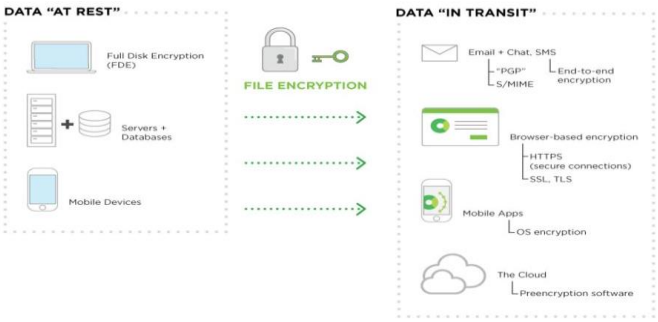

Fig.3. Data at Rest and in Transit

B. Encryption algorithm plays a vital role. It is the fundamental tool for protecting the data. Encryption algorithm converts the data into scrambled form by using "the key" and only user have the key to decrypt the data. In Symmetric key encryption, only one key is used to encrypt and decrypt the data. Another technique is using asymmetric key encryption; two keys- private and public keys are used. Public key is used for encryption and private key is used for decryption. Fig shows some of the symmetric & asymmetric algorithms.

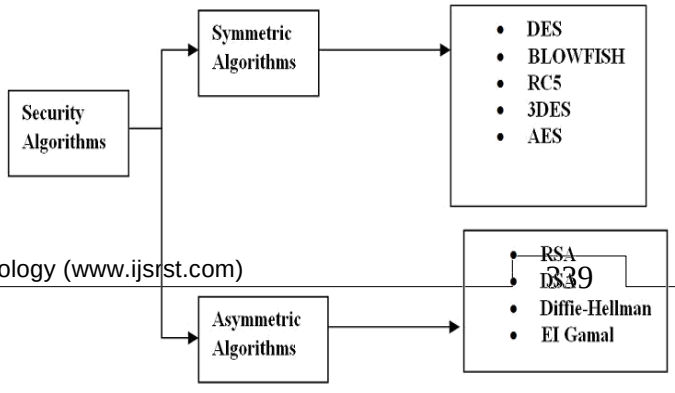

Fig.2. Existing Algorothm

IV. PROPOSED METHOD

In this paper I have been proposed different security algorithms to eliminate the concerns regarding data loss, segregation and privacy while accessing web application on cloud. Algorithms like: RSA, DES, AES, Blowfish and hybrid algorithm have been used and comparative study among them have also been presented to ensure the security of data on cloud.

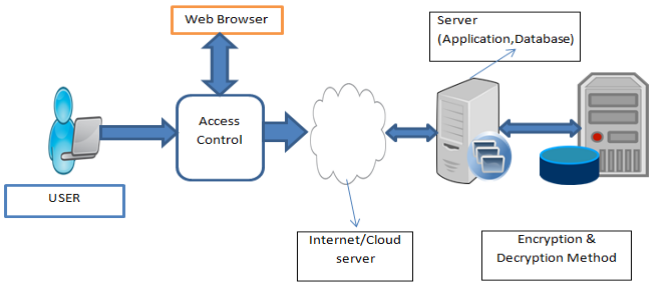

Fig.4. Proposed Architecture

when we upload data in cloud how it reside and how many security are implemented over there. Accordingly I have try to implement Multilevel of Encryption and Decryption algorithm. Thus, in our proposed work, only the authorized user can access the data. Even if some intruder (unauthorized user) gets the data accidentally or intentionally, he must have to decrypt the data at each level which is a very difficult task without a valid key. It is expected that using multilevel encryption will provide more security for Cloud Storage than using single level encryption.

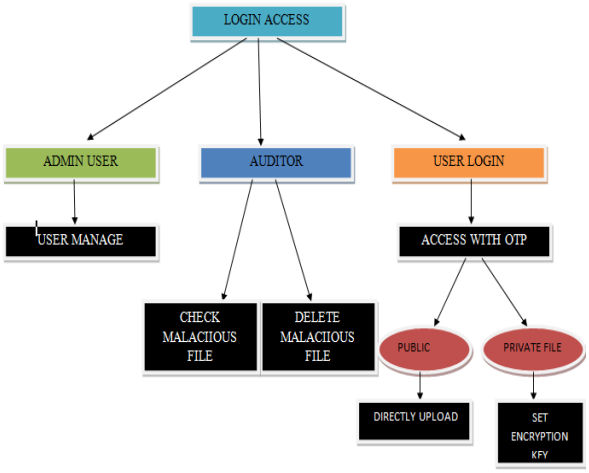

Fig. 5. Implementation Design

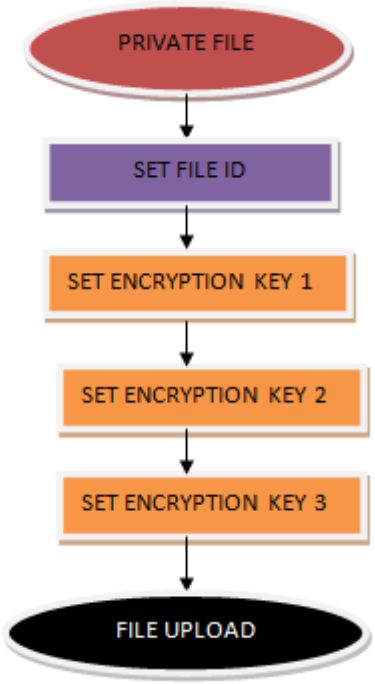

Fig.6. Uploading Section of Private section

V. ALGORITHM

A. Login Module:

Keygen procedure: It consist of different procedure.

Login(userid, password)

This procedure is used Login the user into the system by generating, sending and verifying OTP/private key :

i. VerifyUserIDandPassword(userid,password)
//To check userid and password

ii. If(verified)
iii. Generate_OTP_private_key_and_send_email()
iv. VerifyOTP() //By matching key entered by user and stored in database.
v. If(OTP_verified)
Redirect_to_userSection()
Else
Show_message()
redirect_to_loginPage()

B. **FileUpload()**

Procedure uploads desired file in the cloud by encrypting the contents of file and storing it in cloud and it encrypt the given file with the help of FILENAME, SECRET KEY and encryption algorithm.

i. Generate_file_random_ID()
ii. Save_File_name_entered_by_user()
iii. Select_file_access() //public or private
iv. If(file_access == public)
Upload_file()//MAX 25MB OF FILE
Set_file_access_to_public()
Else
Upload_file()
set_file_access_to_private()
v. Generate_encryption_key_1_entered_by_user()
vi. Generate_encryption_key_2_entered_by_user()
vii. Generate_encryption_key_3_entered_by_user()
viii. Encrypting the contents of file and storing it in cloud.
ix. END

C. File_Download(fileid)

download (): This procedure sends the decrypted file to user

i. Find_file_access_by_fileid()
ii. If(access == public)
Downloadfile()
Else if(access == private)
Verify_encryption_key_1_entered_by_user()
Verify_encryption_key_2_entered_by_user()
Verify_encryption_key_3_entered_by_user()
Decrypt the contents of file and download from cloud.

D. Audit_file_uploaded_on_cloud()

Audit(): this procedure to check the file content using extention if it found any thing malacious it will deleted.

i. If(malicious_file_found)
Delete_from_the_cloud()
Write_remark()
Send_email_with_file_deletion_reason_to_the_user()

Auditing_process()

i. List_file_uploaded() //all files both private and public
ii. If(file_is_malicious == true)
Show_file_in_red_color()
Click_on_delete_button_to_delete_the_file();
Ask_reason_for_deleting()
After_deletion_send_email_to_user_with_reason();

E. Admin_process()

Admin(): this procedure administrator check the any unauthorized user access the cloud services it will delete that user.

i. List_all_users() //all users with emailid and contact number
ii. If(user_is_not_authorized == true)
Delete_the_user();

VI. RESULT & ANALYSIS

1. our proposed system is in hybrid drive in cloud commuting hence we have implement as in application form which is hybriddrive.in.
2. It is high security is provided using hybrid encryption algorithm.
3. Using hybrid encryption leads to high security of text file and make the access of original file by intruders near to impossible.
4. If a user logins and forgets to log out or leaves the system idle. In that case if a intruder tries to download the data from the system then that person will be asked to enter to verify the three level of encryption key. we can see in the picture how data is flowing using encryption.

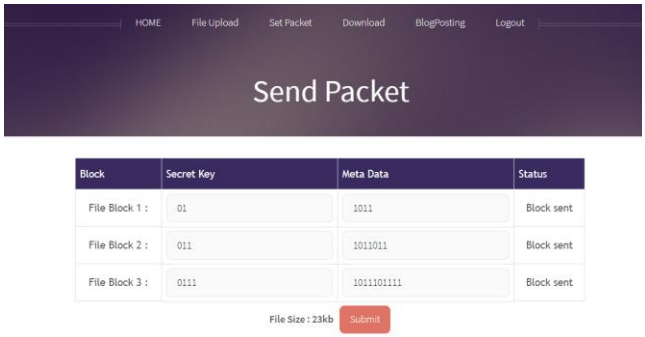

Fig. 7. level of encryption to upload file

5. To download the data in a secure way the user is always required to enter the private key and secret key. Since the private key and secret is not even known to the Cloud's Administrator. Thus, the main advantage of proposed system is that even the Cloud's Administrator cannot access the data of the user.

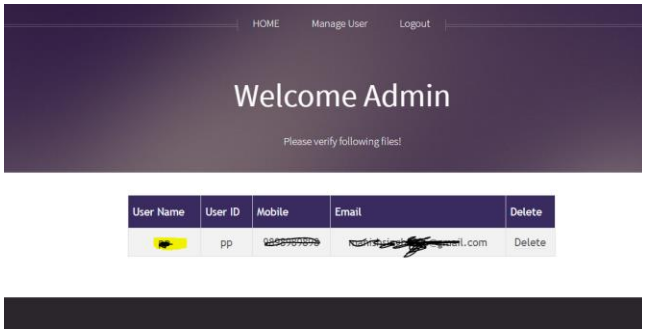

Fig.8. Admin Authorization for user mange

VII. CONCLUSION & FUTURE WORK

This paper is proposed a hybrid encryption algorithm providing data security to the user in the Cloud. here we use s a Multilevel Encryption and Decryption algorithm. in our proposed work, only the authorized user can access the data. Even if some intruder (unauthorized user) gets the data accidentally or intentionally, he must have to decrypt the data at each level which is a very difficult task without a valid key. It is expected that using multilevel encryption. even the Cloud's Administrator cant access the user data. will provide more security for Cloud Storage than using single level encryption. In the future we would emphasize on finding an encryption algorithm which will be more light and secured for data in Cloud Computing. The strength of Cloud Computing is the ability to manage risks in particular to security issues. Security algorithms mentioned for encryption and decryption can be implementing in future to enhance security over the network. In the future, we will extend our research by providing algorithm implementations and producing results to justify our concepts of security for Cloud Computing.

VIII. REFERENCES

[1] Md Sajid Khan, Mayank Deep Khare and Dr. Chandra Shekhar Yadav. "An Approach for Ensuring Data Security in Cloud Computing Based on Hybrid Cloud-A Survey." International Journal for Scientific Research and Development 5.12 (2018): 596-599.

[2] Vishwanath S Mahalle, Aniket K Shahade, "Enhancing the Data Security in Cloud by Implementing Hybrid (Rsa & Aes) Encryption Algorithm" 978-1-4799-7169-5/14/ IEEE

[3] Adviti Chauhan, Jyoti Gupta, "A Novel Technique of Cloud Security Based on Hybrid

Encryption by Blowfish and MD5" 4th IEEE International Conference on Signal Processing, Computing and Control ('SPCC 2k17), Sep21-23, 2017, Solan, India

[4] Mohammad Nashir Uddin, He Lie, & Hao Li. "Hybrid Cloud Computing and Integrated Transport System" 2017 International Conference on Green Informatics, IEEE DOI 10.1109/ICGI.2017.27

[5] Vikas K.Soman, Natarajan V, "An Enhanced hybrid Data Security Algorithm for Cloud" 2017 International Conference on Networks & Advances in Computational Technologies (NetACT) |20-22 July 2017| Trivandrum.

[6] Aarti Singh, Manisha Malhotra, "Hybrid Two-Tier Framework for Improved Security in Cloud Environment" 978-9-3805-4421-2/16, 2016 IEEE

[7] Divya Prathana Timothy, Ajit Kumar Santra," A Hybrid Cryptography Algorithm for Cloud Computing Security" 978-1-5386-1716-8/17/,2017 IEEE

[8] Shweta Kaushik, Charu Gandhi, "Cloud data security with hybrid symmetric encryption" 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), 978-1-5090-0082-1/16, IEEE

[9] Santosh Bulusu, Kalyan Sudia "A Study on Cloud Computing Security Challenges" Thesis School of Computing, Blekinge Institute of Technology, SE-371 79 Karlskrona,Sweden