IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 6, June 2022
Impact Factor: 6.252

File Storage using Cloud and Cryptography Technologies

Viswanathan S[1], Isaac Johnson A[2], Sasirekha R[3], Reena R[4]
Students, Department of Computer Science and Engineering[1,2]
Assistant Professor, Department of Computer Science and Engineering[3]
Associate Professor, Department of Computer Science and Engineering[4]
Prince Shri Venkateshwara Padmavathy Engineering College, Chennai, India

Abstract: *In this era cloud computing is employed in various fields like industry, military, college, etc. for various services and storage of big amount of information. Data stored during this cloud will be accessed or retrieved on the users request without direct access to the server computer. But the foremost concern regarding storage of knowledge online that's on the cloud is that the Security of the information. Many different approaches have also been proposed to produce data protection within the cloud, like AES, BlowFish, and RC6, but Existing systems often fail when only a specific type of encoding is utilised, either AES or RC6 reckoning on a consumer requirement. As when there are encrypted the keys are leaked thus making the info to be accessed by anyone. So we've proposed hybrid cryptography because the solution for this problem. So when the user uploads the info, it is divided into three sections, the primary is encrypted with AES, the second is completed with DES and eventually the third section is completed with RSA.*

Keywords: Cloud, Security, AES, DES, RSA

I. INTRODUCTION

The distribution of computing resources as a service, or "cloud computing," means that the cloud provider, rather than the end user, owns and manages the resources. Aside from third-party servers used to support the computing architecture of a business, research, or personal project, these resources could be anything from browser-based software programmes to third-party data storage for pictures and other digital assets.

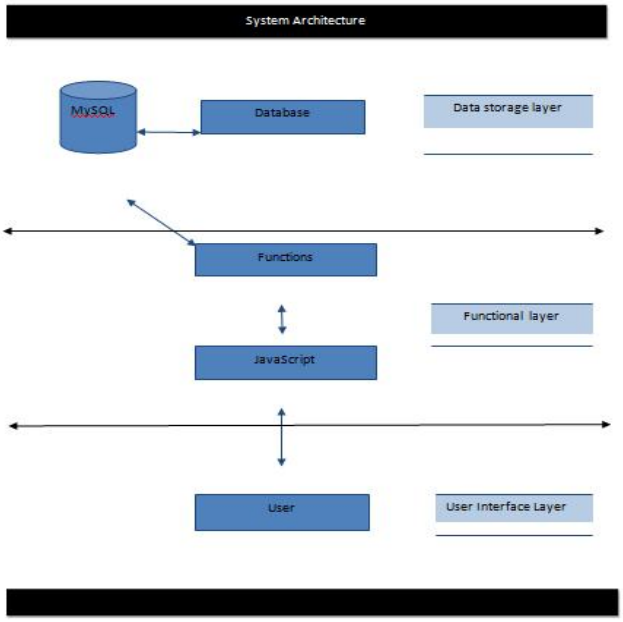

Fig. 1. Architecture Diagram

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 6, June 2022
Impact Factor: 6.252

Businesses and consumers now have access to a variety of on-demand computing resources as internet-accessed services because to the rising availability of cloud-based apps, storage, services, and devices. Unprecedented access to computing resources has led to the emergence of a new generation of cloud-based firms, altered IT procedures across industries, and disrupted numerous routine computer-aided procedures. The use of codes to secure information and communications in such a way that only the intended recipients can decipher and process them is known as cryptography. Hence, information access by unauthorised parties is prevented. "Crypto" means "hidden," and "graphy" means "writing," respectively. The techniques used in cryptography to protect data are derived from mathematical ideas and a set of rule-based calculations known as algorithms to transform messages in ways that make them difficult to decode. These algorithms are employed in the creation of cryptographic keys, digital signatures, data privacy protection, online browsing on the internet, and the security of private transactions like debit and credit card purchases.

II. EXISTING SYSTEM

AES is the only algorithm now in use for data encoding and decoding. For high level security, however, it is not advised to utilise a single algorithm. Because a single key is used for both data encoding and decoding in this type of technique, if we employ single symmetric key cryptography, we will run into security issues. Therefore, when sharing keys in a multiuser context, key transmission issues arise. High security is achieved using public key cryptography techniques, however maximum time is required for data encoding and decoding. Another existing system stores information on a third-party cloud, which is not advised. The data had been encrypted using the AES and BLOWFISH algorithms. The BLOWFISH algorithm's drawback is that encoding and decoding take time.The current system's shortcomings include the user having to perform a lot of computation, which increases traffic to the storage servers. The customer is completely responsible for managing his cryptographic keys. If the key's component device is missing or compromised, the key is lost, and the security is compromised. It is challenging for the servers to directly offer other functions in addition to storing and restoring data.

III. PROPOSED SYSTEM

The proposed system has the storage of data on the public cloud as it could be accessed and encrypted using hybrid cryptography techniques AES ,DES,RSA. So When the owner registers and login into the account he would be able to upload the files which will be secure using the above algorithms which could be viewed using split data and when the authorised user login into the account he could view the files uploaded by the owner and to access it it should be verified using the key given in the database and then finally the user could able to download the files.

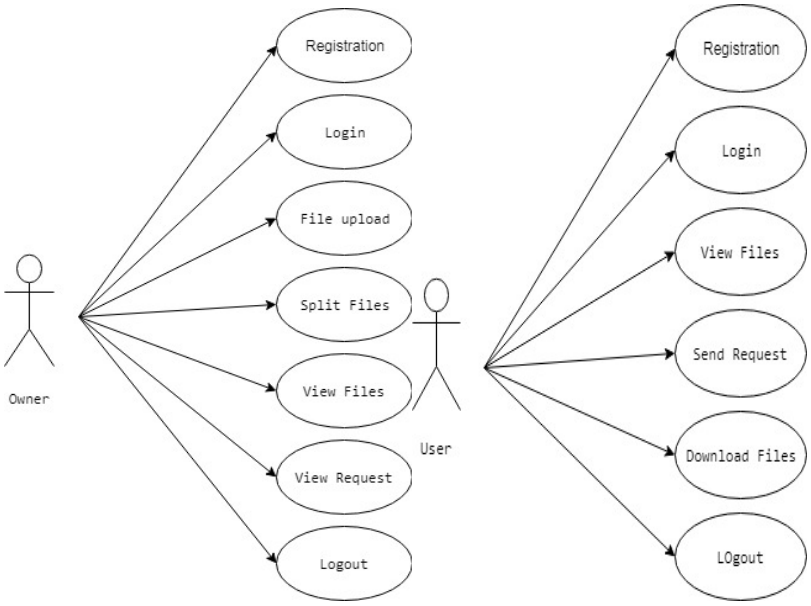

Fig. 2. Process Flow

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 6, June 2022
Impact Factor: 6.252

IV. MODULE DESCRIPTION

4.1 Registration Phase (Owner & User)

When the owner or the user enters the website, it should register into the account. As when the owner / user wants to upload/download any of the documents, first the owner/user should register the account by giving username password, mail id.

Fig. 3. Login Page

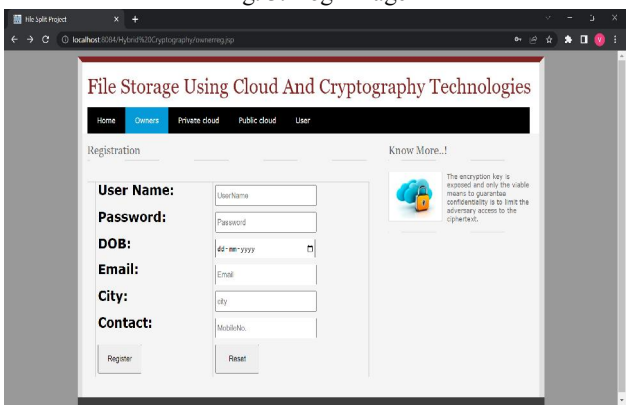

Fig. 4. Registration Page

4.2 Uploading Phase

When the owner logs into the account, it would be redirected to the home page of the application. So in this when the owner wants to upload the document, it should be selected from our files and then the file which is uploaded should be given a name to be identified by the users.

Fig. 5. Uploading File

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 6, June 2022
Impact Factor: 6.252

4.3 Splitting Phase

When the owner uploads the document, it would be splitted into three parts so that it could be encrypted by three cryptographic algorithms like AES,DES,RSA .After encryption the splitted data could be viewed by the owner.

Fig. 6. Split Data

4.4 User Request & Verifying Phase

Finally when the owner had successfully uploaded the document, the user could be able to login into the account and then the user could be able to access the documents. First the user could view the files uploaded by the owner. For accessing it, the user has to give request to the owner ,when the owner accepts the request ,it would lead to the verifying page where the user should enter the key provided by the owner.

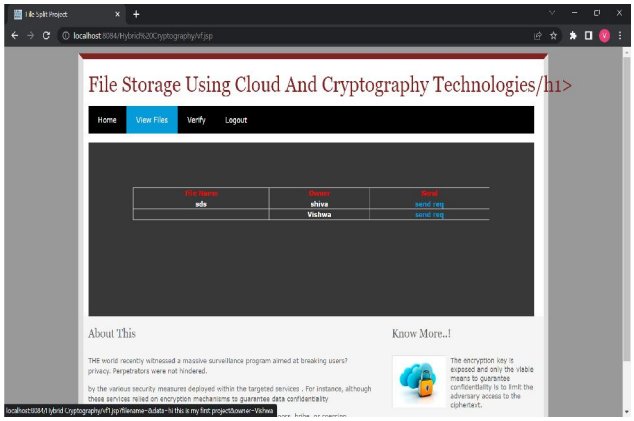

Fig. 7. View Files

Fig. 8. Verifying Phase

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 6, June 2022
Impact Factor: 6.252

4.5 Downloading Files

After successful verification done by the user, the user could be able download the document and access it anytime by the user

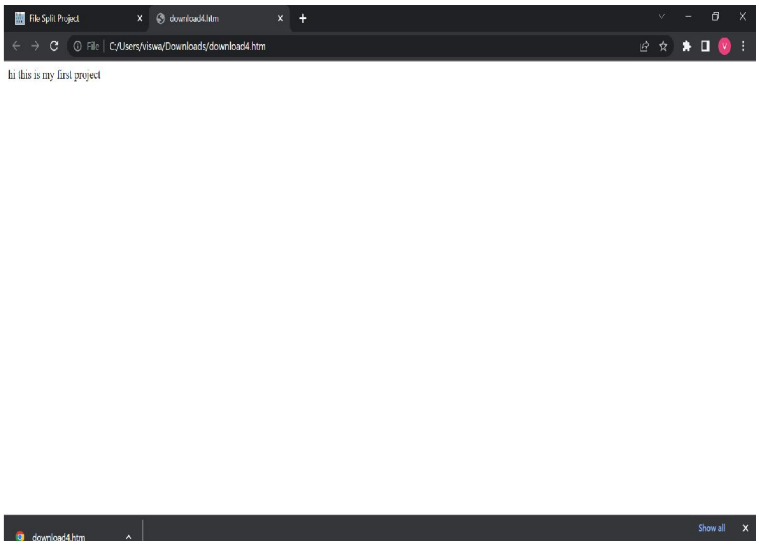

Fig 9 Downloading Phase

V. CONCLUSION

The major objective is to safely store and access data in the cloud that is not under the data owner's control. We use hybrid cryptography as a method of encryption to safeguard data files on the cloud. The cloud server's two components improved the speed at which data was stored and accessed. We believe that this method of data access and storage is highly efficient and safe. As in this scheme only members of the group can access the data stored over shared data section, our attempts to tackle the problem of group sharing of data in the shared data section are still ongoing. Communication from one to many, many to one, or many to many is impossible.

VI. FUTURE SCOPE

It is impossible to create a system that meets every user requirement. As the system is used, user requirements are always evolving. Future improvements to this system include some of the following: It is feasible to upgrade the system as new technology is developed.be flexible to fit the surroundings. Depending on potential security problems, security can be enhanced utilising new technologies, such as single sign-on.

ACKNOWLEDGMENT

I'm taking advantage of this opportunity to express my gratitude to everyone who helped me with the direction of studies venture report. We'd want to express our gratitude to all of our professors, friends, and family members who have directly and indirectly contributed to the successful completion of our project. Ms. Sasirekha maam, Assitant Professor, Computer Science and Engineering, Prince Shri Venkateshwara Padmavathy Engineering College, Chennai, Tamil Nadu, India, and Mrs. R. Reena maam, Head of Department, Computer Science and Engineering, Prince Shri Venkateshwara Padmavathy Engineering Collenge, deserves special recognition for guiding us to a successful conclusion of this endeavour.

REFERENCES

[1]. Surya Nepal, Carsten Friedrich ,Leakha Henry, Shiping Chen “A Secure Storage Service in the Hybrid Cloud”, Fourth IEEE International Conference on Utility and Cloud Computing,2011

[2]. Manikandan G et al., "A changed cryptographic plan improving information", Journal of Theoretical and Applied Information Technology, vol. 35, no.2, Jan. 2012.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 6, June 2022
Impact Factor: 6.252

[3]. Peter Mel and Tim Grace, "The NIST Definition of Cloud Computing", NIST, 2010

[4]. Srinivasa rao D et al., "Breaking down the Superlative symmetric Cryptosystem Encryption Algorithm", Journal of Global Research in Computer Science, vol. 7, Jul. 2011

[5]. Punam V Maitri , Aruna Verma , "Secure File Storage in Cloud Computing Using Hybrid Cryptography" International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET),2012