International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

User Authentication and Symmetric Keys Using Cryptographic Technique

M.Anitha[1], K . Venkata Sai Rohini [2]

#1 Assistant Professor & Head of Department of MCA, SRK Institute of Technology, Vijayawada.
#2 Student in the Department of MCA, SRK Institute of Technology, Vijayawada

ABSTRACT_ In today's environment, overcoming problems with sharing files in cloud technology is a difficult undertaking. To accomplish so, we're leveraging the Attribute-based Cryptography format based on Cipher policy in Python, which we're encryption with the pyAesCrypt library package. This is among the most popular encryption technologies. The file sharing concepts are particularly significant in areas such as healthcare, military, etc. where we need to keep confidential material secure and don't want to offer authorization to all types of users. Instead, we choose secured form file sharing concepts. We will maintain the data in a secure format using cloud computing technology during this procedure. We will keep the data in encrypted and original versions by using the pyAesCrypt utility packages and the block cypher algorithm. In addition, because the data server for the retail store is unstable, we are going to collect the data file and store it in a safe manner by making use of a CSRF (Cross-site Request Forgery) Middleware token. For the purpose of the current project, we are utilising typical ways to attribute encryption in order to generate data in an encrypted format by making use of the user's key. We are now compiling a list of all the attributes linked with the information of our customers, which we will later have the option to encrypt and decode. Therefore, in order to implement the Attribute Encryption standard Block cypher approach, we will be making use of the pyAesCrypt package in this project.

1.INTRODUCTION

The primary goal of the project is to facilitate secure file transfer through the generation of secret keys. We propose employing the Attribute Based Encryption method using the pyAescrypt library

package system, which incorporates a secret sharing scheme. This method ensures data security and allows data owners to control access to encrypted data by granting permissions. Administration of data access is solely managed by admin users. To access files, users must request permission from admin users, who can then approve or deny the request. Only upon approval will users be able to open and browse the file. The system utilizes Attribute Based Encryption, implemented using the pyAesCrypt library, to generate keys and maintain file security. This approach ensures that data remains secure and inaccessible to unauthorized users. All user types can access the system, with no prerequisite for accessing the administrative interface; however, admin approval is required for file access by other users

2.LITERATURE SURVEY

2.1 Facility-Based Access Control for Computing Services Hosted in the Cloud

This project entails implementing two different methods to put ideas into action. The initial approach involves trustee users conducting the data processing for the setups. An alternative option is to incorporate key-based encryption principles to deliver the code in an encrypted format. The user authentication process is divided into two stages, with three separate procedures required for user cryptography. Initially, the user generates a secret key, which is then utilized during the setup process. Subsequently, the trusted user can save the document according to predetermined security settings. Another set of requirements is implemented to ensure that only authenticated users can access the file. Ultimately, the user is tasked with generating the coding key by employing Cryptosystems to implement Attribute Based Encryption concepts.

2.2 An Efficient Cloud-based System to Meet Your Needs Scheme for revocable identity-based proxy re-encryption to facilitate data sharing in public cloud environments

In addition to encryption, another cryptographic method for generating secret codes to safeguard data from unauthorized access is based on the concept of the identity element. Throughout our research, we explored various potential solutions for

efficiently exchanging file-related information. Mobile device users have access to numerous applications that enable them to gather data and share files within a system environment efficiently. Whoever possesses the data is responsible for granting authorization to any user requiring access to the file, ensuring the owner retains full control over the data. For example, in healthcare systems, maintaining the confidentiality and anonymity of individual patients' medical records is crucial. Consequently, data owners may opt to keep files in an encrypted format, retaining the authority to use a secret key for accessing the file collection. The private key method is implemented using the encryption technique provided by pyAesCrypt.

2.3 A dependable OSPM schema for conducting micropayment transactions in a safe manner via mobile agents

In response to the prevalent use of mobile ecommerce methods and online payment systems among consumers, our project focuses on implementing mobile offline payment solutions. This approach, akin to micropayments, emphasizes utilizing the user's micropayment systems offline within the mobile network infrastructure design. We employ Way hash concepts to secure information in offline transaction micropayment networks, extending the utilization of SPKI in the current system. Presently, lightweight micropayment offline methods are predominantly adopted in networks, accompanied by innovative conceptual designs to protect payment details, known as the Mobile Commerce Offline Method. This method involves three transaction processing types, with the most severe being the maximum scenario cases. Additionally, we establish two distinct payment systems for different types of mobile users to enhance data protection through security parameters and a smaller network footprint.

2.4 Developing a dependable m-commerce payment system for use on an offline wireless network

The E-commerce market stands out as one of the most popular methods for all types of mobile payment consumers in today's technology landscape. It encompasses surrounding area networks for present users across various payment systems. Despite its widespread adoption, the security of online payment systems remains a significant concern. In our project, we highlight credit and debit card

data theft as a prevalent form of criminal activity. Criminals often target sales data systems to steal customer information, posing a significant risk to both merchants and consumers. While the Modern POS System offers cost-effective solutions with enhanced security measures, user information remains vulnerable to theft. Security breaches can lead to the unauthorized acquisition of users' card details within a short period. To address this, we propose implementing robust security measures, particularly when the system is offline. Disconnecting the connection for users and potential attackers during offline periods can help mitigate the risk of data breaches and unauthorized access to sensitive information.

3.PROPOSED SYSTEM

We utilize the pyAesCrypt library package to generate encrypted secret keys, ensuring secure access to files in the proposed system. Each data file is stored in a protected environment, and only authorized administrators can upload files and manage user permissions. This approach guarantees the confidentiality and security of files. By employing encrypted secret keys, only designated users can access files, thereby enhancing security levels.

3.1 IMPLEMENTATION

In this project, we utilize various methods to securely share files, employing cryptographic algorithms. The modules included are:

1. Users Admin and User Registration:

- Users and administrators can create accounts by providing details like account name and email address. This facilitates account creation for subsequent steps, such as login, enabling admins to monitor user requests to upload files.

2. Admin and User Login:

- Admin users authenticate by entering their username and password. Upon successful login, they can utilize cloud security architecture features like file upload, download, and monitoring user requests.

3. Upload File:

- Both admins and users can upload files, granting access to users who require it. Permission-granted users can then download or upload files as needed.

4. View Request:

- Admin users receive notifications when

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

new users request file access. They can then grant or reject access to the file. Users can only view files if access is granted by the admin.

5. Submitting a Request:

- Users must submit a file access request to view files. Admins can then provide access or download authorization within a specified timeframe.

6. Secure Key Authentication:

- After file permissions are granted for a user's email ID, a secret key is generated. Users must enter this key to download the file. If the key is invalid, file download is not permitted

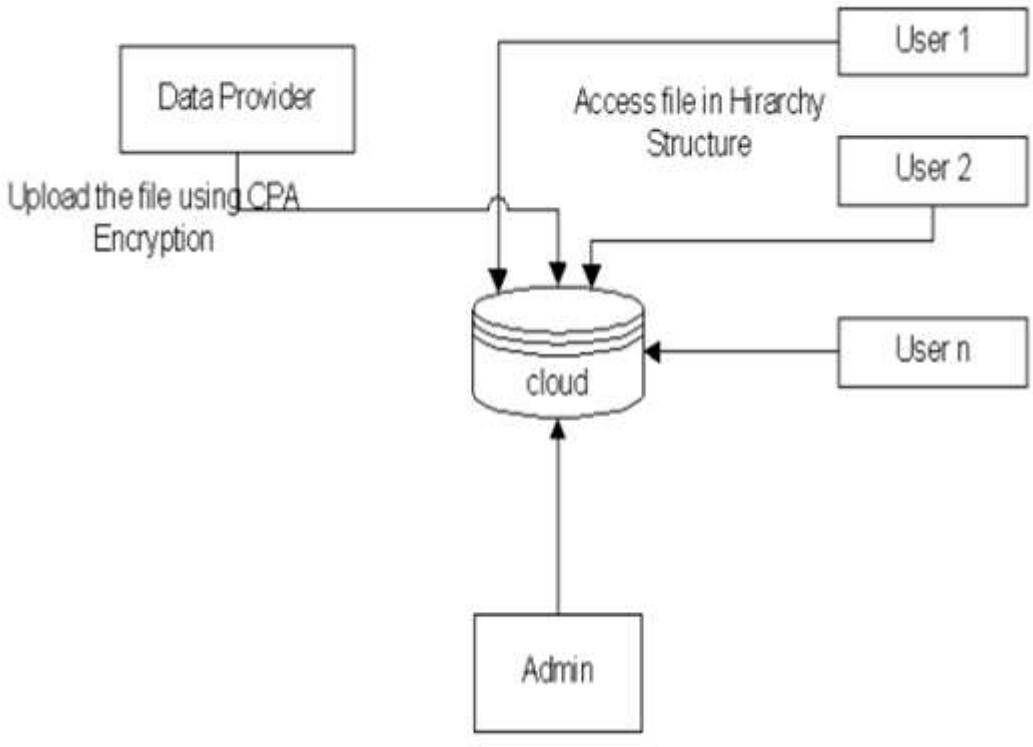

Fig 1:Architecture

4.RESULTS AND DISCUSSION

This page is admin home page, in this page admin can update the account, upload file and also logout.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
IJARST
ISSN: 2457-0362

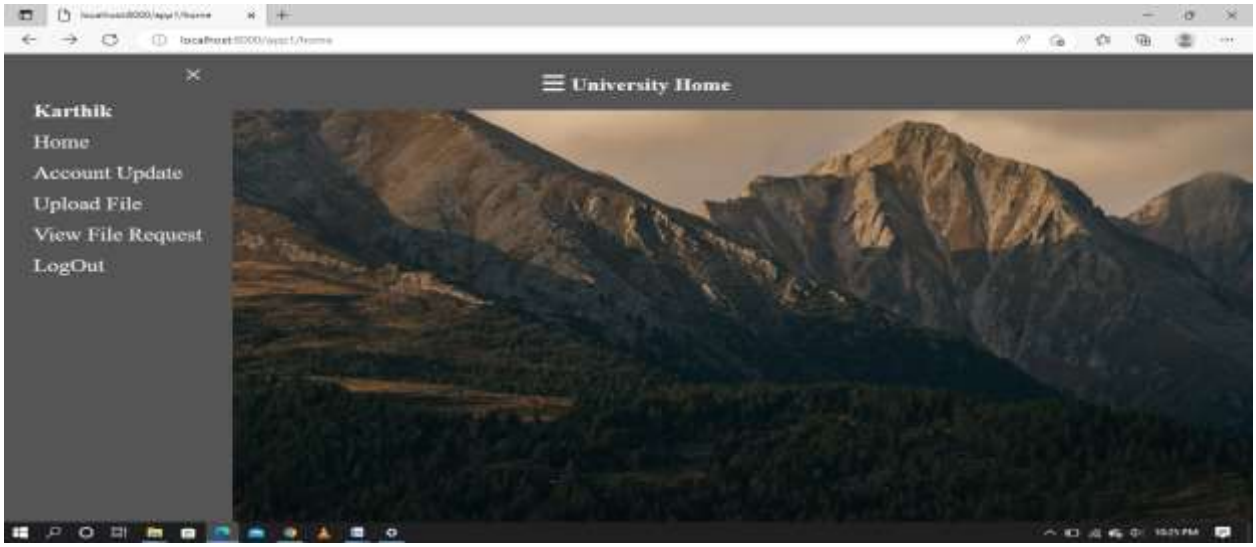

Figure 2. Admin home page

This page is the file upload page, admin can upload the any type of file for the user who are register.

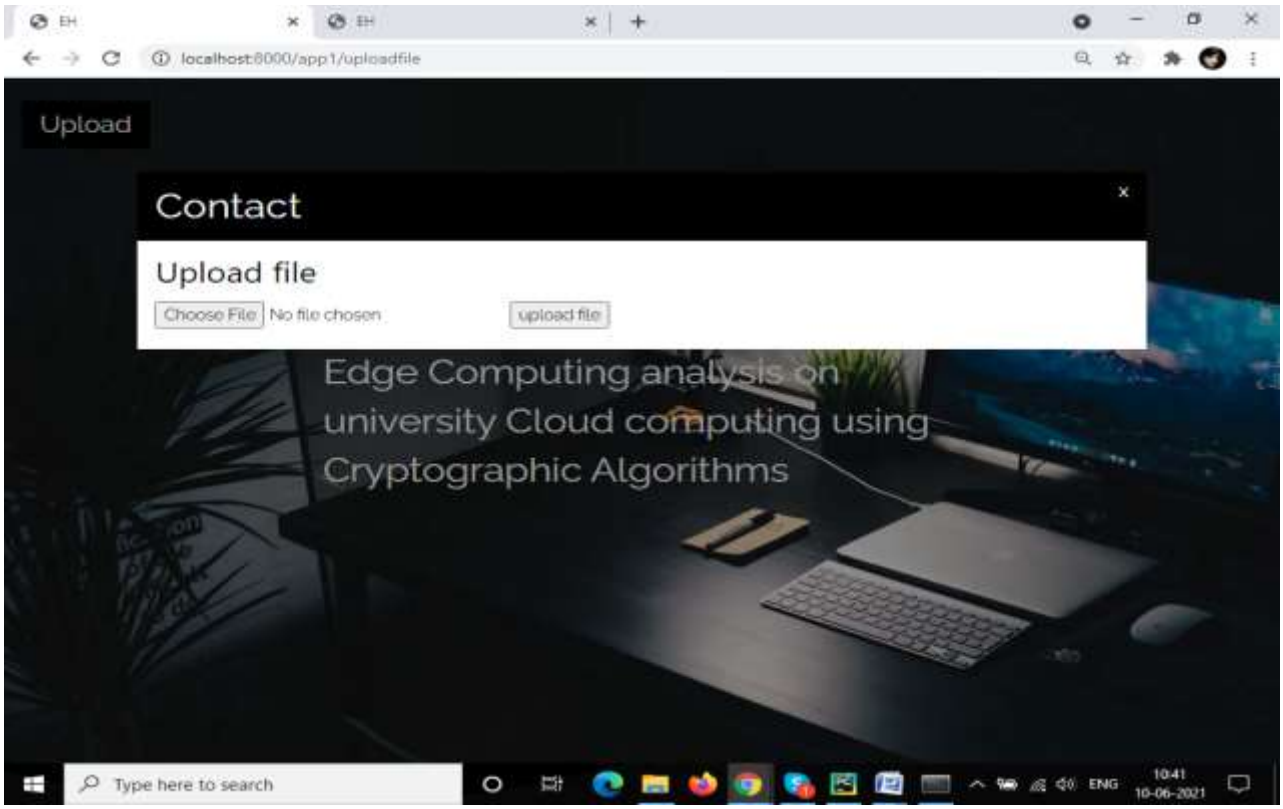

Figure 3 Upload File Form

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

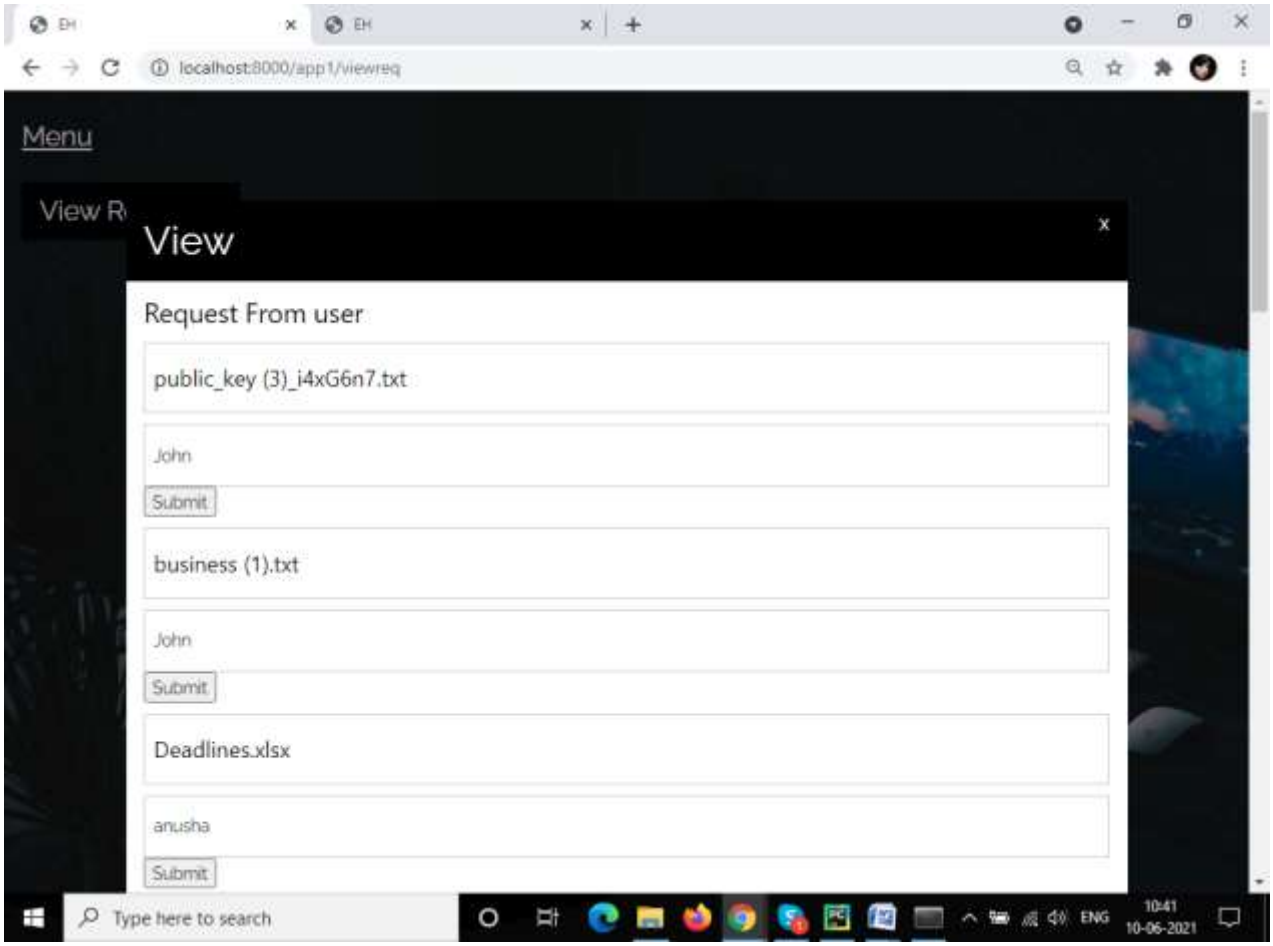

Figure 4: View File Request Form

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

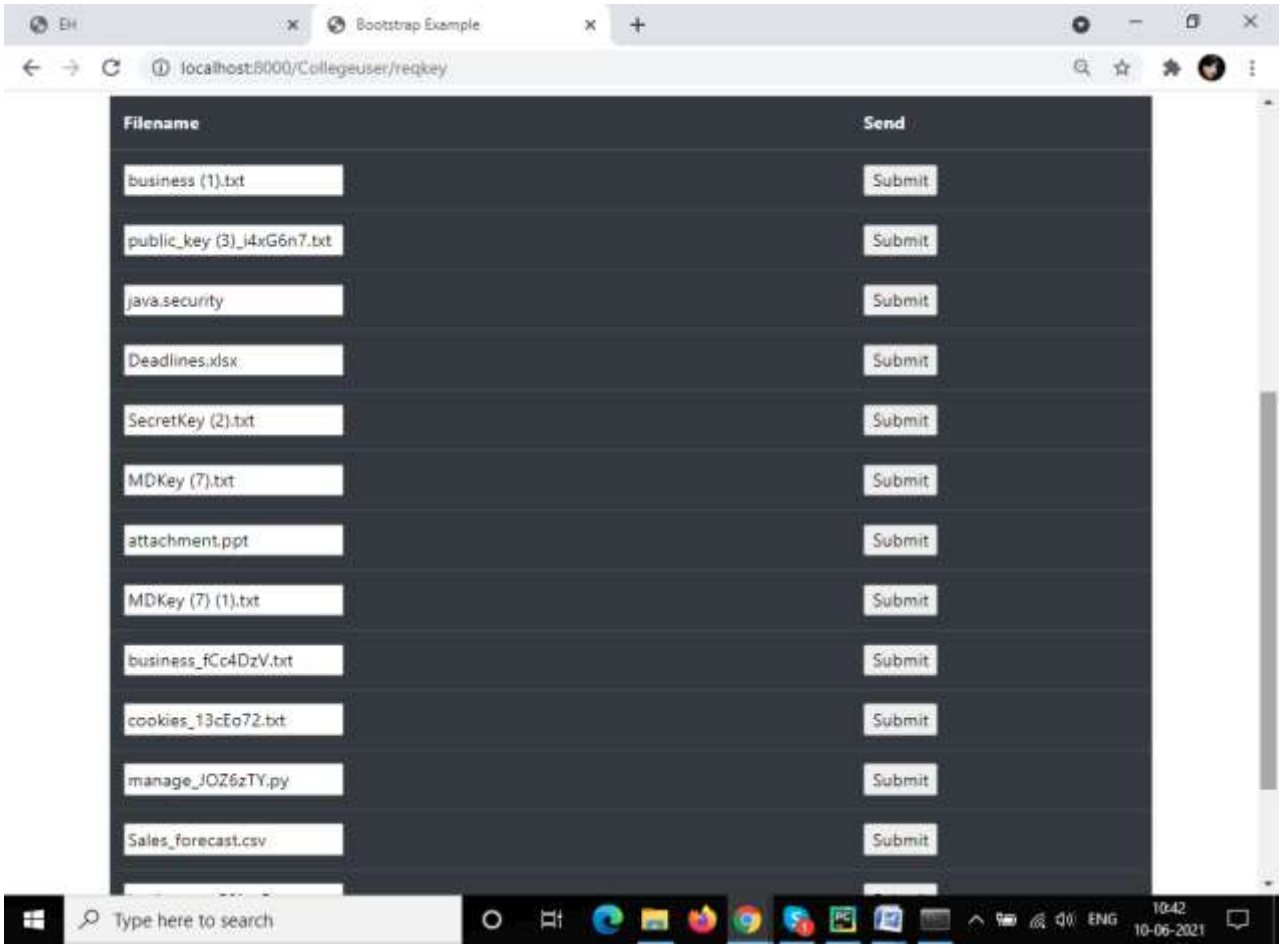

Figure 5: Send File Request Form

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

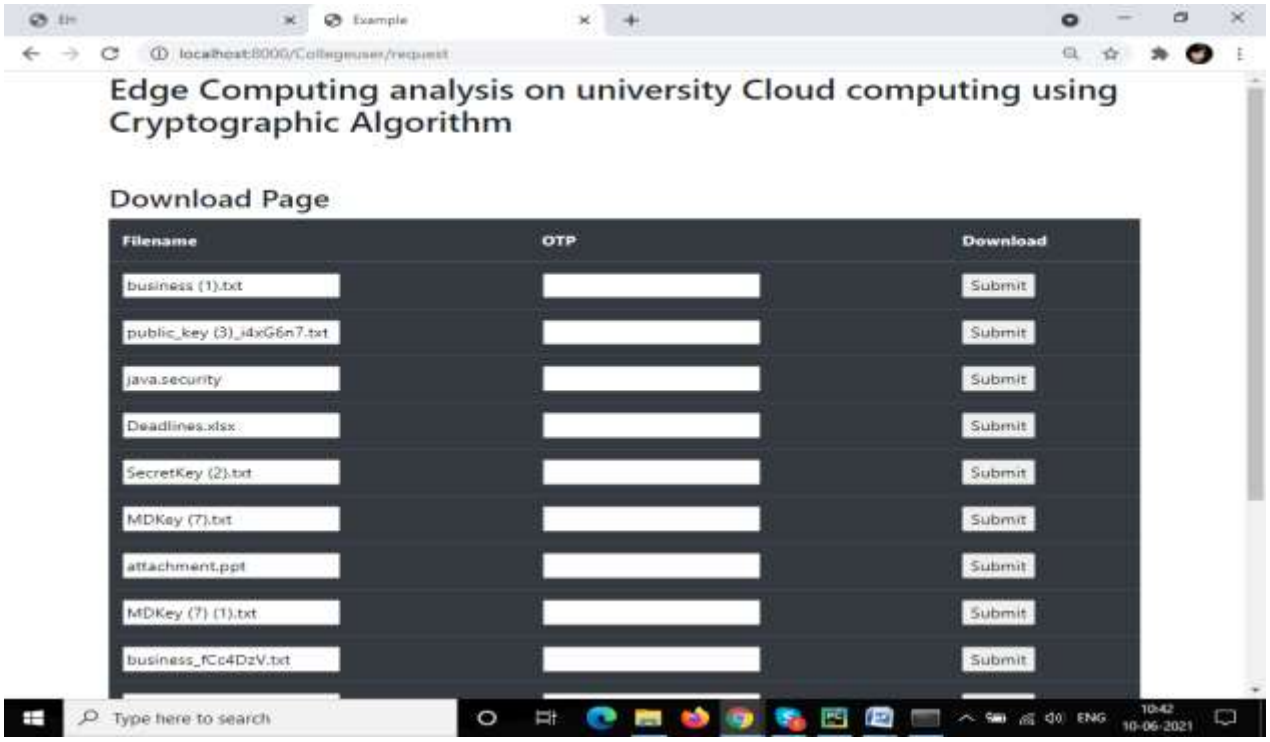

Figure 6. Download File Form

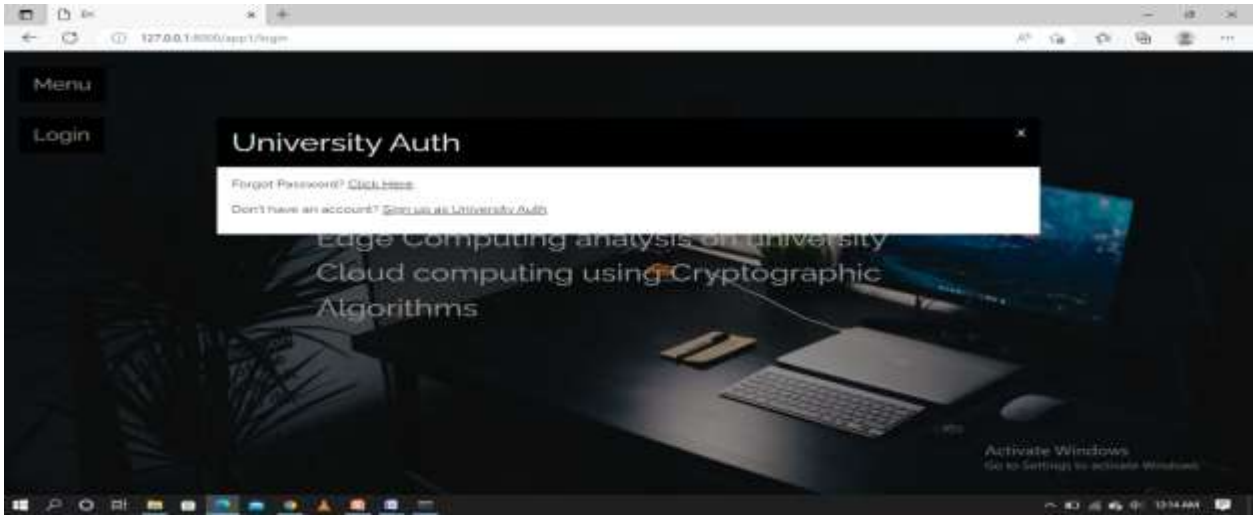

Figure 7: admin menu

5.CONCLUSION

File sharing using the Cipher Text Attribute Based Encryption (CP-ABE) technique provides a practical and efficient solution for transferring files across various applications securely. We can employ various organized approaches to distribute files, ensuring that only

authorized users can access them. In this project, we introduced an encryption algorithm to store both the original and encrypted files securely.

The primary objective of the project is to facilitate secure data sharing by distributing the secret key to authorized individuals, enabling them to access, store, and retrieve data securely. Only admin users have the capability to manage files within the project, ensuring controlled access to the shared data. This approach ensures the security of the file-sharing process.

To implement encrypted file distribution, we utilize the pyAesCrypt encryption library packages to generate the secret key code. This enables us to maintain the confidentiality and integrity of the shared files effectively.

REFERENCES

[1] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A breach in the clouds: towards a clouds definition," ACM SIGCOMM multComput. Commun. Rev., vol. 39, no. 1, pp. 50–55, 2009. [2] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lind

[2] "Data encryption online storage," by S. Kamara and K. Lauter, published in RLCPS, January 2010, LNCS by Springer, Heidelberg. [Citation needed]

[3] A. Singhal submitted an essay titled "Modern information retrieval: A short summary" for the IEEE Data Science Bulletin in 2001. The article was published on pages 35–43.

[4] I. H. Witten, A. Moffat, and T. C. Bell wrote "Managing gigabytes: Compressing and indexing words and images," which was published by Morgan Kaufmann Publishing in May 1999 in San Francisco.

[5] C.-K. Chu, W.-T. Zhu, J. Han, J.-K. Liu, J. Xu, and J. Zhou, "Security problems in popular cloud storage services," IEEE Pervasive Compute., vol. 12, no. 4, pp. 50–57, October/December 2013. [Security problems with popular cloud storage services]

[6] T. Jiang, X. Chen, J. Li, D. S. Wong, J. Ma, and J. Liu, "TIMER: Reliable and secure cloud storage versus data re-outsourcing," in Proc. 10th Int. Conf. Inf. Secur. Pract. Exper., vol. 8434. May 2014, pp 346–358. [7] T. Jiang, X. Chen, J. Li, D. S. W

[7] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, "An efficient infrastructure as a service based revocable personality proxy re-encryption system for public clouds data sharing," in Proc. nineteenth Eur. Symp. Res. compute. Secur., vol. 8712.

Sep. 2014, pp. 257–272; this was published inside the Proceedings of the 19th European Symposium on Research in

[8] T. H. Yuen, Y. Zhang, S. M. Yiu, and J. K. Liu wrote an article titled "Identity-based encryption with comment auxiliary inputs for cloud security applications and sensor networks," which was published in the Deliberations of the 19th European Symposium on Computational Security, volume 8712, September 2014, pages 130–147.

[9] K. Liang and colleagues authored an article titled "A DFA-based functional proxy re-encryption strategy for safe public cloud data sharing," which can be accessed here. October 2014 issue of the IEEE Transactions of Data Forensics and Cybersecurity, volume 9, issue 10, pages 1667–1680.

AUTHOR'S PROFILES

M.Anitha Working as Assistant Professor & Head of Department of MCA ,in SRK Institute of technology in Vijayawada. She done with B .tech, MCA ,M. Tech in Computer Science .She has 8 years of Teaching experience in various Engineering Colleges.

K . Venkata Sai Rohini From MCA In SRK Institute of Technology,Vijayawada Enikepadu.