e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:05/May-2023 Impact Factor- 7.868 www.irjmets.com

SECURE FILE STORAGE AND TRANSFER USING CLOUD

Suyog Khutale[*1], Viraj Patil[*2], Shivam Rajmane[*3], Pratik Shinde[*4], Shubham Raykar[*5], Prof. Samrat Babar[*6]

[*1,2,3,4,5]Student, Department of Computer Science and Engineering, SETI, Panhala, Kolhapur, Maharashtra, India.

[*6]Assistant Professor, Department of Computer Science and Engineering, SETI, Panhala, Kolhapur, Maharashtra, India.

ABSTRACT

In today's interconnected world, file transfer is a fundamental requirement for businesses and individuals a like. However, the transfer of sensitive and confidential files requires additional security measures to ensure confidentiality, integrity, and availability. In this paper, we propose a secure file transfer mechanism over the cloud using Angular, Node.js, MongoDB, and AWS S3. The proposed system utilizes RSA and AES algorithms for key transfer and pairing to provide secure and confidential file transfers. The system also stores user data and files securely on AWS S3, making it scalable, cost-effective, and easily accessible from any location. The system's modular architecture and optimized rendering engine ensure high performance and a user-friendly experience.

Keywords Secure file transfer, cloud, RSA, AES, Angular, Node.js, MongoDB, AWS S3

I. INTRODUCTION

File transfer is an essential requirement for many applications, including cloud-based services, e-commerce, and online collaboration tools. However, the transfer of sensitive and confidential files requires additional security measures to prevent unauthorized access, tampering, or interception. Traditional file transfer mechanisms such as FTP, HTTP, and SMTP are not secure enough to transfer sensitive data over the internet. Therefore, there is a need for a secure and reliable file transfer mechanism that can ensure the confidentiality, integrity, and availability of data. Cloud computing has emerged as a popular solution for providing scalable and cost-effective computing resources over the internet. Cloud-based file storage and transfer services such as Dropbox, Google Drive, and AWS S3 have become widely popular due to their ease of use, accessibility, and scalability. Ensuring the security of such services has become an increasingly pressing issue, particularly given the handling of confidential and sensitive information. In this paper, we propose a secure file transfer mechanism over the cloud using Angular, Node.js, MongoDB, and AWS S3. The proposed system utilizes RSA and AES algorithms for key transfer and pairing to provide secure and confidential file transfers. The system also stores user data and files securely on AWS S3, making it scalable, cost-effective, and easily accessible from any location. The system's modular architecture and optimized rendering engine ensure high performance and a user-friendly experience.

II. SYSTEM DESIGN

The proposed system is made of three main components: front-end development using Angular, development of back-end using Node.js, and file storage and transfer using AWS services.

III. SYSTEM ARCHITECTURE

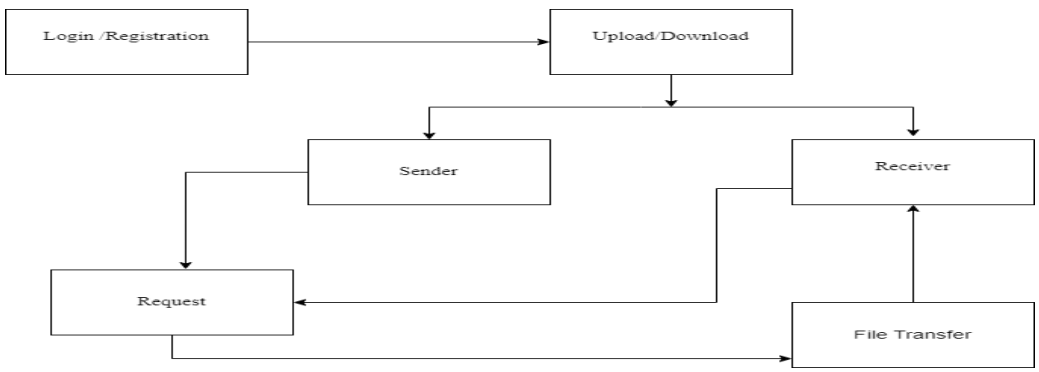

Figure 1: System Architecture

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:05/May-2023 Impact Factor- 7.868 www.irjmets.com

IV. FRONT-END DEVELOPMENT USING ANGULAR

The front-end of the file transfer application is developed using Angular, a popular front-end development framework. Angular's modular architecture and reusable components make it easy to create and manage different parts of the application. The optimized rendering engine and change detection mechanism of Angular ensure fast performance and a responsive user interface.

The front-end of the proposed system is designed to provide a simple and intuitive user interface for file transfer operations. The user interface consists of a file upload form, file download form, file sharing form, and user account management form. The file upload form allows users to select a file and upload it to AWS S3. The file download form allows users to download files from AWS S3. The file sharing form allows users to share files with other users by providing their email address. The user account management form allows users to manage their account details such as email, password, and personal information.

V. BACK-END DEVELOPMENT USING NODE.JS

The back-end of the file transfer application is developed using Node.js, a popular server-side runtime environment. Node.js's non-blocking I/O model and event-driven architecture ensure fast performance and scalability for handling large amounts of data. Node.js also provides access to a large ecosystem of open-source modules and libraries, making it easy to build and maintain complex web applications.

VI. UML DIAGRAM

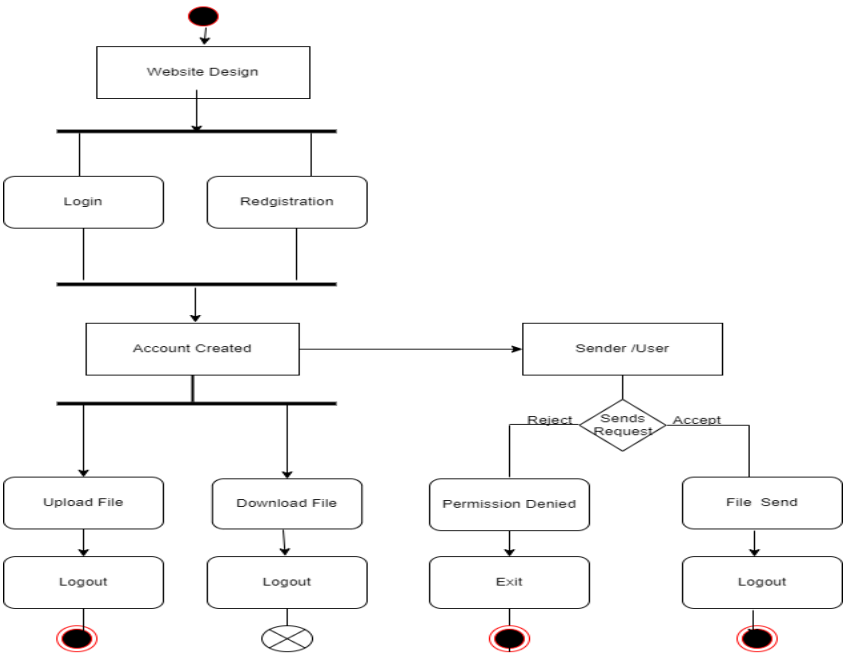

Figure 2: UML Diagram

VII. FILE STORAGE AND MANAGEMENT USING AWS S3

The file storage and management component of the system are implemented using AWS S3, a cloud-based object storage service. AWS S3 provides high durability and availability of data, advanced security features, and scalability to handle large amounts of data. The cost-effective pricing model of AWS S3 makes it an ideal choice for storing and managing data in the cloud.

VIII. KEY TRANSFER USING RSA AND AES ALGORITHMS

The proposed system uses RSA and AES algorithms for key transfer and encryption during the file transfer process. RSA is used to exchange session keys between the client and server, while AES is used to encrypt the actual file data during transfer. RSA is a public-key cryptosystem that uses two keys, a public key and a private key, for encryption and decryption. AES is a symmetric-key encryption algorithm that uses the same key for encryption and decryption. Pairing is used to establish a secure connection between the client and server by exchanging a shared secret or key.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:05/May-2023 Impact Factor- 7.868 www.irjmets.com

AES Algorithm:

The Advanced Encryption Standard (AES) algorithm is a symmetric encryption algorithm that is widely used for securing sensitive data. It was selected by the U.S. National Institute of Standards and Technology (NIST) in 2001 as the standard encryption algorithm for government and commercial use. The algorithm uses a block cipher that encrypts data in blocks of 128 bits using a key length of either 128, 192, or 256 bits.

The AES algorithm consists of four main operations: SubBytes, ShiftRows, MixColumns, and AddRoundKey. In the SubBytes operation, each byte of the input block is replaced with a corresponding byte from a fixed lookup table. In the ShiftRows operation, the rows of the input block are shifted by a certain number of bytes. In the MixColumns operation, the columns of the input block are multiplied by a fixed matrix. Finally, in the AddRoundKey operation, each byte of the input block is XORed with a corresponding byte from the encryption key.

RSA Algorithm:

The RSA algorithm is a public-key encryption algorithm that is widely used for secure communication over the internet. It was developed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1977 and is named after their surnames. The RSA algorithm uses two keys - a public key and a private key - to encrypt and decrypt data.

The RSA algorithm works by using the mathematical properties of prime numbers. The public key consists of two numbers - the modulus, which is the product of two large prime numbers, and an exponent. The private key consists of the same two prime numbers used to generate the modulus, and a different exponent.

To encrypt a message using the RSA algorithm, the sender first encrypts the message using the recipient's public key. To decrypt the message, the recipient uses their private key to decrypt the encrypted message.

IX. CONCLUSION

The proposed secure file transfer mechanism over the cloud using AWS provides a secure and efficient way to transfer sensitive and confidential files. The system's use of modern web technologies and AWS services ensures scalability, security, and cost-effectiveness. The use of RSA and AES algorithms for key transfer and encryption, along with pairing, provides an additional layer of security to prevent unauthorized access, tampering, or interception.

X. REFERENCES

[1] K. Jamsa, Cloud Computing: SaaS, PaaS, IaaS, Virtualization, Business Models, Mobile, Security and More. Burlington, MA, USA: Jones & Bartlett.

[2] A. Bouayad, A. Blilat, N. E. H. Mejhed, and M. El Ghazi, ‘‘Cloud computing: Security challenges,’’ in Proc. Colloq. Inf. Sci. Technol., Oct.

[3] S. M. Habib, S. Ries, and M. Muhlhauser, ‘‘Cloud computing landscape and research challenges regarding trust and reputation,’’ in Proc. 7th Int. Conf. Ubiquitous Intell. Comput. 7th Int. Conf. Autonomic Trusted Comput.

[4] N. Sultan and S. van de Bunt-Kokhuis, ‘‘Organisational culture and cloud computing: Coping with a disruptive innovation,’’ Technol. Anal. Strategic Manage.

[5] H. Tianfield, ‘‘Security issues in cloud computing,’’ in Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC).