ONLINE SECURE FILE STORAGE SYSTEM FOR DATA SECUIRITY

K. VENKATESWARLU, Asistant Professor, Dept. of Master of Computer Applications, Narayana Engineering College(Autonomous), Gudur.SPSR Nellore, AP.
U.PRATHYUSHA, PG Scholar, Dept. of Master of Computer Applications, Narayana Engineering College(Autonomous), Gudur.SPSR Nellore, AP

Abstract_ Due to the recent innovations in the internet and the network applications and the wide spread of internet and networks, it is now completely possible to conduct electronic commerce on the internet or through the local area networks, and the wide spread of computer and communication network promoted many users to transfer files and sensitive information through the network, this sensitive data requires special deal. This work presents a security system that can provides privacy and integrity for exchanging sensitive information through the internet or the communication networks, based on the use of recently developed encryption algorithms, such as AES, IDEA and RSA. The aim of the work is to develop a simple file transfer system that can obtain privacy, integrity and authentication for the file transfer process. The proposed system uses symmetric cryptography system. File transfer must provide end-toend visibility, security and compliance management. The goal of this project is to provide a simple file transfer system that ensures file transfer privacy, integrity, and authentication. Symmetric cryptography is used in the suggested system. End-to-end visibility, security, and compliance management are required for file transfer.

1.INTRODUCTION

Because a large amount of personal data is moved to and from enterprises on a daily basis, there is a risk that the data will be lost by accident or stolen on purpose. This is untrustworthy because it poses a major risk to the businesses. The project is an application that ensures the security and confidentiality of data exchanged over the Internet. To avoid any financial or information losses that could be harmful to the company, it is critical that the data being transferred does not get into the wrong hands. Furthermore, only authorised individuals have access to the data storage and transfer, ensuring a safe method of management and transfer.

2.LITEARTURE SURVEY

1) Mobile cloud computing: A survey
AUTHORS: N. Fernando, S. W. Loke, and W. Rahayu
Despite growing utilization of cellular computing, exploiting its full practicable is tough due to its inherent issues such as aid scarcity, time-honored disconnections, and mobility. Mobile cloud computing can tackle these issues through executing cellular purposes on aid companies exterior to the cellular device. In this paper, we supply an sizable survey of cellular cloud computing research, whilst highlighting the precise worries in cellular cloud computing. We current a taxonomy based totally on the key problems in this area, and talk about the one-of-a-kind strategies taken to address these issues. We conclude the paper with a crucial evaluation of challenges that have now not but been completely met, and spotlight instructions for future work.
2) Cloud-based augmentation for cellular devices: motivation, taxonomies, and open challenges
AUTHORS: S. Abolfazli, Z. Sanaei, E. Ahmed, A. Gani, and R. Buyya
Recently, Cloud-based Mobile Augmentation (CMA) methods have received superb floor from academia and industry. CMA is the brand new cell augmentation mannequin that employs resource-rich clouds to increase, enhance, and optimize computing competencies of cellular gadgets aiming at execution of resource-intensive cell applications. Augmented cellular gadgets envision to operate full-size computations and to save large records past their intrinsic competencies with least footprint and vulnerability. Researchers make use of different cloud-based computing sources (e.g., far away clouds and close by cellular nodes) to meet a range of computing necessities of cell users. However, using cloud-based computing sources is no longer a simple panacea. Comprehending integral elements (e.g., modern nation of cell patron and faraway resources) that have an impact on on

augmentation procedure and highest quality determination of cloud-based aid sorts are some challenges that restrict CMA adaptability. This paper comprehensively surveys the cell augmentation area and gives taxonomy of CMA approaches. The goals of this find out about is to spotlight the results of faraway sources on the fine and reliability of augmentation methods and talk about the challenges and possibilities of using assorted cloud-based sources in augmenting cellular devices. We existing augmentation definition, motivation, and taxonomy of augmentation types, along with standard and cloud-based. We severely analyze the present day CMA methods and classify them into 4 corporations of far-off fixed, proximate fixed, proximate mobile, and hybrid to existing a taxonomy. Vital choice making and overall performance hassle elements that impact on the adoption of CMA strategies are added and an exemplary selection making flowchart for future CMA processes are presented. Impacts of CMA methods on cell computing is mentioned and open challenges are introduced as the future lookup directions.

3) Mobile cloud computing: Standard method to defending and securing of cellular cloud ecosystems

AUTHORS: R. Kumar and S. Rajalakshmi

The standards of Cloud computing are naturally meshed with cell gadgets to allow on-the-go functionalities and benefits. The cell cloud computing is rising as one of the most essential branches of cloud computing and it is anticipated to enlarge the cell ecosystems. As greater cellular units enter the market and evolve, sincerely protection problems will develop as well. Also, full-size boom in the range of gadgets related to the Internet will similarly power protection needs. Understanding the proper practicable of cellular cloud computing and figuring out problems with cell cloud security, privacy, feasibility and accessibility continue to be a predominant challenge for each the clients and the enterprises. This paper covers the cell cloud protection troubles and challenges by using searching at the modern kingdom of cloud protection breaches, vulnerabilities of cell cloud devices, and how to tackle these vulnerabilities in future work in issue of cell system administration and cellular information protection. Also, it highlights on utilization of SCWS (Smart Card Web Services) competition to intensify protection of cell cloud computing.

3.PROPOSED SYSTEM

Encryption is the most efficient method of ensuring data security. Encryption hides the contents of a message in such a way that only a decryption process can reveal the original information. The goal of encryption is to prevent unauthorised parties from viewing or altering data. Encryption happens when data is passed through some substitute technique, shifting technique, table references, or mathematical operations. All of those procedures produce data in a different format. The plaintext is the unencrypted data, and the ciphertext is the encrypted data, which is a representation of the original data in a new form. This programme uses a symmetric encryption key, which means the same key is used for both encryption and decryption. Only after the encrypted file has been decrypted to its original file using the symmetric encryption key can it be accessed and read.

3.1 IMPLEMENTATION

1. **Admin File Upload**
2. **User Search**
3. **File Encryption**
4. **Decryption**

1. Admin File Upload:

The Admin will upload an encrypted file onto the server by clicking the upload button, before uploading the file the admin must encrypt it; it is a pre-requisite for uploading. Once the file gets uploaded it gets stored in the File Database. When the user send request for their selected file, admin will send response with the encrypted key according to the file request. Admin maintain the user details, file download details in the database.

2. User Search:

Users search the uploaded files, in order to select and send request to the admin. Admin would view the user selected files and send response according to the filename in which the user request. The file will send along with the encrypted key. Only the authenticated user can login and search files and send request to the admin. Authorized user would view the encrypted key in order to download the file. On Clicking of the download button the user should enter the encrypted key in order to decrypt. Encryption is used to ensure the secure passing of messages and other sensitive documents and information. The encrypted file can only be opened and viewed after it has been decrypted to its original file using the symmetric encryption key.

3. File Encryption:

The process of Encryption hides the contents of a message in a way that the original information is recovered only through a decryption process. The unencrypted data is referred to as the plaintext and the encrypted data as the ciphertext, which is representation of the original data in a different form. A symmetric Encryption key is used for this application, which means the same key is shared for both Encryption and decryption. The encrypted file can only be opened and viewed after it has been decrypted to its original file using the symmetric encryption key. The purpose of Encryption is to prevent unauthorized parties from viewing or modifying the data Encryption occurs when the data is passed through some substitute technique, shifting technique, table references or mathematical operations. All those processes generate a different form of that data.

4. Decryption:

When the data is unscrambled by the use of a key, that is what is known as 'decryption'. It is the opposite of encryption and the 'described method' of scrambling is basically applied in reverse, so as to unscramble it. Hence, the jumbled and unreadable text becomes readable once again. When the private key has been decrypted immediately the file can be download. Then the user can download and save the file.

4.RESULTS AND DISCUSSION

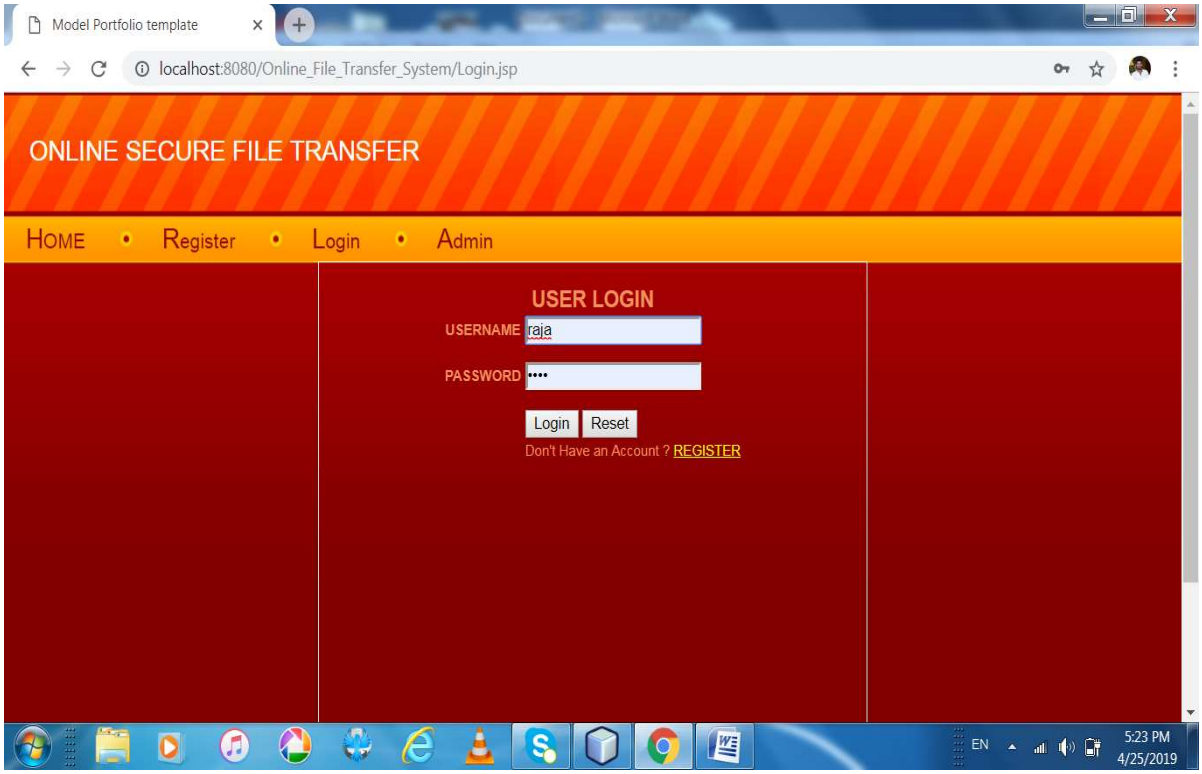

Fig 4.1 User Login Page

Fig 4.2 Sending request for data

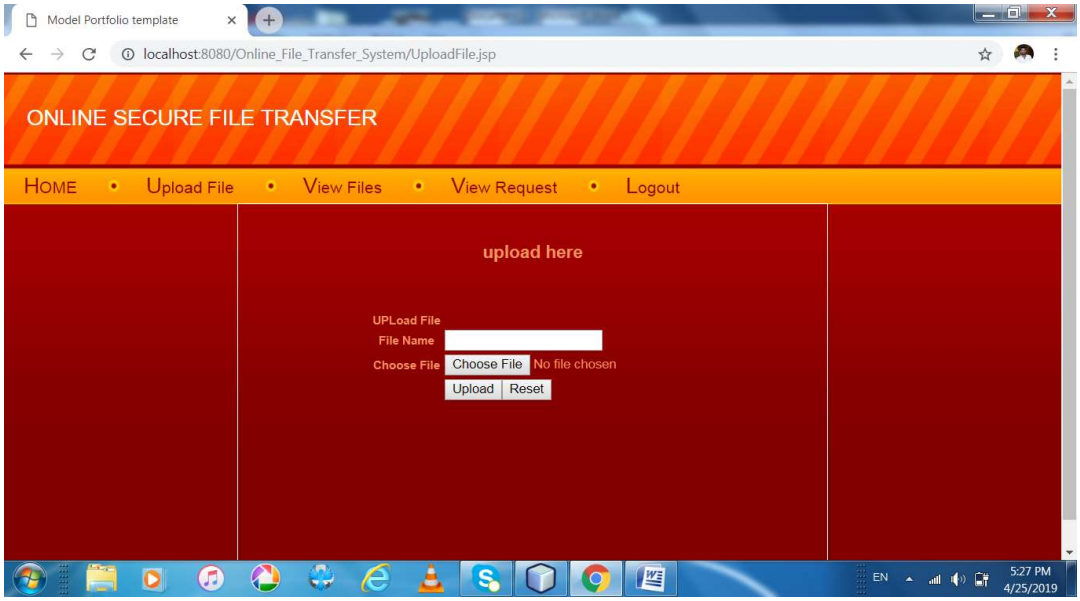

Fig 4.3 Uploading data

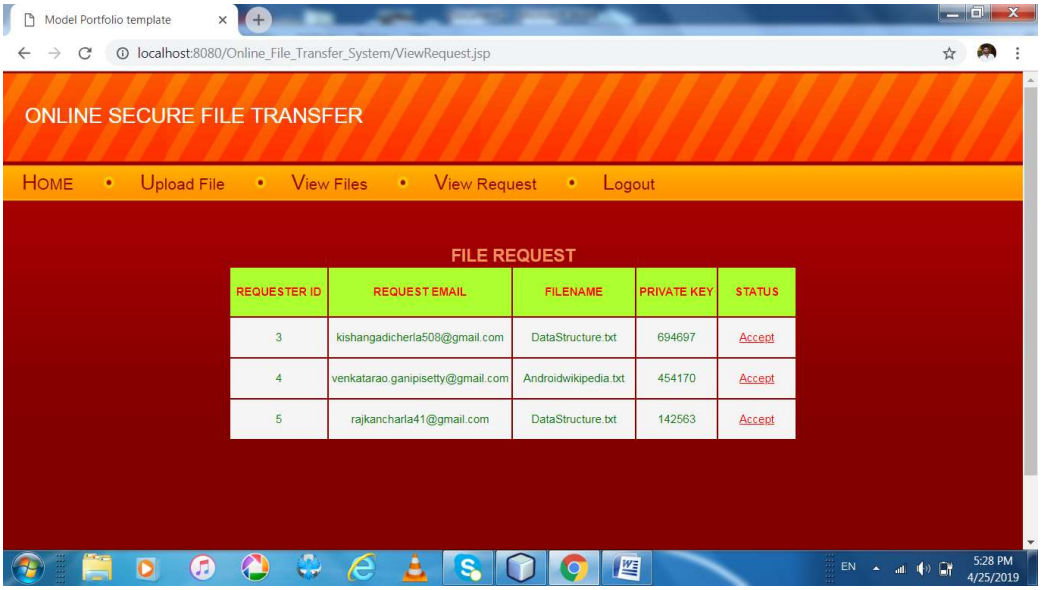

Fig 4.4 Giving Permission to requested user

5.CONCLUSION

This is when we deliver a file from one computer to another in an encrypted format. We can share files and even view files from other computers through a PC folder because all of our computers are connected to one server. When we login in this study, the essential difficulty is the key. If we press the wrong key three times, the user will be blocked by the administrator. As a result, always keep in mind the key that was given to you at the time of login. This adds security during file transfer by first encrypting the file and then decrypting it to display the received data. We can also access files from other linked computers via the PC folder.

REFERENCES

[1] P. Ford-Hutchinson. Securing FTP with TLS. Internet Draft (RFC 4217), 2005.
[2] Analytical framework for measuring network security using exploit Dependency graph by P. Bhattacharya, SGhosh(2012).
[3] Secure file management system over internet by Hua Zhang, Jun – Fen Diao, Qiao – Yan Wen, university of posts and telecommunication (2008)
[4] Secure File Sharing in JXTA using Digital Signature – Erita Skendag, Marenglen Biba – University of NY Tirana(2012)
[5] Information security of Remote File transfer with mobile Devices – Sami Noponen, Kaarina Karppnen(2008)
[6] Penchalaiah, P., & Rajasekar, P. An Efficient Multi-User Hierarchical Authenticated Encryption Using Simultaneous Congruence for Highly Secure Data. International Journal of Future Generation Communication and Networking (WoS), ISSN, 2233-7857.
[7] Moving towards network security and firewalls for protecting and preserving private resources on Internet by Dr.S.S. Riaz Ahmed(2008)
[8] H. B. Pethe and S. Pande, "A Survey on Different Secret Key Cryptographic Algorithms," IBMRD's Journal of Management & Research, vol. 3, pp. 142-150, 2014.

K.venkateswalu has receivedher B.Tech Saraswathi valu college of Engineering,Vellore(dst),Anna University 2010.mTech computer science (cs)PBR vits kavali JNTUA 2014 Assistant professor,Ne Gudur.6 years experience in Narayana Engineering College Gudur.

U.Prathyusha has received her B.Sc degree in Computers from kakathiya Degree College , podhalakur affiliated to Vikrama Simhapuri University, Nellore in 2018 and persuing PG degree in MCA at Narayana Engineering College, Gudur affiliated to JNTU Anantapuram (2018-2021).