WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Advancing IP-Based File Sharing for Seamless and Secure Data Exchange

Nithish K[1] ,Dr. Vaidehi V[2]

[1]PG Student, Email: nithishkuppan37@gmail.com
[2]Professor, Email: vaidehi.mca@drmgrdu.ac.in
Department of Computer Applications,
Dr. M.G.R. Educational and Research Institute, Chennai, India.

ABSTRACT :

In the contemporary digital landscape, the need for efficient and secure data exchange has become paramount. The project titled "Advancing IP-Based File Sharing for Seamless and Secure Data Exchange" aims to address this imperative by developing an innovative framework that leverages Internet Protocol (IP) technology to enhance the file sharing process. The proposed system combines cutting-edge encryption techniques with IP protocols to establish a secure and seamless environment for transferring data between devices. By focusing on IP-based solutions, the project seeks to overcome the limitations of traditional file-sharing methods, ensuring compatibility across diverse platforms and networks.

Keywords – Data Security, Cloud Service Providers (CSP), Secure Sharing, Encryption File System, Access Control, IP Address, IP Spoofing, TCP/IP.

INTRODUCTION :

Ip spoofing is the advent of Internet Protocol (IP) packets which have a changed supply deal with to both cover the identification of the sender, to impersonate some other pc machine or both. It is a way regularly utilized by terrible actors to invoke DoS assaults in opposition to a goal tool or the encompassing infrastructure. Sending and receiving IP packets are a primary way in which networked computers and other devices communicate, and constitute the basis of the modern internet [1].

All IP bundles contain a header that goes before the body of the parcel and contain imperative steering data, counting the source address. In everyday packet, the supply IP cope with is the cope with of the sender of the packet. If the packet has been spoofed, the supply cope with can be forged. IP Spoofing is similar to an attacker sending a package deal to a person with the incorrect go back cope with listed [2].

LITERATURE SURVEY :

Anjali Patel.et al.,2016 says that propose system model for secure data sharing on cloud with intension to provides data confidentiality, access control of share data, removes the burden of key management and file encryption/decryption by users, support dynamically changes of user's membership, owner not be always online when the user to access the data [1].

Raseena.M.et al.,2014 says many issues are remained for achieving fine grained data access control. Such as scalability in key management, flexible access, efficient user revocation and privacy problems. So many encryption techniques are used for achieving these features. To achieve fine-grained and scalable data access control for client's data, different attribute-based encryption (ABE) techniques are used [2].

Kajal Chachapara.et al.,2013 says this framework uses cryptography algorithm like AES and RSA. AES is most secure algorithm in cryptography. Once secret is generated consumer (consumer who've generated a key for his or her personal files) can offer that key to determined consumer (consumer for whom secret is generated). So, when decided user will try to access files on cloud with that key, permission decided by owner will be given to that user [3].

Rishav Chatterjee.et al.,2017 will cognizance upon the reviewing and expertise cloud safety problems via way of means of featuring crypto algorithms and powerful measures which will make certain the statistics safety in cloud. Along with this, we can elucidate a chunk greater approximately a few safety components of cryptography via way of means of showcasing a few privateness problems of modern-day cloud computing surroundings [4].

Yang Ming.et al.,2021 on the basis of the elliptic curve cryptography, we propose an efficient revocable multi-authority attribute-based encryption (RMA-ABE) scheme for cloud storage. The protection evaluation shows that the proposed scheme satisfies indistinguishable beneath adaptive selected plaintext assault assuming hardness of the decisional Diffie-Hellman problem [5].

Jaideep Chandrashekar.et al.,2008 a key characteristic of our scheme is that it does now no longer require worldwide routing records. IDPFs are produced from the records implicit in border gateway protocol (BGP) path updates and are deployed in community border routers. In addition, they are able to assist localize the foundation of an assault packet to a small quantity of candidate networks [6].

PROPOSED SYSTEM:

The system is robust and easy to deploy. During the entire process of complete security code encryption and decryption the file at the nodes do not get crashed. The files remain safe and untouched until the 4-digit security code is matched and verified. The IP address matching (IP spoofing) is encountered to verify the authorized user and the reveal the file sets at the server.
Only after the 4-digit security code is encrypted the file can be viewed by the authorized user in the web phase. The searching of the files in the local nodes is faster and manageable until the limited access of the files. If the number of files to be accessed increase the efficiency is managed using buffer method and making all files requested to be accessible.
Once the receiver has received the file from the destination end, source IP address and must receiver have to give 4-digit secret key with port number in order to download the file. The unauthorized user will try to receive data using IP address is known as IP Spoofing. If the 4-digit secret key is wrong, receiver cannot receive the data whereas the IP address and port number of the receiver has sent to the source end as an error message. If Intruder tries to steal the file means the account will be blocked automatically. Who steal files here IP address and port number will be showing in the current status.

Advantages of Proposed System:

Denying anonymous access and maintaining user authentication allows for better security and a lower chance of data being compromised or being accessed by the wrong people.

METHODOLOGY FOR IMPLEMENTATION

MODULE DESCRIPTION

System development deals with the operations that are carried out in order to get desired output from software product based on certain design specifications. This Application hold the following modules.

LOGIN PAGE:

Logins are utilized by websites, computer applications, and portable apps. They are a security degree planned to avoid unauthorized get to private information. When a login comes up short. (Case, the username and password combination does not coordinate a client account), the client is refused get to. Numerous framework piece clients from indeed attempting to log in after numerous fizzled login end.

1.ADMIN

VIEW USER STATUS PHASE

In this phase, the client administration module is a critical component within the command center, providing administrators with the ability to efficiently manage user accounts. This includes tasks such as view user's and data.
In terms of security controls, administrators wield essential tools to ensure the protection of sensitive data. The emphasis on security underscores the commitment to maintaining the confidentiality and privacy of critical information within the command center.

2. USER

DESTINATION PHASES:

In this phase, the source data is received in the destination end. In order to confirm whether the destination receiver is an authenticated person to view the data, the respective user has to provide the IP address and port number to receive the data.
Once the data is received, the authentication verification is done through 4-digit secret
key whereas the assigned 4-digit secret key is correct then it will ask for filename which has to be provided in the given dialog box.
When the file name gets matched with the sender source, the data is downloaded in our respective path. If the assigned 4-digit secret key is wrong, receiver cannot receive the data whereas the IP address and port number has sent to the source end as an error message.

REGISTRATION PAGE:

Enlistment frame is a list of areas that a client will input information into and yield to person. These are numerous reasons why you would need an individual to fill out enrollment shape. Companies utilize enrollment shapes to sign up client for memberships, administrations, or other programs or plans.

3.PROVIDER

SOURCE PHASES:

In this phase, data are uploaded and encrypted using AES algorithm whereas this kind of encoding is done to avoid unauthorized person to view the context of the data and only the authorized person can able to view through secret key which is provided to corresponding user.
Once the authenticated 4-digit secret key is assigned, the data is sent through IP address and port number in the ABE & AES algorithm which is one of the secured techniques. Block diagram of source phase is as shown in diagram.1

ARCHITECTURE DIAGRAM:

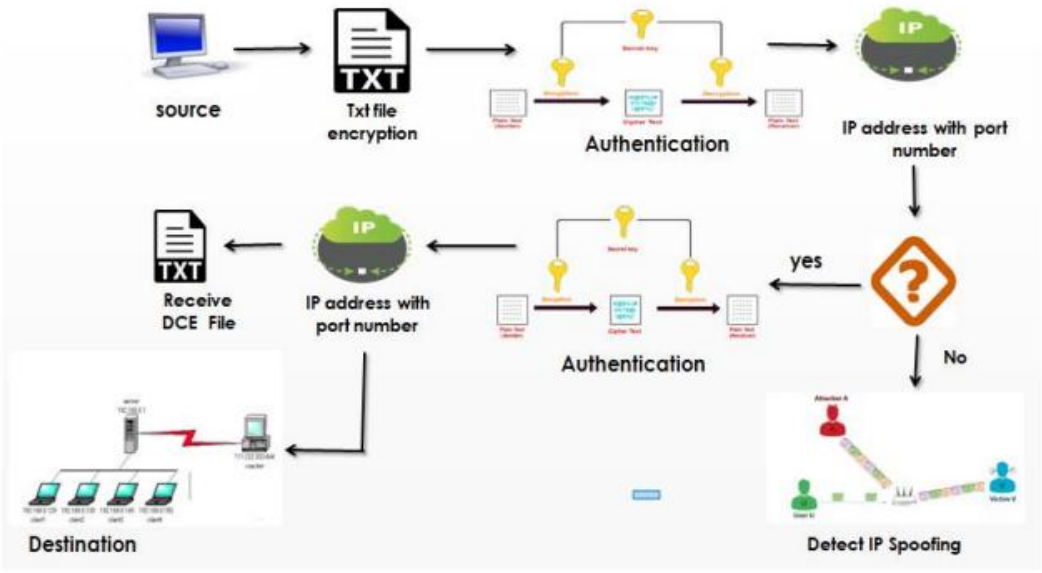

Diagram.1

Architecture diagram illustrating to share the file to end user in a protected manager using IP Address with secret key. Firstly, source or provider sending the text file to destination in the format of encrypted method. In authentication having the secret key. Then, sending the encrypted text file with IP Address with port number via server.
Then, the user receives the file, want secret key, port number and Address.

In case, user entered incorrectly then it will understand IP Spoofing and come out from the screen. In case, user entered correct secret key, port number and IP Address then decrypting the text file and downloaded into destination directory.

RESULTS & DISCUSSION

The implementation of Advancing IP-Based File Sharing for Seamless and Secure Data Exchange presents several noteworthy results and implications, which are discussed in this section. The advanced IP-based file sharing mechanisms effectively

enhances the security posture of cloud-based data storage and sharing systems.

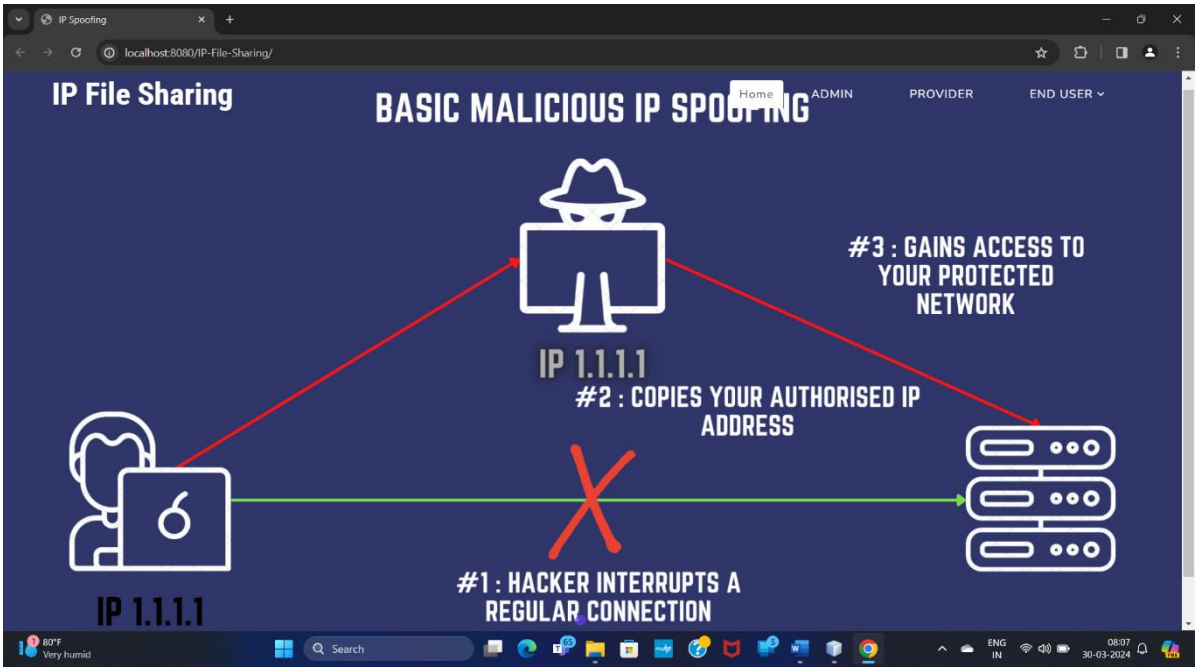

Fig 1: IP File Sharing

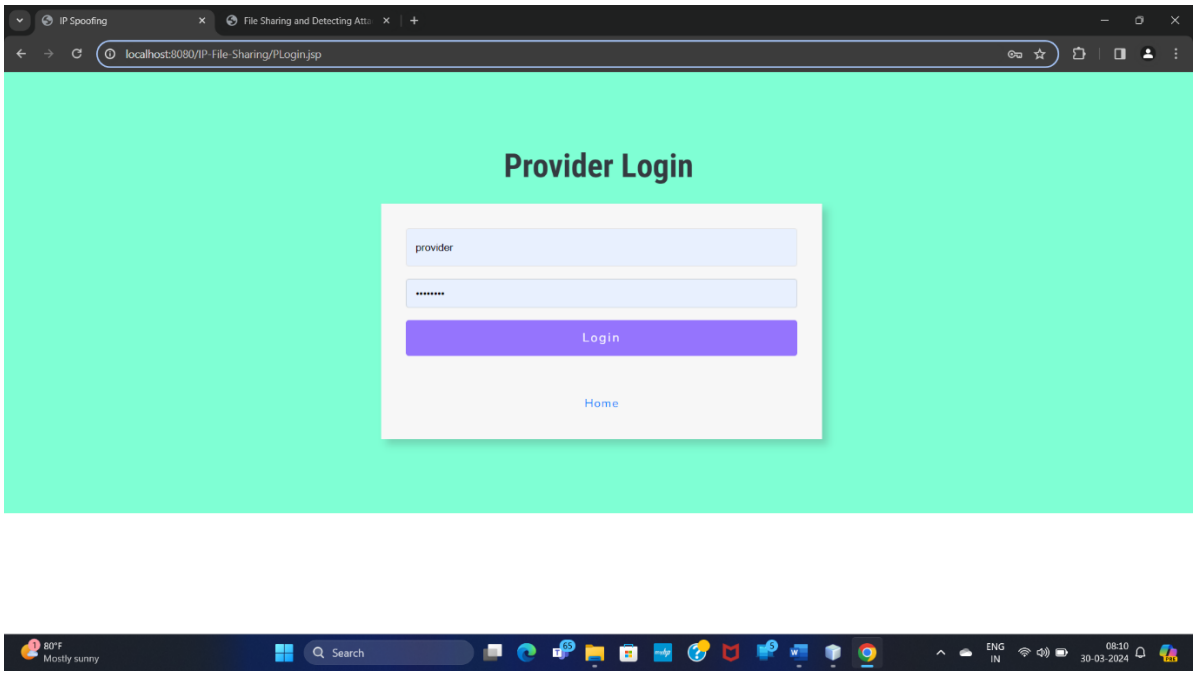

Fig 2: Provider Login Page

The Provider Login Page for the sharing the text file in secured manner to user to access the file. The file contains confidential data. So, the provider sending file was secured, third party or hackers can't steal your data.

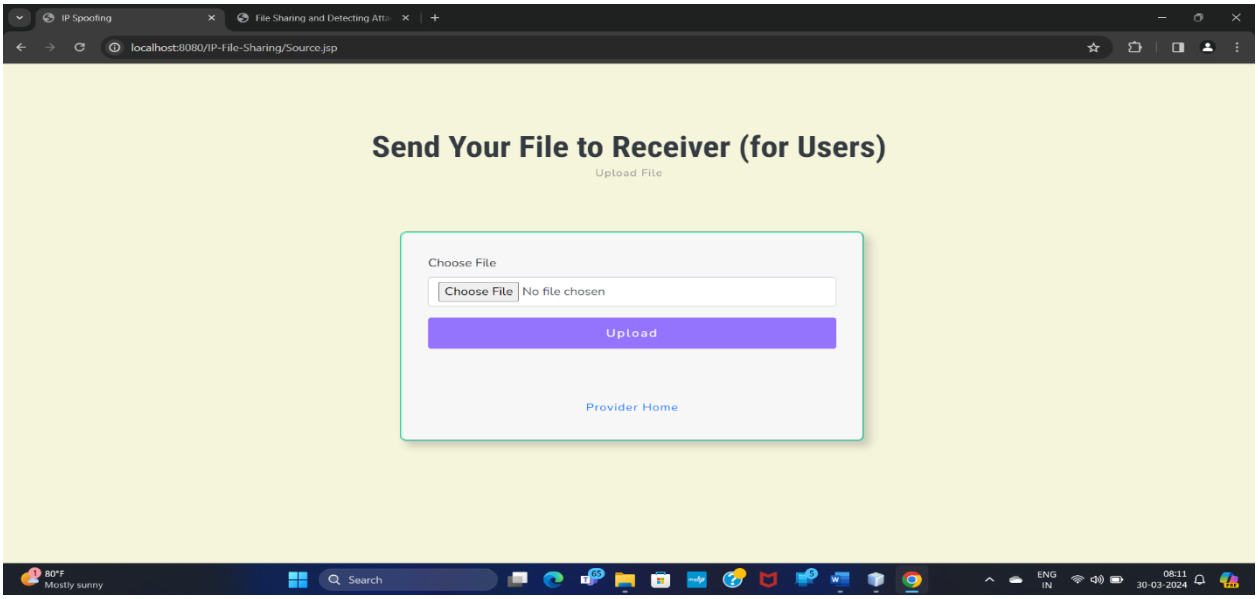

Fig 3: Upload the file

Send the text file to User End to access file with authorize. In generally authorized person only can able to access the file.

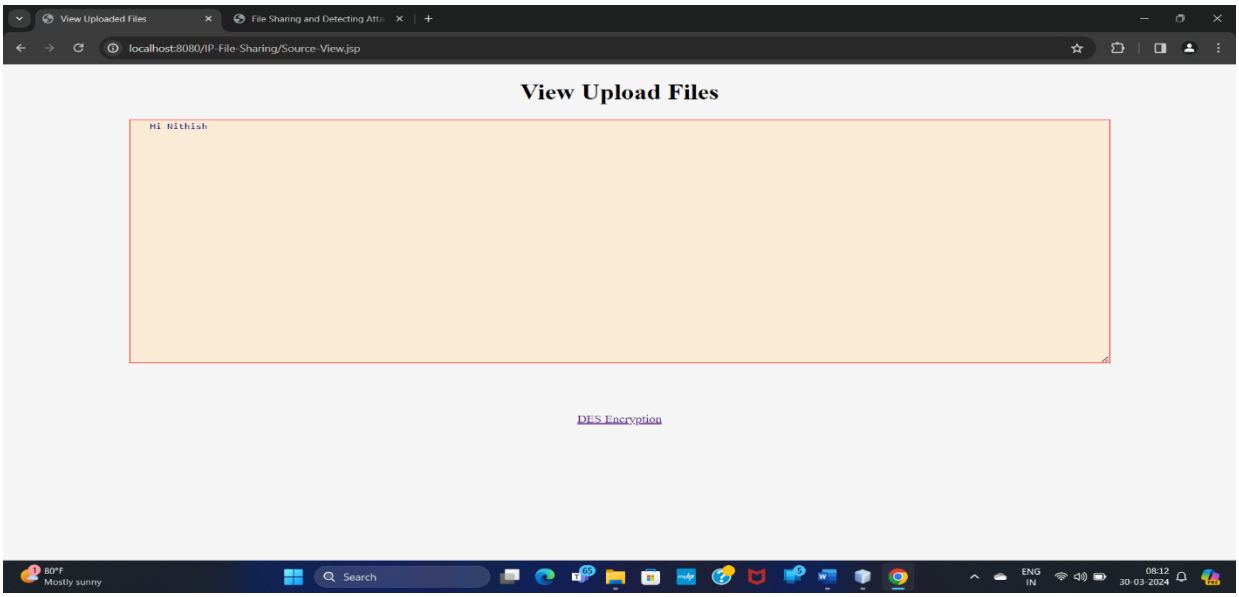

Fig 4: DES Encryption Page

Provider must send the file to user in Encrypted system, because protect our confidential data from third partied or attackers. Incase attacker try to steal your data then need 4-digit secret key to open your file.

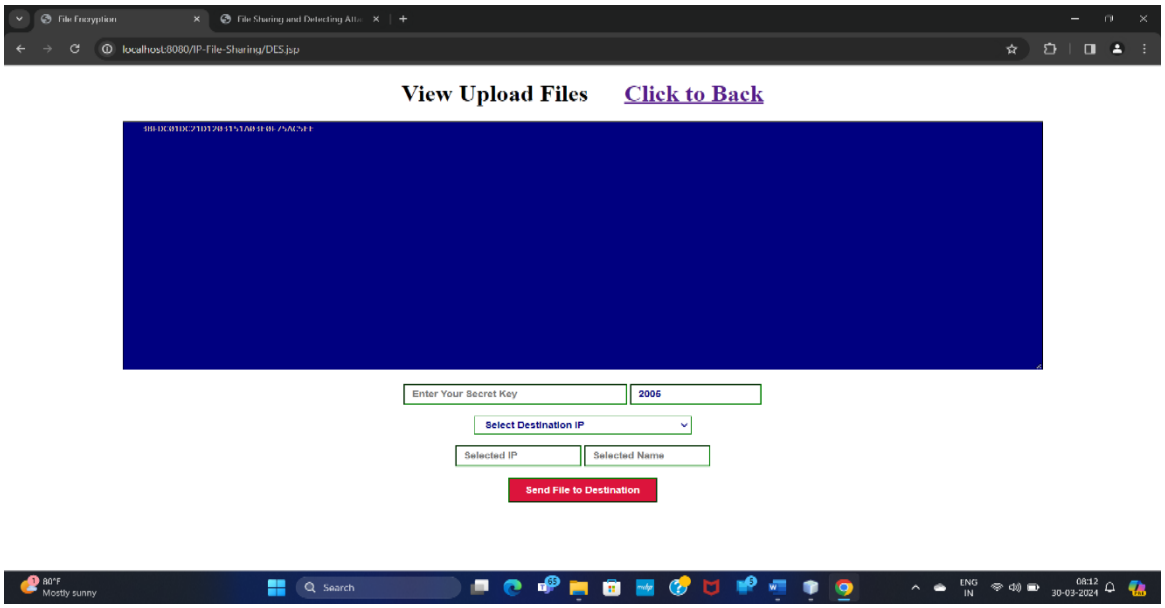

Fig 5: Send File to Destination

Send the Encrypted file with 4-digit secret key and port number and IP-Address. The 4-digit secret key is protecting your confidential data from outside third parties.

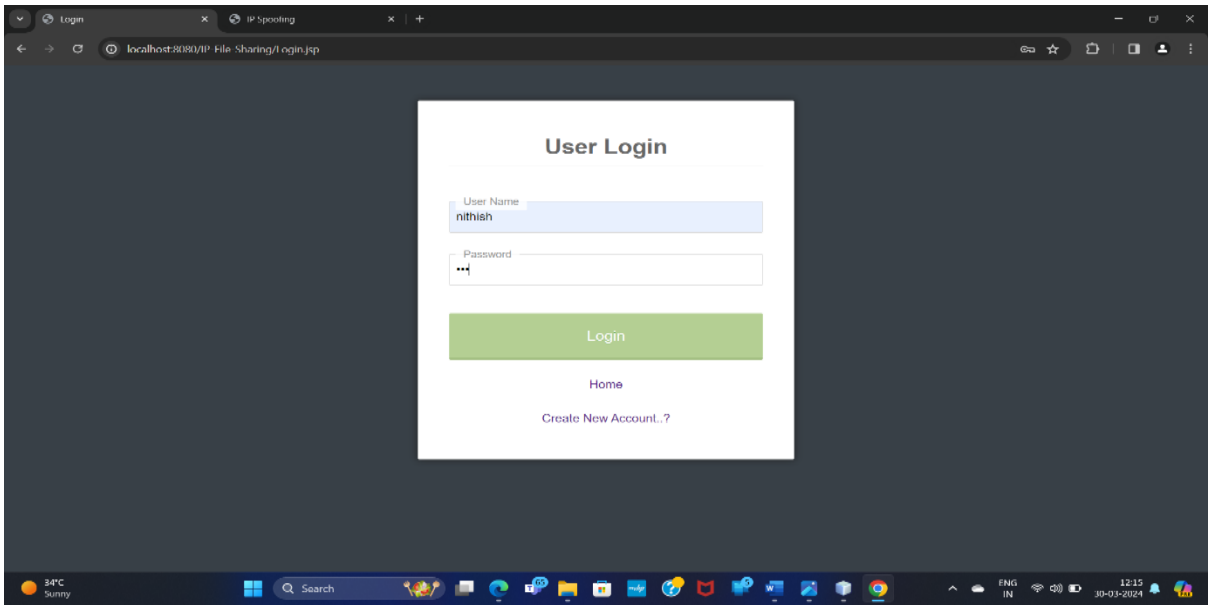

Fig 6: User Login Page

Provider once send the file to user then the user receiving the file from user end and open the IP receive file and download.

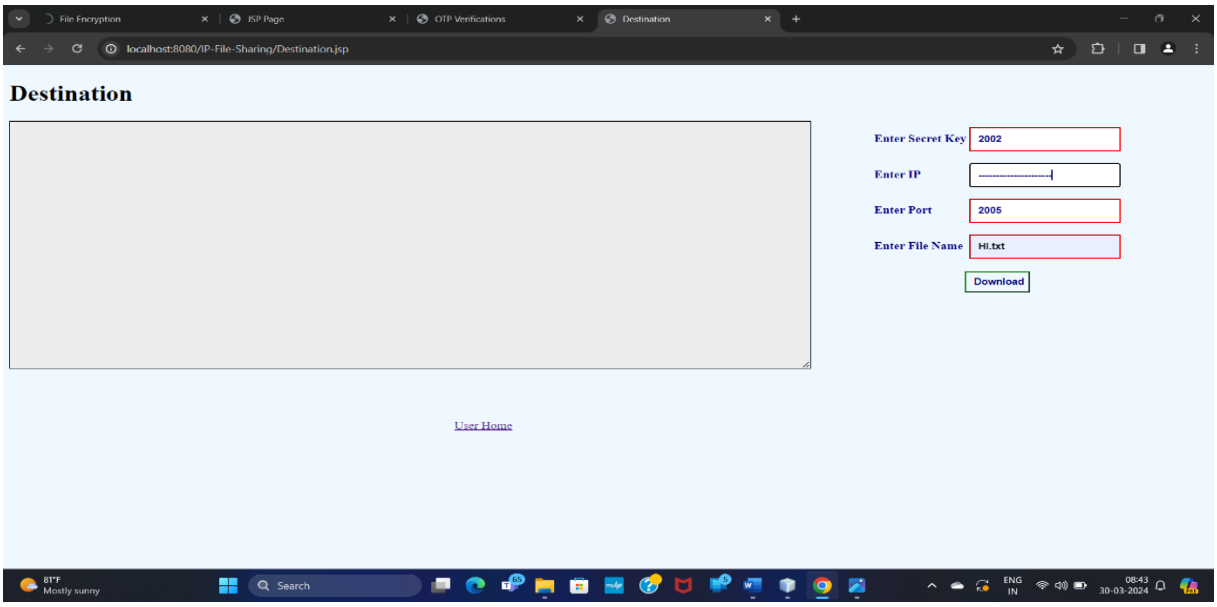

Fig 7: Receive File

When the file is sent to the user then the receiver end user should enter the correct 4-digit secret key and port number and IP-address after that only can download the file. If you enter the wrong input then automatically come out from the location and indicate this is attacker attempt. If successfully download mean's the file and is stored in File Download directory.

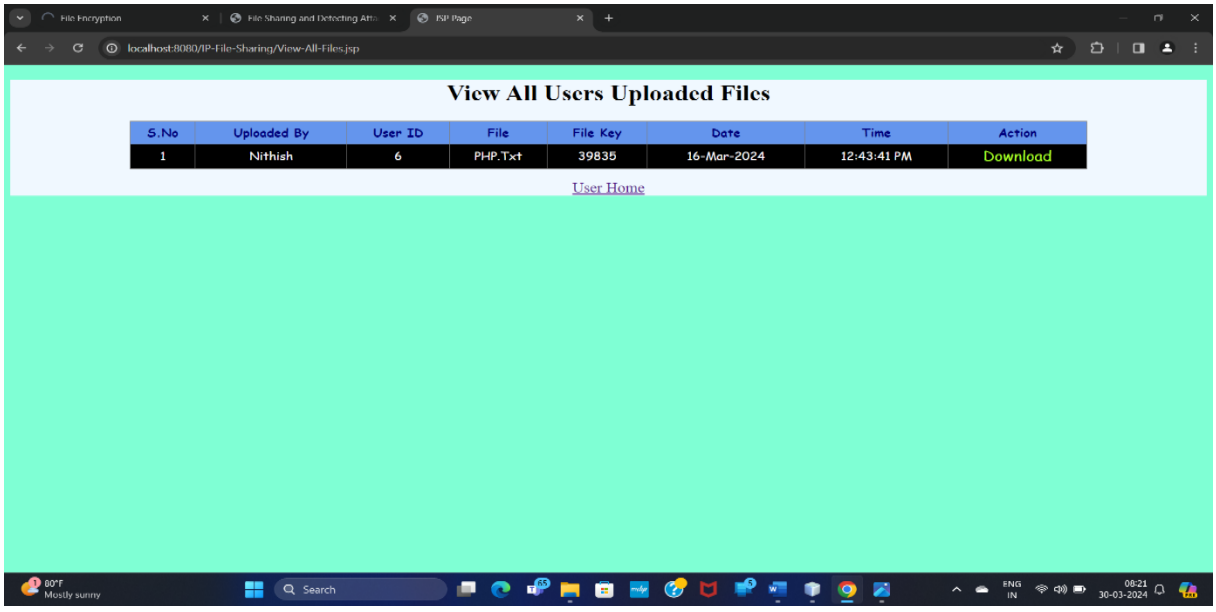

Fig 8: View All Users Uploaded Files

This is user uploaded files to other's and can view all details about shared file. If you want the file then click the download button then it will generate the OTP to user and enter the OTP then download the file and access it.

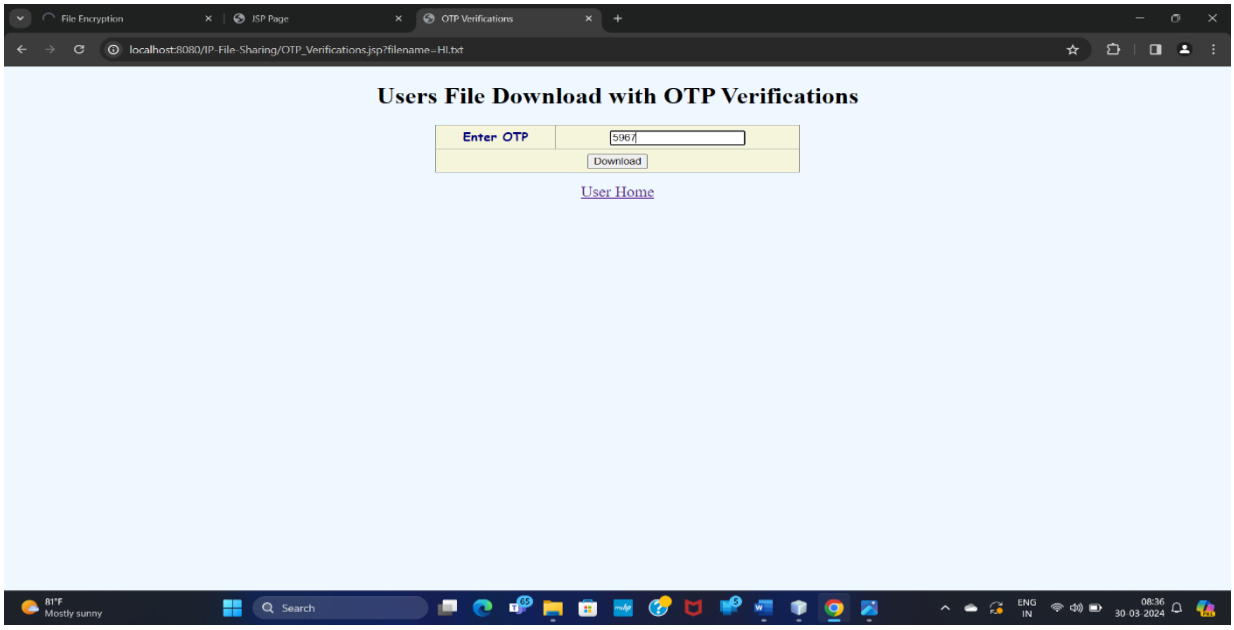

Fig 9: User File Download

If you need the user file then enter the OTP then download the user's file with user permission. This OTP is generated in user end. User only give the OTP authorization to who download the user file.

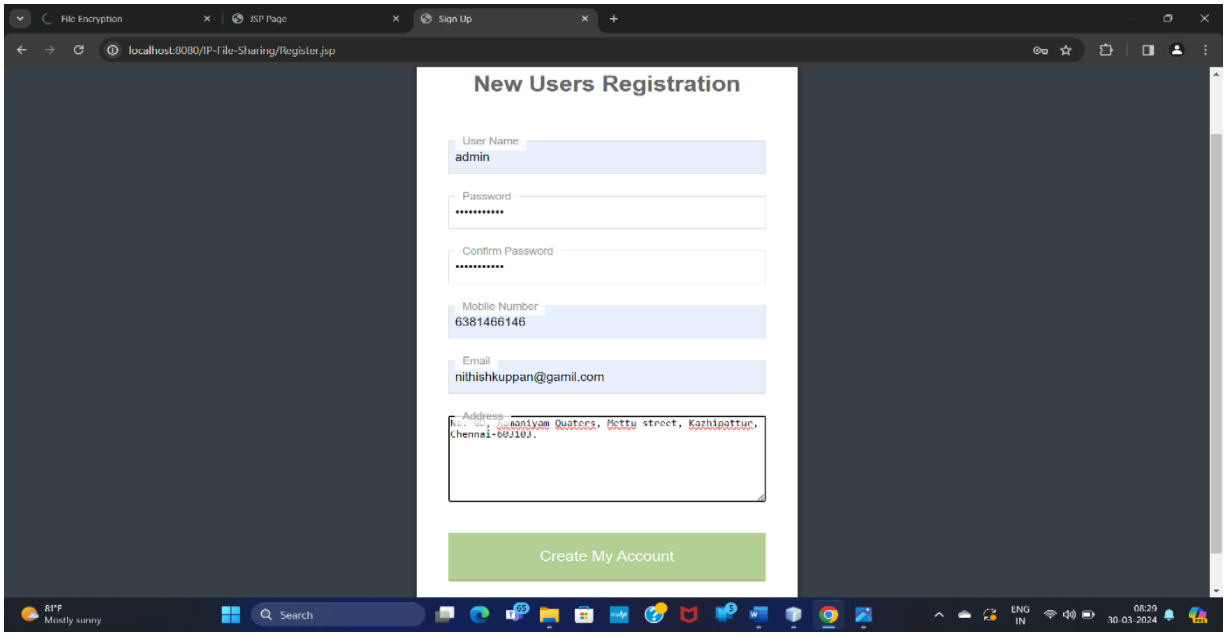

Fig 10: New Users Registration

In this user registration page enter the user details to access the file from the admin end. After creating user account it will automatically store in the admin page.

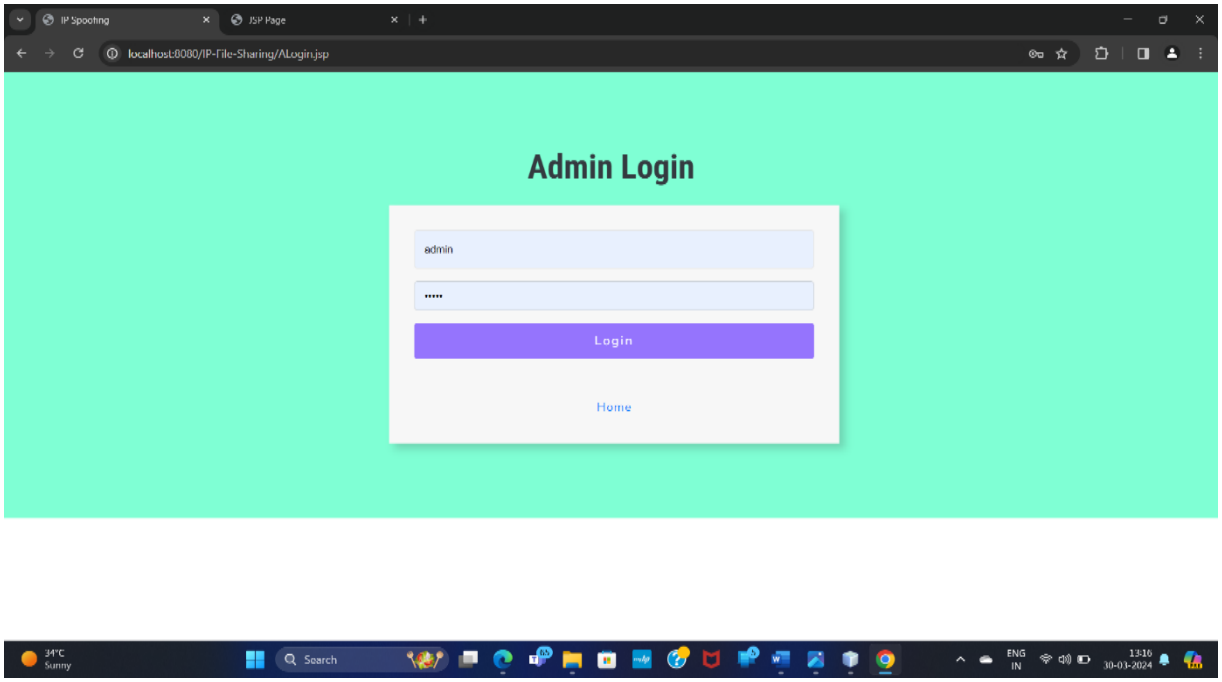

Fig 11: Admin Login Page

The Admin Login page is View the all received files from provider and view all user's status. In this admin page contain every information.

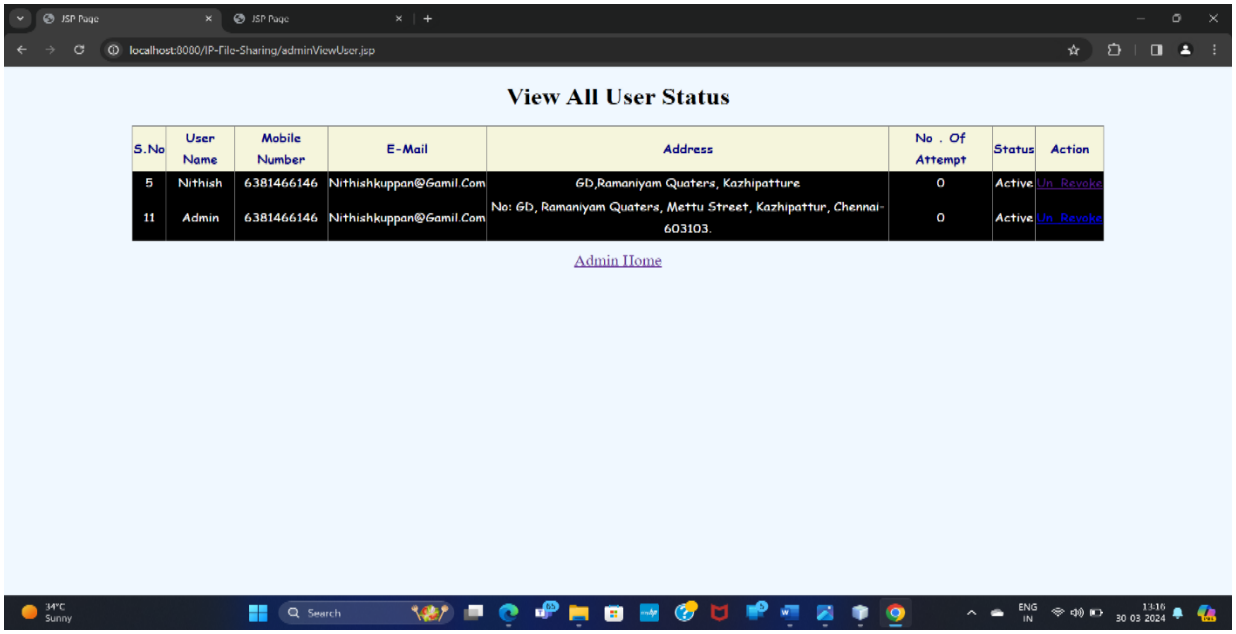

Fig 12: View All User Status

View all registered user's details in this admin page. Incase the user enter wrong password then add count in no of attempts and it will show the user is active or not.

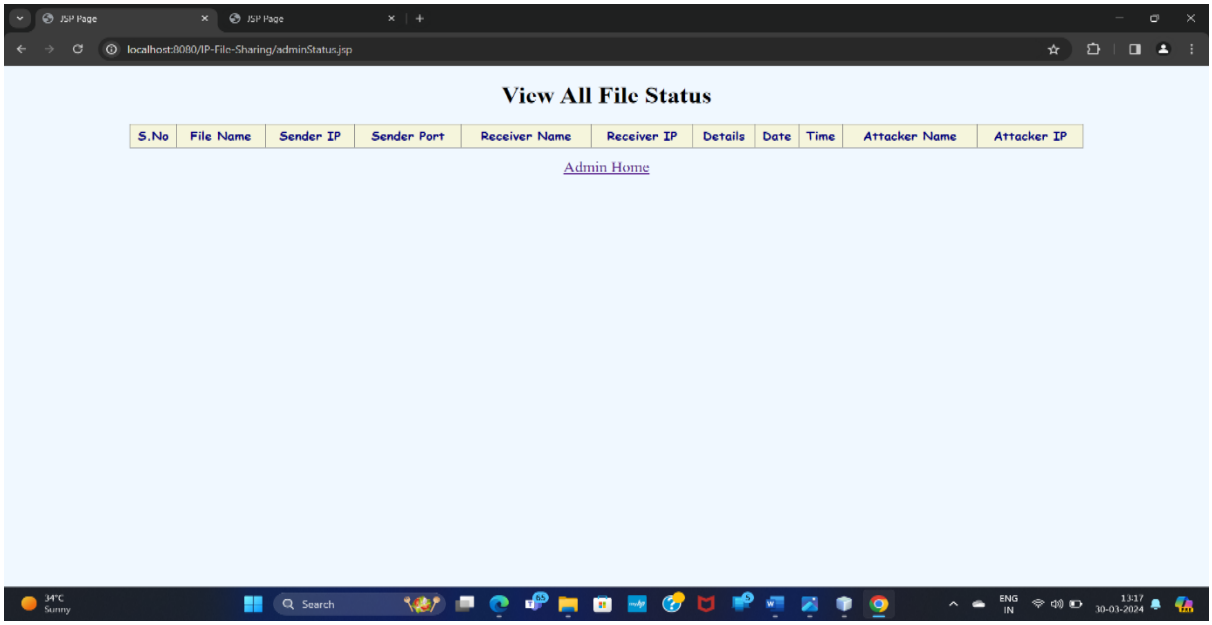

Fig 13: View All File Status

In this page can view the all received files in admin page. Complete file information is stored in admin page, can view anytime.

CONCLUSION :

Our exploration into advancing IP-based file sharing has revealed the critical importance of prioritizing both seamlessness and security in contemporary data exchange systems. The integration of robust encryption mechanisms and authentication protocols is paramount to ensure the confidentiality and integrity of shared data. By leveraging state-of-the-art cryptographic techniques and adopting a defence-in-depth approach, we can fortify IP-based file sharing systems against a wide range of security threats.

Furthermore, the pursuit of seamless data exchange entails enhancing interoperability between disparate platforms and devices. Such as the adoption of open protocols and adherence to established specifications, can facilitate seamless communication and streamline the sharing process for end-users. However, it is crucial to acknowledge the ongoing challenges and complexities associated with advancing IP-based file sharing.

In conclusion, by embracing a holistic approach that balances the imperatives of seamlessness and security,

we can unlock the full potential of IP-based file sharing for the digital age. Through collaboration, innovation, and a commitment to excellence, we can build a future where data exchange is not only efficient and reliable but also fundamentally secure.

REFERENCES :

[1] Rasseena. M. and Harikrishnan, G.R., 2014. Secure Sharing of Data over Cloud Computing the usage of Different Encryption Schemes An overview. International Journal of Computing and Technology, Volume1, (2), pp.8-11.
[2] Pearson, S., 2013. Privacy, safety and believe in cloud computing (pp. 3-42). Springer London.
[3] Chatterjee, R., Roy, S. and Scholar, U.G., 2017. Cryptography in cloud
computing: a simple technique to make certain safety in cloud. International Journal of Engineering Science, 11818.
[4] Kumar, S. and Vineeth, A., 2018. Cryptography in Cloud Computing: A Basic Approach to Ensure Security in Cloud'. International Journal of Advanced Research in Science and Engineering, vol. Volume, (7), pp.5-8.
[5] Ming, Y., He, B. and Wang, C., 2021. Efficient revocable multi-authority attribute-primarily based totally encryption for cloud storage. IEEE Access, 9, pp.42593-42603.
[6] Rashid, S. and Paul, S.P., 2013. Proposed techniques of IP spoofing detection & prevention. International Journal of Science and Research, 2(8), pp.438-444.
[7] Mukaddam, A., Elhajj, I., Kayssi, A. and Chehab, A., 2014, May. IP spoofing detection the usage of changed hop count. In 2014 IEEE twenty eighth International Conference on Advanced Information Networking and Applications (pp. 512-516). IEEE.
[8] Shiaeles, S.N. and Papadaki, M., 2015. FHSD: a stepped forward IP spoof detection technique for internet DDoS attacks. The Computer Journal, 58(4), pp.892-903.