IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Two-Factor Authentication for Secure File Transactions

Kowshikgan.K[1] Dr.V.Vaidehi[2]
1.PG Student 2. Professor
Department of Computer Applications
Dr. M.G.R Educational and Research Institute, Chennai-600095.

ABSTRACT:

This project focuses on improving the security of file transactions by implementing a two-factor authentication (2FA) system. As cybersecurity threats increase, protecting sensitive data in file traffic is paramount. Traditional authentication methods such as passwords are prone to various vulnerabilities that require an additional layer of protection. The main objective of this research is to design, implement and evaluate a customized two-factor authentication system for secure file transfer. The proposed system combines a traditional authentication factor, such as a password or PIN, with another factor that may include biometrics, one-time codes, or hardware identifiers. This two-layer approach aims to strengthen the authentication process and reduce the risks associated with unauthorized access and security breaches. The 2FA methodology involves the development of a prototype 2FA system, integration with file transaction protocols, and rigorous testing to assess its effectiveness in real-world scenarios. Evaluation metrics include information security resilience, user experience and system performance.

KEYWORDS:

AES (Advanced Encryption Standard), Secret Key ,Trustee Issued Certificate, Encryption , Two-Factor Authentication (2FA) , Access Control, Privacy protection.

I.INTRODUCTION:

A cloud service can be a virtual hosted computing system that allows businesses to buy, rent, sell, or share software and other digital resources online as an on-demand service. It does not depend on a server or multiple physically existing machines because it can be a virtual system.Cloud services have many applications such as information exchange, data management, medical information systems, etc.[1].

The benefits of web-based cloud services are enormous, including ease of accessibility, lower costs, and capital expenditures, and increased operational efficiency, scalability, flexibility, and immediate time to market. This article discusses both privacy and data security in online cloud services. Because sensitive information could also be stored in the cloud for sharing or convenient access, and qualified users can also access the cloud system for various applications and services, user identification has become an essential component of any cloud system. [2].

A more secure way is to use two-factor authentication (2FA). 2FA is used for online banking services. In addition to the username/password, the user must have a device that displays a one-time password. Some systems may require the user to have a mobile phone if the OTP is sent via text message to the mobile phone during login. By using 2FA, users can more securely use shared computers to log into online banking services. For the same reason, it is better to get a 2FA system for users of online cloud services to extend the security level of the system.[3].

The user must log in before using cloud services or accessing sensitive data stored in the cloud. There are two problems with the standard account/password-based system. First, standard account/password-based authentication does not protect privacy. However, it is well known that privacy is an important feature and must be considered in this cloud computing system. Second, it is common for a computer to be shared between different people. [4].

The login password can be changed to hack using some spyware. A recently proposed access control model called attribute-based access control may be a good candidate to solve the main problem. It not only provides anonymous authentication but also defines access control policies based on various attributes of the requester, environment, or data object. In an attribute-based access control system, each user has a user secret key issued by the authority. In practice, the user's private key is stored on a private computer. Looking at the second problem mentioned above with web-based services, it is common for computers to be shared by many users, especially in some large companies or organizations. In such cases, the user's secret keys can be easily stolen or used by an unauthorized person. Although a computer can also be locked with a password, it can still be guessed or stealthily stolen by malware.[5].

II.LITERATURE SURVEY

Jing-Chiou Liou et, al. suggested a Feasible and Cost Effective Two-Factor Authentication for Online Transactions", states that authentication is the process of verifying a user's identity when the user is requesting services from any secure IT system. By far, the most popular authentication is a basic username password password-based method that is commonly considered to be a weak technique of authentication. A more secure method is the multi-factor authentication that verifies not only the username/password pair but also requires a second or third unique physical or biological factor. However, the feasibility of multi-factor authentication is largely restricted by the deployment complexity and cost. In this paper, we propose a technique of two-factor authentication, called SofToken, that eases the deployment process and greatly reduces the cost, while maintaining the same level of security as achieved by currently available techniques .[6].

Bijeta Seth, Surjeet Dalal et, al, suggested integrated encryption technologies for secure data storage in the cloud. According to this, cloud computing has emerged as one of the most innovative technologies that have redefined the boundaries of traditional computing technologies. This has led to a paradigm shift and pushed the boundaries of how to access, deploy, and purchase computing resources, including infrastructure resources, software, and applications. The financial benefits offered by cloud services, or rather the fundamental financial change in reducing investments and turning them into operational costs, were the main motivating factor for early adopters. Despite its advantages, such as better access and better management, cloud computing has several caveats that have hindered its growth. [7].

Vijayakumar Varadarajan, Poongodi M., 2020 et al, suggested to create an authentic and ethical keyword search using decentralized (blockchain) verification. As a very attractive computing standard, cloud computing enables resource-constrained customers to easily experience efficient and flexible resources. In the prevailing systems, the traditional cloud storage system is forced to use its primitive functions in a centralized mode. This reason includes issues such as data availability, data protection, and excessive usage fees. With the improvement of blockchain generation, the decentralized system entered the public consciousness.

Compared to modern and state-of-the-art cloud storage, they are expected to be more scalable, secure, and convenient. However, the use of end point encryption in a distributed system limits search functionality, as existing searchable encryption methods are only designed for a centralized device. In addition, existing distributed cloud storage does not prevent any data user from accessing all files through them in a targeted keyword search. [8].

Zia Ullah, Basit Raza(2022) et al, suggested towards Blockchain-Based Secure Storage and Trusted Data Sharing Scheme for IoT Environment. This study offers a blockchain-based decentralized distributed storage and sharing scheme that provides end-to-end encryption and fine-grained access control. In our proposed IoTChain model, fine-grained permission is based on attribute-based access control (A-BAC) policy by employing the Ethereum blockchain as an auditable access control layer. Smart contracts are tailored for the IoTChain model, which combines the Ethereum blockchain and the interplanetary file system (IPFS). We used an advanced encryption standard (AES) for encryption and the elliptic curve Diffie-Hellman key exchange protocol for secret key sharing between data owners and users. [9].

III.PROPOSED SYSTEM

To address these two issues, this research proposes a novel approach we call dual access control. Attribute-based encryption (ABE) is one of the potential possibilities that permits the confidentiality of outsourced data and fine-grained control over the outsourced data, making it an attractive option for securing data in cloud-based storage services. Cipher text-Policy ABE (CPABE) in particular offers an efficient means of data encryption in such a manner that access rules, defining the access privilege of prospective data receivers, may be specified over encrypted data. It is important to note that in this research, we take into account the possibility We're implementing two-factor authentication for the data in this project, as well as private key generation for each file (each file has a unique secret key), so no one can access the information without it.

ARCHITECTURE DIAGRAM

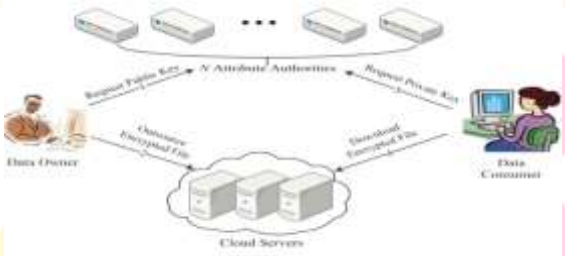

Fig 1: Proposed system architecture

Fig. 1 demonstrates the architecture of the proposed system, which explains how securely we can transfer the file through the cloud with a two-factor authentication technique. As soon as the data owner logins with their credentials, the server verifies the entered credentials against stored data. Before transferring data, the owner requests a public key to secure their data from unauthorized access by encrypting the file, which will be stored on the cloud server after encryption. Later, when the consumer receives the data, they request the authorities for a private key and then download the encrypted file from the cloud server. This setup enhances the security of file transactions through the implementation of a two-factor authentication system.

Module Description:

This Project has four types of modules they area as follows,

1. **CLOUD SERVER**
2. **DATA OWNER**
3. **TPA**
4. **USER**

CLOUD SERVER:

- Login
- View owners
- View users
- View integrity key request

Clouds are used for storage purposes. Cloud should login first by providing a username and password. The cloud can view all data owners and user files. The cloud is responsible for viewing key requests from the TPA. Cloud used to send the secret key to TPA's mail ID.

DATA OWNER:

- Register
- Login
- Upload file
- Send auditing request
- View user file request

The data owner needs to register before logging in. After registration, he or she will login with the username and password. The owner will upload the file into the cloud with the primary key and the integrity key (secret key). To check the integrity of the data, the owner will send an audit request to the TPA.

TPA:

Third-party auditors first login by providing a username and password. After logging in, TPA views all files uploaded by the data owner. And View the data owner's auditing request for the file. TPA has only the primary key, but he needs a secret key to audit the file, so he will send a request to the cloud server. After getting the secret key through mail from the cloud, TPA then audits the file. The result will be sent to the data owner's email address.

USER:

- Register
- Login

- View all files
- Download file from email

The user needs to register with the relevant details. And then login by using the username and password. After logging in, the user can view all files uploaded by the data owner. If the user wants that file, he will make a request to the data owner. If the request is accepted by the data owner, the user can download the file from his or her email. Because the file has been sent to the user's email address.

IV.RESULT AND DISCUSSION

1. Home Page

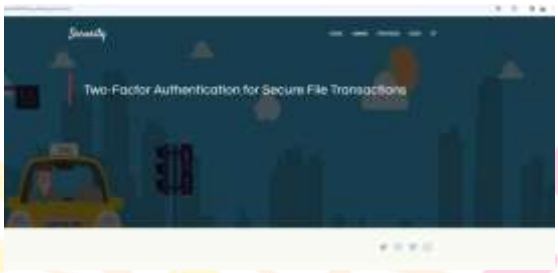

Figure 1: Home Page

In figure 1, it includes the admin, provider, and user login pages.

2. Admin Login Page

Figure 2: Admin Login Form

Figure 2 demonstrates the admin login form, which manages the authentication process. This involves validating the provided credentials, such as a username and password, against stored user data.

3. Admin Home page

Figure 3: Admin Home Page

Figure 3 demonstrates the admin home page, which manages access control for the login of users, providers, and user requests of files. This page also manages the stored dataset information of users and providers.

4.View Request Page

Figure 4: View Request Page

Figure 4 demonstrates the view of the request page. The user-requested dataset can be viewed on this page, which includes information regarding the provider name, user name, email, file key, file name, and request date.

5. Provider Register Page

Figure 5 : Provider Register Page

Figure 5 demonstrates the provider register page. The Registration Module holds all the information related to registration. It is the provider's login gate for signing in.

6. Provide Home Page

Figure 6 : Provider Home Page

Figure 6 demonstrates the provider home page which manages access to uploaded files and view of all files .

7.File Upload Page

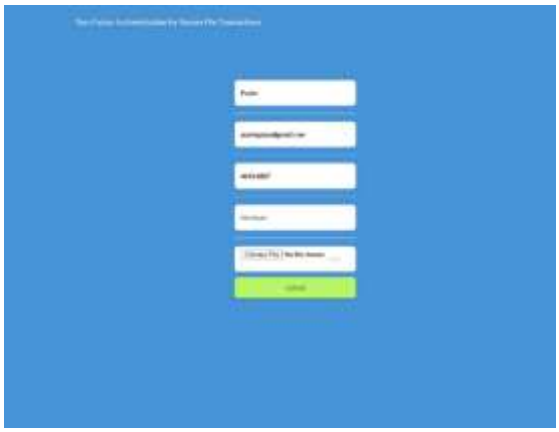

Figure 7: File Upload Page

Figure 7 demonstrates the file upload page, which allows providers to upload files with an attribute key for users to find files.

8.View All Files

Figure 8: View All Files

Figure 8 demonstrates the view of all files. which display all uploaded files of the provider with information regarding the file name, file key, and email.

9. User Home Page

Figure 9: User Home Page

Figure 9 demonstrates the user home page. This page helps the user search for a file with an attribute key and request the file from the admin for access and download.

10.Download Page Result

Figure 10: Download Page Result

Figure 10 demonstrates the download page, which displays all download files with their information.

Conclusion:

We have introduced a new 2FA access control solution for web-based cloud computing services in this work, which includes both a user secret key and a lightweight security device. The suggested 2FA access control method has been determined to not only allow the cloud server to restrict access to those users with the same set of attributes but also to protect user privacy based on the attribute-based access control mechanism. The suggested 2FA access control solution satisfies the required security standards, according to a thorough security study. Through performance evaluation, we proved that the building is "feasible." Future work will need to be done to further increase efficiency while preserving all of the system's wonderful features.

V.References:

[1] Nenghai Yu and Peilin Hong, "TAFC: Time and Attribute Factors Combined Access Control for TimeSensitive Data in Public Cloud" IEEE Transactions on Services Computing available online,2017.

[2] H. Tian, Y. Chen, C.-C. Chang, H. Jiang, Y. Huang. Chen, and J. Liu, "Dynamic-hash-table based public auditing for secure cloud storage," IEEE Transactions on Services Computing, Available online, 2016.

[3] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward secure and dependable storage services in cloud computing," IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220–232, 2012.

[4] K. Yuan, Z. Liu, C. Jia, J. Yang, and S. Lv, "Public key timed-release searchable encryption," in Proceedings of the 2013 Fourth International Emerging Intelligent Data and Web Technologies (EIDWT '13), pp. 241–248, IEEE, 2013.

[5] R. L. Rivest, A. Shamir, and D. A. Wagner, "Time lock puzzles and timed release crypto," tech. rep., Massachusetts Institute of Technology, 1996.

[6] J. Li, W. Yao, Y. Zhang, and H. Qian, "Flexible and fine-grained attribute-based data storage in cloud computing," IEEE Transactions on Services Computing, Available online, 2016.

[7] Z. Qin, H. Xiang, S. Wu, and J. Batamuliza, "A survey of proxy re-encryption for secure data sharing in cloud computing" IEEE Transactions on Services Computing, Available online, 2016.

[8] F. Arm Knecht, J.-M. Bohle, G. O. Karame, and F. Youssef, "Transparent data deduplication in the cloud," in Proceedings of the 22nd.

[9] ACM SIGSAC Conference on Computer and Communications Security, pp. 886–900, ACM, 2015. R.Masood, M. A. Shibli, Y. Ghazi, A. Kanwal, and A. Ali, "Cloud authorization: exploring techniques and approach towards effective access control framework," Frontiers of Computer Science, vol. 9, no. 2, pp.297–321, 2015.