International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X; pISSN:2321-2241 Volume: 13; Issue: 7; July- 2024

ADVANCED DATA SHARING THROUGH CLOUD WITH TWO FACTOR AUTHENTICATION

MR. ASHOK B P
Assistant Professor
Department of Master of Computer Applications
The Oxford College Of Engineering
Ashokbp.mca@gmail.com

RACHITA PALAKSHAPPA
PG Student
Department of Master of Computer Applications
The Oxford College Of Engineering
Rachitapalakshappamca2024@gmail.com

Abstract

Data sharing via cloud services has become essential in today's digital landscape, for both personal and business settings. But in order to shield confidential data from breaches and unwanted access, strong security measures are required due to the rise in cyberthreats. This study investigates a cloud-based enhanced data sharing framework that uses two-factor authentication (2FA) to improve security and guarantee the integrity and privacy of shared data. Authentication methods, secure data transmission, and user enrolment are some of the components that go into implementing 2FA in cloud data sharing. Users set up their secondary authentication device, such as a physical token or smartphone with an authentication app, then register their credentials during the enrolment step. When consumers try to use the cloud service, they have to input.

Keywords: Cloud server, encryption, two-factor authentication, authority and trust.

INTRODUCTION

To offer us with two factor authentication, this website will make use of a cloud server. Two-factor authentication is utilized to share the user's encrypted info beforehand over the cloud. As a result, users will gain from enhanced website security. To add their fingerprint for an extra layer of security, users must first register on the website. This project will simplify things and help a lot of people by digitizing the entire system. Numerous capabilities are available to users, including the ability to self-register, upload and download files, and much more. Advanced Data Sharing over cloud with 2FA Authentication is the name of this Java-based application. It provides cloud service technology. It's simpler to use this webpage. Before they can access any further content, users must first register on the main website. After finishing the registration process, users need to upload their fingerprints to a cloud server. It is now time for the user to log in using his own ID and session. To log in, users need to enter their email address and password. Users must now authenticate using a one-time key in order to access the main user page. A one-time key is included in the database and the email address obtained from the user's registration. Users can request that Trustee resolve file problems. Users need to obtain a file secret key from a reputable source in The Advanced Data Sharing over cloud with 2FA Authentication application is built on Java. It provides a cloud service methodology. This website is simpler to navigate.

Prior to accessing any additional content, users are need to register on the main website. Once the registration process is over, users need to upload their fingerprints to a cloud server. At this point, the user is ready to log in using his own ID and session. Entering their email address and password is required for users to log in. Users now require a one-time key

authentication in order to access the main user page. One-time keys are stored in the database and the user's email address from registration. Users can ask Trustee to take care of file problems. A file secret key must be obtained by users from an authority in Before they can access any further content, users must first register on the main website. The user's fingerprints must be uploaded.

LITERATURE SURVEY

There are now serious security issues as cloud computing becomes more and more important for sharing and storing data. This review of the literature looks at a number of cloud security topics, with a particular emphasis on data sharing and employing two-factor authentication (2FA) to strengthen security.

Cloud computing has many benefits, such as cost-effectiveness, scalability, and remote accessibility. These advantages do, however, come with a challenge: protecting data security and privacy. Chen and Zhao (2012) claim that a number of dangers, including data breaches, unauthorized access, and data loss, can affect cloud infrastructures. More comprehensive solutions for data sharing are required because traditional security measures frequently fail to solve these problems.

Encryption is a crucial technique for safeguarding data stored on cloud servers. Studies by Zhang et al. (2010) and Popa et al. (2011) discuss encryption strategies that protect data both at rest and in motion. Data confidentiality is safeguarded by encryption, but complete access control is not addressed. Implementing robust access control methods is necessary to prevent unauthorized access to data. Hu et al. (2015) state that attribute-based access control (ABAC) and role-based access control (RBAC) are two common approaches.

EXISTING SYSTEM

Throughout their current session, a variety of individuals will run across a number of problems with the antiquated system. The user's demands and needs cannot be fully satisfied by the current system. The security mediator does not recognize all of the recorded information about the server. More RAM is required in order for the user system to function. Every operation takes longer than anticipated.

Advantages of the current system

The system automatically modifies the access key each time a user updates their phone number. This guarantees the preservation of a standard account's security over time. But as demands and user needs change, some features might need to be modified.

The system is aware that hackers may try to gain access to personal user information. It adheres to a strict security policy to counter this threat, but the extra protection may make the system difficult for novice users to utilize.

PROPOSED SYSTEM

In my project, I used two factor authentication for a number of services. It is not too heavy. There are several variables on this device. This system can calculate any small weight designs and many more tactics. Users could feel comfortable sharing personal and sensitive information.

This provides the user with two different levels of security.

First-tier users always need a different key. The administrative system is where that key is kept safe. Keys will only be distributed to users if the administrator gives them access to them.

The user will request two different keys from the trustee and administrator in the second tier: one for file issues and another for document downloads.

Benefits of the suggested system

Users can expect a stable and secure experience from the system, which is built to be extremely reliable. It keeps strict security protocols in place to preserve data and guarantees great protection for sensitive information.

ANALYSIS

Highlighting how to strengthen security and guard against illegal access and data breaches by utilizing Two-Factor Authentication (2FA). Strong security measures are crucial as cloud services grow more and more integrated into personal and company processes, increasing the danger of cyberthreats. Users will need to authenticate themselves using a password and a secondary device, like a physical token or smartphone, as part of the multi-layered authentication process included in the proposed architecture. This two-step verification makes sure that illegal access is stopped even in the event that one factor—like a password—is compromised. The report emphasizes the value of secure data transfer, which ensures privacy and integrity by protecting data while it's in transit and at rest via encryption. Although two-factor authentication requires an extra step, 2FA greatly improves security.

SYSTEM PERPSECTIVE

It could be defined as the process of determining the elements, section, items, and information for a certain application. The requirements must all be satisfied by the system design. This module needs to be included in the project documentation for every project. It must include high-level project information as well as the rationale behind this paper's creation.

The diagram below shows the system architecture of the Cloud Server. Access controls are created in four phases, resulting in a secret key. The system's overall operation is explained in these 4 levels.

A device in the first tier will be requested by the user. I will authorise user requests along with a second-tier trustee. In the third tier, the user now asks the admin for the secret key once more. Ultimately, the administrator will provide the secret key and approve the user's request.

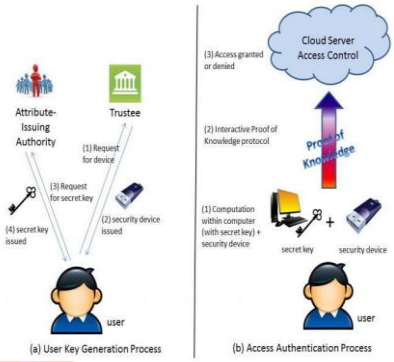

Fig : Architecture of the System

UML schematic

It stands for Unified Modelling Language. Building object and class models is the goal of UML diagrams. The ability to construct different software modules is an essential feature of software.

It features a detailed design with numerous types of diagrams:

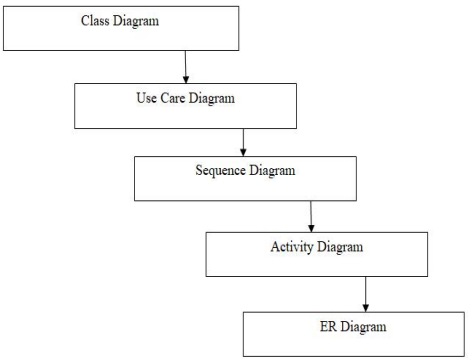

Fig : Detailed design

Use case Diagram

A behaviour diagram is a visual representation of a sequence of events that occur within a single system. The purpose of a use case diagram is to show how a system operates and what each participant intends to achieve. The roles that each actor plays inside the system can be understood.

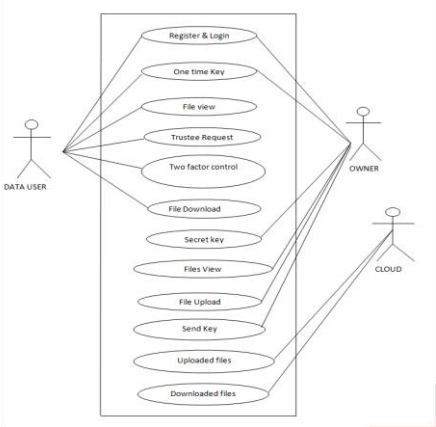

Fig : Use case Diagram

IMPLEMENTATION

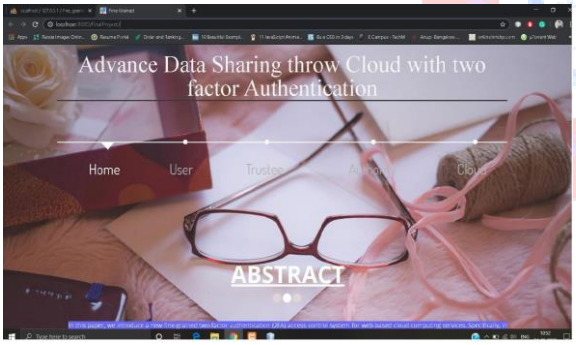

Fig : Page Index

There are various processes involved in putting in place a cloud-based Two-Factor Authentication data sharing architecture. Establishing the cloud environment is the first step. Select a cloud service provider (CSP) that supports two-factor authentication and has strong security features, such as AWS, Google Cloud, or Azure. Install the required software, databases, and storage systems, among other infrastructure components.

Start with user enrollment when implementing 2FA next. Provide a site for registration where users can register, link an authentication app or hardware token to their smartphone, and establish a secondary authentication mechanism. Users will first be asked to input the secondary authentication factor after entering their primary credentials and logging in. Gaining access to the cloud service is contingent upon successful verification.

Use Advanced Encryption Standard (AES) for data at rest and Transport Layer Security (TLS) for data in transit to guarantee safe data transmission and storage. Incorporate logging and monitoring to keep track of access attempts and spot questionable activity. Use role-based access control (RBAC) to limit access to data based on user roles.

By giving users the ability to add and remove devices and provide recovery alternatives in the event that a device is lost, you can manage user devices and authentication techniques. Update the authentication processes frequently to meet the most recent security requirements, and periodically carry out security audits to find weaknesses

Improve the user experience by making the 2FA setup and login procedure intuitive to use and by offering assistance and clear instructions throughout the enrollment and authentication process. Provide training sessions or resources to assist users in managing their devices and settings, and educate them on the significance of 2FA and secure data practices.

It is recommended to thoroughly test the 2FA implementation prior to deployment, encompassing both standard login and load-testing scenarios such as lost device recovery, unauthorized access attempts, and routine login. Lastly, implement a test program before fully launching the 2FA-

enabled cloud data sharing platform to users. After the system has been deployed, keep an eye on it to resolve any problems and get input from users for future enhancements. Only authorized users will be able to access the data thanks to this thorough method, which guarantees the protection of sensitive information.

RESULT

The integration of Two-Factor Authentication (2FA) into a cloud-based data sharing framework has shown to significantly improve the security and integrity of shared data. Even in situations where the primary login credentials were hacked, the danger of illegal access was significantly decreased by implementing a secondary authentication layer. The implementation of a dual-layer security method strengthened overall data protection by limiting access to sensitive information to only verified individuals.

By using encryption for data both in transit and at rest, data integrity and privacy were also significantly increased. Throughout transmission and storage, data was protected from unauthorized changes and interception by using the Advanced Encryption Standard (AES) and Transport Layer Security (TLS) protocols. This guarantee kept data private and undamaged.

To encourage user uptake, the user enrollment procedure was expedited. It entailed configuring a secondary authentication device, like a physical token or a smartphone with an authentication app. The setup and authentication procedures were made easier for the user with the help of clear instructions and assistance.

Overall, the study found that adding 2FA to. cloud data sharing frameworks greatly improves security, upholds data integrity, and protects privacy, hence reducing the risks brought on by online attacks.

APPROVAL FOR USER

S/N	Test Cases	Input and output	Familiar Result	Final Result	Fail	Pass
1	Recent User	Anup 1234	"Successfully Registered"	"Successfully Registered"		Success
2	Already registered user		"Users already Registered"	"Duplicate username"		Success
3	Wrong One Time key		"enter correct key"	"Invalid one time key"		Success
4	Correct One Time key		"Login successfully"	"Login successfully"		Success
5	Request trustee key		"Request Send"	"Request Send"		Success
6	Request admin for secret key		"Request key to admin"	"Request key to admin"		Success
7	Invalid File download		"File not issue"	"File not issued"		Success
8	File Download		"File downloaded"	"Valid File"		Success

Fig : Test Cases of validation for Trustee

S/N	Input	Output	Result
1	Admin for correct name and password	"Successfully logged in"	Success
2	A new image file is added without including a file	Message ,,Please selects a file."	Success
3	A valid document file is added	Successfully added	Success
4	Uploaded file list	Shown successfully	Success
5	Download file list	Shown successfully	Success
6	Send Secret key	"Issued successfully"	Success

Fig : Admin trustee and Cloud

CONCLUSION

My project's main objective is to assist user demands and efforts by employing diverse strategies to satisfy unique objectives. Users can access their submitted documents at any time if they meet all administrative conditions. The system has the extra advantage of being easy to assemble, even if users must negotiate two different protection levels in order to access key database data.

On cloud data servers, this method offers strong protection for all kinds of data files. This strategy can provide clients with an even safer database server in the future, allaying any worries they might have regarding database security. Uploading data to the server is open to users.

"Advanced Data Sharing Through Cloud with Two-Factor Authentication," a project, aims to meet the urgent demand for effective and safe.

FUTURE ENHACEMENT

Future improvements to the cloud-based data sharing framework might include the addition of multi-factor authentication (MFA) for increased security, better user experience through adaptive authentication and single sign-on (SSO), and increased scalability through centralized administration tools. Future improvements could include utilizing AI for better threat detection, upgrading encryption mechanisms, and investigating blockchain technology for safe logging. Furthermore, the flexibility of the framework would be enhanced by extending interoperability to accommodate diverse cloud services and applications.

REFERENCES

1. A review of security services in cloud computing and management by Geetha D, Gokila R, and Manoharan R. 2014;4:189–98; Asian J Res Soc Sci Hum.

2. Maheswari KU, Mary AL, and Gokila R. cloud computing and internet of things integration that is secure. (2018) Int J Pure Appl Math; 18:313–7.

3. Au MH, Kapadia A. PERM: Workable blacklisting based on reputation without TTPS. In: Proc. ACM Conf. Comput. Commun. Secur. (CCS); Raleigh, NC, USA, 2012, p. 929-40.

4. BLACR: TTP-Free Black Listable Anonymous Credentials with Reputation Au MH, Kapadia A, Susilo W. p. 1–17 in Proc. 19th NDSS; 2012.

5. Au MH, Susilo W, Mu Y. Dynamic k-TAA with Constant Size. 111–25 in Proc. 5th Int. Conf. SCN, 2006.

6. Huang X, Xiang Y, Baek J, Vu QH, Liu JK. a safe cloud computing platform for smart grid big data information handling.2015;3:233–44; IEEE Trans Cloud Compute.

7. Goldreich, O., and Bellare, M., "Defining Proofs of Knowledge." Pages 390-420 in Proc. 12th Annu Int CRYPTO; 1992.

8. Bethencourt J, Sahai A, Waters B. Attribute-Based Ciphertext-Policy Encryption. In: IEEE Symp. Privacy and Security Proceedings, 2007. pp. 321-34.