A Survey on
Private Cloud Storage Security using Multifactor Authentication

Prof. D. H. Patil
Department of Information Technology
Rajarshi Shahu College of Engineering,
Tathawade,Pune, India.
patil.dipali07@gmail.com

Varsha Sanjay Asbe
Department of Information Technology
Rajarshi Shahu College of Engineering,
Tathawade,Pune, India
varsha.asbe26@gmail.com

Mahima Shubhakar Chavan
Department of Information Technology
Rajarshi Shahu College of Engineering,
Tathawade,Pune, India.
mschavan97@gmail.com

Pooja Laxman Birajdar
Department of Information Technology
Rajarshi Shahu College of Engineering,
Tathawade,Pune, India.
poojabirajdar276@gmail.com

Gauri Ashok Joshi
Department of Information Technology
Rajarshi Shahu College of Engineering,
Tathawade,Pune, India.
gaurijoshi41212@gmail.com

***ABSTRACT*- Many organizations prefer to use the private cloud to store the organization data.. Even though private cloud is considered to be more secure than public cloud, there are security risks associated with it. The issues such as confidentiality and integrity are needed to be taken care of, and should not be overlooked in case of private cloud. This paper proposes a solution to the security problem by using Multi-factor authentication (MFA) where, data confidentiality is achieved using CP-ABE (Cipher text Policy-Attribute based Encryption) and integrity is ensured i.e. the data is safeguarded from unauthorized user modification with two levels. The first level would involve static username and password and the second level would involve a QR code based OTP.**

KEYWORDS-Confidentiality, OTP, CP-ABE, MFA, Availability, Private Cloud.

I. INTRODUCTION

Private clouds are preferred by organizations who want security, data privacy as top priority. Private clouds are used in areas like banks, financial institutions and government organizations so that only authorized users can get access to the system. Private clouds offer high level data security. Private clouds are usually deployed inside company’s firewall and hence provide a very good performance. The hardware and other resources can be customized easily by the organization.

a. Types of private cloud:

A. On-premise Cloud-

It is also called as internal cloud, which is hosted in the organization's own offices and data centers. This cloud is managed by the IT department of the organization itself. It is usually preferred by very huge organizations as they have their own qualified staff for cloud management.

B. Hosted private cloud-

This cloud is hosted by third party service providers. The support and management is provided by the third party service providers. It is usually preferred by organizations who don't have their own qualified employees for cloud management. [2]

The content of this paper is as follows: Section II contains a brief survey of the different factors used in Multi factor Authentication different OTPs used. Section III contains the proposed over as solution over the existing ones. Section IV contains a the advantages of the proposed system and Section V contains the limitations. Section VI contains the summarization and future work for the system.

II. LITERATURE SURVEY

In private clouds, many times the security is compromised as there is controlled access. This leads to security issues like data confidentiality and integrity. This can be solved by using CP-ABE for data security.

User authentication can be achieved by using static username and password. But static password is the least secure one (though mostly used), as it can be easily brute forced by malicious users. It can be easily attacked as users many times use same passwords or same patterns of passwords for different systems. Many times users use weak passwords as strong ones are difficult to remember. Even if they use some strong passwords they note it down somewhere which can be easily hacked. To overcome these issues the multi factor authentication was a solution. In multi factor authentication two or more independent user credentials are combined: what the user knows (a password), what the user has (security token) and what the user is(biometric identity).

The most common MFA scenarios are-

1) Swiping a card and entering a PIN.

2) Logging in with a static username and password followed by an additional OTP (one time password) which is forwarded to the user via an email or SMS.

The various authentication factors used are-

Knowledge factors-Information that the user has i.e. IDs, passwords, PINS etc.

Possession factors-anything a user possesses in order to log in with a security token, a one-time password (OTP) token, employee id card or SIM card.

Inherence factors-The biometric authentication such as retina scans, iris, finger prints, face recognization, voice recognization etc.

Location Factors-Users current location is often suggested as a fourth factor for authentication. Users typically carry their smartphones which have a GPS device, enabling reasonable surety confirmation of the login location.

Time Factors-Current time is also sometimes considered as a fourth factor for authentication.[9]

In private cloud, user authentication is achieved by using static username or password or multi factor authentication is used in which user login is done by static username or password and then an OTP is sent to the user via SMS or email.

One time password (OTP) is automatically generated. It consists of numeric or alphanumeric string of characters that authenticates the user for a single bank transaction or a single login session.[11]

It is only valid for a specific amount of time, usually for 30 or 60 seconds. OTP is more secured than static passwords as most of the times the user's password is weak .These OTPs are mostly forwarded via SMS or email by the authentication server. But nowadays this SMS OTPs are not that much secured unfortunately.

There are two reasons for it. Firstly, the security of SMS OTPs relies on the confidentiality of SMS messages that heavily relies on security of the cellular networks. The several attacks against GSM and even 3G networks have shown that confidentiality for SMS messages is not necessarily provided. The second reason is that the criminals have adjusted and created specialized mobile Trojans since they are widely used by service providers.[13]

The alternative for SMS based OTP would be using one-time QR codes. The one time QR codes are more reliable, practical and effective to use. Most of the OTPs are numeric/alphanumeric and of static length(between 6 and 12 characters).If a system generates eight digit numbers as OTPs, the total number of combinations will be 10^8 .On the other QR codes are capable of storing a large amount of data in small are in an efficient and faster way. For example, If we consider the smallest QR code version1 with alphanumeric mode and error correction level as 40H (highest level),the total no. of combinations would be 44^{10} ,which is much greater than 10^{8}.[10].Hence a random QR code would be a more efficient and reliable option than an random OTP.

Encryption is followed by authentication so that data confidentiality and data integrity can be achieved. In PKI the data is encrypted by using the public key. Franklin and D. Boneh [12] introduced Identity Based Encryption which encrypts and decrypts data on the basis of some user identity. For example, using an email id instead of a random string commonly used in PKI systems.

Attribute based encryption(ABE) was introduced by Sahai and Waters in the year 2005 in which set of attributes are used. Attribute based encryption is of two types[8]-

1) Key Policy Attribute based encryption (KP-ABE) proposed by Goyal
2) Cipher text Policy Attribute based encryption (CP-ABE) proposed by Sahai and Water

In KP-ABE the sender encrypts the data by using a group of attributes. The user is able to decrypt only if he has the access structure. [5]

For example, if the access structure in the user's private key is (P^Q)vS, and the a cipher text is formed by using the attributes {P,R} he will not be able the decrypt the data. But if the data is encrypted using the attributes {P, Q} then it could be decrypted by the user with an attribute set {P,Q}.

In CP-ABE the policy defined over a set of attributes carry the encryption process. The user's private key consists of set of attributes and the cipher text is based on the access structure defined over system specific attributes. For example, consider a universe of set of attributes over the entire system {P, Q, R, S}.Consider user A and B. User A gets a key with a set of attributes {P,Q} and B get a key with a set of attributes {S}.The cipher text is encrypted on a policy (P^R)vS. Then only user B is able to decrypt the data, while A is not. The benefits of using CP-ABE is it is collusion resistant and hence suitable for a multiuser platform like cloud.

III. PROPOSED SYSTEM

The solution aims at developing a private cloud using and providing secure storage service using MFA (for authentication) and CP-ABE(for data Confidentiality).

The following diagram shows a UML (Use case diagram) the flow of the proposed system.

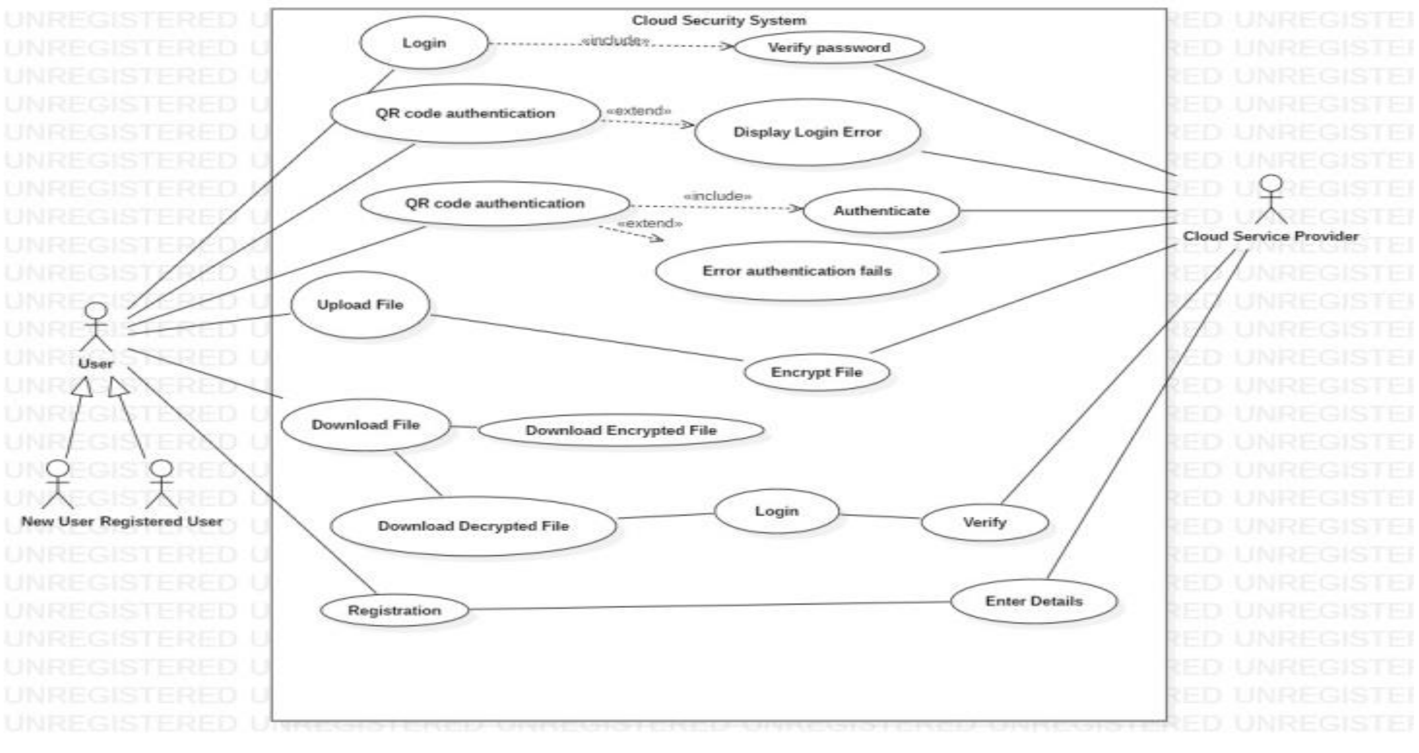

Fig 1. Flow of proposed system

The flow of the system would include-

Stage-1: Entry level user Authentication

1. User authentication is achieved using static username and password.
2. Multiple hashing encryption is used for passwords.
3. Password protection using multiple encryption is used to ensure that password is not decrypted using reverse engineering**.**

Stage-2: QR based OTP generation for authentication

1. OTP is in token(QR Code) form which is provided by Google Authenticator Application.
2. QR based OTP makes it more difficult to gain unauthorized access to files.
3. The provision of default tokens is also available for genuine users.

Stage-3:Data confidentiality using CP-ABE

a. For uploading a file

1. User provides file as input and cloud services encrypts it using CP-ABE algorithm.
2. The encrypted file is stored on cloud.

b. For downloading a file

1. If the user requests to download encrypted file:Cloud service sends it to the user.
2. If the user requests to download decrypted file:Attributes are to be filled by the user into the verification page(i.e. user again has to login),which provides additional layer of security.

IV. ADVANTAGES

- The proposed system suggests using MFA i.e. a username and static password followed by a QR code based OTP.
- The proposed system is much efficient and reliable as QR code OTP can store more information than a SMS based alpha-numeric OTP which consists of entering the OTP manually and a very short range of OTPs can be generated**.**
- Larger OTPs would be hectic to enter manually and hence using QR codes would be much efficient as more information can be used and no manual entering of data is to be done.
- For data confidentially CP-ABE encryption is much more efficient for a cloud as it has multiple users.
- Tokens generated by QR code is the second factor of authentication in the proposed solution. But, for authorized users, there is a provision of backup tokens, for situations where QR code scanning is not possible. This preserves availability for genuine users.
- Automatic resource scaling –Users are provided dedicated resources as per their needs.
- Backup services are provided.
- Files encrypted using CP-ABE technique cannot be viewed in plain-text even by the system administrator. Therefore, administrative interference is null.

V. LIMITATIONS

- Security related weakness of QR codes based OTPs found are attackers can view since they are available over the screen itself, QR codes are also prone to malware attacks.
- It could be a little bit time consuming to login as QR code is to be scanned.
- Mobile device is mandatory for login.

VI. CONCLUSION AND FUTURE SCOPE

- The proposed system presents private Cloud deployment so as to achieve better customization in services and data protection methods as stated above. Security levels taken into consideration are Confidentiality, access control. Data Confidentiality is achieved through CP-ABE encryption technique.
- Access control and availability is maintained using Multifactor Authentication principle. Therefore, a novel MFA technique, that
- incorporates, Inherence factor-Fingerprint, with Knowledge and Possession factors, is planned in future. This aims to achieve a level of security, which is difficult to break, because, Passwords can be changed, but the human anatomical characteristics tend to change very rarely. This can be realized using Artificial Neural Networks

VII. REFERENCES

[1] www.techopedia.com/definition/2/cloud- computing

[2] www.paranet.com/blog/bid/128267/the-three-types-of-cloud-computing-services

[3] www.linkedin.com/pulse/3-service-4-deployment-models-cloud-computing-sankar-somepalle

[4] Niharika Gupta, Rama Rani, "Implementing High Grade Security in Cloud Application using Multifactor Authentication and Cryptography", International Journal of Web & Semantic Technology (IJWesT) Vol.6, No.2, April 2015

[5] Attribute based Encryption" 2016 [Online].Availbale: http://gleamly.com/article/introduction-attribute-based-encryption-abe

[6] Cheng-Chi Lee , Pei-Shan Chung , and Min-Shiang Hwang, "A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments", International Journal of NetworkSecurity, Vol.15, No.4, PP.231-240, July 2013

[7] John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-policy attribute-based encryption.In IEEE Symposium on Security and Privacy, pages 321-334, 2007

[8] V. Goyal, O. Pandey, A. Sahai, and B. Waters. "Attribute-based encryption for fine-grained access control of encrypted data." In CCS ’06: Proceedings of the 13th ACM conference on Computer and communications security, pages 89–98, New York, NY, USA, 2006. ACM.

[9] Margaret Rouse, " Multi-Factor Authentication ", 2015 [online], http://searchsecurity.techtarget.

[10] Two-factor authentication system with QR Codes for Web and Mobile Applications by MeteEminagaoglu,Ete Cini,Gizem,Sert,DertZor

[11] https://searchsecurity.techtarget.com/definition/one-time-password-OTP

[12] D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. In CRYPTO ’01: Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, pages 213–229. Springer-Verlag, 2001.

[13] SMS-Based One-Time Passwords: Attacks and Defense (Short Paper) Collin{ravii,patrickx,jpseifert}@sec.t-labs.tu-berlin.de