© 2017 IJSRSET | Volume 3 | Issue 5 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Improved Authentication and Protection of Data in the Cloud

K Dronam Raj*, C Shoba Bindu, P Dileep Kumar Reddy

JNTUA College of Engineering, Ananthapuram, Andhra Pradesh, Andhra Pradesh, India

ABSTRACT

In 2016 Perez et.al proposed a data-centric access control scheme for self- protected data that can run in untrusted CSPs. Their scheme is vulnerable to Man-in-Middle attack and uses more complex encryption methodologies. So this paper presents a solution in which security is focused on protecting the user data regardless of the cloud service provider that holds it. The solution in this paper takes advantage of Two-Factor Authentication (2FA) and encryption of data to be uploaded to cloud using Advanced Encryption Standard (AES).

Keywords : Cloud Computing, Two-Factor Authentication, Advanced Encryption Standard, Man-in-Middle attack.

I. INTRODUCTION

Security and protection are the significant factors in the implementation of cloud for putting away information. It is imperative to guarantee the information integrity, security and assurance for the cloud benefit. For this reason, a few specialist centers are utilizing diverse approaches and instrument that rely on the nature, sort and size of information.

Sharing information among different associations is the key preferred standpoint of Cloud Computing. Be that as it may, this preferred standpoint itself represents a hazard to information. To keep away from this potential hazard to the information, it is important to secure information archives**.**

Two-factor Authentication (2FA) [1] for client verification is one of the helpful and successful two-factor validation components. This innovation has been utilized generally for different sorts of verification applications which incorporate remote host login, Internet saving money, get to control of limited repositories, initiation of security gadgets and some more. A few plans and upgrades for remote client approval designs using one-time passwords have been proposed. This paper is the study of data security and discuss about AES encryption algorithm (RIJNDAEL) that secure data stored on clouds. AES is block cipher algorithm and is secure against cryptanalytic attacks. It is versatile, which means it can be implemented on different working environment efficiently, its key agility is proficient which means setup time of key is less and this algorithm is easy to understand and to use it.

Section 2 presents the sorts of threats and some proficient information security methods hold all through the world to information in cloud. In Section 3 we review perez.et.al scheme and its problems. Section 4 describes the proposed schema and its Security analysis is presented in section 5. The last section contains the conclusion.

II. Threats and security worries in Cloud computing

A few threats and security concerns are related with cloud computing and its information. In any case this schema inspects, the capacity out in the open cloud and multi occupancy which are related to the data security in cloud computing [3].

2.1. Storage in Public Cloud

The security worry in cloud computing is putting away information in an open cloud. Cloud brought together storerooms, which can be an engaging focus for programmers. Capacity resources and convoluted structures that are blend of gear. Programming utilization can also cause presentation of data if a slight burst occurs in the all inclusive community cloud [5].

Keeping in mind the end goal to maintain a strategic distance from such threats, it is constantly prescribed to have a private cloud if workable for great degree touchy information.

2.2. Multi tenancy

Shared or multi tenancy is moreover considered as one of the genuine risk to data in cloud computing [4]. Since different clients are utilizing the same shared figuring assets like CPU, Storage and memory and so forth it is risk to a client's as well as numerous clients.

In such situations there is dependably a threat of private information overflow together to different clients. Multi tenancy can be particularly perilous in light of the fact that fault in the structure can empower another client or programmers to get to each and every single other data [6]. These sorts of issues can be dealt with by carefully validating the clients before they can approach the information. A few verification systems are being used to keep away from multi tenancy issues in cloud computing [7].

III. Review of Perez et.al. Scheme

In this section, we review the Perez.et.al.[2] scheme**.** This scheme is composed of 6 phases namely setup phase, key generation phase, encryption phase, re-key generation phase, re-encryption phase and decryption phase. An identity-based proxy Re-encryption (IBPRE) approach has been used by perez. It combines both Identity-based encryption (IBE) and Proxy re-encryption (PRE), allowing a proxy to translate a ciphertext encryption under a user's identity into another ciphertext under user's identity. For authorization purpose Role Based access control (RBAC) was used in this scheme which takes more complex work to authorize the user to encrypt the file as well as to decrypt it. The phases were described each as follows:

Setup Phase:
Initializes the cryptographic scheme. Takes the input from the user public parameters p and security parameter k and outputs both the Master secret key *msk* and a set of public parameters p that is used as input for the rest functions.

Key Generation Phase:
Generates secret keys. It takes input as *msk* and an identity id_{α} and outputs the secret key sk_{α} corresponding to that identity.

Encryption Phase:
Encrypts data. It takes an input an identity id_{α} and a plain text m, and outputs the encryption of m under specified identity c_{α}.

Re-key Generation Phase:
Generates Re-encryption keys. It takes as input the source and target identities id_{α} and id_{β} as well as the secret key of the source identity sk_{α} and outputs the Re-encryption key $rk_{\alpha\rightarrow\beta}$ that enables o re-encrypt from id_{α} to id_{β}.

Re-Encryption Phase:
Re-encrypts data. It takes as input a ciphertext c_{α} under identity id_{α} and a Re-encryption key $rk_{\alpha\rightarrow\beta}$ and outputs the re-encrypted cipher text c_{β} under identity id_{β}.

Decryption Phase:
Decrypts data. It takes as input a cipher text c_{α} and its corresponding secret key sk_{α}; and outputs the plain text m resulting of decrypting c_{α}.

3.1 Problems in Marin Perez Model:

The Perez.et.al proposed scheme does not provide a secure authentication process which may leads to a security threat. If userid and password of a user were hacked then there is possible chance of stealing the data from user's cloud account. The algorithm Identity-based proxy re-encryption (IBPRE) that perez team used to encrypt data doesn't provide end-to-end authentication for accessing data, even the complex encryption methodologies and the decryption method becomes more resource-complex which leads to Man-in-Middle attack.

To address these issues in Martin Perez model, we propose a new model that overcomes existing system model problems**.** The proposed model uses Two-Factor Authentication (2FA) for User authentication and Advanced Encryption standard (AES) to encrypt the data which performs more efficiently than existing system algorithm.

IV. Proposed Model for Authentication and Encryption Process:

Proposed model combines Two-Factor Authentication (2FA) and Advanced Encryption Standard (AES), Where Two-Factor verification is utilized for authenticating the client and Advanced Encryption Standard (AES) is utilized for encrypting the data.

4.1 User Authentication using Two-Factor Authentication:

Login with a One Time Password (OTP) code is a secure method for the user authentication process. In this technique, a one-time password is generated dynamically and sent to the user who attempts login. OTP can be sent to the user's email or to the user's mobile phone. When the user enters the OTP code then the application will authenticate the user via this code.

This entire setup of generating a dynamic OTP code and transferring that code to the user who attempts login will be done at the Cloud Service provider (CSP) side (See Fig.2).The following will be the algorithm for generating one-time password (OTP).

OTP Algorithm:

The algorithm can be described in 4 steps:

```
    Step 1: Generate the HMAC-SHA-1 value Let
          HMK = HMAC-SHA-1(Key, T)
        // HMK is a 20- byte string
    Step 2: Generate a hex code of the HMK.
          HexHMK=ToHex (HMK)
    Step 3: Extract the 8-digit OTP value from the string
          OTP = Truncate (HexHMK).
    Step 4: OTP (Key,T) = Truncate(ToHex(HMAC-SHA-1(Key,T)))
```

Where –Truncate converts the value generated through HMAC-SHA-1to an OTP value.

The Truncate function in Step 3 does the dynamic truncation and reduces the OTP to 8-digit.

Figure 1 : Algorithm for OTP generation

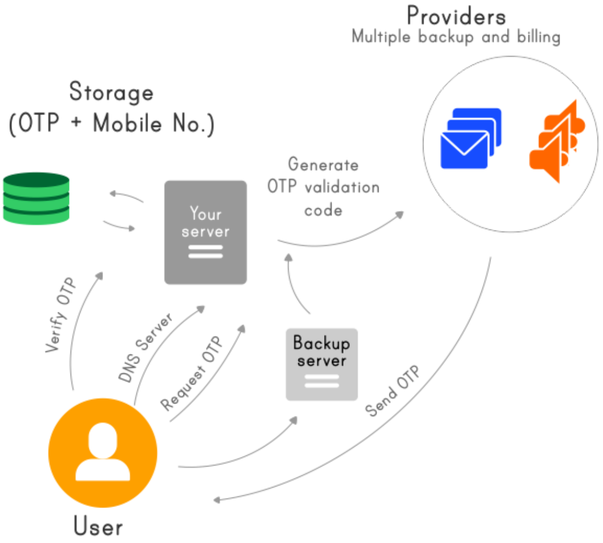


Figure 2 : Working of Two-Factor Authentication (2FA)

4.2 Proposed Scheme:

The design demonstrates how the mix of two algorithms two Factor Authentication (2FA) and Advanced Encryption Standard (AES) attempts to confirm client and to scramble information in the Cloud. This proposed scheme contains 3 phases which are Authentication phase, key generation phase and Data transmission phase.

4.2.1 Authentication Phase:

User and data owner gets registered with a few public parameters *p*, security parameters *k* with user identity $id_{\alpha,\beta}$. Utilising user registered parameters $(p, k, id_{\alpha}, id_{\beta})$, domain authority sends client an *OTP* to validate, utilising that *OTP* user need to confirm identity $id_{\alpha,\beta}$ to domain authority. When user and data owner gets confirmed with domain authority then user can search for the encrypted file C_{α} and requests for key *PK* to decrypt that encrypted file.

4.2.2 Key Generation Phase:

Domain authority generates a random key *PK* based on users and data owner's parameters and *id* that were taken at the registration phase. Domain authority sends those generated key to their respective identity person.

4.2.3 Data transmission Phase:

Data transmission phase contains encryption phase and decryption phase.

(a) Encryption Phase:

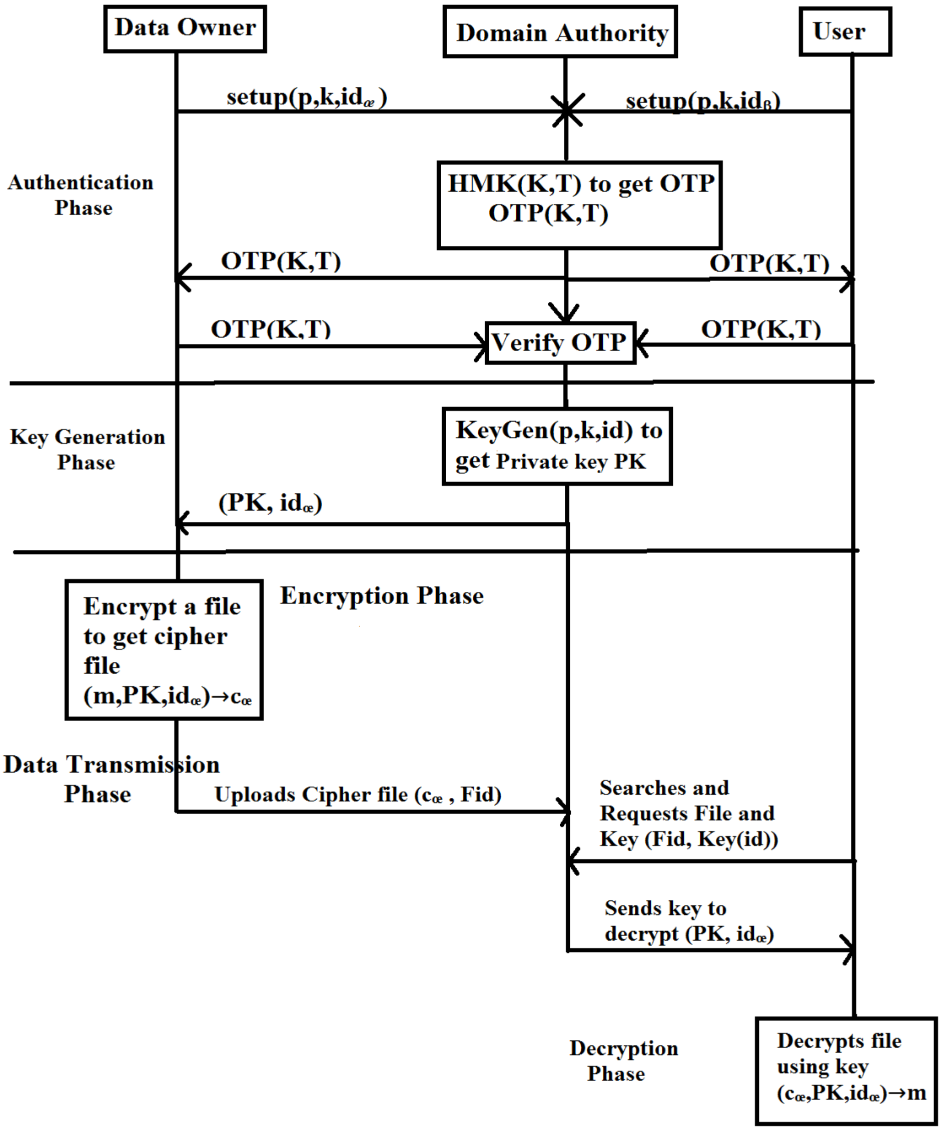
Data owner encrypts the file *m* using data owner's identity id_{α} private key *PK* and uploads it to the cloud. The key that was used to encrypt the file is only used to decrypt that encrypted file C_{α}.

$$(m, PK, id_{\alpha}) \rightarrow C_{\alpha}$$

(b) Decryption Phase:

Data owner encrypted file C_{α} that is uploaded to cloud gets decrypted, when user proves identity. The user requests key to decrypt the encrypted file to the domain authority. Domain authority sends key PK along with identity of the data owner $\text{id}_{\oe}$ to decrypt the file.

$$(C_{\oe}, PK, id_{\alpha}) \rightarrow m$$



Data Owner
Domain Authority
User
setup(p,k,idœ)
setup(p,k,idβ)
Authentication Phase
HMK(K,T) to get OTP OTP(K,T)
OTP(K,T)
OTP(K,T)
OTP(K,T)
Verify OTP
OTP(K,T)
Key Generation Phase
KeyGen(p,k,id) to get Private key PK
(PK, idœ)
Encrypt a file to get cipher file (m,PK,idœ)→cœ
Encryption Phase
Data Transmission Phase
Uploads Cipher file (cœ , Fid)
Searches and Requests File and Key (Fid, Key(id))
Sends key to decrypt (PK, idœ)
Decryption Phase
Decrypts file using key (cœ,PK,idœ)→m

Figure 3 : Flow of Mechanism of Proposed System

V. Performance Analysis and Security Analysis:

In this section, we show that our scheme works more efficient than Perez scheme.

5.1 Performance Analysis:

Time taken by both the schemes in various phases is given in Table 1.

Table 1: Comparison of Two Schemes

Phases	Perez et.al Scheme	Our Scheme
User Authentication	178	276
Key Generation	29	21
Encryption	29	27
Decryption	247	23
Total	483	347

The comparisons of two schemes were showed below using a graph which shows performance of both schemes in milliseconds (See Fig: 5).

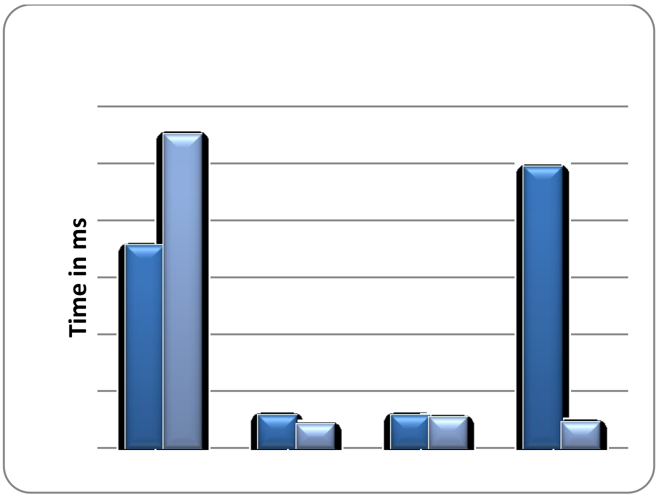


Figure 4 : Graph comparing both schemes

5.2. Defend Man-in the Middle Attack:

This scheme defends the man-in-the middle attack as different OTP's are used for every login.

VI. CONCLUSION

The threat of security is an urgent concern, where some secret data is put away in cloud. It is critical to judge the client validation appropriately to remove information from the cloud. On the off chance that we utilize single factor to approve the client it might break downs the whole information security then certainly some extra counter measure ought to be taken while outlining he demonstrate.

We have composed a model that defeats all security issues to secure information in the cloud. Notwithstanding, the 2FA and AES security is guaranteed just on the off chance that it is accurately executed and great key administration is utilized.

VII. REFERENCES

[1]. C Shoba Bindu P. Chandra sekhar Reddy B.Satyanarayana "Improving Remote User Authentication Scheme preserving user anonymity" IJCSNS International journal,Vol.8 No.3, March 2008.

[2]. Juan M. Marin Perez gregorio Martinez Perez Antonio F. Skarmea Gomez "SecRBAC: Secure data in the Clouds" IEEE Transactions , DOI 10.1109/TC.2016.2553668.

[3]. P. S. Wooley, "Identifying Cloud Computing Security Risks," Contin. Educ., vol. 1277, no. February, 2011.

[4]. F. Sabahi, "Virtualization-level security in cloud computing," 2011 IEEE 3rd Int. Conf. Commun. Softw. Networks, pp. 250–254, 2011.

[5]. Cloud Security Alliance, "The Notorious Nine. Cloud Computing Top Threats in 2013," Security, no. February, pp. 1–14, 2013.

[6]. A. U. Khan, M. Oriol, M. Kiran, M. Jiang, and K. Djemame, "Security risks and their management in cloud computing," 4th IEEE Int. Conf. Cloud Comput. Technol. Sci. Proc., pp. 121–128, 2012.

[7]. T. Mather, S. Kumaraswamy, and S. Latif, "Cloud Security and Privacy," p. 299, 2009.