I J C T A, 9(41) 2016, pp. 1241-1246

Privacy Preserving Public Auditing for Multi-level Encryption Based Cloud Storage

Karuna Arava[*] and L. Sumalatha[**]

ABSTRACT

Cloud computing is a build out technology in modern era with a hypothesis of ubiquitous on demand (ODC) in terms of storage and services. In cloud storage the outsourced data might be at risk due to public access which leads to adding fault tolerances and compromising of vendors. The public auditing scheme checks against corruptions and added fault tolerances for the data stored in cloud storage by providing both data integrity and failure reparation. The existing privacy preserving method with single level encryption could not give sufficient security to outsourced data. This paper proposes data security enhancement by applying the 'Rule-of-Two' which is a data security principle from the NSA's Commercial Solutions for Classified Program (CSFC). We are using "Key Stretching" for generating master key for Multi-level encryption. Multi-Factor authentication makes Key sharing more secure while user wants to access the cloud data.

Keywords: PBKDF2, challenge/response protocol, multi-factor authentication, entropy.

1. INTRODUCTION

Cloud computing is most popularly used IT Buzz word: clients migrate their data and applications to "Cloud" and access them in a lucid and ubiquitous way. Cloud computing provides cloud storage service, grants user to shift data from local storage and place it in cloud and relish on demand quality services. So that users need not care about the complexities of hardware and software managements. In reality sharing cloud data is virtuous among a large number of users in group.

There are many issues with cloud security like availability, integrity, confidentiality, data access, privacy, recovery, accountability, multi-tenancy.

Once data is saved in cloud it is handed over to Cloud Service Provider (CSP). Thus, correctness, availability and integrity of the data are under risk. CSP may act dishonestly and may hide data loss from owner or corruption of data in the cloud for reputation reasons. So there is a need for users to provide security to their sensitive data in the cloud. Precautions that are needed to safeguard owner's data proposed in this paper.

The 'Rule-of-Two' is a data security principle. It specifies two completely independent layers of cryptography to preserve privacy.

Our scheme focuses on multi-level encryption based cloud storage so that data is more secured. Integrity checking, the public auditing[1] is done by semi trusted Third Party Auditor (TPA).The cloud data is shared to authorized users by the process of Multi-Factor authentication.

The remaining topics are organized in this manner: section I introduces some schemes about outsourced data that could not be compromised and achieves confidentiality. The detailed description of performing public auditing by TPA for integrity achieving in Section II is provided; Section III analyzes the validation of authorized users by performing multi-factor authentication. Finally, Section IV concludes the paper.

[*] Assistant Professor, Dept of CSE, UCEK(A), JNTUK, AP, India, *E-mail: karunagouthana@jntucek.ac.in*

[**] Professor, Dept of CSE, UCEK(A), JNTUK, AP, India, *E-mail: lsumalatha@jntucek.ac.in*

2. RELATED WORK

Initially integrity checking of remote data was being solved and implemented through PDP and POR models, by Ateniese *et al.* [2] and Juels *et al.*[3]. Ateniese gave definition to PDP model for ensuring possession of files on public storage and also described RSA based Homomorphic tags. Homomorphic operations are malleable by definition i.e., malleable is something that "can be intelligently modified. The subsequent work from them[2][3] was a dynamic version PDP scheme based on MAC. Jian liu *et al.*[1] proposed auditing scheme as for each of the *n* servers, TPA verifies the possession of α coded blocks by randomly checking samples of segments of every block and performing a batch verification.

Evolution of key generation algorithms started with SHA (secure hash algorithm)-2 which was implemented by the U.S National Security Agency (NSA) which is computed with 34 bit words. And also Bcrypt gives stronger key than PBKDF2 but it has inability to use more than 55 character of passphrase and the estimated cost is also very high. PBKDF2 the passphrase is truly secure than SHA, which is pretty random and out of reach of any systematic enumeration process.

2.1. Entropy

PBKDF2 produces a master password D_k with high entropy. To find a key by number of guesses which certainly need base-2 logarithm of that number is called as "entropy bits" which explained in information theory. Difficulty of predicting a key through guessing, brute force attack, dictionary attacks and rainbow attack are interpreted by entropy.

$$H = \Sigma \log_2 N^L = L \log_2 N = L \log N/\log 2$$

Here *N* represents the number of possible symbols and *L* represents the number of symbols in the password. "Bits" is the measurement of Entropy H.

Florencia and Herley[4] approximated average of entropy as 42.02 bits. using a key derivation function which requires 2^s cryptographic operations to compute, the cost of performing a brute-force attack against passwords with H bits of entropy is raised from 2^H to 2^{s+H} operations.

Lamport[5] suggested remote user identification scheme in 1981, in which hashed value of user's passwords are stored in server. Mostly web based architectures have adopted ID/password mechanism for identification and authentication. Currently most popularly used authentication is smartcard system [6, 7] where a user typically has an ID, a password, and also a generated One Time Password (OTP) from the smart card which changes every 60 seconds. Biometric mechanism is most secured authentication which demonstrates what you are. Biometrics credentials can take many dimensions, from finger prints, to retinal scans to pupil images etc. The proposed scheme is based on dynamic secure multi-factor authentication which takes two levels of factors for authentication.

3. SYSTEM MODEL

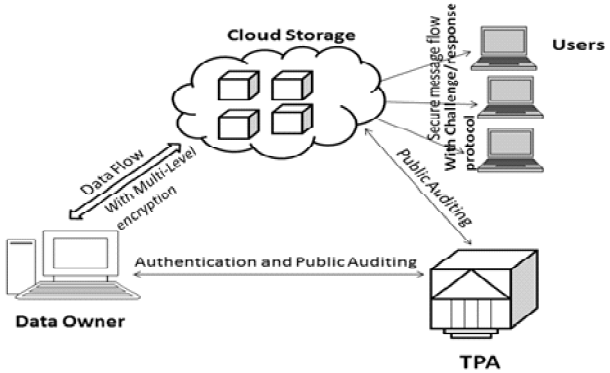


Figure 1: The system model

Figure 1 illustrates three different modules and shows the flow of communication between actors. These actors are scattered at different geographical locations but are connected as a network.

3.1. Design Goals

Our model aimed to cope up with standard security services as:

- *Public Auditability*: TPA performs accurate integrity check for owner's data periodically.
- *Privacy Preserving*: The sensitive data i.e., kept in cloud is unintelligible form.
- *Secure Key Exchange*: key should be exchanged securely to authenticated users and also not to compromise data with intruders.
- *Alert*: To ensure the correctness of cloud data. Data owner gets alert mail if data is modified by vendor/intruder.

Table 1
Notations in our scheme

Notation	*Description*
M	Plain text
c_i	Output of RSA algorithm
c_{ii}	Output of AES algorithm
Pu_B	Public key of RSA algorithm
PR_B	Private key of RSA algorithm
D_k	Derived key from PBKDF2
E	Entropy
q1,q2	Challenges for Multi-factor authentication
a1,a2	Responses from user
h^x	Hash function of server s_x
h^y	Hash function of server s_y
h^z	Hash function of server s_z

3.2. Design

The following section is divided into Encryption phase, audit phase and key-exchange phase.

3.2.1. Encryption phase

In this phase, the data is encrypted through multi-level encryption using the RSA and AES algorithms to get protection against intruders.

AES uses symmetric encryption algorithm key D_k for both encryption and decryption. Our aim is to generate D_k by using "key stretching" property to achieve more security. D_k is generated by using password based key derivation function (PBKDF2) rather use of pseudo random function. This method attains high entropy.

3.2.2 Audit phase: In this phase, data is checked for Integrity. The HMAC employed for hash code generation for multi-level encrypted data. TPA generates

digests for both data at owner and cloud periodically. This process checks against corruptions and added fault tolerance of data.

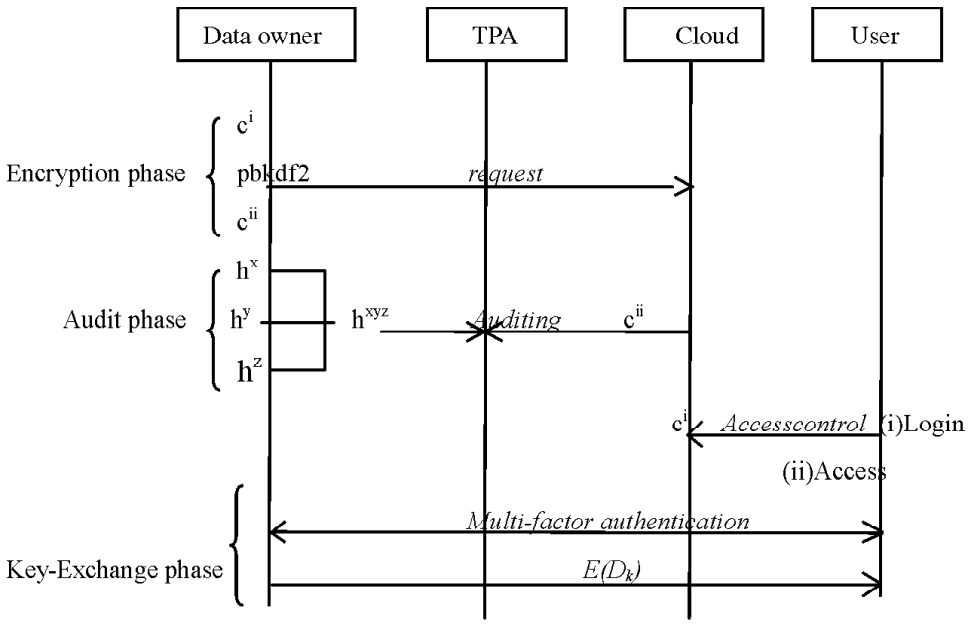


Figure 2: Overview of our scheme

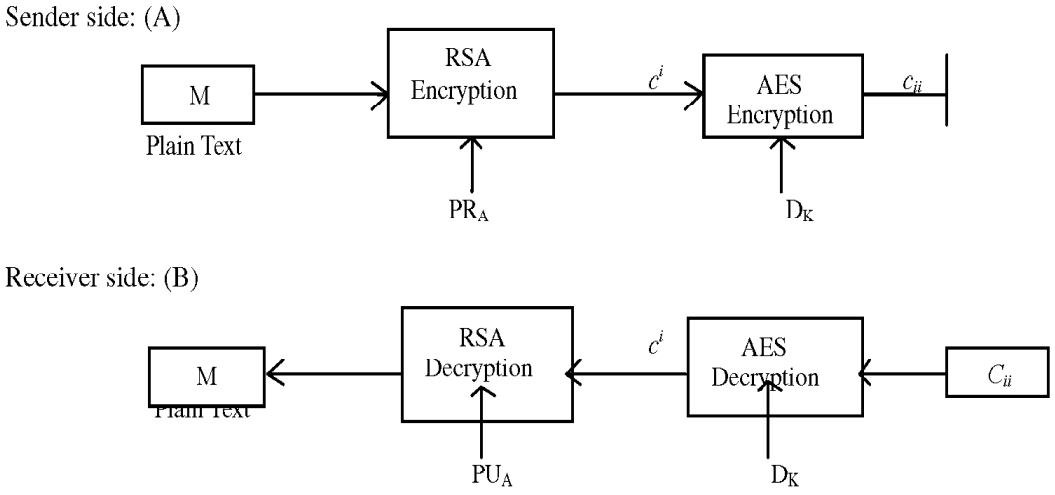


Figure 3: Multi-level Encryption

3.2.3. Key-exchange phase

In this phase, owner uses challenge/response protocol in multi-factor authentication [8] for user identity checking if user is authorized then only D_k is exchanged using Public key encryption algorithm.

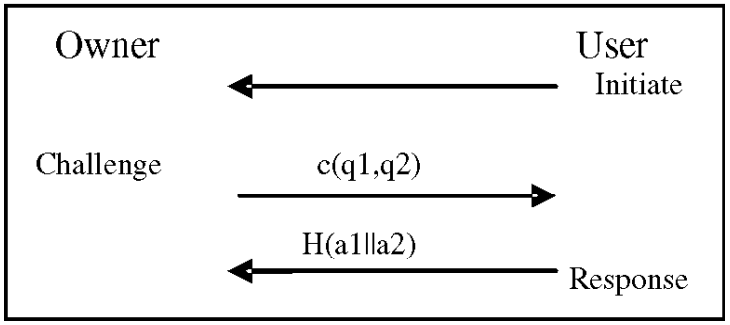


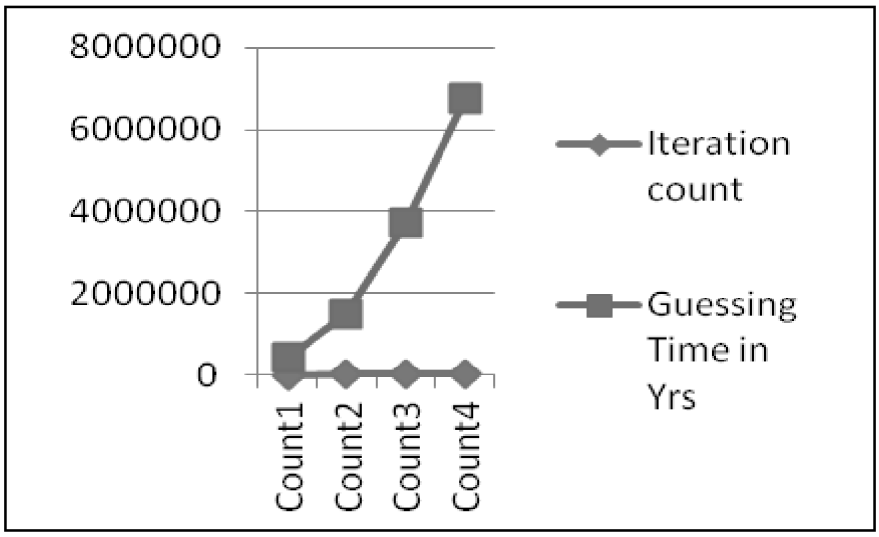
Figure 4: Challenge/response protocol

3.3. Results

Table 2
Entropy values of PBKDf2 delivery key

Test Cases	*PBKDF2 key(bits)*	*AES key (bits)*
Test1	359.5	115.3
Test2	366	182.3
Test3	362.2	192.7
Test4	358	184.2

Table2 compares the key produced from password based key derivation function and the key produced from AES algorithm. Test cases test1,test2,test3 and test4 results in the entropy measured in bits for both PBKDF2 and AES. The average key strength analysis illustrates that D_k which is produced by PBKDF2 is having better entropy values than AES.



Graph 1: Time analysis against Brute Force attack

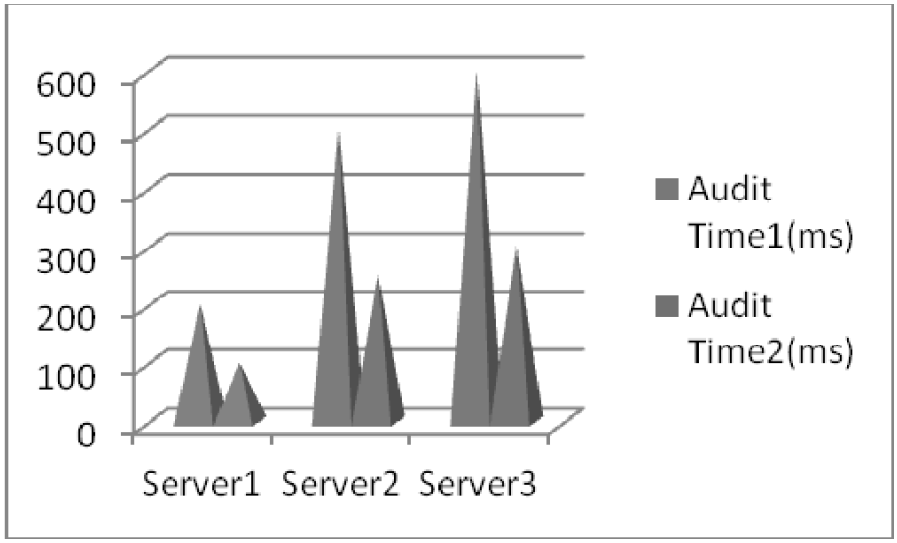
The graph1 shows the result about time analysis against Brute-Force Attack [9]. Here, the x-axis represents the iteration count that is in increasing order and y-axis represents the guessing time which is measured in years. From the result we can say that increase in the iteration count makes the brute-force attack much more difficult to guess the key.

The graph 2 shows result of auditing time comparison [1]. Here, x-axis represents the servers from which the data has to be obtained to perform auditing. The auditing is done for each server sequentially. And y-axis represents the time taken to perform auditing for each server in milliseconds. From the results analysis we can strongly say that our scheme has reduced the Public auditing time when compared with the existing.

4. THREAT MODEL

Apparently threat in our scheme comes from the compromised servers and TPA. The kind of threats that our scheme can resist are:

- *Man-in-Middle attack:* Our scheme can survive from this attack by using encryption of key during key exchange.



Graph 2: Analysis of public auditing

- *Brute Force attack*: In this attack intruder may attempt combination of possible keys to find out actual key but in our scheme the usage of PBKDF2 makes stronger key and reach out of any systematic enumeration process.
- *Rainbow table attack*: In this attack perpetrator tries to use a rainbow hash table to crack the password. By using key derivation function, a salt makes this attack infeasible.
- *Impersonation attack:* Adversary can successfully speculate the existence of one of the legitimate parties in system or in a communication protocol. In the multi-factor authentication, the details of user are never transmitted in plain text. Only hashed value of h(q1,q2) is transmitted to owner. And also these questions are selected randomly by the owner. Hence the proposed scheme is strong and safe against impersonation attack.
- *Phishing attack*: It is attacked through emails, to thieve personal information. In this scheme user authentication process by owner, based on multi-factor credentials is performed. Only the genuine user can reply with authenticated information. And those responses can be verified by genuine owner only.

REFERENCES

[1] Jian Liu, Kun Huang, Hong Rong, Huimei Wang and Ming Xian"Privacy-Preserving Public Auditing for Regenerating-Code-Based Cloud Storage" *IEEE TRANSACTIONS ON INFORMATION AND SECURITY Vol 1 No 2015.*

[2] Shucheng Yud, Cong Wang†, Kui Ren†, and Wenjing Loud "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing" *dDept. of ECE, Worcester Polytechnic Institute.*

[3] A. Juels and B. S. Kaliski Jr, "Pors: Proofs of retrievability for large files," in *Proceedings of the 14th ACM conference on Computer and communications security*. ACM, 2007, pp. 584–597.

[4] D. Florencio and C. Herley. A large-scale study of web password habits. In *WWW '07: Proc. of the 16th international World Wide Web conference*, pages 657–666, 2007.

[5] Daniel Mouly (2002), Strong User Authentication, Informa-tion Systems Security, 11:2, 47-53.

[6] Subashini S, Kavitha V (2011), *A survey on security issues in service delivery models of cloud computing,* Journal of Network and Computer Applications: 1-11.

[7] Viega J (2009), *Cloud computing and the common man,* Computer 42(8):106-08.

[8] Rohitash Kumar Banyal, Pragya Jain, Vijendra Kumar Jain, "Multi-factor Authentication Framework for Cloud Computing" in *2013 Fifth International Conference on Computational Intelligence, Modelling and Simulation.*

[9] Percival, C., Stronger Key Derivation Via Sequential Memory-Hard Functions, BSDCan '09, May.