ISSN 2395-1621

Secure Key Management Using Session Based Encryption and Re-Encryption System

[#1]Shraddha Banne, [#2]Maitreyee Shende, [#3]Sneha Gade, [#4]Shravani Varute, [#5]Mrs Priti Jorvekar

[#12345]Department of Computer Engineering, NBN Sinhgad School of Engineering, Savitribai Phule Pune University, Pune, India

ABSTRACT

To the cloud, outsourcing data is the most beneficial for the reasons of economy, scalability, reliability and accessibility. but still there remain some significant technical challenges. Sensitive data that is stored into the cloud must be protected by a cloud provider. In addition to that, cloud-based data is being increasingly accessed by resource-constrained mobile devices which needs minimized processing and communication cost. Fresh modifications to attribute-based encryption are proposed to allow the users an authorized access to cloud data such that it will satisfy required attributes. Higher computational load from cryptographic operations is assigned to the cloud provider and total communication cost is minimized for the mobile user. Furthermore, data re-encryption may be an optional part performed by the cloud provider to reduce expense of user abrogation in a mobile user environment preserving the privacy of user data stored in cloud. The proposed protocol has been realized on commercially popular mobile and cloud platforms to demonstrate real-world benchmarks that show the potency of the scheme. A simulation calibrated with the benchmark results shows the scalability potential of the scheme in the context of a realistic workload in a mobile cloud computing system.

ARTICLE INFO

Article History

Received :6th April 2016

Received in revised form :

8th April 2016

Accepted : 10th April 2016

Published online :

13th April 2016

Keywords— Encryption, Decryption, Re-Encryption, Security.

I. INTRODUCTION

Cloud Computing is the newly emerging model for the distributed computing which consists of various centralized data centres. These data centres provide various resources for scalable units of computing. Internet is that insecure medium, over which these computational facilities are being delivered in the form of services. Cloud computing enables convenient and on-demand access to its multiple users. It is also responsible for increasing the effectiveness of shared resources. Cloud provider is the one who provides all these services to the clients requesting for the data to cloud. With the help of cloud provider, client can address various changes for its processing needs, for client's convenience cloud provider can also create replicas of the data stored in cloud. The data is provided to the clients on rent basis, where the clients which have access to data pays only for the storage amount, network communication amount and related computational work but not for maintenance and capital cost of an in-house solution. Cloud provider provides the facilities like high scalability, longevity, safety and hence it is a best option. But along with these various facilities provided by cloud provider there is still a limitation that, the data stored in cloud may be accessed or read by cloud administrator without the knowledge of client. Also sensitive data carries the continuous risk of being manipulated or intercepted by an unauthorized party despite of the safeguards promised by the provider. So, it is always helpful to apply software techniques, such as encryption-decryption keys, which ensures the privacy and confidentiality of cloud data is preserved at all times and it also increases the safety. There are five entities in our system, they are: Data owner, user or client, controller, CSP(Cloud Service Provider) and manager. All the work in the system is distributed amongst these five entities. Data owner is the one who initiates this work. Data owner first

uses some symmetric key encryption algorithms to encrypt the data. The data owner uploads the encrypted data to the network i.e. onthe cloud. The Cloud Service Provider (CSP), or cloud provider, is an entity which provides the cloud services. The CSP manages and acquires the structure required for providing the services, it runs the cloud software providing those services, and provides the cloud services through network access. Client is an entity which subscribes to a service provided by a cloud provider. A controller monitors access through external client interfaces. Manager is a trusted authority within the system and is completely independent of the CSP. It is sufficiently trusted to authorising access to the cloud and to contain key material as necessary; however, to minimize the risk of it being compromised, a user will only share as much of its own key material with the manager as is necessary in the security scheme utilized. Manager has a access over private group key store. Further, the manager will not be as economical as a cloud provider due to its more limited computational resources.

The main contributions of the proposed work are as follows:
1. A protocol for outsourcing data storage to a cloud provider in protected fashion is provided.
2. Re-encryption allows efficient refilling of users; it does not require removal of attributes and subsequent key regeneration, and may be monitored by a trusted authority without involving of the data owner. Further, re-encryption stores the data on cloud on separate servers in an encrypted form. So that no other involved person can read the data directly, and also the data is safe on the servers even when it is lost from cloud due to some unavoidable reasons.
3. Manager is additional entity which can provide additional layer of security by preventing the unauthorized users from using or accessing the data directly.

II. RELATED WORK

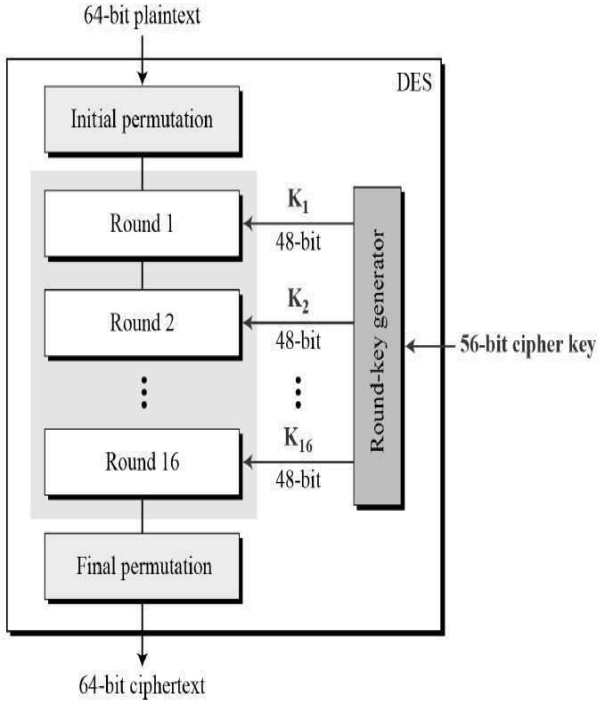
The Data Encryption Standard (DES) is a symmetric-key block cipher algorithm. DES is an implementation of a F Cipher. It uses 16 round F structure. The block size is 64-bit. Although, key length is 64-bit, DES has an productive key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only).The DES allows both the desired properties of block cipher. These two properties make cipher very strong:

Avalanche effect − A small change in the plaintext can result in the very grate change in the ciphertext.

Completeness − each bit of the ciphertext depends on many bits of the plaintext.

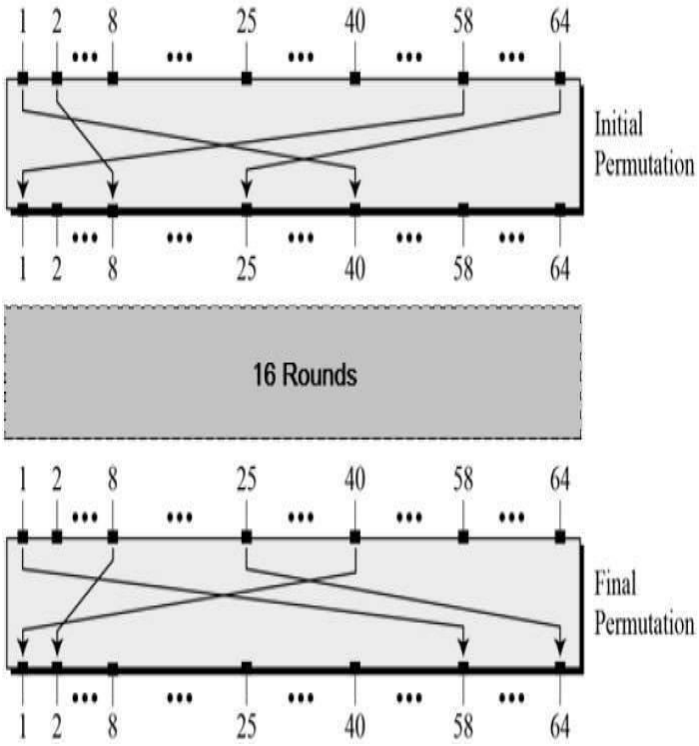
During the last few years, cryptanalysis have found some weaknesses in DES when key selected are weak keys. These keys shall be avoided.

DES has proved to be a very well designed block cipher. There have been no significant cryptanalytic attacks on DES other than timing key search. As DES is based on Fiestel cipher, all required to specify DES is key schedule, Round function, any additional processing- first & final permutation.General Structure of DES is depicted in the following illustration −



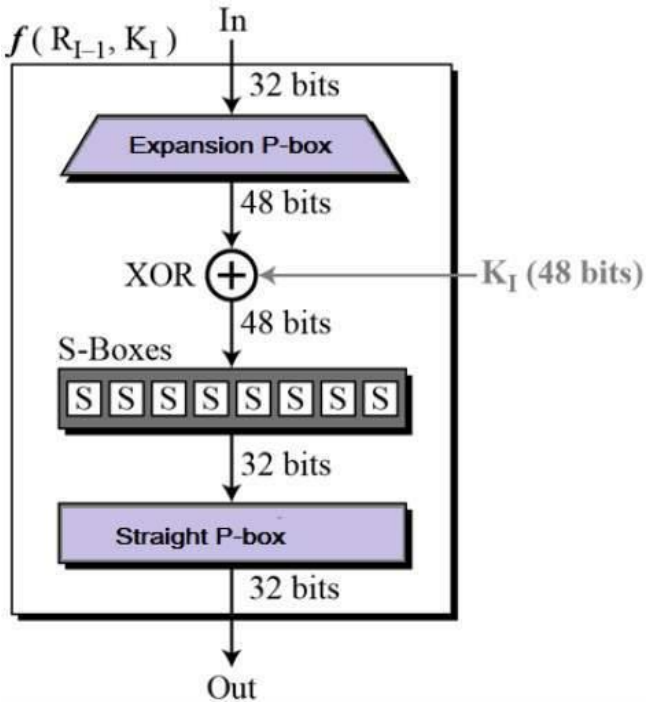
Initial and Final Permutation:-

The initial and final permutations are straight Permutation boxes (P-boxes) that are inverses of each other. They have no cryptography significance in DES. The first and final permutations are shown as follows −

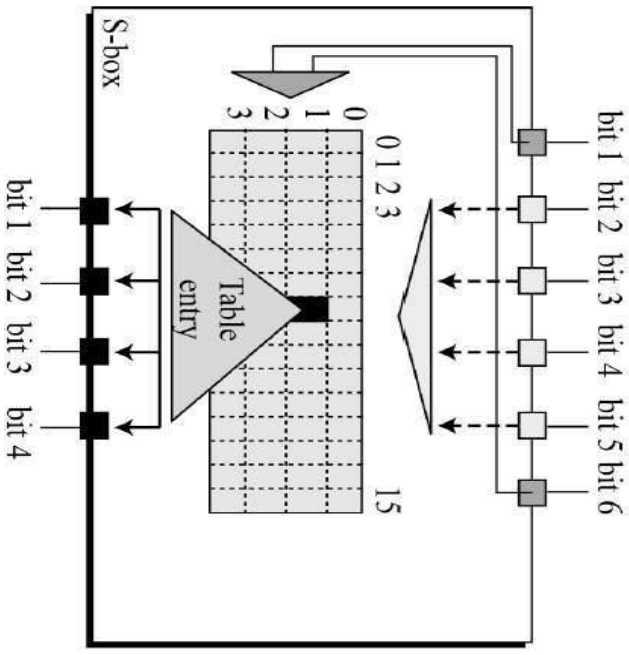


Round Function

The heart of this cipher is the DES function, *f*. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.

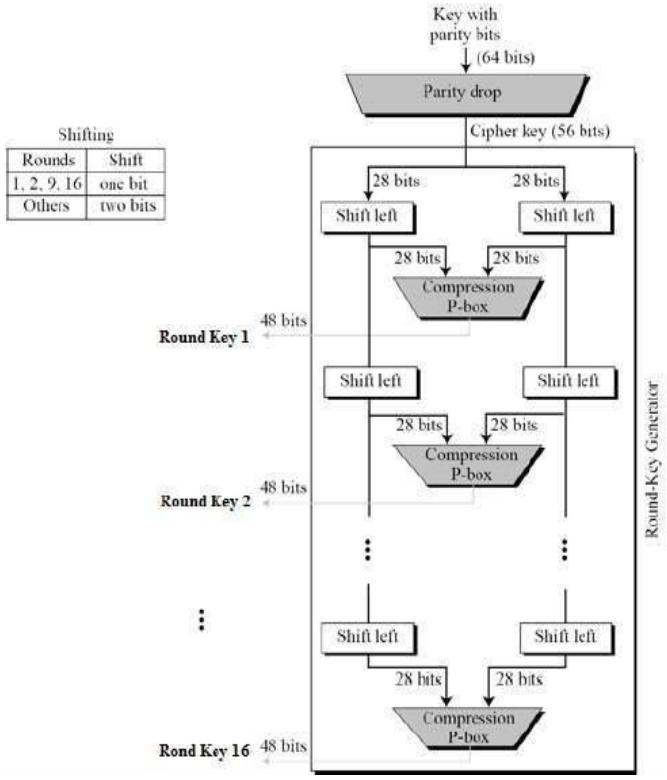


The S-box rule is illustrated below-



Key Generation-

The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key. The process of key generation is depicted in the following illustration −



Shifting

Rounds	Shift
1, 2, 9, 16	one bit
Others	two bits

III.EXISTING SYSTEM

In existing system, there is a cloud which includes various entities such as user, manager, controller, encryptiondata store and data owner.Data owner stores his data on a cloud. With the help of encryption techniques and by generating some private and public keys it securesthe data.

When user wants to access a particular data he has to send the request to the manager. Manager sends the same request to the data owner through the controller where as data owner is an entity which stores his data on a cloud and controller is an entity who acts as an interface in between user and manager.

If data owner permits to the user for accessing the data controller gives public key to the user and user gets that public key through a manager.

Once user gets public key, user can access the data as many times he wants by using same key for every next session also.

It is crucial to secure the sensitive and important data. It reduces the data security level and increases the possibility of data theft. An additional risk is that sensitive data carry the persistent risk of being intercepted by an unauthorized party despite safeguard promised by the provider.

As well as here user or client only pays for amount of storage, related computation and amount of network communication. They do not pay for capital and maintenances of an in- house solutions.

For avoiding all those security issues as well as for the purpose of increasing cost-effectiveness there is a need of proposed system which can help to over come from all these drawbacks.

IV. PROPOSED METHODOLOGY

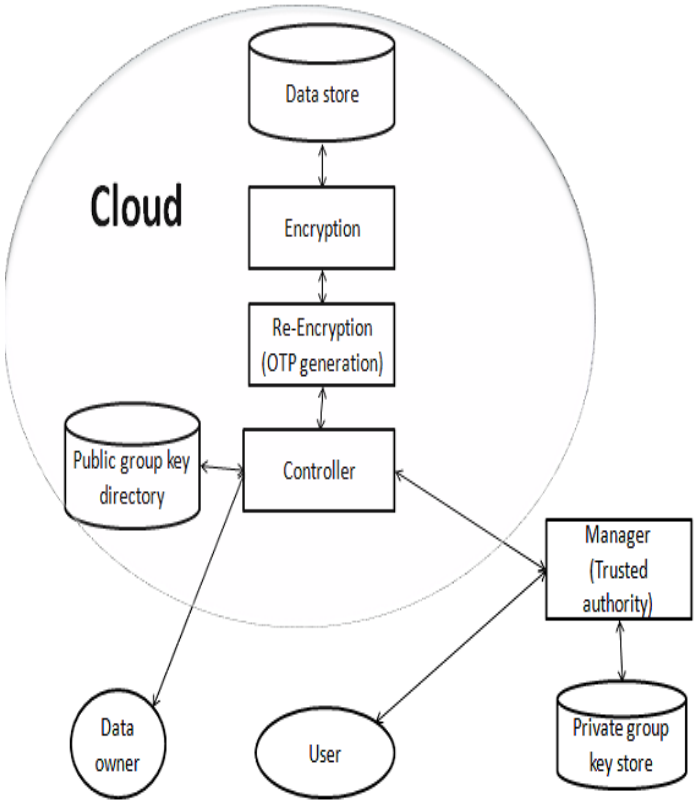
A cloud administrator may not be trusted despite the presence of contractual security obligations, if data security is not further enforced through technical means. An additional risk is that sensitive data carry the persistent risk of being intercepted by an unauthorized party despite safeguards promised by the provider.
Thus we have implemented the proposed system which overcomes some of the faults of the existing system.Our proposed system comprises of 4 entities namely a Client, Data owner, Cloud service Provider and the Manager.Initially the client who wants to access a particular data from the cloud needs to or sends a request to Cloud Service Provider.Once the CSP receives the request of the client, it sends the same request to the Data Owner who owns the requested data.
If the Data owner wishes to grant the permission then he sends a positive acknowledgement to the CSP.After that the Encryption key is send to the data owner and the OTP (One Time Password) and the Decryption key is send to the client.The OTP is session based key which is sent to the same e-mail address of the client which he has entered during the registration process.Using that OTP the client can download the required file.

After the client finishes the use of that particular file and he closes the browser or ends that particular session the file is again encrypted and is sent back to the cloud.Once the client ends a particular session then the validity of that OTP expires, as it is session based.Next time even if the same user wants to access the same data he needs to follow the entire process. Thus this may increase the security to the data in the cloud to some extent.

Also, as cloud computing has the main feature of creating replicas, those replicas will be secured as we have included the tasks like encryption, decryption as well as re-encryption.

Re-encryption has an extra level of security as it stores the data in another folder, this stored data will be encrypted. That means nobody can access it easily. In order to access the re-encrypted data the client or user will have to have the permission from data owner. It is not possible to access the encrypted files or data without the involvement of data owner.

V. SYSTEM ARCHITECTURE



VI. MATHEMATICAL MODEL

System S is defined as collection of following sets:

S = {C, O, M, F, OT, F, K, En, Dec, Up, Dw, Cloud}

where,

C = Client {C1, C2,.....Cn}

O = data owner {O1, O2,....On}

M = Manager

OT = OTP {OT1, OT2,.....OTn}

F = file{F1, F2,.....Fn}

En= Encode

Dec = Decode

Up = Upload

Dw = Download

Input:

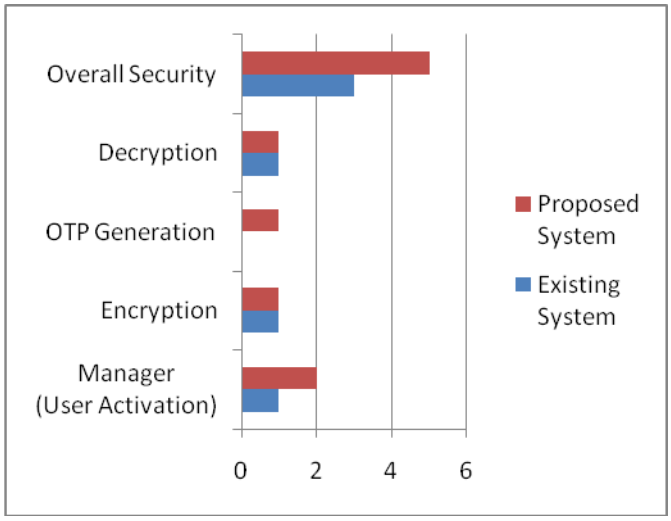
Input1 = Client= {username, Password, Name, Email id, DOB}
Input2 = Data Owner= {username, Password}
Input3 = File= {Encode, Decode}
Input4 = Key= {Secret Key}

Input5 = OTP= {Key, File}
Input6 = Upload= {Key, File}
Input7 = Encode= {Key, File}
Input8 = Decode= {Key, File}
Input9 = Download= {OTP, File}

Output:

Output1 = Client= {Registeration Successful}
Output2 = Data Owner= {File uploaded successfully}
Output3 = File= {Encode, Decode}
Output4 = Key= {Session id generated successfully}
Output5 = OTP= {OTP generated successfully}
Output6 = Upload= {File uploaded successfully }
Output7 = Download= {File downloaded successfully }

VII. EXISTING VS. PROPOSED



In existing system and proposed system, encryption and decryption have same level of security as the message is getting encrypted and decrypted easily using the respective algorithm. In existing system, there was also a manager but was not having the task of activation of user each time. But proposed system has this feature, therefore security level increases by one level.

In existing system, OTP was not in use whereas in proposed system it is the main feature. Therefore, here also security increases by one more level. Therefore, overall security gets increased by two levels. We can say, Proposed system can be said as more secured with two more levels than that of existing system.

VIII. CONCLUSION

In this paper we have proposed secure key management using session based encryption and re-encryption scheme. A protocol for outsourcing data storage to a cloud provider in secure fashion has been provided. However, some additional security mechanisms such as re-encryption will be added to provide formal security and also to reduce increasing data theft. Our improved approach performs double encryption to generate an OTP(One Time Password).

REFRENCES

[1] P.K. Tysowski and M.A. Hasan, "Hybrid Attribute-Based Encryptionand Re-Encryption for Scalable Mobile Applications inClouds," Technical Report 13, Centre for Applied CryptographicResearch (CACR), Univ. of Waterloo, 2013.

[2] R.L. Rivest, A. Shamir, and L. Adleman, "A Method for ObtainingDigital Signatures and Public-Key Cryptosystems," Comm. ACM,vol. 26, no. 1, pp. 96-99, Jan. 1983.

[3] N. Balasubramanian, A. Balasubramanian, and A. Venkataramani,"Energy Consumption in Mobile Phones: A Measurement Studyand Implications for Network Applications," Proc. Ninth ACMSIGCOMM Conf. Internet Measurement Conf. (IMC '09), pp. 280-293,2009.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-PolicyAttribute-Based Encryption," Proc. IEEE Symp. Security and Privacy(SP '07), pp. 321-334, 2007.

[5] A. Tassanaviboon and G. Gong, "OAuth and ABE BasedAuthorization in Semi-Trusted Cloud Computing: Aauth," Proc.Second Int'l Workshop Data Intensive Computing in the Clouds

[6] X. Liang, R. Lu, and X. Lin, "Ciphertext Policy Attribute Based
Encryption with Efficient Revocation," Technical Report BBCR,
Univ. of Waterloo, 2011.

[7] J. Hur and D.K. Noh, "Attribute-Based Access Control with
Efficient Revocation in Data Outsourcing Systems," IEEE Trans.
Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214-1221, July
2011.

[8] G. Zhao, C. Rong, J. Li, F. Zhang, and Y. Tang, "Trusted Data
Sharing over Untrusted Cloud Storage Providers," Proc. IEEE
Second Int'l Conf. Cloud Computing Technology and Science
(CLOUDCOM '10), pp. 97-103, 2010.

[9] P.K. Tysowski and M.A. Hasan, "Towards Secure Communication
for Highly Scalable Mobile Applications in Cloud Computing
Systems," Technical Report 33, Centre for Applied Cryptographic
Research (CACR), Univ. of Waterloo, 2011.

[10] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved
Proxy Re-Encryption Schemes with Applications to Secure
Distributed Storage," ACM Trans. Information and System
Security, vol. 9, pp. 1-30, Feb. 2006.

Shraddha V. Banne
Pursuing B.E.(Computer Science & Engineering),
Savitribai Phule Pune University, NBN Sinhgad School of Engineering, Ambegaon (Bk), Pune 411041, India.

Maitreyee N. Shende
Pursuing B.E.(Computer Science & Engineering),
Savitribai Phule Pune University, NBN Sinhgad School of Engineering, Ambegaon (Bk), Pune 411041,India.

Sneha T. Gade
Pursuing B.E.(Computer Science & Engineering),
Savitribai Phule Pune University, NBN Sinhgad School of Engineering, Ambegaon (Bk), Pune 411041,India.

Shravani S. Varute
Pursuing B.E.(Computer Science & Engineering),
Savitribai Phule Pune University, NBN Sinhgad School of Engineering, Ambegaon (Bk), Pune 411041,India.

