A Secure Anti-collusion Data Sharing Scheme for Dynamic Group in Cloud

Mangesh Hangekar
Dept. of Information technology
Dr. V.V.P. C.O.E. Ahmednagar
Maharashtra, India

Kiran Dngargave
Dept. of Information technology
Dr. V.V.P. C.O.E. Ahmednagar
Maharashtra, India

Prof. R.G. Raut
Dept. of Information technology
Dr. V.V.P. C.O.E. Ahmednagar
Maharashtra, India

Amit Bhatpure
Dept. of Information technology
Dr. V.V.P. C.O.E. Ahmednagar
Maharashtra, India

Ashish Patil
Dept. of Information technology
Dr. V.V.P. C.O.E. Ahmednagar
Maharashtra, India
mailto:Ashishpatil.ain@gmail.com

Abstract : In cloud computing, customers can accomplish a thriving and direct system for information sharing among social occasion people in the cloud with the characters of low upkeep and little organization cost. At that point, security affirmations to the sharing information records will be given since they are outsourced. Terribly, due to the ceaseless change of the enrolment, sharing information while giving security sparing is as yet a testing issue, especially for an untrusted cloud due to the understanding attack. What's more, to exist arranges, the security of key scattering relies on upon the sheltered correspondence channel, on the other hand, to have such channel is a strong feeling and is troublesome for practice. In this paper, we propose a sheltered information sharing arrangement for component people. Right off the bat, we propose a protected course for key scattering with no sheltered correspondence channels, and the customers can securely gain their private keys from social event director. Plus, the arrangement can fulfill fine-grained get to control, any customer in the social occasion can use the source in the cloud and denied customers can't get to the cloud again after they are rejected. Thirdly, we can shield the arrangement from guile attack, which suggests that rejected customers can't get the principal information record paying little heed to the likelihood that they conspire with the untrusted cloud. In this system, by using polynomial limit, we can accomplish an ensured customer disavowal arrange. Finally, our arrangement can achieve fine profitability, which infers past customers require not to upgrade their private keys for the condition either another customer participates in the social occasion or a customer is surrender from the get-together.

Keywords- Access control, Privacy-preserving, Key distribution, Cloud computing

I. INTRODUCTION

Cloud Computing, with the attributes of normal information sharing and low support, gives a predominant use of assets. In Cloud Computing, cloud organization providers offer an impression of unlimited storage space for clients to host information. It can offer clients some support with diminishing their cash related overhead of information organizations by moving the adjacent organizations structure into cloud servers. However security concerns transform into the rule control as we now outsource the limit of information, which is maybe sensitive, to cloud providers. To defend information security, a run of the mill approach is to encode information records before the clients exchange the mixed information into the cloud. Lamentably, it is difficult to plot a protected and beneficial information sharing arrangement, especially for component aggregates in the cloud. We showed a cryptographic supply system that enables secure information sharing on untrust servers considering the strategies that disconnecting reports into filegroups and scrambling each file_group with a record square key. Regardless, the record square keys ought to be redesigned and circled for a customer disavowal, thusly, the structure had a broad key allocation overhead. . Distinctive arrangements for information sharing on untrusted servers have been proposed. As it may, the complexities of customer intrigue and denial in these arrangements are straightly extending with the amount of information proprietor and the revoked customers. We modified and joined strategies of key procedure quality based encryption, go-between re-encryption and ease back re-encryption to finish fine-grained information get to control without introduction information substance[1][2]. In any case, the single-proprietor way may hinder the use of employments, where any part in the social affair can use the cloud organization to store and give information records to others. We proposed a protected cause arrange by using pack marks and ciphertext-game plan trademark based encryption techniques[2]. Each customer gets two keys after the enlistment while the allocate key is used to disentangle the information which is mixed by the quality based encryption and the social event check key is make use for security ensuring and traceability. On the other hand, the disavowal is not maintained in this arrangement[2][3]. We showed a protected multi-proprietor information sharing arrangement, named Mona. It is ensured that the arrangement can accomplish fine-grained get to control and repudiated customers won't have the ability to get to the sharing information again once they are denied. Regardless, the arrangement will actually encounter the evil impacts of the plot attack by the revoked customer and the cloud . The repudiated customer can use his private key to unravel the encoded information record and get the mystery information after his foreswearing by plotting with the cloud. In the time of report access, as an issue of first significance, the disavowed customer sends his sales to the cloud, then the cloud reacts the relating mixed information record and refusal summary to the renounced customer without checks. Next, the disavowed customer can figure the interpreting key with the help of the ambush count. Finally, this attack can incite the denied customers getting the sharing information and revealing diverse mystery of true blue people[3][4][5].

We showed a protected get to control anticipate mixed information in conveyed stockpiling by summoning part based encryption strategy. It is ensured that the arrangement can achieve imaginative customer foreswearing that joins part based get to control approaches with encryption to secure wide information supply in the cloud. sadly, the affirmations between components are not concerned arrangement easily encounter the evil impacts of ambushes, for example, scheme attack. Finally, this strike can incite edifying delicate information archives. We showed a sensible and versatile key organization framework for trusted agreeable enlisting. By using access control polynomial, it is expected to achieve capable get to control for component bundles. Tragically, the protected way to share the individual immutable adaptable puzzle between the customer and the server is not empowered and the private key will be uncovered once the individual ceaseless helpful secret is gained by the attackers. In this paper, we propose a protected information sharing arrangement, which can accomplish secure key order and information sharing for component group. The guideline responsibilities of our arrangement include: 1. We give a sheltered way to deal with key transport with no protected correspondence channels. The customers can securely get their private keys from social affair boss with no Authentication Specialists in light of the affirmation for individuals when all is said in done key of the customer. 2. Our arrangement can achieve fine-grained get to control, with the help of the social affair customer list, any customer in the get-together can make utilization of the source in the cloud and repudiated customers can't get to the cloud again after they are denied. 3.We propose a sheltered information sharing arrangement which can be protected from assention attack. The denied customers can not have the ability to get the principal information records once they are dismisses paying little respect to the way that they think up with the untrusted cloud. Our arrangement can achieve secure customer dismissal with the help of polynomial limit[5]. 4. Our arrangement can empower dynamic social events adequately, when another customer participates in the get-together or a customer is repudiated from the get-together, the private keys of exchange customers ought not to be recomputed and redesign[6]. 5. Security examination to show the security of our arrangement. In development, execution of reenactments to display the adequacy of our arrangement.

II. PORPOSED APPOROCH

THREAT MODEL, SYSTEM MODEL AND DESIGN GOALS

Threat Model:-

In this paper, we propose our plan considering the, in which the attacker can catch, catch and blend any message at the correspondence channels. With the model, the most ideal approach to shield the data from attack[7].

System Model:-

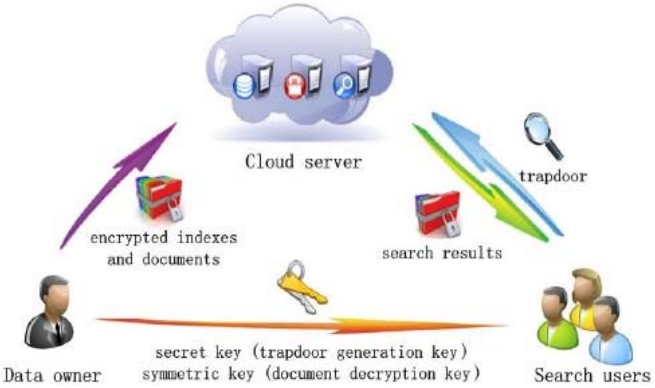


Fig.1. Proposed Framework

Here the proposed model is outlined in figure 1, the framework display comprises of three distinct substances: the cloud, a group manager and countless members.

The cloud, managing by the cloud service providers, gives storage room to facilitating data records in a compensation as-you-go way. then again, the cloud is untrusted since the cloud service providers are effortlessly to wind up untrusted. In this way, the cloud will attempt to take in the substance of the put away data. Group manager will acquire charge of framework parameters era, user registration, likewise, client disavowal. Cluster people (clients) are a course of action of join clients that will store their own specific information into the cloud and confer them to others. In the arrangement, the social event enlistment is effectively changed, in view of the new client ring and client dissent[6][7][8].

Design Goals:-

We depict the principle plan objectives of the proposed plan including key circulation, information secrecy, access control and effectiveness as takes after:

Key Distribution:-

The essential of key transportation is that clients can securely get their private keys from the social event executive with no Certificate Authorities. In other existing arrangements, this reason for existing is skilful by expecting that the communication channel is secure, then again, in our arrangement, we can fulfill it without this strong thought[9].

III. SYSTEM MODULE

Data owner module

The Owner module can perform 4 operations as shown in Figure 3. In upload operation, the data owner selects file F and generates a secret key k for a file. To achieve privacy preserving, the owner creates an encrypted file F =Ek (F). The owner sends encrypted file to the TTP. TTP computes hash value for file H(F) and sends file F to CSP. Key response operation is used by the data owner to grant or revoke access to the outsourced file. In this operation, the data owner checks key requests from authorized users and if data owner wants to grant access then sends key[10][11].

Cloud Service Provider module:

The Cloud Service Provider (CSP) module is used to store and retrieve data. The CSP stores encrypted files F sent by Owner and sends file to authorized users on demand. Figure 4 shows the CSP module[11][12].

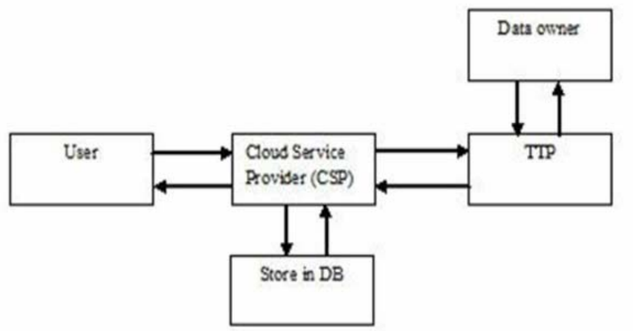


Fig.2. System Modules

Authorized user module :-

Authorized users are set of owners clients who have the right to access the remote data. To access the data, the authorized user sends a data-access request to the CSP and TTP, and receives the data file in an encrypted form F from CSP and hash value of encrypted file H(F) from TTP. To decrypt file authorized user requires secret key k generated by data owner. Authorized user sends key request to the data owner.

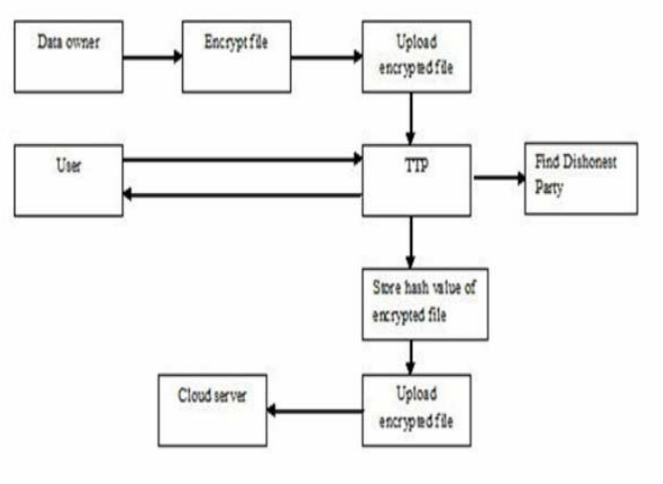


Fig.3. Block diagram of the Authorized user

IV. ALGORITHM

AES encrypts messages through the following algorithm, which is divided into 3 steps[12]:

1. Key Generation

I. Choose two distinct prime numbers p and q.

II. Find n such that n = pq. n will be used as the modulus for both the public and private keys.

III. Find the totient of n, (n) (n)=(p-1)(q-1).

IV. Choose an e such that 1 ¡ e ¡ (n), and such that e and (n) share no divisors other than 1 (e and (n) are relatively prime). e is kept as the public key exponent.

V. Determine d (using modular arithmetic) which satisfies the congruence relation de 1 (mod (n)).

In other words, pick d such that de - 1 can be evenly divided by (p-1)(q-1), the totient, or (n).

This is often computed using the Extended Euclidean Algorithm, since e and (n) are relatively prime and distobe the modular multiplicative inverse of e. diskept as the private key exponent. The public key has modulus and the public (or encryption) exponente. The private key has modulus n and the private (or decryption) exponent d, which is kept secret[11][12][13].

2. Encryption

I. Person A transmits his/her public key (modulus and exponente) to Person B, keeping his/her private key secret.

II. When Person B wishes to send the message ”M” to Person A, he first converts M to an integer such that 0 ¡ m ¡ n by using agreed upon reversible protocol known as a padding scheme.

III. Person B computes, with Person A’s public key information, the ciphertext c corresponding to c me (mod n).

IV. Person B now sends message ”M” in ciphertext, or c, to Person A. 3.

3. Decryption

I. Person A recovers m from c by using his/her private key exponent, d, by the computation m cd (mod n).

II. Given m, Person A can recover the original message ”M” by reversing the padding scheme.

This procedure works since c me (mod n), cd (me)d (mod n), cd mde (mod n). By the symmetry property of mods have that mde mde (mod n). Since de = 1 + k(n), can write mde m1 + k(n) (mod n), mde m(mk)(n) (mod n), mde m (mod n).

From Euler’s Theorem and the Chinese Remainder Theorem, system can show that this is true for all m and the original message cd m (mod n), is obtained document length during comparison[12][13].

V. RESULTS

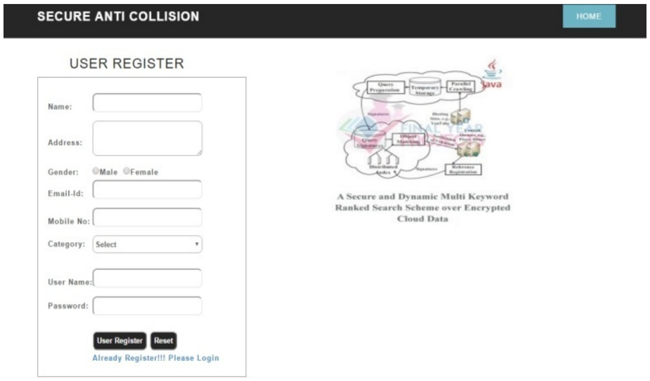
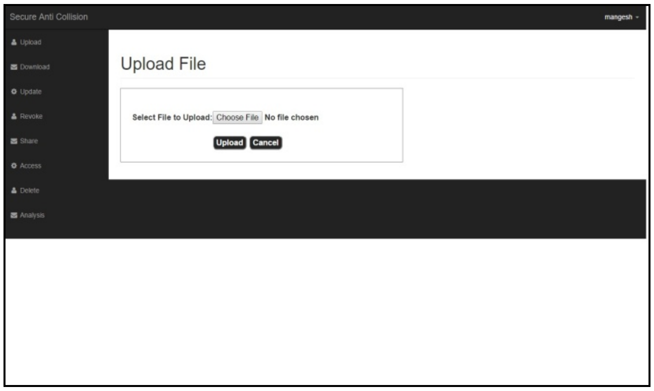
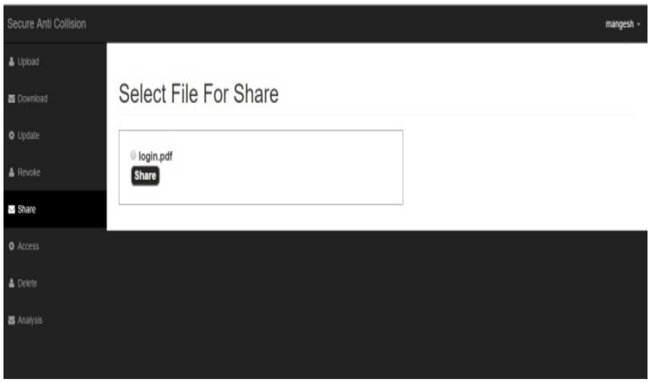


Fig.4. User Registration



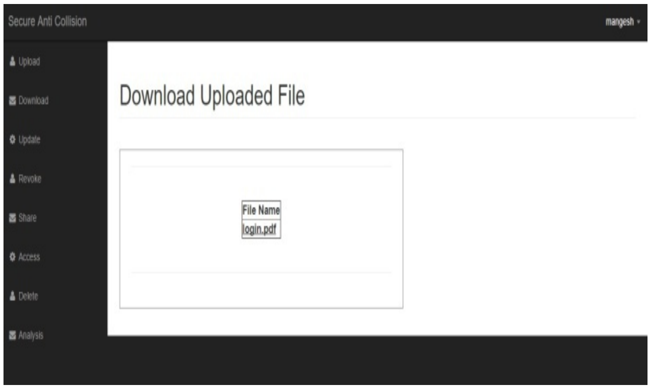
Select File to Upload: Choose File No file chosen

Fig.5. File Upload



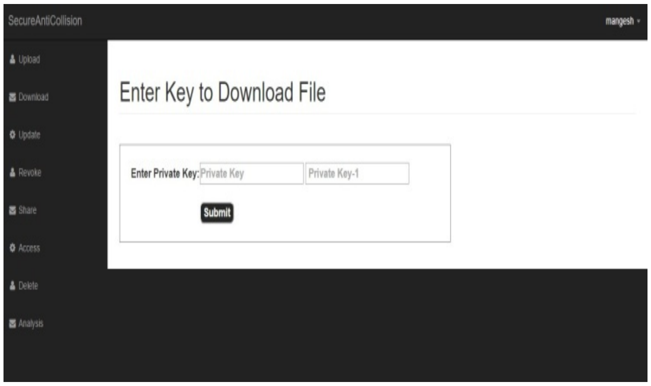
○ login.pdf

Fig.6. File Share



File Name
login.pdf

Fig.7. File Download



Enter Private Key: Private Key Private Key-1

Fig.8. Enter Private Key

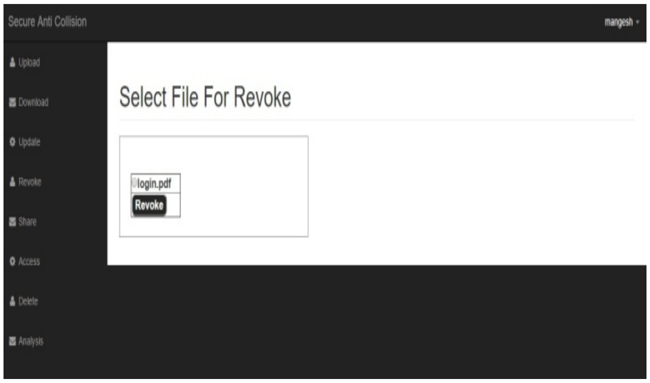


Fig.9. Revoke User

COLCLUSION

This paper proposes methodology, when a communication link is unreliable a sender transmits its signal together with its partner delivering the signal more reliability. Introducing NCAC-MAC the advantages of both NC and CC can be exploited. A network coding aware utility based relay selection strategy to select best relay in an efficient and distributed manner. Motivated by the practical needs in data sharing, we proposed a new notion called forward secure ID-based ring signature. It allows an ID-based ring signature scheme to have forward security. It is the first in the literature to have this feature for ring sig- nature in ID-based setting. Our scheme provides unconditional anonymity and can be proven forward secure unforgivable in the random oracle model the running cost of key generation ,key update ,signing and verifying algorithm log square of the to tal no. of time period. To share media content in a controllable manner. SHA-1 and MD5 algorithm is used for data encryption. In this algorithm is used for large size of data should be encrypted. sharing data on one ring members to another ring members. Then enhance security on data sharing and upload the data on cloud. We consider a provably secure scheme with the same features in the standard model as an open problem and our future research work

REFERANCES

[1] Vidhate, Deepak A and Kulkarni, Parag "Performance enhancement of cooperative learning algorithms by improved decision making for context based application", International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT)IEEE Xplorer, pp 246-252, 2016

[2] Xiaoyan Wang, Student Member, IEEE, Jie Li, Senior Member, IEEE, and Feilong Tang, Network Coding Aware Cooperative MAC Protocol for Wireless Ad Hoc Networks, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 1, JANUARY 2014.

[3] Vidhate, Deepak, A; Kulkarni, Parag (2014):"Improvement In Association Rule Mining By Multilevel Relationship algorithm" in International Journal of Research in Advent Technology, 2(1), pp.366-373

[4] Chunxiao Cai, Yueming Cai, Senior Member, IEEE, Xiangyun Zhou, Member, IEEE, Weiwei Yang, Member, IEEE, and Wendong Yang, Member, IEEE When Does Relay Transmission Give a More Secure Connection in Wireless Ad Hoc Networks?VOL. 9, NO. 4, APRIL 2014.

[5] Vidhate, Deepak, A; Kulkarni, Parag (2014):" A Novel Approach to Association Rule Mining using Multilevel Relationship Algorithm for Cooperative Learning" Proceedings of 4th International Conference on Advanced Computing & Communication Technologies (ACCT-2014), pp 230-236

[6] Gaojie Chen, Member, IEEE, Zhao Tian, Student Member, IEEE, Yu Gong, Member, IEEE, Zhi Chen, Member, IEEE, and Jonathon A. Chambers, Fellow, IEEE Max-Ratio Relay Selection in Secure Buffer-Aided Cooperative Wireless NetworksVOL. 9, NO. 4, APRIL 2014.

[7] Vidhate, Deepak, A; Kulkarni, Parag(2014): ""To improve association rule mining using new technique: Multilevel relationship algorithm towards cooperative learning", International Conference on Circuits, Systems, Communication and Information Technology Applications (CSCITA), pp 241—246, 2014 IEEE

[8] Boyang Wang, Student Member, IEEE, Baochun Li, Senior Member, IEEE, and Hui Li, Member, IEEE has proposed a system on "Public Auditing for Shared Data with Efficient User Revocation in the Cloud".

[9] Vidhate, Deepak, A; Kulkarni, Parag (2013) : "Mining Association Rule by Multilevel Relationship Algorithm: An Innovative Approach for Cooperative Learning" in International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), 2(6), pp. 130-137

[10] Cheng-Kang Chu, Sherman S.M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H Deng proposed a system on "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage.".

[11] Seung-Hyun Seo, Member, IEEE, Mohamed Nabeel, Member, IEEE, Xiaoyu Ding, Student Member, IEEE, and Elisa Bertino, Fellow, IEEE" proposed a system on "An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds".

[12] Mohamed Nabeel and Elisa Bertino, Fellow, IEEE proposed a system on "Privacy Preserving Delegated Access Control in Public Clouds".

[13] Jiawei Yuan and Shucheng Yu, Member, IEEE proposed a system on "Public Integrity Auditing for Dynamic Data Sharing With Multiuser Modification".