ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

Hybrid Key Aggregation and Trust Based Security System

Dr.S.Suma Christal Mary[1], V.Joy Infant Poala[2],P.Sharmila[3], R.Shraddha[4]

Assistant Professor, Department of Information Technology, Panimalar Institute of Technology, Chennai, Tamil Nadu, India. [1]

U.G. Students, Department of Information Technology, Panimalar Institute of Technology, Chennai, Tamil Nadu, India.[2,3,4]

ABSTRACT: Data sharing and security is a vital practicality in cloud computing. The trust management theme that uses a brand new reasonably trust, referred to as foregone conclusion trust that is in a position to predict future trust values supported past behaviours with associate economical and versatile style. The first goal is for every node to discover neighbouring On-off attack nodes by using foregone conclusion trust to acknowledge a pattern of malicious behaviours. The second goal is for badly reputed nodes to own a chance to regain trust so as to stop faulty detections. Efficient delegation of secret writing that of stable size of cipher text is attainable. The new factor is that one will any mixture set of secrete keys and build them compact as one key that may embrace the facility of all keys aggregative. The new created aggregative keys are often sending via email or mobile OTP or tiny memory device to the consumer. Guaranteeing the safety of cloud computing is second major issue and managing attribute to service handiness failures the "single cloud" supplier's incontestable less famed failure and the chance malicious insiders within the single cloud. A movement towards "Multi-Clouds", in different words "Inter Clouds" or "Cloud-Of-Clouds" as emerged recently. This works aim to scale back security risk and higher flexibility and potency to the user.

KEYWORDS*:* Cloud Storage, Key mixture coding, Multi-cloud infrastructure, knowledge Sharing

I.INTRODUCTION

Now a day's cloud is gaining quality. The demand knowledge of information outsourcing is handled and manages of company data. Typically several online free house suppliers provides free space for storing quite fifteen GB take few thousands quantity additional that trust management theme will be wont to aid an automatic decision-making method for associate in nursing access management policy. Since unintentional temporary errors are doable, the trust management resolution should offer a redemption theme to permit nodes to recover trust. However, if a malicious node tries to disguise its malicious behaviours as unintentional temporary errors, the malicious node is also given additional opportunities to attack the system by distressful the redemption theme. Existing trust management schemes that use redemption schemes fail to discriminate between temporary errors and disguised malicious behaviours during which the wrongdoer smartly behaves well and badly as an alternative. In this, gift the vulnerabilities of existing redemption schemes, and describe a replacement trust management and redemption theme which will discriminate between temporary errors and disguised malicious behaviours with a versatile style. The most profit that it's not solely providing flexibility and measurability however it conjointly provides maintainability and accessing the knowledge. Cloud service suppliers have most criticise knowledge of information integrity and privacy as a result of knowledge not store on his own servers the privacy will be accomplish by diving and encrypted knowledge store on service suppliers with the respect of quality access data. In cloud shared travelling environments, things become even worse. Totally different purchasers will be denote on separate Virtual machines however resides on one physical machine. For the info privacy a cryptography resolution are assured in a very sharable knowledge. The quantity abstractive assumption is additional fascinating however user isn't dead happy likewise because the technical employees of service suppliers might not be sure. Assume that Suha puts his all documents in Google

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

drive, and He doesn't wish to show to others attributable to knowledge escape chance Suha cannot feel protection his knowledge. Therefore he encrypts his knowledge mistreatment his own keys before uploading. One day, Suha's partners Pritam raise his to share some knowledge for security a doable choice. Suha opt for it to firmly send Pritam. The secrete keys concerned. Generally, there are 2 ways that for ancient cryptography paradigm:
•Suha encrypts all files with one cryptography key and offers Pritam the corresponding secret key directly.
• Suha encrypts files with distinct keys and sends Pritam the Corresponding secret keys. Example, in enterprise settings, each consumer will transfer encrypted knowledge on the cloud storage server while not the data of the company's master-secret key. Thus, the simplest resolution for the higher than drawback is that Suha encrypts files with distinct public-keys, however solely sends Pritam one (constant-size) cryptography key. Since the cryptography key ought to be directed through a secure channel and unbroken secret, little key size is usually fascinating. For instance, we have a tendency to can't guess nice storage for cryptography keys within the resource-constraint devices like good phones, The good cards or the wireless detector nodes. Especially, these secret keys are sometimes keep within the tamper-proof memory, that is comparatively pricey.

II. LITERATURE SURVEY

1. Identity Bases Encryption (IBE): IBE is a type of a public-key encryption. User's public key (it's a set of encryption that is Identity-String). In IBE, Master secret keys are generated by the private key generator and here on the basis on user's identity secret key is provided. Sender wants to share files. So sender will encrypt the files by making use of user identity and public parameter and sends the files. By making use of his secret key Receiver will Decrypt Files. But out of key-aggregation and IBE, Random oracles assumed by only one. .From various identity key aggregation is inhibited as key to be aggregated.

Advantages:

- Encryption type is public-key encryption.
- This scheme has a dependable party which will grasp secret key.
- Based on the identity, secret key will be provided. Size of decryption key is Constant.

Disadvantage:

- Cipher text size is non-constant.
- Cost of storing cipher text and transmitting it expensive.

2. Symmetric Key Encryption: Benaloh proposed an encryption scheme, where a huge number of keys can be sent rapidly in a broadcast consequence. The key origin is as follows. Initially choose two prime numbers p and q for a composite module. Master secret key will be chosen randomly. Dissimilar prime numbers will be allied with each class. All the prime numbers will be put for the purpose of a public System parameter. The outcome of this is a constant size key. For the purpose of symmetric-key setting, this method is designed so with corresponding secret keys sender should encrypt the files which will not be practicable.

Advantages:

- Cipher text size is constant.
- Decryption key size is constant.
- For storing cipher text and keys it required fewer spaces.
- Construction is simple.

Disadvantage:

- Both encryption and decryption is done by same key.
- Encryptor should get corresponding key to encrypt files.

3. Attribute Based Encryption (ABE): In Attribute Based Encryption method an attribute will be linked with cipher text. From master secret key, the secret key will be derived. This secret key is used to decrypt the files merely if all its associate elements go after the rules. Before Attribute Based Encryption method was introduced, the user who wanted secret key must go to third party and proving he is real by providing his identity and then he was capable to decrypt the file the secret key of user was not allowed to a single center in the ABE Scheme. Instead it was authorized by

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

independent authorities. But still this scheme has drawback i.e. no solidity on secret key. Here in this scheme there is linear rise in key size, with the rise in attributes.

Advantages

- Encryption type is public key encryption.
- Cipher text size is constant.

Disadvantage

- Decryption key size is non-constant.
- Requires more space to store keys.
- The size of Decryption key rises linearly.
- Managing keys is expensive.

4. Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data(2006): Each cipher text to be associated with an attribute allowed by ABE(Attribute-based encryption), and the master-secret key holder can extract a secret key for a policy of these attributes so that a cipher text can be decrypted by this key if its related attribute follows to the policy. For example By using secret key for the policy (2v3v6v8), one can decrypt cipher text tagged with class number 2, 3, 6, or 8Collusion resistance but not the compactness of secret keys is the major concern in ABE. Indeed, the size of the key often rises linearly with the number of attributes it encompasses, or the cipher text-size is not constant.

III. PROBLEM STATEMENT

A. System model:

Our work in this paper involves three parties: the cloud server, the data owner and the admin. The group members are allowed to upload the file. Other user who needs to access the file can access it only if the data owner and the admin response to their request. Shared file and its verification information are both stored in the cloud server.

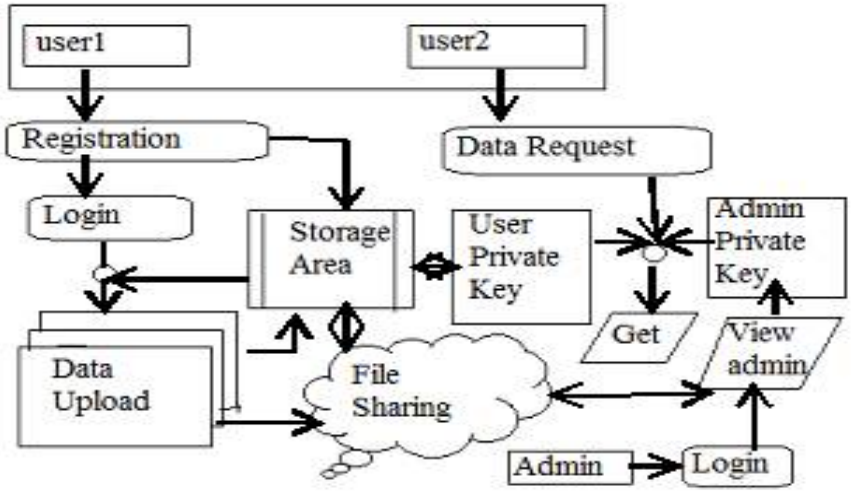

Fig.1:Architectural diagram:

B. Design Goals:

In this Section we describe the main design goals of the proposed scheme including access control, data confidentiality and efficiency as follow:

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

Access Control: First requirement of access control is fold. First, group members and admin are able to use the cloud resource for data transferring and access operation. Second unauthorized cannot access the cloud resources and data files at any time.

Data confidentiality: It requires those unauthorized user are incapable of knowing the contents of shared data without the key generation. New user should decrypt the data using the keys of the data owner and the admin before accessing it.

Efficiency: Group members can share the data files with the other group members in the cloud. The users other than the data owner can download and access the data file with the help of keys been generated by the response of the data owner and the respected group admin

IV. PROPOSED SYSTEM

In proposed System, Predictability Trust (PT) algorithm is used. This trust management framework relies on two key concepts: Predictability Trust and Dynamic Sliding Windows. Predictability Trust works with some other type of trust to detect On-off attacks. It uses sliding windows (SWs) to keep track of previous behaviours so that it can determine how quickly to redeem trust. The main purpose of a Sliding Window is to keep track of the past behaviours of a node. It would be best if we could observe the entire history of each node, but this is unattainable when a system has limited storage and processor speed as in a network. It might be best if we tend to may observe the whole history of every node, however this can be unrealizable once a system has restricted storage and processor speed as during a network during this any range of subdivision of the cipher text is decrypted by victimization the coding key. The matter is resolved by the summary of key combination cryptosystem. In key combination cryptosystem user can encode message not simply public key however additionally to a lower place an symbol. The owner can have the most secret key. The key keys square measure extracted from the most secret key, these secrets keys square measure accustomed encode the less. The extracted key is combination key that is as compact single key.

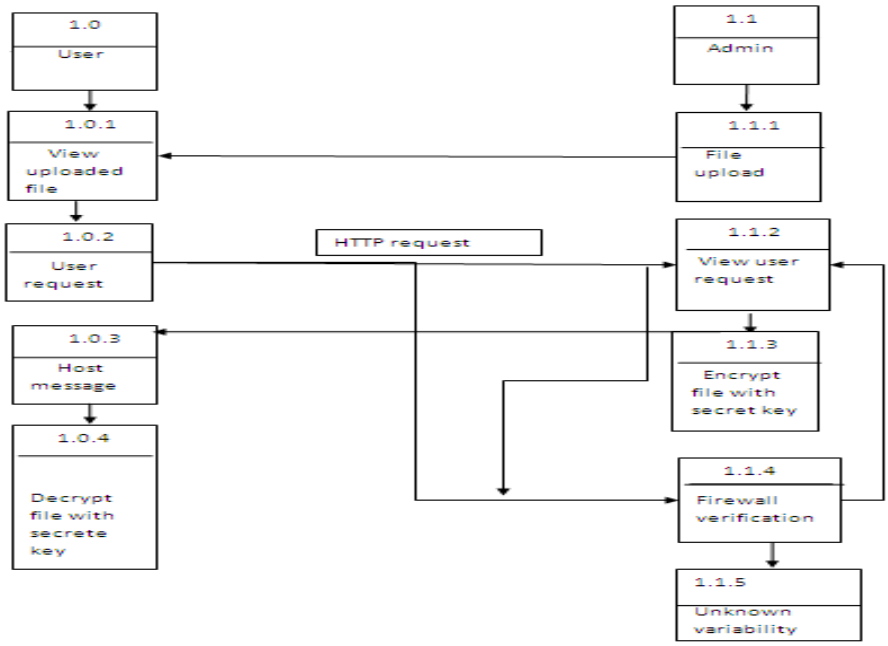

Fig.2:Data Flow Diagram

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

V. IMPLEMENTATION

Our proposed system says that, Initially cloud storage system maintains some database along with the group application details also. If the user already has the account in the cloud storage system then he needs to go to the login page. In login page user enters his ID and password correctly. If the user does not have the account in the cloud storage then user needs to register himself in the database. In registration process, user enters his own details like user name, gender, password, etc. after registration process only, he can access the cloud storage system application.

User register:

- In this module, user can register in that page by giving their details like name, password, email, mobile number, address, etc and that details given by the user store in the database.

User login:

- In this module, login to next page by using username and password. If the username and password is correct, then only can able to login to own page. If it is incorrect, then you cannot able to move to own page.

Admin module:

- In this module, admin login and upload the file. After that the user view the admin uploaded file and then send request to the user.

Finding malicious node:

- In this module, the admin send file to the particular user based on the user requirement. Based on the proposed algorithm, check that there is malicious node and then send a file.

Trust Management:

- In this module, based on the proposed algorithm by the past behavior of node and find temporal errors in the network and finally reach the file to the particular user with trust in the network.

Request File:

- In this module, user who needs the data file access which is been uploaded will leave a request to the data owner and the respected group admin. Details for requesting the files includes file ID, user ID and the date.

Responding to the file request:

- In this module, data owner and the group admin will send response to the requested file by generating the key and sending it to the requested user.

Download File:

- This is the last module where the requested user gets the response keys for the data file he has requested. Using both the keys user can download the file and access it

VI.CONCLUSION

In this work we've got reviewed 3 authentication techniques: Attribute primarily based cryptography(ABE), Identity primarily based cryptography (IBE) and Key mixture Cryptosystem(KAC) the foremost concern in ABE is collusion resistance however not compression of secret keys. Certainly, the cipher text-size isn't constant. In IBE, random set of individualities aren't match with our style of key aggregation. Key mixture Cryptosystem defends user's information privacy by compression the key publicly key cryptosystem that supports delegation of secret key for dissimilar cipher text categories. For forthcoming extension it's needed to order decent cipher texts categories as a result of in cloud cipher texts grows apace and also the limitation is that predefined sure of the quantity of most cipher text categories.To share information flexibly is important issue in cloud computing. Users opt

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

to transfer there information on cloud and among dissimilar users. Outsourcing of information to server could cause leak the personal data of user to everybody. Cryptography may be a one answer that provides to share selected information with needed candidate. Sharing of decipherment keys in secure means plays vital half. Public-key cryptosystems offers allocation of secret keys for dissimilar cipher text categories in cloud storage.

VII. ACKNOWLEDGMENT

Our sincere thanks to our guide Dr.S.Suma Christal Mary who gave us the proper guidance for completing this project. Our special thanks to our Head Of the Department (Information Technology) Dr.A.Joshi who provided us a great support throughout. We would also like to thank Dr.R.josephine Leela Coordinator of our project. We also thank all the other staff members of our department for their help.

REFERENCES

1. I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: A survey,” Comput. Netw., vol. 38, no. 4, pp. 393–422, 2002.
2. S. Marti, T. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” in Proc. 6th Annu.Int. Conf. Mobile Comput.Netw., pp. 255–265, 2000
3. K. Paul and D. Westhoff, “Context aware detection of selfish nodes in DSR based ad-hoc networks,” in Proc. IEEE Global Telecommun. Conf., vol. 1, pp. 178–182, 2002.
4.S.Buchegger and J. Le Boudec, “A robust reputation system for mobile ad-hoc networks,” in Proc. P2PEcon Workshop, http://www.eecs.harvard.edu/p2pecon/program.html, Jun. 2004.
5. P. Michiardi and R. Molva, “Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks,” in Proc. IFIP TC6/TC11 6th Joint Working Conf. Commun. Multimedia Security: Adv. Common. Multimedia Security, pp. 107–121, 2002.
6. S.Bansal and M.Baker, “Observation-based cooperation enforcement in ad hoc networks,” Technical report, Stanford University, NI/0307012, Fig. 10.9G-1B results, 2003.
7. S. Capkun, L. Buttya, and J.-P.Hubaux, “Self-organized public-key management for mobile ad hoc networks,” IEEE Transactions on Mobile Computing, vol. 2, no. 1, pp. 52-64, Jan. – Mar., 2003.
8. J.H. Cho, A. Swami, and I.R. Chen, “Modeling and Analysis of Trust Management with Trust Chain Optimization in Mobile Ad Hoc Networks,” Journal of Network and Computer Applications, vol. 35, no. 3, pp. 1001-1012, May 2012.
9. N.V.Vinh, M.-K. Kim, H. Jun, and N. Q. Tung, “Groupbased public-key management for self-securing large mobile ad-hoc networks,” Int’l Forum on Strategic Technology, pp. 250-253, Oct. 2007.