Indian Journal of Science and Technology, Vol 8(12), DOI: 10.17485/ijst/2015/v8i12/65598, June 2015
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Location as Attribute and Re-Encryption-Based Secure and Scalable Mechanism for Mobile based Applications in Cloud

Chavali Sai Koushik, Koripelli Rohith Reddy, Yeradoddi Rohith Reddy, P. Padmakumari* and A. Umamakeswari

Department of CSE, School of Computing, SASTRA University, Thanjavur - 613401, Tamil Nadu, India;
padmalec.sastra@cse.sastra.edu, psychoushik@outlook.com, reddyrohith705@gmail.com,
koushu.yavs143@gmail.com, aum@cse.sastra.edu

Abstract

When outsourcing the data on to public cloud by data owner from mobile devices which are resource constrained a secure method of encryption model has to be used. As the mobile devices are resource constrained a trusted model is been deployed as an intermediate between mobile user and cloud service provider. The trusted model takes care of securely encrypting, Re-encrypting (upon the criticality of data) the data and uploading on to the cloud and then providing the data to the authenticated user upon his request. Different type of encryption techniques provide security for the data. The choice of encryption technique is made by comparative analysis between different attribute based encryption techniques like Cipher Policy based Encryption (CP-ABE), Location as a attribute encryption key policy based Encryption (KP-ABE). It is found to be the best to provide the required level of security for data outsourcing. The parameters that play a significant role in this technique is obtaining the current latitude and longitude position of the user who want to access the data. If the user is in authenticated location then access can be granted for the data. For this an android application has been developed and a trusted model with data base for storing the data, Re-encrypted data and secure keys for data security. The algorithm used for encrypting the data is RSA algorithm which is a public key encryption technique. If user wants to retrieve his data which is uploaded onto cloud he sends the filename to trusted model and he downloads the encrypted text from cloud, runs decryption algorithm and sends user data to user. If any exceptional case where user tries to access other user's data trusted model simply sends an error message to user who is trying to hack the data and trusted model intimates data owner regarding data hack and Mac-Id of device who is trying to hack. So we can confirm that data encryption is done based on Mac-Id of device.

Keywords: Cloud Computing, Cryptography, Mobile Computing, Scalability, Security

1. Introduction

Information trading to a cloud is suitable for any class of utilizations that obliges information to be kept away. Customers that make utilization of a cloud supplier ordinarily pay for the measure of capacity, related calculation, and measure of system correspondence really expended; they don't cause the capital and support expenses of an in-house arrangement. A noteworthy worry that is regularly not sufficiently tended to by and by, in any case, is that information, of course, are put away free; it might be gotten to and read by a cloud head without learning of the client. Despite the vicinity of contractual security commitments a cloud administrator may not be trusted, if information security is not further upheld through specialized means. An extra hazard is that touchy infor-

*Author for correspondence

mation conveys the constant danger of being captured by an unapproved gathering regardless of shields of the supplier. So it is fundamental that the information ought to be secured while it cloud prepared. Be that as it endless supply of these qualities the expense ought not to be expanded for the portable client. So the quantity of transmissions must be minimized to preserve the battery and over the-air information utilization charges and the measure of reckoning must additionally be minimized[1].

The total effective RAM usage of the device should also be kept in mind during design because mostly the mobile devices are resource shortage devices. Data should ideally be stored in the cloud in encrypted form so that the cloud provider cannot access it. This notion is dependent on the keys being securely managed by an entity outside of the provider's domain. The difficulty arises when new users join the system, and existing ones leave, necessitating new keys to be generated. The encrypted data should ideally be transformed such that it may be unlocked with new keys, without an intermediate decryption step that would allow the cloud provider to read the plaintext; this process is known as data re-encryption. Although it appears to neither be a promising technique in managing encrypted data as access rights evolves over time, current solutions in the literature do not address the issue of high scalability to a sufficient and satisfactory degree; nor do they necessarily strive to lessen the computational and communication burden on users connecting to the cloud from resource constrained mobile devices.

A crucial security feature of Attribute-Based Encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access. Lot of work has been done in the area of the attribute based encryption. One of the ABE is Cipher text-Policy ABE[2]. CP-ABE hence permits to acknowledge understood approval, i.e., approval is incorporated into the scrambled information and just individuals who fulfill the related arrangement can unscramble information. An alternate pleasant highlight is that clients can acquire their private keys after information has been scrambled regarding arrangements. So information can be encoded without learning of the genuine arrangement of clients that will have the capacity to decode, however just indicating the approach which permits to unscramble. Any future clients that will be given a key concerning characteristic such that the approach can be fulfilled will then have the capacity to decrypt the information. The other sort is Key approach ABE. KP-ABE is the double to CP-ABE as in an entrance strategy is encoded into the client's secret key. However, despite the extensive research being conducted in this area, the results have been far from satisfactory. It is hence proposed a new attribute based encryption technique so that the security would be achieved at a good pace in accordance with optimizing the resource usage.

2. Problem Statement

The task of the system is to maintain the user's data security which he is uploading onto public cloud's such as Salesforce, Amazon web-services etc.

- The system recognizes the Mac-Id of the user and the geographical location of user.
- To maintain data security, Re-encryption is performed.

A crucial security feature of Attribute-Based Encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access. Lot of work has been done in the area of the attribute based encryption. One of the ABE is Cipher text-Policy ABE. CP-ABE hence permits to acknowledge understood approval, i.e., approval is incorporated into the scrambled information and just individuals who fulfill the related arrangement can unscramble information. An alternate pleasant highlight is that clients can acquire their private keys after information has been scrambled regarding arrangements[3]. So information can be encoded without learning of the genuine arrangement of clients that will have the capacity to decode, however just indicating the approach which permits to unscramble. Any future clients that will be given key concerning characteristics such that the approach can be fulfilled will then have the capacity to decrypt the information. The other sort is Key approach ABE. KP-ABE is the double to CP-ABE as in an entrance strategy is encoded into the client's secret key. However, despite the extensive research being conducted in this area, the results have been far from satisfactory. It is hence proposed a new attribute based encryption technique so that the security would be achieved at a good pace in accordance with optimizing the resource usage.

2.1 Location Based Encryption Technique

While considering the secure data related to an organiza-

tion the access rights of the data should only be given to the employees of the organization. So here current latitude and longitude range of the organization taken in to account for accessing the data. The users who are at this location can only access the data. If any authenticated user wants to upload data on to the cloud he/she should be inside the organization (geographic location)[11].

3. Existing System

The attribute based encryption techniques used previously are key management while reducing the mobile user computational and communication workload. The thought of this key administration is not that a solitary power does not produce all key material the versatile information holder and cloud substance coordinate to together figure keys. The cloud supplier has inadequate data to translate the client information that it forever stores. Trusted model tries to minimize the communication cost for the data owner. This sort of key era is called as gathering key. What's more this framework is known as gathering key administration. the weaknesses of this sort of procedure is the administrator gets to be in charge of the principle computational workload of the key recovery action, which involves a blending operation, It will likewise regularly cause the correspondence expense of circulating information mystery keys, expelling the onus from the information manager, The supervisor is required to have the capacity to scale appropriately to meet the handling requests, yet requires sufficient customer framework to do as such, (for example, a private cloud), which perhaps uneconomical.

4. Modules

The work presented here are to overcome the failures of existing system and to improve the owner's data security.

4.1 Sending Module

Once a user is authorized in an organization he can upload his data onto any of the public clouds with help of trusted model. The user will be sending text message and his geographic location to trusted user. To send the data user should send a message to trusted model stating which file he is sending and then trusted model can create a room for him and there user data is stored. User data also contains Mac-Id of the device from which the file was uploaded.

4.2 Encryption Model

Once trusted-model receives the user data he encrypts them using RSA encryption algorithm and new concept of encryption technique is used know as Re-Encryption[1,5]. In this concept of re-encryption both the private and public keys will be encrypted after successive intervals. Trusted model takes the user data from the room created for user and encrypts the data .These encrypted text messages are send onto public cloud with user details such as Mac-Id, File name[4,6].

4.3 Decryption Model

If a user wants to retrieve his data from cloud he sends a request to trusted model. Trusted model that keeps track of all user's data searches for particular user who wants to retrieve his data. Trusted model downloads user's encrypted message from cloud and then performs decryption algorithm with encrypted text as input. Once he decrypt's the data he pushes the message to user. If any user is trying to decrypt other user's data, trusted model simply returns error message to him and also he sends a mail to data owner with subject of data hacking and by whom it is happening[6].

4.4 Security Model

This is advancement in proposed system; whenever trusted model receives a request for file retrieving he validates the user. Validation is done against user and his file name i.e., the user who uploads only should retrieve and in case of any exceptions trusted model simply returns error message and alerts data owner. Exceptions are like if we have three authorized users consider A, B, C in an organization and every user uploads their data onto cloud and suppose if user A wants to retrieve data uploaded by C then trusted model sends an error message to A and alerts C[5,7,10].

4.4.1 Location Based Encryption Technique

While considering the secure data related to an organization the access rights of the data should only be given to the employees of the organization. So here current latitude and longitude range of the organization taken in to account for accessing the data. The users who are at this

location can only access the data. If any authenticated user wants to upload data on to the cloud he/she should be inside the organization (geographic location).

4.5 MAC–Id Based Sending or Retrieving of Data from Cloud

Every user has a unique MAC-Id and he can send data on the cloud. The process includes intermediate Middle-Man (Server), whenever a user wants to send a particular data onto cloud he should send a request message to middle –man and then trusted model creates a file where all user data is saved. Once the user data is received, trusted model performs encryption. Here we will be using an advanced security mechanism that the person who uploads a file only should decrypt and if any other user wants to access the data, middle-man simply returns an error message to other user and he alerts the data owner[7].

User who wants to retrieve data from cloud sends a request message to middle-man, where trusted model validates user. Validation is done against Mac-Id and file name which he uploaded. Once this is done, trusted model pushes the data to the user. If any user is trying to hack the system i.e., if any user is trying to access data of another user, trusted model simply returns error message and sends a mail to actual data owner stating which user tried to hack the data.

4.6 RSA Algorithm

The following algorithm is a public key encryption method where the Plain text is encrypted in blocks, here a binary value should be taken with value less than number n. i.e., the block size must be less than or equal to $\log_2(N)$[8].

Calculation for cipher text

C = M^e mod n
M C^d mod n = (M^e) ^d mod n = M^ed mod n

The public key is PU = {e, n}
The private key is PR = {d, n}

The private key consists of {d, n} and the public key consists of {e, n}

Now between two users A, B. B calculates C=M^e mod n and transmits C. On receipt of this cipher text, user A decrypts by calculating M = C^d mod n.

5. Results and Discussions

In this section, a thorough discussion about the result and performance measures of the proposed system is discussed. If users access data more frequently, then there is a proportional increase in computational workload for users consisting of decryption work, which is unavoidable; the data owner is not involved in this activity, however. If cloud data have a shorter lifetime and requires more frequent replacement, then the data owner becomes significantly more engaged due to the associated encryption and key regeneration workload that is required. The system is most suitable, where the same data will be shared many times and not replaced on each consumption[9].

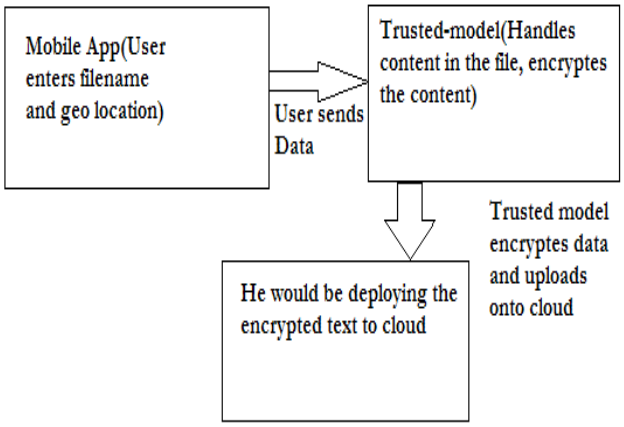

Figure 1. Sending Module.

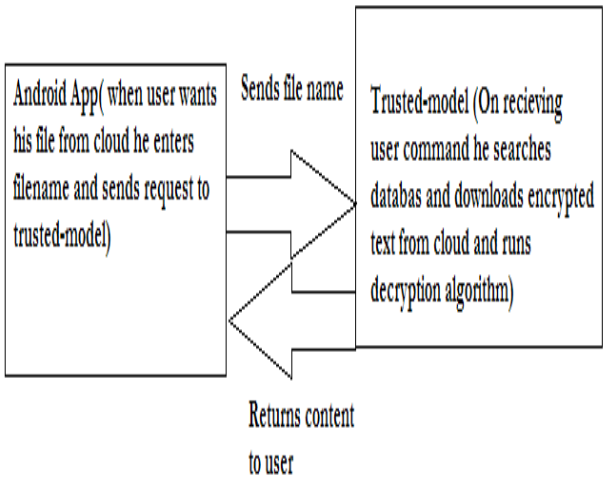

Figure 2. Receiving Module.

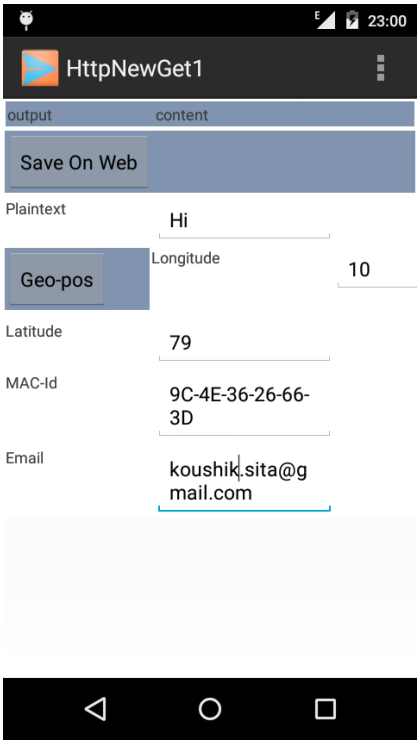

Figure 3. Sending Data to Cloud via Trusted Model.

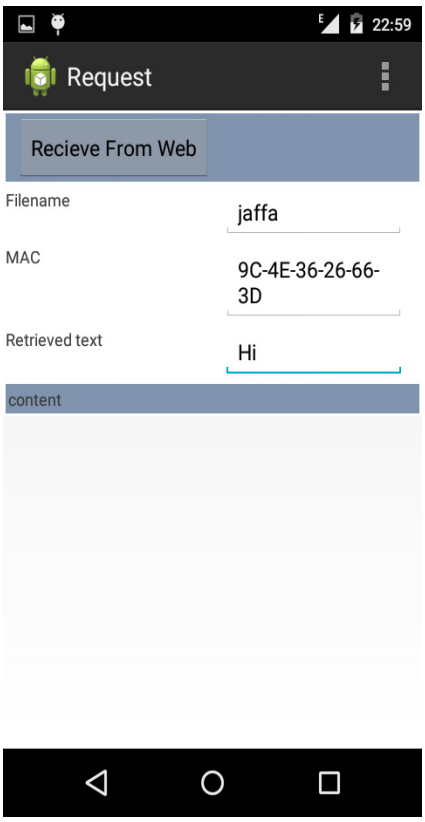

Figure 4. Receiving from Cloud via Trusted Model.

Location based encryption, the manager becomes responsible for the main computational workload of the authentication process The manager is expected to be able to scale accordingly to meet the processing demands, but requires sufficient client infrastructure to do so (such as a private cloud), which may be uneconomical.

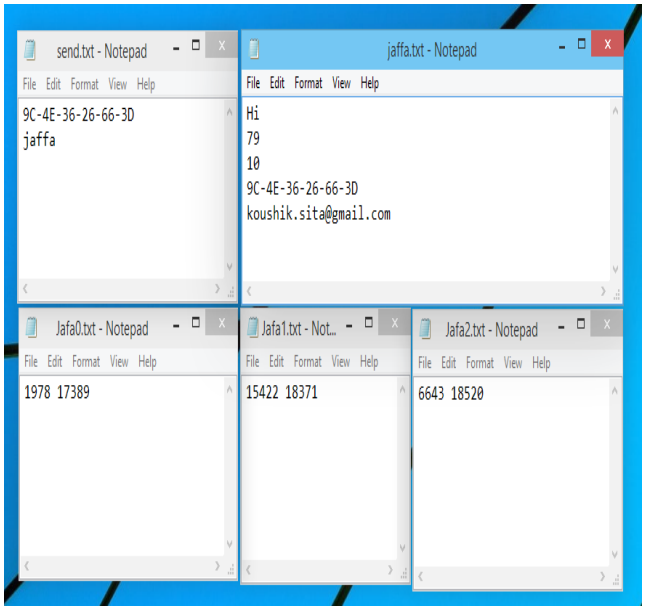

Figure 5. Encrypted Data on Trusted Model.

6. Conclusion and Future work

Attribute-based encryption effectively permits authorized users to access secure content in the cloud based on the satisfaction of an attribute-based policy. The plan has been changed so that an information manager and a trusted power chip in the key era and encryption courses of action such that computationally concentrated cryptographic operations and appeals are minimized for the information holder; this is of significance to a populace of versatile clients that must ration their utilization of battery and use of remote correspondence. Additionally, it allows re-encryption to occur, and thus revocation to become efficient without necessitating existing common remedies and their limitations; an example is the expiration of attributes specified in the attribute-based policy that leads to constant key updates as time elapses. In future, this work can be extended by using multiple attribute based encryption. An authenticated user can upload and retrieve the file even he is out of organization range. Multimedia files also can be encrypted as advancement.

7. References

1. Hasan MA, Tysowski PK. Hybrid attribute-based encryption and re-encryption for scalable mobile applications in clouds. Waterloo, ON, Canada: Centre for Applied Cryptographic Research (CACR), University of Waterloo; 2013.
2. Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption. Proceedings of IEEE Symposium on Security and Privacy (SP '07); 2007. p. 321–34.
3. Lu R, Liang X, Lin X. Ciphertext policy attribute based encryption with efficient revocation. Waterloo, ON, Canada: BBCR, University of Waterloo; 2011.
4. Rong C, Zhao G, Li J, Zhang F, Tang Y. Trusted data sharing over untrusted cloud storage providers. Proceedings of IEEE Second International Conference on Cloud Computing Technology and Science (CLOUDCOM '10); 2010. p. 97–103.
5. Hasan MA, Tysowski PK. Towards secure communication for highly scalable mobile applications in cloud computing systems. Waterloo, ON, Canada: Centre for Applied Cryptographic Research (CACR), University of Waterloo, 2011.
6. Fu K, Ateniese G, Hohenberger S, Green M. Improved proxy re-encryption schemes with applications to secure distributed storage. ACM Trans Inform Syst Secur. 2006 Feb; 9:1–30.
7. Song Y-J, Park N, Do J-M. Attribute based proxy re-encryption for data confidentiality in cloud computing environments. Proceedings of First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering (CNSI); 2011 May. p. 248–51.
8. Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Comm ACM. 1983 Jan; 26(1):96–9.
9. Ren K, Yu S, Wang C, Lou W. Attribute based data sharing with attribute revocation. Proceedings of 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS '10); 2010; p. 261–70.
10. Rajathi A, Saravanan N. A survey on secure storage in cloud computing. Indian Journal of Science and Technology. 2013 Apr; 6(4):4396–401.
11. Jothi Neela T, Saravanan N. Privacy preserving approaches in cloud: A survey. Indian Journal of Science and Technology. May 2013; 5(6):4532–5.