IOP Conf. Series: Materials Science and Engineering **263** (2017) 042069 doi:10.1088/1757-899X/263/4/042069

Privacy authentication using key attribute-based encryption in mobile cloud computing

Mohan Kumar M and Vijayan R

School of Information Technology Engineering, VIT University, Vellore – 632014, Tamilnadu, India

E-mail: rvijayan@vit.ac.in

Abstract. Mobile Cloud Computing is becoming more popular in nowadays were users of smartphones are getting increased. So, the security level of cloud computing as to be increased. Privacy Authentication using key-attribute based encryption helps the users for business development were the data sharing with the organization using the cloud in a secured manner. In Privacy Authentication the sender of data will have permission to add their receivers to whom the data access provided for others the access denied. In sender application, the user can choose the file which is to be sent to receivers and then that data will be encrypted using Key-attribute based encryption using AES algorithm. In which cipher created, and that stored in Amazon Cloud along with key value and the receiver list.

1. Introduction

Cloud computing is getting more popular in nowadays because storage of data in systems costs more and inefficient. So, users were looking into cloud storage which is more efficient and more cost effective. Mobile Cloud Computing is a platform where data processing happens totally outside the mobile, and most of the data storage will be outside that is in the cloud.

Mobile users access different types of mobile cloud computing services from various providers it is challenging to register to service providers and to remember authentication details. So, the data outsourced for storage. While the data of users outsourced the possibility of data stealing is increasing, and the attackers can hack data. So encrypting data before outsourced for storage is important.

Using cloud user uploaded data will be encrypted based on cloud providers encryption algorithm so, the data will not be secured there is chances of outsourcing the data. Though the data is encrypted the security over the data is based on the trust on cloud providers. The users are sharing the data with others they were not sure whether the data is read only by the receivers to whom they sent.

Data sharing within the organization or between the organization and outer world made more difficult for some data not shared to all. So the application with access control over the data to be uploading will resolve this problem where the user can choose their receiver based on that only the access provided. For this own encryption algorithms can be used by which decryption is made controlled by the sender of data over the cloud. The main aim is to make data sharing via the cloud in a much secured manner and data handling based on access control over the data using ABE (Key-

Attribute based Encryption) algorithm. The unprejudiced is to develop a mobile application to make data sharing more secured by implementing Key-ABE in cloud gateway and also providing access control over data based on sender's interest to make data available to all or for a particular group.

2. Related Works

The Author explains that[1] selected content will be encrypted as a document, which conserves the privacy of the users to whom the papers sent, and that based on valid and original group key-management scheme. They have an approach based on access control specifying which user can access which document. They were not getting secret information about the receiver details for encryption using attribute-based access control. They need not send the decryption keys to a receiver that provided with the document by which the decryption keys would generate. Proper criteria for grouping subscribers depends on different requirement have to be developed.

The Author describes that [6] to avoid the problem of key cloning they introduced token-based attribute grounded encryption that provides strong deterrence for key cloning where it reveals some personal information of the users. In token based technique token server breaks the decryption into two-step process and requires interaction with a token server where the trust on the token server is minimal that may reveal personal information of users.

The Author says [5] the attribute-based infrastructure technique, they construct a privacy-preserving and secure system that enables users to share their data among various systems. Secure the necessary records in a distributed computing environment such as cloud computing where the third party provides resources including storage. They used secure infrastructure for designing privacy-preserving electronic record systems where they combined attribute-based cryptography and public key encryption with a keyword search to provide privacy preserving systems. It includes high trust requirement in key generators.

The Author says [7] attribute based encryption allows for fine-grained access control on encrypted data. The key policy allows the data sender to encrypt data under certain attributes and private keys based on access structures that maintain which data the key holder can decrypt. The private generated will be longer which instantiated expressivity or the size of ciphertexts.

3. Privacy Authentication using Key Attribute-based Encryption in Mobile Cloud Computing

In this proposed work the user can send the data to receivers by choosing their receivers to those the data for sharing. After choosing the data to be shared, it encrypted, and then the sender can choose their receiver from the receiver list. In key- Attribute based encryption the security level of the data maintained in key generation. In key-ABE, the document will be encrypted based on the attributes. After encryption, the key provided to the receiver through trusted attribute authority. The key given to receiver can decrypt only the cipher which they have access. The key generated will be maintained as secret in the cloud. When the receiver requests the data the access over data by the receiver will be checked, and then the key will be fetched and validated. The cipher will be decrypted based on the key provided by receiver other data cannot be downloaded.

The challenges in privacy authentication over the sender data by providing access control to the data. The sender of data will add access control by choosing a receiver to whom access of data has given. The Key-Attribute based encryption encrypts the data based on a key generated for that data file, and that stored with receiver list. By getting receiver list those who have access the decryption key sent as email by which privacy protected.

Thus, the benefits of privacy of the data users maintained by providing access control to the data sender.Key-attribute based encryption maintains the security over the data stored in the cloud. Data sharing between sender and the receiver will be more secured. Security over the data maintained by providing encryption to the data to be stored in the cloud and the cipher stored in the cloud.

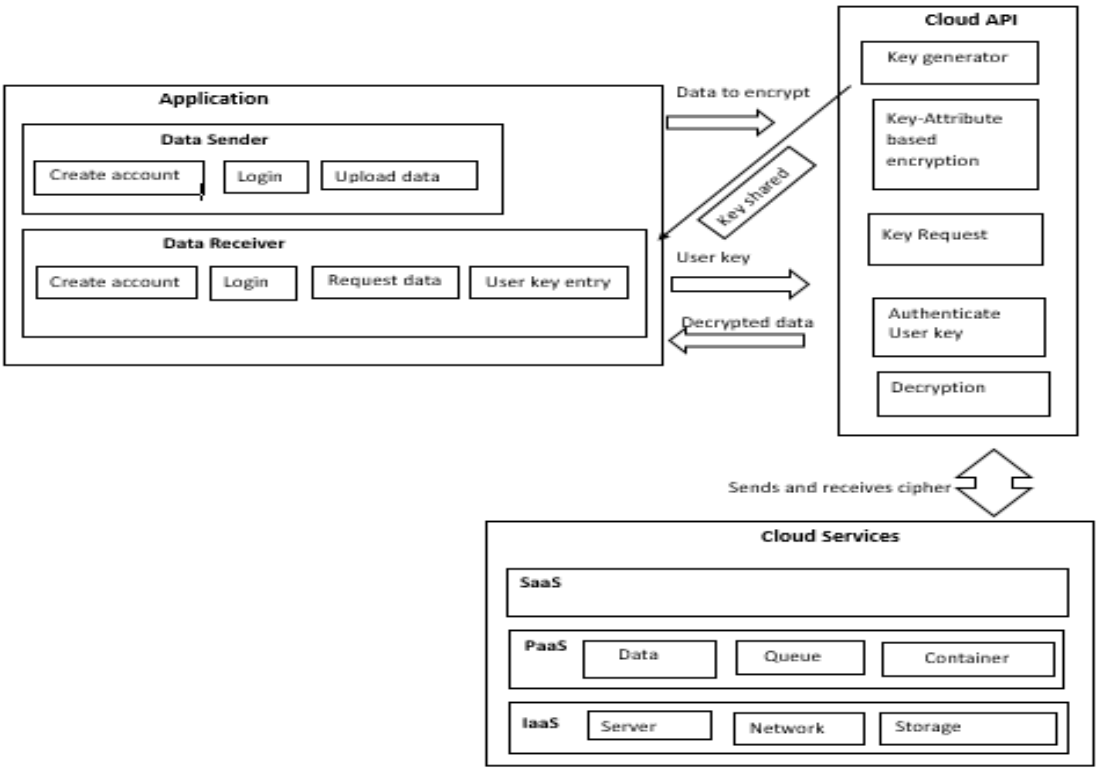


Figure 1. Privacy Authentication Using Key-Attribute Based Encryption System Architecture

3.1. User Interface

This module provides user to interact with the application to encrypt the file which user want to encrypt. The application for mobile enables the user to choose the file from mobile, and it forwarded to cloud gateway where encryption of key policy attribute based encryption implemented.

The user interface (receiver) allows the user those have the key to decrypt data which already authenticate the user by their credentials. The request for data will be made to cloud gateway which requests data from cloud and decryption will be done based on the access control policies.

3.2. Key Generation

This module provides key based on the algorithm and the data's security level. The key generated will be distributed to the users (receiver). In setup algorithm, the master key produced with the attribute of the sender of data. The key generated based on the concatenation of the attribute of the originator and the random number which is unique for the data. With that master key and id as an input, the encryption done, and the cipher generated.

3.3. Encryption

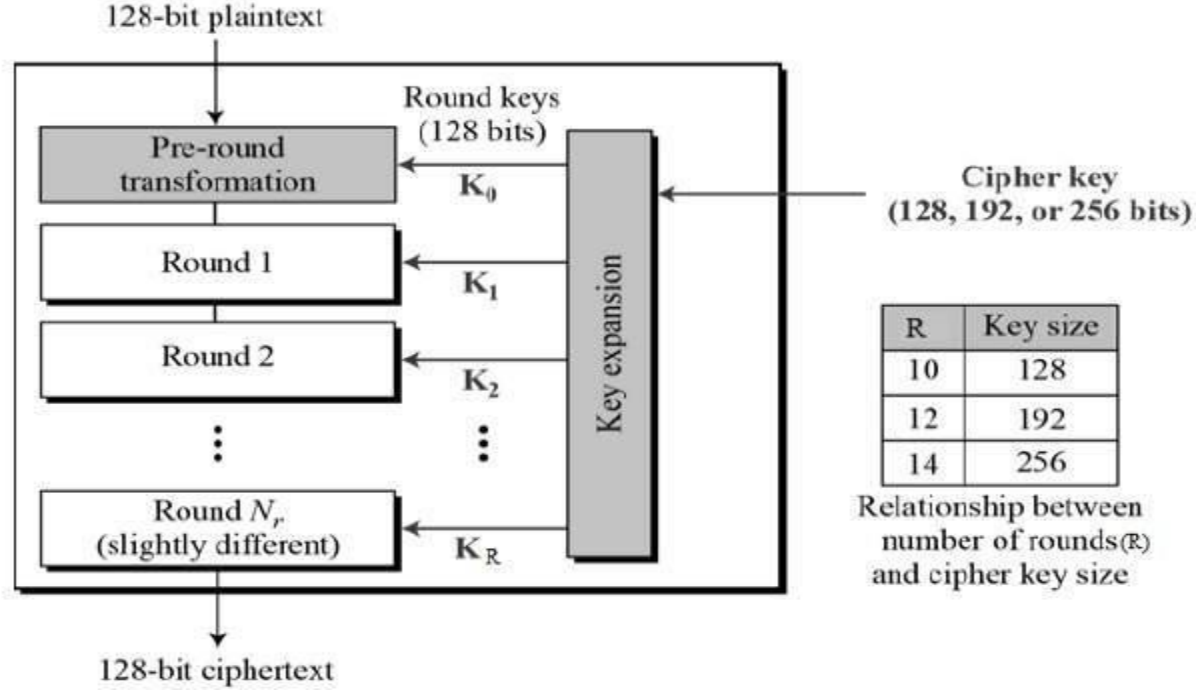
This module provides the user the cipher based on key-Attribute based encryption. Based on the private key the message will be encrypted. The cipher created will be stored in the device storage with the application name. Then the cipher will be stored in cloud storage along with the receivers list those have access to data.

3.4. Decryption

This module decrypts the cipher based on the receiver's key and the original data which sender sends. Based on the private key, attribute the cipher decrypted. On request to cloud the cipher will be fetched, and then user key will be asked, and if the key is valid, then cipher will be decrypted to original data in cloud gateway.

4. AES Algorithm Implementation

The Advanced Encryption Standard(AES) is a symmetric encryption algorithm and it as various features like a Symmetric key symmetric block cipher, 128-bit data, and key. It based on permutation combination network. It executes every one of its calculations on bytes as opposed to bits. AES treats the 128 bits of a plaintext hinder as 16-bytes. These 16-bytes orchestrated in four segments and four lines for handling.



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

Figure 2. AES Structure

In encryption, the data of 128-bit plaintext given as input, and then cipher key generated, and cipher generated. Moreover, the key is also of 128 bit and based on the key by which encryption done will be used to decrypt.

5. Implementation using Android Studio

In Access control as in the figure, 5the receivers registered to the application displayed and the sender of data can add their receivers to those access privileges will be provided. By providing the access control to the sender, the privacy of the data to be shared to receivers is authenticated based on that cloud data is preserved.

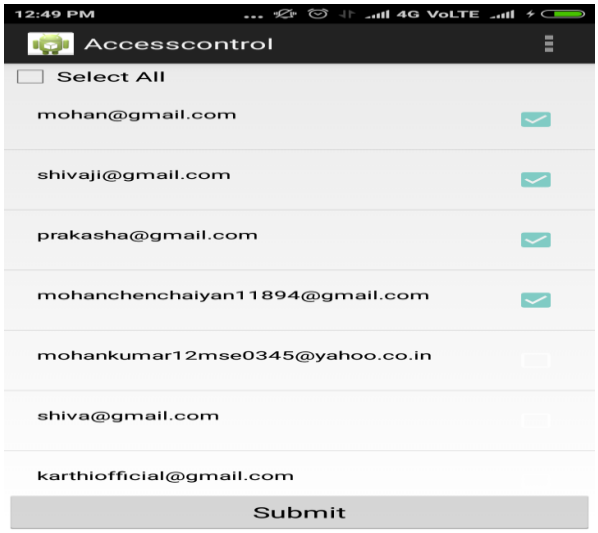


Figure 3. Access Control

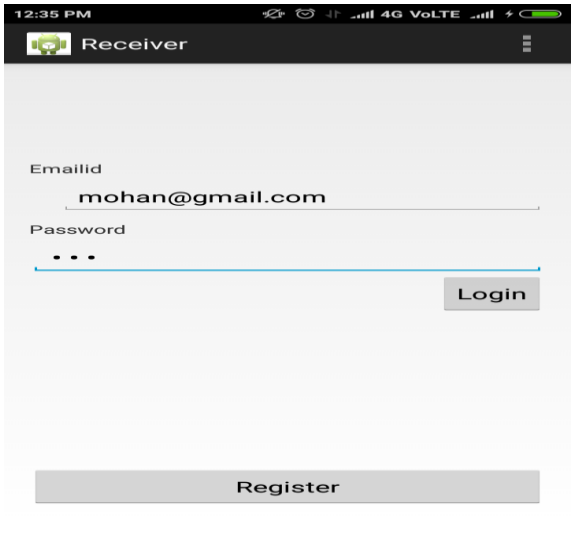


Figure 4. Receiver login

In receiver login as in figure 4 the receivers registered to application those credentials will be validated and then homepage will be displayed. In receiver register, the receivers can provide their details and then they can register to the application with data only they can log into the application. Once the credentials are validated, then the list of files uploaded will be shown. If the receivers have access to the data, they can decrypt it and then it will download.

Figure 5. Access Control

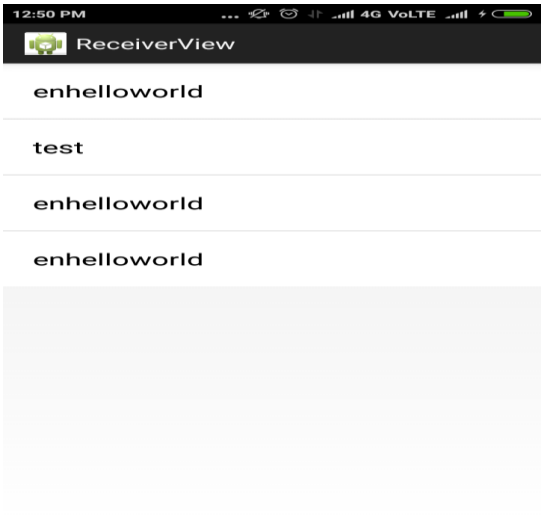


Figure 6. Receiver login

6. Results and Discussion

The application monitors the access to the uploaded data. The application developed will make the data sharing much secured than existing systems. The sender chooses the data file and then encrypt the data using key attribute based encryption and cipher will be stored along with receiver list to those data access have to be provided. Then the receiver can see all file list but they can only files which they have access. When they request file if they have access, they will-will validated over decryption key by which original data downloaded.

Data security of the proposed system is higher than the existing system where the decryption key will be authenticated based on the received credential. Moreover, the access control given to the sender by choosing the receiver.

7. Conclusion

The Privacy Authentication using key-characteristic based encryption causes clients to computerize the protection strategy settings for their transferred documents. The framework gives an exhaustive system to construe protection inclinations in view of the data accessible for a given client. The System effectively tackled the issue of controlling access to the user uploaded the file. The sender of the data will have the privilege to add the recipient to the data to those data has to be shared. The receivers chosen by sender the decryption key shared. The receiver requesting the data the access over the data will be checked based on that only the decryption key will be shared.

In future Application developed is One-way interaction as efforts to make it have two-way interaction. The system improved by making communication between sender and receiver by including chatting facility. As encryption algorithm used in future more advanced encryption techniques also are used to encrypt the data. In developed the id for sender can be produced with that receivers can register to their sender and then the application can be utilized in the real world more effectively.

References

[1] Kathar, M.C.P. and Dhamdhere, V., 2016. Privacy Aware Authentication Scheme for Distributed Mobile Cloud Computing. *International Journal of Engineering Research*, **5**(5), pp.408-410.

[2] Lakshmi, R.N., Laavanya, R., Meenakshi, M. and Dhas, C.S.G., 2015. Analysis of Attribute Based Encryption Schemes. *International Journal of Computer Science and Engineering*, **3**(3), pp.1076-1081.

[3] Lee, C.C., Chung, P.S. and Hwang, M.S., 2013. A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments. *IJ Network Security*, **15**(4), pp.231-240.

[4] Modi, C., Patel, D., Borisaniya, B., Patel, A. and Rajarajan, M., 2013. A survey on security issues and solutions at different layers of Cloud computing. *The Journal of Supercomputing*, **7**(6),pp.1-32.

[5] Narayan, S., Gagné, M. and Safavi-Naini, R., 2014, Privacy preserving attribute-based infrastructure. *International Journal of Computer Science and Engineering Communications*, **112**(8), pp 33-37, 2014.

[6] Hinek, M.J., Jiang, S., Safavi-Naini, R. and Shahandashti, S.F., 2012. Attribute-based encryption without key cloning. *International Journal of Applied Cryptography*, *2*(3), pp.250-270.

[7] Attrapadung, N., Libert, B. and De Panafieu, E., 2011, March. Expressive Key-Policy Attribute-Based Encryption with Constant-Size Ciphertexts. In *Public Key Cryptography*,**6571**, pp. 90-108.

[8] Dwork, C., Lotspiech, J. and Naor, M., 1996, July. Digital signets: Self-enforcing protection of digital information (preliminary version). In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing* (pp. 489-498). ACM.

[9] Lewko, A.B., Okamoto, T., Sahai, A., Takashima, K. and Waters, B., 2010, May. Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption. In *Eurocrypt* ,**6110**, pp. 62-91.

[10] Narayan, S., Gagné, M. and Safavi-Naini, R., 2010, October. Privacy preserving EHR system using attribute-based infrastructure. In *Proceedings of the 2010 ACM workshop on Cloud computing security workshop* (pp. 47-52). ACM.