International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 05 | May -2017 www.irjet.net p-ISSN: 2395-0072

Attribute Based Security

Amrapali Nivrutti Lamkhade[1], Pooja Sanjay Lingayat[2], Jyoti Ganpat Wagh[3] , Prof. Pushpendu Biswas[4]

[1]Amrapali Nivrutti Lamkhade,Comp. dept.,SCOE,Nashik
[2] Pooja Sanjay Lingayat, Comp. dept,SCOE,Nashik
[3] Jyoti Ganpat Wagh, Comp dept.,SCOE,Nashik
[4]Prof. Pushpendu Biswas, HOD of Comp.dept,SCOE,Nashik.

Abstract - *Attribute-based encryption (ABE) is a public-key based one-to-many encryption that allows users to encrypt and decrypt data based on user attributes. As more sensitive data is shared and stored by third-party sites on the internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data is that it can be selectively shared only at a coarse-grained level. Attribute based encryption is a public-key-based one-to-many encryption that allows users to encrypt and decrypt data based on user attributes. A promising application of ABE is flexible access control of encrypted data stored in the cloud using access policies and ascribed attributes associated with private keys and ciphertexts. This functionality comes at a cost. In typical implementation, the size of the ciphertext is proportional to the number of attributes associated with it and the decryption time is proportional to the number of attributes used during decryption. Specially, many practical ABE implementations require one pairing operation per attribute used during decryption. One of the main efficiency drawbacks of the existing ABE schemes is that decryption involves expensive pairing operations and the number of such operations grows with the complexity of the access policy.tn such a system a user provides an untrusted server, say a cloud to translate any ABE ciphertext satisfied by that user's attributes or access policy into a simple ciphertext and it only incurs a small computational overhead for the users to recover the plaintext from the transformed ciphertext. Security of an ABE system with outsourced decryption ensures that an adversary will not be able to learn anything about the encrypted message; however it does not guarantee the correctness of the transformation done by the cloud.*

Key Words: **Attribute-Based Encryption(ABE), Outsourced Decryption, Verified Decryption, Security**.

1.INTRODUCTION

There is a trend for sensitive user data to be stored by third parties on the internet. For example personal email, data and personal preferences are stored on web portal sites such as Google and Yahoo. The attack correlation center, dshield.org, presents aggregated views of attacks on the internet, but stores intrusion reports individually submitted by users.In distributed settings with untrusted servers, such as the cloud, many applications need mechanisms for complex access-control over encrypted data. ABE is a new public key based one-to-many encryption that enables access control over encrypted data using access policies and ascribed attributes associated with private keys and ciphertexts. There are two kinds of ABE schemes: key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE).To protect the data contents privacy via access control various techniques have been proposed. Identitybased encryption (IBE) was introduced first, in which the sender of a message can specify an identity such that only a receiver with matching identity can decrypt it. Few years later, Fuzzy Identity-Based Encryption is introduced, which is also known as Attribute-Based Encryption (ABE). In such encryption scheme, an identity is viewed as a set of descriptive attributes and decryption is possible if a decryptor‟s identity has some overlaps with the one specified in the ciphertext.

1.1 . Motivation of the Project

Cloud computing mainly focuses on sharing computing resources rather than having local servers to handle applications. Cloud computing also provides a prominent service which is storing of data on cloud. In this, customers do not need to store the data on their own servers; rather they can store the data on cloud service provider's servers. It also focuses on cost-effective data storage in which customers have to pay only for the amount of data they need to store for a particular period of time. Customers can easily access their data remotely from anywhere, where the Cloud Service Providers network or Internet can be accessed. There are many risks in single cloud due to which customers are moving towards a new concept of multi clouds which

overcomes all the risks of single cloud and provide benefits of efficient and cost-effective data storage. The goal of this paper is to store the data in encrypted form on multi clouds by using Shamir„s secret sharing algorithm. It also provides an important feature of cost-effective data storage which is beneficial for users to store their sensitive information securely according to their available budgets.

1.2 Literature Survey

In cloud environments if a data owner wants to share data with users he will encrypt data and then upload to cloud storage service. Through the encryption the cloud cannot know the information of the encrypted data. Besides to avoid the unauthorized user accessing the encrypted data in the cloud, a data owner uses encryption scheme for access control of encrypted data. In existing schemes many encryption schemes can achieve and provide security assure data confidentiality and prevent collusion attack scheme. One of the attribute based encryption scheme. According to the access policy two types of these schemes can be classified the key-policy and ciphertext policy attribute-based encryption schemes. The key-policy attribute-based encryption scheme is that the access policy is attached to the user‟s private key and a set of descriptive attributes is in the encrypted data. ABE model was proposed by Sahai and Waters in 2005 year. ABE is the mechanism in which users are allowed to encrypt and decrypt data based on user attributes. User attributes are used to decide the secret key of the user and cipher text. If the set of attributes of the user key matches the attributes of the cipher text; then only decryption of a cipher text is possible. ABE enforces access control through public key cryptography. The central purpose for these models is to provide access control and security. The main aspects are to provide scalability, flexibility and fine grained access control. Considering classical model, this can be achieved only when user and server are in a trusted domain. Another problem with attribute based encryption (ABE) scheme is that data owner needs to use public key of every authorized user to encrypt data. So various ABE based access control schemes have been proposed to overcome this problem. The ciphertext-policy attribute-based scheme is that the access policy is associated to the encrypted data, and a set of descriptive attributes is in the user‟s private key. If a set attribute satisfies the access policy, the user can decipher the encrypted data. In the subsection we review some closely related works including non-interactive verifiable computation, pairing delegation and proxy re-encryption.

2. System Architecture

The general diagram of system has been shown in Fig. As it can be seen, Attribute based Encryption with Verifiable Outsource Decryption will specified the users domain and cloud storage.

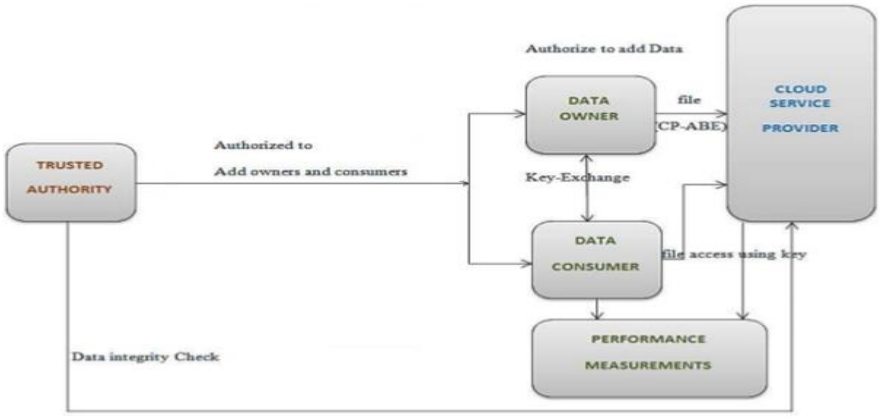


Fig 1.1. System Architecture.

Trusted Authority:

In distributed settings with untrusted servers, such as the cloud, many applications need mechanisms for complex access-control over encrypted data. ABE is a new public key based one-to-many encryption that

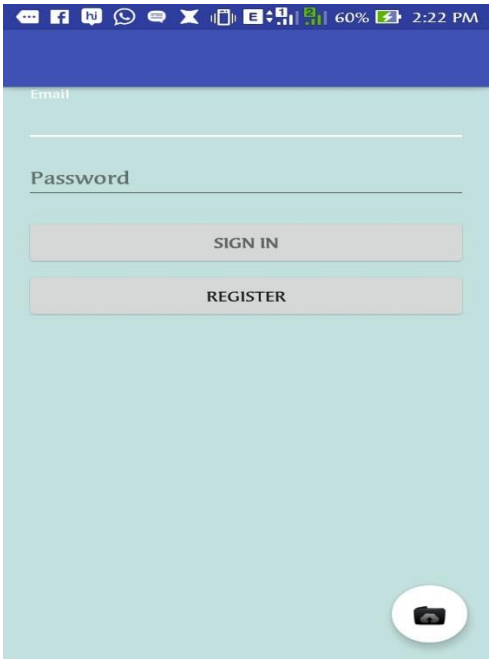
enables access control over encrypted data using access policies and attributes associated with private keys and ciphertexts. There are two kinds of ABE schemes: key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). In a CP-ABE scheme, every ciphertext is associated with an access policy on attributes, and every user‟s private key is associated with a set of attributes. A user is able to decrypt a ciphertext only if the set of attributes associated with the user‟s private key satisfies the access policy associated with the ciphertext. In a KP-ABE scheme, the roles of an attribute set and an access policy are swapped from what we described for CP-ABE: attributes sets are used to annotate the ciphertexts and access polices.

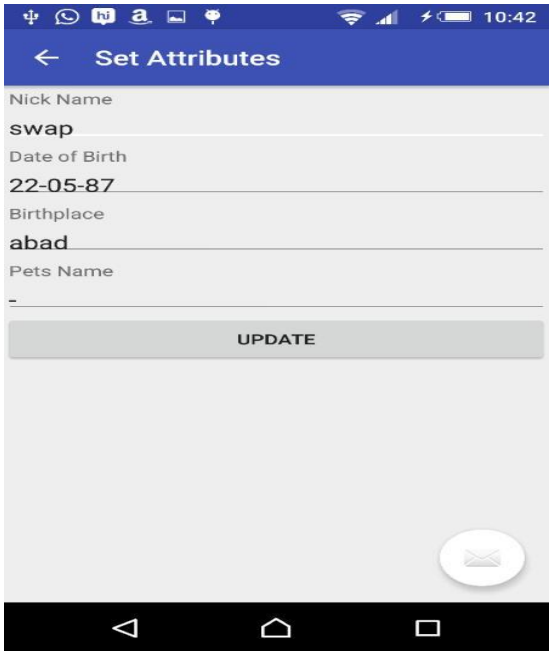
Data Owner or User:

ABE is the mechanism in which users are allowed to encrypt and decrypt data based on user attributes. User attributes are used to decide the secret key of the user and cipher text. If the set of attributes of the user key matches the attributes of the cipher text; then only decryption of a cipher text is possible. ABE enforces access control through public key cryptography. The central purpose for these models is to provide access control and security. The main aspects are to provide scalability, flexibility and fine grained access control. Considering classical model, this can be achieved only when user and server are in a trusted domain.
Cloud Provider:
The cloud provider CP-ABE algorithm and secret key. its provided with verifiability of the cloud‟s transformation and provided a method to check the correctness of the transformation. However the authors did not formally define verifiability.

Cloud Service Provider:

One of the main efficiency drawbacks of the most existing ABE schemes is that decryption is expensive for resource limited devices due to pairing operations, and the number of pairing operations required to decrypt a ciphertext grows with the complexity of the access policy. At the cost of security, only proven in a weak model (i.e., selective security), there exist several expressive ABE schemes where the decryption algorithm only requires a constant number of pairing computations.
Results





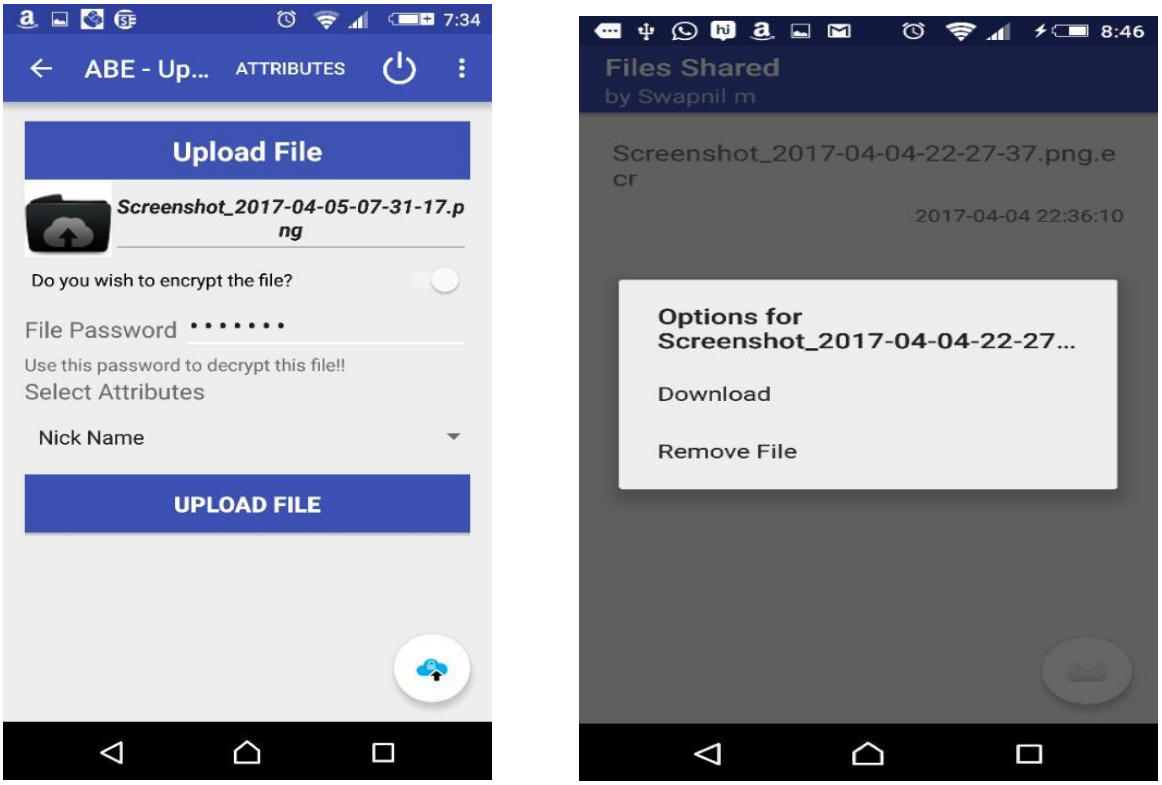


Fig 2. Screenshots of Results

3. CONCLUSIONS

The system is designed for securing the database of CRM on cloud with the help of encryption and CP-ABE and KP-ABE protocol API‟s configuration. It has become easy to encrypt as well as upload data simultaneously on cloud on one click only that is scheduling. The data which are visible to the user on CSP is in Encrypted form. So here the hacker could not understand what exactly the information is about or which record it is. we considered a new requirement of ABE with outsourced decryption: efficiency, verifiability. We proposed Concrete ABE scheme with verifiable outsourced decryption and proved it is secure and verifiable. As scheme substantially reduced the computation time required for resource limited devices to recover plaintexts. Log file describes the logged in details of, user or any other person who is trying to access the account. Compare button which gives the alert sending message (Email) from the Email Server on Email Id and also send text message on your mobile phone. It describes which data has been updated by hackers. But the best part is only data which is visible to hacker on the cloud is updated, the original data is not updated. So when user will get an alert user can again upload data on cloud and the original data is secure and protected from hacker.

REFERENCES

[1] A. Sahai and B.Waters, “Fuzzy identity-based encryption,” in Proc. EUROCRYPT, 2005, pp. 457–473.
[2] .Goyal, O. Pandey,A. Sahai, and B.Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proc. ACM Conf. Computer and Communications Security, 2006, pp. 89–98.
[3] .Ostrovsky, A. Sahai, and B. Waters, “Attribute-based encryption with non-monotonic access structures,” in Proc. ACM Conf. Computer and Communications Security, 2007, pp. 195–203.
[4] .Waters, “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” in Proc. Public Key Cryptography, 2011, pp. 53–70.

[5] unzuo Lai, Robert H Deng, Chaowen Guan, JianWeng, "Attribute-Based Encryption with Verifiable Outsourced Decryption", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, Vol . 8, No. 8, PP. 1343-1354, AUGUST 2013.

[6] inghui Zhang, Xiaofeng Chen, Jin Li, Duncan Wong, Hui Li, "Anonymous Attribute-Based Encryption Supporting Efficient Decryption Test", In Proc of ASIA CCS'13, Hangzhou, China, PP. 511-516 ACM Press. 2013.

BIOGRAPHIES

"Amrapali Nivrutti Lamkhade
Student of B.E(Computer Dept.)
Sanghavi Collage of Engg.,Nashik.
Area of Interest:PG and Business."

"Pooja Sanjay Lingayat
Student of B.E(Computer Dept.)
Sanghavi Collage of Engg.,Nashik.
Area of Interest:Business."

"Jyoti Ganpat Wagh
Student of B.E(Computer Dept.)
Sanghavi Collage of Engg.,Nashik.
Area of Interest:PG and Business."

"Prof.Pushpendu Biswas
HOD of Computer Dept.
in Sanghavi College of
Engg.,Nashik."