International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 05 | May-2016 www.irjet.net p-ISSN: 2395-0072

Attribute-Based Encryption with Verifiable Outsourced Decryption

Manish Kothe,HarshalKarandikar,NikhilWani,SumitTamkhane

Student, Computer Department, Met's BkcIoeNashik, Maharashtra, India

---

Abstract-*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 cipher texts. This functionality comes at a cost. In typical implementation, the size of the cipher text 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. Recently green et al. proposed an ABE system with outsourced decryption that largely eliminates the decryption overhead for users. tn such a system a user provides an untrusted server, say a cloud to translate any ABE cipher text satisfied by that users 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. In this Project we consider a new requirement of ABE with outsourced decryption: verifiability. Informally, verifiability guarantees that a user can effectively check if the transformation is done correctly.*

***Keywords*—Attribute base encryption, Outsource Decryption, AES, Hellman Key Exchange, Verification.**

1. INTRODUCTION--

We give new methods for efficiently and securely outsourcing decryption of ABE ciphertexts. To propose new Attribute Based Encryption method with outsourced decryption with recoverability. Propose System tend to change the initial model of ABE with outsourced decryption with verifiability. Propose system concrete ABE theme with verifiable outsourced decryption and proved that it is secure and verifiable .

The encrypted content as cipher-text is associated with the access policy and the attributes what user uses to encrypt the data is associated with the Private Key. Cipher-Text Policy Attribute Based Encryption (CP-ABE) and Key Policy Attribute Based Encryption (KP-ABE) These two schemes that are associated with the Attribute Based Encryption.

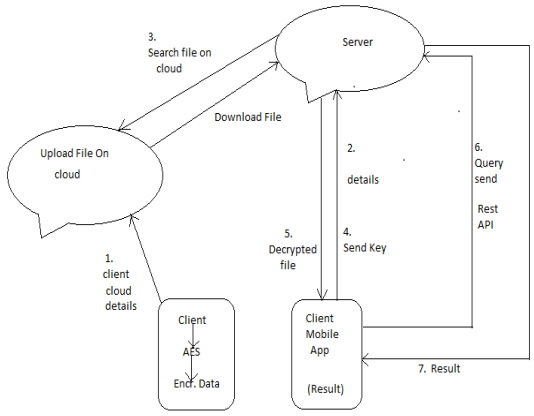
First approach would be for a user to simply hand over their secret key, SK, to the outsourcing service. The service could then simply decrypt all ciphertexts requested by the user and then transmit the decrypted data. However, this requires complete trust of the outsourcing service using the secret key the outsourcing service could read any encrypted message intended for the user.

We are using only Cipher-Text policy attribute based encryption where the user will encrypt the file using the private key. Later, for the decryption purpose the Access Policy plays a very important role. All the attributes of the user that uses to encrypt the data. If the access policy is matched with the attributes only then the user authentication is successful and will be able to decrypt the data that will be sent by the server. ABE also introduce the proxy server that plays a vital role in reducing the work load of the main server. The user once he encrypts the file, the file will be stored in the cloud server. User once in need of file will request to the intermediate server that is proxy server and the proxy server will in turn send the user details to the server and will ask the server to check whether the user is the authorized user or not. Based on the reply of the server, proxy server will takes the further action. If the user is an authorized user the server sends the reply as an authorized user, once getting the reply as such, the proxy server will request the user to send the transformation key. By using the transformation key the proxy server will partially decrypts the file that will be known as transformed cipher-text. The transformed cipher-text is than sent to the user for the complete decryption where the plain text will be generated. As the proxy server is the transparent server there are chances of proxy server taking the wrong file or taking the correct file with the wrong information in it on the request of the authorized user. To eliminate this we are using the checksum, which

verifies whether the file that was encrypted and stored to the server and the file that is been received through the proxy server for the partial decryption that is the transformed cipher-text is the same. Attribute Based Encryption with Verifiable Outsourced Decryption guaranty the security property that no malicious cloud will be able to learn anything about the encrypted data. One of the demerit that is related to the existing scheme of ABE is, for resource limited devices the decryption is very expensive due to pairing operation.

A system for realizing complex access control on encrypted data that we call Ciphertext-Policy Attribute-Based Encryption. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. Previous Attribute Based Encryption systems used attributes to describe the encrypted data and built policies into users keys while in our system attributes are used to describe a users credentials, and a party encrypting data determines a policy for who can decrypt. Thus, our methods are conceptually closer to traditional access control methods such as Role- Based Access Control .

2.SYSTEM ARCHITECTURE --



Attribute Based Encryption With Verifiable Outsourced Decryption

As shown in above figure attribute base encryption with verifiable outsource decryption client by applying AES algorithm on selected text data file and encrypt data file uploaded on cloud side with secret private key.

Then after file successfully uploaded on cloud Mobile app will send cloud details on server.

From server searching requested file on cloud and searched file will download to server. all the data will be in the encrypted format its downloaded as it is which already stored on the cloud.

Then from client receiving side user send private key details on the server. This key details is secret only in between server and receiving side client. This key valid only for that particular session after the session completed the key is invalid.

Decrypt the all file by outsource as server and verified the all data is correct or not then as per the client request from receiving side decrypted Data Send to the mobile app.

Suppose user do not have to access all the data on device then he can generate query from the app and send this query by user to server. server resolving the query and selected data from large file send to user.

After Sending the response from server result display on mobile app.

3.SYSTEM DESCRIPTION--

The System S can be define as
S=(I,O,R1,RSA,Pk,K1,E,C,Q)
I= I is The Set Of Input
O=O is The Set Of Output
K1=K1 is The AES Algo Key
RSA=RSA is The Function Of AES Algo
Pk=Pk is The cloud Key
Function (f1)=Read The User File To Upload And Get Key From User
f1(I,K)=(I1,I2,I3.....In)=(I)
Function(f2)= Function f2 Read File and Apply AES Algo on It and Generate
Encrypted File
f2(K1,f1)=(K1(f1,f2,f3))=(E1,E2.....En)=E
i.e is The Encrypted File
Function F3 Read The App Request and Connect To cloud server
F3(I,K)=(Pk1,Pk2,.....Pkn)=Pk=C
C= C is The cloud server Connection
Function (f4)= it Read Quey From App and Display Result
F4(Q)= (Q1,Q2,Q3,.....Qn)=Q= P

4.CONCLUSION--

A requirement of ABE with outsource decryption with verifiability is considered. Developing the original model of ABE with outsource Decryption. This ABE scheme with Verifiable outsource decryption and proven that it is secure and verifiable . Provided encrypted data is store in cloud and resilient access control . It eliminates Decryption on resource limited devices. This data flow is provide more secure connection between server and small devices .We more improve the data security process by ABE outsourced decryption technique .We use AES algorithm and Hellman Key Exchange technique for improving the

security in data flow between server and small resource limited devices.

REFERENCES--

[1]J. Breckling, "Generic and Efficient Constructions of Attribute-Based Encryption with Verifiable Outsourced Decryption".Xianping Mao, Junzuo Lai, Qixiang Mei, Kefei Chen, JianWeng 2015 IEEE.

[2] S. Zhang, C. Zhu, J. A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology EUROCRYPT 2005, ser. Lecture Notes in Computer Science, R. Cramer, Ed. Springer Berlin Heidelberg,2005, vol. 3494, pp. 457–473.

[3] D. Boneh, A. Sahai, and B. Waters, "Functional encryption: Definitions and challenges," in Theory of Cryptography, ser. Lecture Notes in Computer Science, Y. Ishai, Ed. Springer Berlin Heidelberg, 2011, vol. 6597, pp. 253–273.

[4] R. E. Sorac B. G. Kang, M. S. Lee, and J. H. Park, "Efficient delegation of pairingcomputation," IACR Cryptology ePrint Archive, vol. 2005, p. 259, 2005.

[5] A. B. Lewko and B. Waters, "Decentralizing attribute-based encryption," in Proc. EUROCRYPT, 2011, pp. 568–588.

[6] BrentWaters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In PKC, pages 53–70, 2011.

[7] VipulGoyal, Abishek Jain, OmkantPandey, and AmitSahai. Bounded ciphertext policy attributebased encryption. In ICALP, pages 579–591, 2008.

[8] J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, "Securely outsourcing attribute-based encryption with checkability," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 8, pp. 2201– 2210, Aug 2014.

[9] Allison Lewko, YannisRouselakis, and Brent Waters.Achieving leakage resilience through dual system encryption. In TCC, pages 70–88, 2011.

BIOGRAPHIES--

Manish Kotheappearing for BE degree from the Department of Computer Engineering, MET's Bhujbal Knowledge City IOE, Nashik.

HarshalKarandikarappearing for BE degree from the Department of Computer Engineering, MET's Bhujbal Knowledge City IOE, Nashik.

Nikhil Waniappearing for BE degree from the Department of Computer Engineering, MET's Bhujbal Knowledge City IOE, Nashik.

SumitTamkhaneappearing for BE degree from the Department of Computer Engineering, MET's Bhujbal Knowledge City IOE, Nashik.