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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Study on Attribute Based Encryption With Verifiable Time Stamped Decryption

A new way to strngthn the security of Encrypted Data

Rahul Gaikwad, Madhavi Phalak

Asst. Professor, Dept. of Computer, GF's G.C.O.E Jalgaon, Maharashtra, India

M.E Student, Dept. of Computer, GF's G.C.O.E Jalgaon, Maharashtra, India

ABSTRACT—Keeping Data Secured and in unreadable format while the mail has been delivered to someone else was a big issue in earlier days. With the introduction of Encryption Technology it was little bit secure but the hackers have also managed to extract important information even if it is being encrypted using the available technology. The public key generation depending on the attributes of the specified text to be encrypted, that will generate multiple keys to be used to encrypt or decrypt the data. Additional private key to be added is the server time stamping with the encryption key to ensure that the information shall not be retrieved after specific period of time. Proposed algorithm shall focus on reducing the overhead on the decryption process. Many a cases where the data is get stored on the cloud server and can be accessed from there. I will prove that the proposed way of encryption is more secure and efficient.

KEYWORDS—Attribute Keys, Encryption, Decryption, Time Stamping

I. INTRODUCTION

Information is get stored, Managed and accessed by many user over a server commonly known as Cloud Server. The information can be stored based on the various attribute to which it is associated with. And the use with required information with proper authentication can access it. This is what a normal behavior of Cloud Service. Let's take an example these days many mobile devices offers you cloud storage for your information. And we simply keep some important data such as bank account details or some other secrete information over that server for a particular period of time say 1 year or two year till the phone is not get changed due to some reason. However some other person gets some illegal access to your account and you will be completely loss of your secrete information. This can be very dangerous situation. The Attribute based key Encryption shall be used to solve this kind of problem. As the information stored on the cloud can be encrypted by considering the mobile IMEI number, contact Number, corresponding email address and the local time zone along with the GMT time at the time of saving of information as the attribute to the data before the actual parameters comes into the picture. These attributes can be used to encrypt the information and when any one is trying to access this information the request for the decryption is made with the attributes specified above.

The proposed Attribute based encryption algorithm will generate a public access key based on the Attributes specified to it. The cipher text shall be associated with each of the attributes specified. Following Sections defines the way to access the cipher text via attribute key. One of the major problem that can be faced as it is in many of the ABE algorithms related to decryption of encrypted. Following figure shows how to use Attribute based encryption.

II. OTHER AVAILABLE TECHNIQUES

There are some other techniques available for the attribute based encryption description technology. It includes Concrete Attribute - Based Encryption Scheme with Verifiable Outsourced Decryption in which the focus is on the reducing the overheads of decryption process present within the traditional approach. Another approach described in paper titled Lock-In to the Meta Cloud with Attribute Based Encryption With Outsourced Decryption is it does the vast majority of the work to encrypt a message or create a secret key before it knows the message or the attribute list/access control policy that will be used (or even the size of the list or policy). A second phase can then rapidly assemble an

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

ABE cipher text or key when the species become known. This concept is sometimes called as online encryption when only the message is unknown during the preparation phase; we note that the addition of unknown attribute lists and access policies makes ABE significantly more challenging.

III. RELATED WORK

There are many researchers working towards the security of the information stored in the clouds. Many more research is going on in order to make the information stored in encrypted form. Many researchers introduces the technique to encrypt the information and get is decrypted as and when it is to be accessed by some of the users considered as valid users to access the encrypted information. Even if the information is get accessed by some unauthenticated user it becomes difficult to decrypt it and get proper information. In this regard I have gone through some of white papers describing the information as per requirement in the area of security of information stored in the cloud.

[1] Amit Sahai and Waters at university of California loss Angeles stated in the paper Entitled Fuzzy Identity based Encryption about the fuzz Identity based encryption containing a private key as an identity and a cipher text to be used to decrypt along with fuzzy identity key value. This technique gives us idea about implementing the attribute base information system.

[2] Katsuyuki Takashima at Mitsubishi Electric in his paper about Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption specifies the scheme about the functional encryption large class of relations based on non monotonous relations present inside the product information. Study of this paper provided us the idea about the specific attribute associated with the information and its relation with the actual information. The proposed scheme consists of large contribution about this paper.

[3] Minu George and C. Suresh Gnanadhas writes in the Journal of Engineering and Interdisciplinary Research: 2014 about the Cipher Text Policy Attribute Based Encryption with Heuristics on Cloud Server about the public key for data encryption and decryption of using the attribute based information and cloud encryption and decryption. This paper also describes the importance of access policies and attributes association. The importance of use of attribute based public key for securing data stored in cloud can be highlighted with this white paper published in international journal.

IV. PROPOSED SYSTEM

The entire Attribute based Encryption decryption algorithm shall be divided into to four phases for the implementation purpose. Following is the description of each phase.

Phase 1: Setup Phase is responsible to authenticate the user accessing the proper credential and shall public key to be used for the encryption purpose.

Step 1: m chooses a group G of prime order p and a generator g.

Step 2 choose for every attribute ai where $1 \leq i \leq n$, the authority generates random value {ai, t ∈ * Z p } $1 \leq t \leq ni$ and computes {T i, t = i t a g , } $1 \leq t \leq ni$

Step 3: Compute Y = e (g,g)α where α

Step 4: The public key PK consists of [Y,p,G,G1 ,e ,{{T i,t } $1 \leq t \leq ni$ }$1 \leq i \leq n$]

Step 5: Get the local time zone value and use it as another private key

Phase 2: Is responsible for generation of key to be used for the encryption purpose using the master key generated in the earlier phase.

Step 1: Read the Master Key (PK)

Step 2: Prepare the attribute list from the information to be encrypted / decrypted.

Step 3: Select the random value from trusted authority and compute D_0

Step 4: Now for I = 1 to N compute D_1 D_2 D_3 … D_n

Phase 3: Actually encrypts the information using the generated keys based on the attribute.

Step 1: Read Original Message

Step 2: Read cipher text

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Step 3: Select s ∈ * Z p and compute C0=g s and C~ = M. Ys = M.e (g, g)$^{\alpha s}$
Step 4: Set the root node of W to be s, mark all child nodes as un-assigned, and mark the root node assigned.
Step 5: Execute step no 6, 7, and 8\
Step 6: If the symbol is /\ and its child nodes are unassigned, we assign a random value si , 1 ≤si ≤p-1 and to the last child node assign the value
Step 7: If the symbol is \/, set the values of each node to be s. Mark this node assigned.
Step 8: Each leaf attribute ai can take any possible multi values; the value of the share si is distributed to those values and compute

Phase 4: This is the part of the proposed scheme where you can get back the information encrypted using attribute based encryption algorithm. This phase is responsible to extract the original information.
Step 1: Get the encrypted text from authenticated user.
Step 2: Extract SK (secrete key) and Generate the SK. If found matching then use this key to decrypt the information
Step 3: Extract time zone value for the information decrypted
Step 4: If found within the time limit then extract the information
Step 5: Decrypt the information.

V. CONCLUSION

In this scheme I have considered a new requirement of attribute based encryption that is time stamping. We modified the original model of ABE with verifiable outsourced decryption to include time stamping concept for better security. The proposed method seems to be more secure than any other method used for encrypting the information. This shall be the new information security lock presented for the cloud services. Fast encryption as well as decryption shall be possible with this method. This paper presents you the step by step approach towards the attribute based encryption with time stamping. The proposed method is flexible, robust and reliable.

REFERENCES

1. Amit Sahai and Brent Waters: Fuzzy Identity based encryption published in Advances in Cryptology – EUROCRYPT 2005 Lecture Notes in Computer Science Volume 3494, 2005, pp 457-473
2. Katsuyuki Takashima at Mitsubishi Electric : Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption published in 30th annual conference on Advances in cryptology Pages 191-208.
3. Minu George and C. Suresh Gnanadhas writes in the Journal of Engineering and Interdisciplinary Research: 2014 about the Cipher Text Policy Attribute Based Encryption with Heuristics on Cloud Server about the public key for data encryption and decryption of using the attribute based information and cloud encryption and decryption
4. J Ayo Akinyele, Gary Belvin, Christina Garman, Matthew Pagano, Michael Rushanan, Paul Martin, Ian Miers, Matthew Green, and Avi Rubin. Charm: A tool for rapid cryptographic prototyping. Available from http://www.charm-crypto.com/, 2012.
5. Nuttapong Attrapadung, Javier Herranz, Fabien Laguillaumie, Benoˆıt Libert, Elie de Panafieu, and Carla R`afols. Attribute-based encryption schemes with constant-size ciphertexts. Theor. Comput. Sci., 422:15–38, 2012.
6. Nuttapong Attrapadung, Benoˆıt Libert, and Elie de Panafieu. Expressive key-policy attribute based encryption with constant-size ciphertexts. In Public Key Cryptography, pages 90–108, 2011.
7. Amos Beimel. Secure Schemes for Secret Sharing and Key Distribution. PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.
8. John Bethencourt, Amit Sahai, and Brent Waters. Cipher text-policy attribute-based encryption. In IEEE Symposium on Security and Privacy, pages 321–334, 2007.
9. Dan Boneh, Xavier Boyen, and Eu-Jin Goh. Hierarchical identity based encryption with constant size cipher text. In EUROCRYPT, pages 440–456, 2005.
10. Dan Boneh and Matthew K. Franklin. Identity-based encryption from the Weil pairing. In CRYPTO, pages 213–229, 2001. [8] Dan Boneh, Craig Gentry, and Brent Waters.