ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

Biometric Based Approach for Data Sharing in Public Cloud

Renu S[1], Hasna Parveen O H[2]

Department of Computer Science and Engineering, Cochin College of Engineering and Technology, Kerala, India[1,2]

Abstract: The most important challenge faced by a public cloud is hacking or data intrusion. If an attacker hack the cloud they can manipulate the information or disable the services. We all know that a Biometric system can ensure that rendered services can only accessed by a registered user only. It can identify an authorized user by checking the physiological features of that person. Here I wish to propose a new approach based on biometric encryption for to improve the security of data sharing in public cloud. In this approach we combine the digital key with the biometric image to create bioscrypt. These digital keys can be used as the cryptographic key. During the verification the biometric image is combining with bioscrypt to retrieve the key for the encryption and decryption of the data. The cipher text is then uploading to the public cloud. And an authorized user can retrieve data by his digital key. This approach ensures the data integrity and confidentiality.

Keywords**:** Biometric Encryption, Bioscrypt, Attack, Public Cloud

INTRODUCTION

In public cloud the service providers make the resources and services are accessible to everyone over the internet. Its service may be free or pay as per the use. Due to all these advantages of the public cloud many of the organizations are now use the pubic cloud to store the data. But there are some problems with this public cloud. The most important challenge faced by the public cloud is the confidentiality of its sensitive data. For improve the security of data we will perform encryption and convert the data into the corresponding cipher text [1]. But the major drawback of this system is the key management. In order to avoid this drawback we introduced a mediated certificateless encryption method for the secure data sharing [4]. But this system doesn't assure the confidentiality of the data. It only guarantees the protocol will work properly. So here a new approach is introduced to assure the confidentiality of the sensitive data in the public cloud.

A. Cloud Computing

Cloud computing is defined as a model for enabling ubiquitous, convenient, on- demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models[3].One of the four deployment model is the public cloud. The most recognizable model of cloud computing is the public cloud model, here the cloud services are provided in a virtualized environment, constructed using pooled shared physical resources, and accessible over a public network such as the internet. Public clouds, however, provide services to multiple clients using the same shared infrastructure. The major issues in cloud are the security and privacy. So to improve the storage security the major research areas in cloud are at authorization level, at encryption level and by data segmentation. In this paper we mainly concentrate at the encryption level[3].

B. Biometric Encryption

The word biometric is originated from Greek language and which refers the identification of human by their unique measurable biological characteristics. The common physical characteristic used for security purpose are finger print, eye, voice, hand and face. Here we use physiological measurements. Since they are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods. Biometric identification consists of two stages: enrollment and verification. During the enrollment stage, a sample of the designated biometric is acquired. Some unique characteristics or features of this sample are then extracted to form a biometric template for subsequent comparison purposes. During the verification stage, an updated biometric sample is acquired. As in enrollment, features of this biometric sample are extracted. These features are then compared with the previously generated biometric template[4].

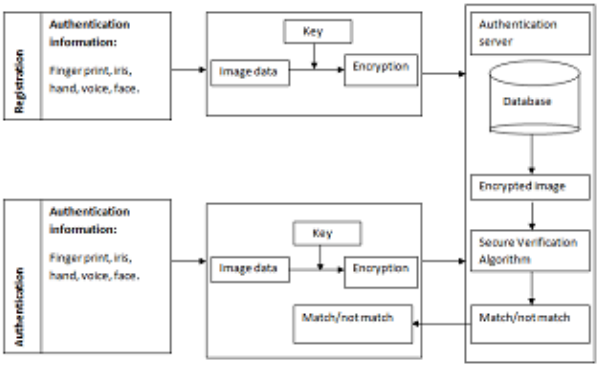

Fig: Biometric Encryption System

After the authentication process if the user is an authorized one he can retrieve the digital key and using this he/she can upload or retrieve the data from the cloud. Here the chance for both active and passive attack is very less due to the presence of bioscript. This approach can ensure the confidentiality and integrity of the data. This system can avoid the drawback of the mediated certificateless encryption.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

II CONVENTIONAL APPROACH FOR DATA SHARING

The conventional approaches for the sensitive data sharing consist of Identity based encryption, Certificateless public key encryption and mediated certificateless encryption.

A. Identity Based Public Key Cryptosystem

This is an important primitive of Identity based cryptography. It can be generate a public key from a known identity value. A trusted third party private key generate corresponding private key. Here it generate a master public key and private key corresponding to the identity ID to compute the private key and public key for the identity ID. So we can perform encryption without the key distribution [5].

The main limitation of this system is that the PKG is highly trusted so no need to perform authentication before decryption this leads to key escrow problem. This is the arrangement of the key for encryption and decryption in an escrow, but under some circumstance a third party can gain access to these keys. Another drawback of this approach is when the PKG is compromised then the entire public-private key pairs also get compromised. So to overcome from this the master private public keys needs to update, this leads to the key management problem.

B. Certificateless Public Key Cryptography

Certificateless public key cryptography is the combination of public key infrastructure and public key cryptosystem [6]. This approach can avoid the problem that caused by key escrow in the above approach. While using this approach a trusted authority cannot recover the session keys and forge signatures because it doesn't knows every bodies private key. This method doesn't need to verify the certificate, thus the certificate related redundancies are not present and also it need less storage and communication bandwidth due to the identifier contain only relevant information. But the main drawback of this approach is computational cost for the paring is high.

C. Mediated Certificateless Encryption

This is a secure approach for data sharing in public cloud. Here the cloud acts as both key generation center and storage. It consists of a SEM which can reduce the cost of decryption by the partial decryption of data inside the cloud [7][8].User decrypt the partially decrypted data by his/her private key. It can instantly revocate the compromised or malicious users. It can easily manage the key and the user revocation. Here the private key of user not needs to change.

But the major drawback of this approach is that it doesn't assure the data confidentiality since the KGC is inside the cloud. It assures only the protocol works properly. And it may be suffer from partial searching. Thus the confidential information of data owner also may be partially searched. Even though the cloud service provider may be trusted the malicious system admin may violate the integrity and confidentiality of the data uploaded into the cloud.

III PROPOSED APPROACH

A . Biometric Based Approach

This approach can overcome the issues that are appeared in the conventional methods. Here we perform a biometric based authentication to ensure that the user is an authorized person. For the authentication purpose we use the physiological measurement as the encrypted image, here it is analysis graph of heartbeat. In this method we use a latest technology called heart rate developed by azmio to sense the heartbeat [9]. It generates an analysis graph which shows our rate. This generated graph can be share by email system. So we can reduce the hardware cost for the registration. This generated image can be combined with a digital key and encrypt it to generate a bioscrypt [10]. This is uploading to the authenticating server. During the verification process both the encrypted images are compared without decryption. Here the Secure Matching Technology uses a unique algorithm to calculate the similarity between the registered data and authentication data even though they are in their encrypted format. It can ensure the security of the data even if the server were out sourced and also the system administrators also doesn't understand the original content of the data since they are not undergo any decryption.

Due to the presence of bioscrypt we can assure the integrity and confidentiality of data. While uploading the data into the cloud we can classify it as whether it is a sensitive data or not. If the shared data is a sensitive one, we can encrypt the data with the bioscrypt and upload to the public cloud. So only the owner has the right to read, write such type of data. Unless if the data is not confidential then we can upload it by performing encryption with the cryptographic key, which is similar to the mediated certificateless encryption.

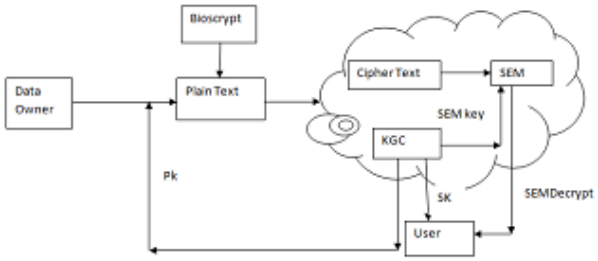

Fig: Proposed Method

B. Entities Of The Approach

The new approach consists of five entities such as data owner, user, KGC, SEM and bioscrypt.

Data Owner: Data owner is the person who is uploading the service or content to the public cloud..

User: User is the person who accesses the service and data that shared by the owner.

- **KGC**: Which means the key generation center where the secrete key, public key and SEM keys are distributed. This KGC is located inside the cloud.
- **SEM**: It is a trusted security mediator which is used for the partial decryption of data. This can reduce the computational overhead of user.

Bioscrypt: It is an encrypted image that can be obtained by combining the cryptographic key with the biometric image.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

This can be used for the secure authentication and can be used to encrypt highly secured data of data owner which doesn't viewed by other.

C. Definitions

The new approach consists of four keys they are secret key, public key, SEM key and the bioscrypt. The first three are generated by the KGC and the bioscrypt can be obtained by combine cryptographic key with the biometric image respectively.

- **Secret Key**: Secret key SK is the key which is not revealing to every person. It is unique value for everyone. It is generated by the key generation center and which is used to decrypt the shared data from the cloud.
- **Public key**: Public key PK is the key that can be used to encrypt the data that are willing to share among the registered users. This key also distribute by the KGC. This is not a unique value for every user. There is no problem when these keys are revealing to anyone.

SEM key: They are the keys which are used for the partial decryption of data by the cloud. This partial decryption can reduce the computational overhead at the user side.

- **Bioscrypt key**: This module can only used when the data uploaded by the data owner is highly confidential or which is not searched by others or only need to search by limited number of users like the higher authorities of an organization

D. Bioscrypt And Instant Heart Rate

Instant heart rate is an android app that can be used to monitor the pulse from our finger tips. It works by tracking color changes in the light that passes through your blood capillaries in the finger tip. First we want to press gently on the camera. Our finger changes the colors during the capillaries expand and contract with respect to the heartbeat [9].The sensor senses these changes using the right algorithm and generates a PPG graph which plots the heart rate. Even though the heart rate may change the characteristics of graph for each individual is unique. This generated graph is shared by email. So during the registration process we can avoid the hardware cost.

The generated graph can be used as biometric image and combine it with a cryptographic key to generate an encrypted data which is called as bioscrypt. During registration this bioscrypt is uploaded to the authentication server. During the authorization the users bioscrypt is compared with the bioscrypt stored in the server without decryption by using security verification algorithm. If the user is an authorized one he/she can proceed to further process. Along with authorization process this bioscrypt can be used to encrypt the data which is highly sensitive and doesnt need to view or shared by other users.

IV HOW ALGORITHM WORKS

Registration

Step1: Image Processing.

- Step2: Key linking, Link the image with the cryptographic key.
- Step3: Create an identification code and upload to the database.

A. Authentication

Step1: Image Processing.

- Step2: Link with the cryptographic key.

Step3: Compare the newly created identification code with the code stored in the Authentication server.

D .Decoding

- **Step1**: Check whether the sensitivity of the data is high, low or medium.
- **Step2**: If the sensitivity is high then perform step3 else go to step4.
- **Step3**: Use the bioscrypt as the key for encrypt the data and perform SHA2 algorithm. And go to Step 5.
- **Step4**: Encrypt the data using the public key.
- **Step5**: Uploading the cipher to the cloud.

D .Decoding

- **Step1**: Check whether the sensitivity of the data is high, low or medium.
- **Step2**: If the sensitivity is high then perform step3 else go to step4.
- **Step3**: print access permission is only for the data owner.
- **Step4**: Retrieve SEM key and decrypt the data partially.
- **Step5**: Decrypt completely using the private key of the user.

V CONCLUSION

In this paper we have proposed the biometric encryption scheme without pairing operations and provided its formal security. Our scheme solves the key escrow problem and revocation problem., we proposed an improved approach to securely share sensitive data in public clouds.

vI FUTURE SCOPE

Even though the system is secure against the active attack like data confidentiality and integrity and free from revocation and key escrow problem because of the biometric encryption and SEM mediators respectively I desired to include a new module to improve the security of data. I wish to embed the cipher text inside a noise and upload to the cloud. So when a attacker enter into cloud and try to modify the content, the actual content is not visible to him. They can only find the noise.

REFERENCES

[1] http://www.interoute.com/cloud-article/what-public-cloud.
[2] en.wikipedia.org/wiki/Public-key-cryptography.
[3] NIST Special Publication 800-145 The NIST Definition of Cloud Computing Peter Mell Timothy Grance http://csrc.nist.gov/publicationce s/nistpubs/800-145/SP800- 145.pdf.
[4] Himabindu Vallabhu, R V Satyanarayana "Biometric Authentication as a Service on Cloud: Novel solution" International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-4, September 2012.
[5] discovery.csc.ncsu.edu/Courses/csc774-S08/reading.../shamir84.pdf.
[6] S. Al-Riyami and K. Paterson. "Certificateless public key cryptography". In C.-S. Laih, editor, Advances in Cryptology - ASIACRYPT 2003, volume 2894 of Lecture Notes in Computer Science, pages 452473. Springer Berlin / Heidelberg, 2003.
[7] Seung-Hyun Seo; Mohamed Nabeel; Xiaoyu Ding; and Elisa Bertino "An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds" IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING 2013.
[8] Zhongmei Wan; Jian Weng;Jiguo Li "Security Mediated Certificateless OF COMPUTERS, VOL. 5, NO. 12, DECEMBER 2010.
[9] www.azumio.com/apps/heart-rate/.
[10] SP.Venkatachalam; P.Muthu Kannan; Dr.V.Palanisamy "Combining Cryptography INSTITUTE OF TECHNOLOGY AND SCIENCE on March 03, 2010.