International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 3 154 – 158

BICRYPTO: An Efficient System to Enhance a Security Protection

[#]1.R.Manimozhi,[#]2.G.Priyadharshini,[#]3.J.ThamizhThendral,[#]4.A.R.Narendrakumar,
[#]1[#]2[#]3,Student,Department of Computer Science and Engineering, University College of Engineering-Thirukkuvalai,[#]4,Assistant Professor,Departmentof Computer Science and Engineering-Thirukkuvalai,NagapattinamDistrict,Tamilnadu,India.

ABSTRACT:In this paper, we propose a two factor data security protection mechanism with factor revocability for cloud storage system. We leverage two different encryption technologies. One is IBE (Identity Based Encryption) and other is PKE (Public Key Encryption). This can be done by the cloud server which will immediately execute some algorithms. Many techniques effectively provide the security for cloud storage data. During transmission of data in cloud environment, encryption is an efficient and widely used technique for data security. It can be done by public key, private and other identical information between the sender and receiver.The security and efficiencyanalysis show that system is not only secure but also practical.

KEY WORDS*: Public key encryption, Identity based encryption.*

*****

I. INTRODUCTION

Cloud computing is the practice of using network of a remote server hosted on the internet to store, manage and process data rather then a local server or a personal computer. Cloud storage is a model of networked storage system where data is stored in pools of storage which are generally hosted by third parties.Cloud computing has been visualized as the next generation of distributed computing in an emerging network field. The National Institute of Standards and Technology (NIST) describes emerging cloud environment by four deployment models, five essential characteristics and three service models. The three models are infrastructure as a service (IAAS), platform as a service (PAAS), and software as a service (SAAS). The characteristics of cloud computing are broad network access, location-independent resource pooling, rapid resource elasticity, on-demand self-service and measured service. The three service models in cloud are private cloud, public cloud, community cloud, and hybrid cloud.

Cryptography:

The word cryptography comes from the Greek words κρυπτο (hidden or secret) and γραφη (writing). Oddly enough, cryptography is the art of secret writing. More generally, people think of cryptography as the art of mangling information into apparent unintelligibility in a manner allowing a secret method of unmingling. The basic service provided by cryptography is the ability to send information between participants in a way that prevents others from reading it. In this book we will concentrate on the kind of cryptography that is based on representing information as numbers and mathematically manipulating those numbers. This kind of cryptography can provide other services, such as integrity checking—reassuring the recipient of a message that the message has not been altered since it was generated by a legitimate source.Authentication—verifying someone's (or something's) identity But back to the traditional use of cryptography. A message in its original form is known as plaintext or clear text. The mangled information is known as cipher text. The process for producing cipher text from plaintext is known as encryption. The reverse of encryption is called decryption. While cryptographers invent clever secret codes, cryptanalysts attempt to break these codes. These two disciplines constantly try to keep ahead of each other. Cryptographic systems tend to involve both an algorithm and a secret value. The secret value is known as the key. The reason for having a key in addition to an algorithm is that it is difficult to keep devising new algorithms that will allow reversible scrambling of information, and it is difficult to quickly explain a newly devised algorithm to the person with whom you'd like to start communicating securely. With a good cryptographic scheme it is perfectly OK to have everyone, including the bad guys (and the cryptanalysts) know the algorithm because knowledge of the algorithm without the key does not help unmingle the information. The concept of a key is analogous to the combination for a combination lock. Although the concept of a combination lock is well known (you dial in the secret numbers in the correct sequence and the lock opens), you can't open a combination lock easily without knowing the combination.

II. RELATED WORKS

We first review some solutions which may contain similar functionalities.For security enhancement using two algorithms. One is Feature Based Finger print Matching Algorithm. Another one is Edge Base Face Detection and Recognition Algorithm.

1.Feature Based Finger print Matching Algorithm- Minutiae Extraction the first stage in our fingerprint verification system is the extraction of minutiae points from a fingerprint image. The algorithm proposed by Jain et al. The first step is the estimation of the orientation field of the fingerprint image. This is followed by the segmentation of the fingerprint area from the background. Both these steps are achieved by computing block-wise gradients of the input image. The ridges are extracted from the input image by applying two masks that adaptively capture the maximum level values along the direction perpendicular to the ridge orientation. Several heuristics are then applied to remove the holes and speckles in the binary ridge map. The extracted ridges are then thinned and minutiae are detected in the thinned image. The location, orientation, and the points on the ridge (sampled at the inter-ridge distance) associated with the minutia are stored for each minutia point. The ridge points are useful in the alignment of the template and the query during the minutiae matching stage.

2.Edge Base Face Detection and Recognition Algorithm:

Step1: Load the image and preprocess it.

Step2: Convert the RGB image to HSV image and calculate the H and S values

Step3: Compare the pixel value of the face and cr and cb constants (H and S values).

If 140<=cr(I,j) && cr(I,j)<=185 &&

140<=cb(I,j) && cb(I,j)<=205 &&

0.01<=hue(I,j) && hue(I,j)<=0.1

Segment (I,j)=1;

Else

Segment (I,j)=0;

Step4: Apply edge detection using Sobel operator.

Step5:Perform binarization and morphological operations to reconstruct the false edges by calculating a mean value.

Step6:Fill the boundaries of hole (used to represent the face region).

BW filled=imfill(BWa.'holes');

Boundaries=bwboundaries(BW filled);

Step7: Plot shape over the face.

3.Diffie-Hellman algorithm-(DH algorithm) is a way of generating a shared secret key between twopeople in such a way that the secret key cannot be intruded by observing the communication over aninsecure communication channel. The distinguishing feature is that you are not sharing information during thekey exchange, you are creating key together. perform encryption with public key of the receiver, and then start encrypting your incoming data with your private key. And even if the incoming data is recorded and later analyzed, there is absolutely no way to figure out what the private key was, even though the exchanges that created it may have been visible. In Diffie Hellman algorithm, initially there will be one private key and public key this two keys oncombination a shared key is generated. In the generation process two common variables are used. The two common variable here we are using as α and q.

Constraints for the variable α & q:

Q-it should be the prime number.

α should be lesser than Q

α-it should be the primitive root of Q

The mechanism of this algorithm is that we use two common variables such that one is a prime numberand the other is primitive root of that prime number. Using these two common variables the private key isselected for both sender and receiver. In this algorithm the public key is generated for both sender and receiver.

III. BIOMETRIC APPROACH

In biometric this approach is used for exchanging secret key between two parties and ensures bothauthentication and non-repudiation. Here, Diffie-Hellman based encryption scheme used, instead of transmitting secret key, user's finger print is stored in database, it is retrieved only at the time of authentication,and no one can pose as a sender, because of his finger print identity. This works puts the cryptanalysts underpressure. The use of this novel algorithm in biometric signature creation improves the electronic bankingsecurity, as the public and private keys are created without storing and transmitting any private information anywhere over the network.In now a days cryptography reports are given below some of the properties or some of the report we identified,

CryptosystemswithTwoSecretKeys:

There are two kinds of cryptosystems that requires two secret keys for decryption. They are certificate less cryptosystem and certificate-based cryptosystem.

Cryptosystems with Online Authority:

It requires an online mediator, referred to a SEM (Security Mediator), for every transaction.

Double encryption:

In this method, the plain text is encrypted using a public key or identity of the user. Again this cipher text is

 ISSN: 2321-8169
154 – 158

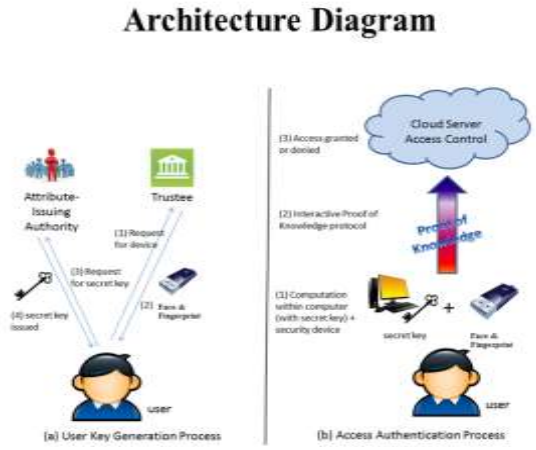
decrypted using some hardware device like pen drive. To decrypt, we first put hardware device, which will decrypt the cipher text once. Finally, secret key of the receiver isused to decrypt to get the original plain text. We should have these two things to encrypt as well as decrypt (Secret key and hardware device).

Disadvantages:

This disadvantage of this method is, if the hardware device is lost or stolen, then it is not possible to decrypt the cipher. Its easy to hack the secret key stored in the personal computer or a trusted server. Computational cost is high**.**

IV. ARCHITECTURE

Our system is an Identity Based Encryption based mechanism. Our system provides two-factor dataencryption protection. One is private key and other bicrypto.

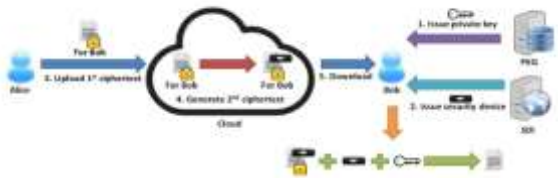


1.1 Authentication Process Diagram

Advantages:

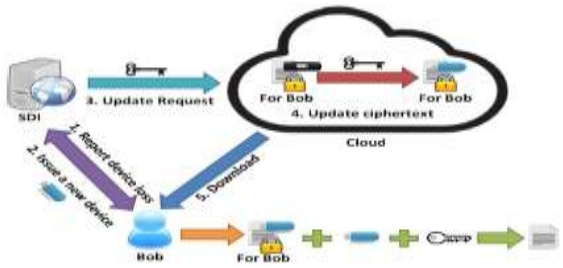
The cloud server cannot decrypt any cipher text at any time. The running time of our prototype is Nano seconds. Intruder still cannot access the record. Enhances the confidentiality of the data Revocability.

Ordinary data sharing:



1.2 Ordinary Data Sharing Diagram

Update Cipher text after issuing a new security device:



1.3 Update Cipher Text After Issuing a New Security Device Diagram

1.Cloud service provider:

In this module we create and upload a media sharing application in cloud environment. Cloud server provider has two models.[1]Backend Server. [2]Cloud UI.

Backend Server:

In this module the backend server module is created for enabling convenient, on-demand network access to a shared pool of configurable computing resources.This can be rapidly provisioned and released with minimal management effort or service provider's interaction.

Cloud UI:

The foreground server provides the services which are always online. A server is often operated by a cloud service provider (CSP), but sometimes, a user able to run own services on the cloud platform too. The foreground services may include web service, database service, media maker service, etc.

2.Cloud Consumer:

This module creates data owner application where User may be a data owner, or a data consumer, or both. A data owner produces (protected or unprotected) media content (text, voice, video, etc.), and uploads the media content to cloud servers. To enforce access control to his data, the data owner assigns access privileges to data consumers whom the data owner may or may not know. A data consumer downloads media content of her interest from cloud servers, and obtains the content based on her attributes and the access policy of the data owner. To this end, the data consumer must obtain from AA a personal secret key bound to her set of attributes. In this data owner-consumer model, the backend servers provide the fundamental platform for storage, networking, etc; the foreground servers provide the interface for media generation, transmission, and computational assistance to users; while AA issues personal secret keys so that access control can be enforced flexibly based on user attributes and media scalability.

3.Security Mediator:

In this module a pair of private key and public key is generated. A private key is kept secretly by the user, while

the corresponding public key is commonly embedded in a certificate digitally signed by a certification authority. The certificate is made available to others for sharing the public key among different users. The private key is used to encrypt the messages send between the communicating machines and both encryption and verification of signature is accomplished with the public key. Biometrics is a method by which a person's authentication information is generated by digitizing measurements (encoded value) of a physiological or behavioural characteristic. Users may biometrically authenticate via their fingerprint, voiceprint, or iris scan using provided hardware device. The device scans the physical characteristic, extracts critical information, and then stores the result. Biometric authentication verifies user's claimed identity by comparing an encoded value with a stored value of the concerned biometric characteristic.

4. Two factor Security mechanism:

In this module split secret key into two parts. First part is stored in the computer and second part is embedded into a hardware device like fingerprint or face, then the drawback is that again without either part, one cannot decrypt the cipher text and also, if the device is lost, anybody who is having that device can break into the computer where the other part of the key is stored and he/she can decrypt all cipher text.

5. Verification Module:

There are three basic resources in the proposed model which includes users, data owner, cloud service provider. The communication between data owner and CSP is authenticated by encrypting the data files and capability list using the private key of owner. At the time of user registration, user is authenticating at owner by signing with his private key, and also data owner authenticated at cloud provider by signing with his private key. The communication between users and cloud service provider is authentication using two step verification approach with the help of security key and bio crypto.

6. Integrity Module:

For the purpose to ensure integrity MD5 is used in the scheme. For checking the integrity user computes a new hash and compares it with the one created by owner and stored in csp. If both new calculated hash and old one match, then integrity violation is reported and a message is sent to the data owner.

V. CONCLUSION

For the evaluation of the Report, the analysis is done based on two parameters they are,
1.Encryption& Decryption time: This is the time that will be taken to encrypt a selected file using AES and Blowfish. 2. Upload & Download time: This denotes the time taken to store the encrypted file on cloud server.

REFERENCES:

[1] J.K. Liu, F. Bao, J. Zhou. By “Short and efficient certificate-based signature. In: International Conference on Research in Networking.”Springer Berlin Heidelberg.2011; 167-178.

[2] B. Libert, D. Vergnaud. By “Unidirectional chosen-ciphertext secure proxy re-encryption.”IEEE Transactions on Information Theory. 2011; 57(3), 1786-1802.

[3] X. Wu, M. C. Wang, W. Zhang, Y. Guo. By “Cloud program with a pricing strategy for Issac in cloud computing. In Parallel and Distributed Processing” Symposium Workshops & Ph.D. Forum (IPDPSW), 2012 IEEE 26th International, IEEE.2012; 2316-2319.

[4] X. Cao, L. Xu, Y. Zhang, W. Wu. By “ Identity-based proxy signature for cloud service in seas.” In: 2012 4th International Conference on Intelligent Networking and Collaborative Systems (INCoS). IEEE.2012; 594-599.

[5] K. Liang, Z. Liu, X. Tan, D. S. Wong, C. Tang. By “ACCA-secure identity-based conditional proxy re-encryption without random oracles.” In: International Conference on Information Security and Cryptology. Springer Berlin Heidelberg.2012; 231-246.

[6] A. Sahai, H. Seyalioglu, B. Waters. By “Dynamic credentials and ciphertext delegation for attribute-based encryption.” In: Advances in Cryptology–CRYPTO 2012. Springer Berlin Heidelberg. 2012; 199-217

[7] J. Shao, Z. Cao. By “Multi-use unidirectional identity-based proxy re-encryption from hierarchical identity-based encryption.” Information Sciences, 2012; 206, 83-95.

[8] H. Guo, Z. Zhang, J. Zhang, C. Chen. By “Towards a secure certificateless proxy re-encryption scheme.” In: International Conference on Provable Security. Springer Berlin Heidelberg. 2013; 8209, 330-346.

[9] C. Wang, S.S. Chow, Q. Wang, K. Ren, W. Lou. By “Privacy-preserving public auditing for secure cloud storage.” IEEE Transactions on computers. 2013; 62(2), 362-375.

[10] J. H. Seo, K. Emura. By “Efficient delegation of key generation and revocation functionalities in identity-based encryption.” In: Cryptographers’ Track at the RSA Conference. Springer Berlin Heidelberg.2013; 343-358.

[11] C.K. Chu, S.S. Chow, W.G. Tzeng, J. Zhou, R.H. Deng.By“Key-aggregate cryptosystem for scalable data sharing in cloud storage.”IEEE Transactions on Parallel and Distributed Systems. 2014; 25(2), 468-477.

[12] H.C. Chen, Y. Hu, P.P. Lee, Y. Tang. By “NC Cloud: a network-coding-based storage system in a cloud-of-clouds.” IEEE Transactions on Computers, 2014; 63(1), 31-44.

[13] L. Ferretti, M. Colajanni, M. Marchetti. By “Distributed, concurrent, and independent access to encrypted cloud databases.”IEEE transactions on parallel and distributed systems, 2014; 25(2), 437-446.

[14] F .F. Moghaddam, M. B. Rohani, M. Ahmadi, T. Khodadadi, K. MadadipouyaBy ”Cloud computing: Vision, architecture and Characteristics.” In: 2015 IEEE 6th Control and System Graduate Research Colloquium (ICSGRC), IEEE. 2015; 1-6.

[15] H. Ziglari, S. Yahya By "Deployment models: Enhancing security in cloud computing environment. In: 2016" 22nd Asia-Pacific Conference on Communications (APCC), IEEE. 2016; 204-209.

[16] Y. Jinzhou, H. Jin, Z. Kai, W. Zhijun. By "Discussion on private cloud Papas construction of large scale enterprise." In: 2016 IEEE International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), IEEE. 2016; pp. 273-278.

[17] R. R. Pavithra, V. R. Nagarajan.By"A survey on certificate revocation scheme using various approaches."Indian Journal of Innovations and Developments. 2016; 5(5), 1-3.

[18] J.K. Liu, K. Liang, W. Susilo, J. Liu, Y. Xiang. By "Two-Factor Data Security Protection Mechanism for Cloud Storage System." IEEE Transactions on Computers, 2016; 65(6), 1992-2004.