ENSURING DATA INTEGRITY USING BIOMETRIC MECHANISM ALONG WITH ACCESS CONTROL AND USER REVOCATION ON CLOUDCOMPUTING

JITHIKA .M
Computer Science and Engineering
Malabar Institute of Technology
jithikarejin@gmail.com

RIJIN I.K
Computer Science and Engineering
Malabar Institute of Technology
rijinik@gmail.com

Abstract

To provide the outsourcible data protection ,Access control mechanism and user revocationis used.Access policy is defined by the data owner for the data user .User revocation is done by the cloud service provider with the updation of ciphertext that is stored in the cloud.Data owner itself and encryption proxy is used for converting the plaintext into ciphertext .For the keygeneration ,attribute authorization is used.RSA & AES encryption methods are used for encryption and decryption process. Data user receives the ciphertext to the decryption proxy then partial ciphertext is generated.From that partial ciphertext exact plaintext will be recomputed .To enhance the security mechanism ,biometric mechanism is used .One-time message authentication code MACLESS is embedded with in the message/image documents for the integrity.MACLESS is generated from the message and one-time biokey using MAC-SHA-1 . One time biokey is the feature vector that is generated from the handwritten signature of the data owner using LBP filter mechanism. For the message documents MACLESS is appended at sender side and recomputed at receiver side.For the image documents MACLESS is hidden in the image through DWT based steganography mechanism., recomputed MACLESS for data integrity checking at the receiver side.This can be used in any environment that uses cloud for data storage to provide security.

1. Introduction

Cloud computing is an emerging technology related with industry,academia and many other applications. Many users outsources their data to the cloud for storage and related services.The outsourcing data contain many secret data. So data privacy is the main concern in the cloud computing. In a cloud computing system, since the cloud service provider (CSP) is usually untrusted, cloud
users may worry about the privacy of their data stored in CSP.So here providing encryption scheme to provide the data security in the cloud enviornement.Also other mechanism that is used to provide data security includes outsourcible user revocation and access control .Access policies are used for each data user with in the system to provide access control.If any user want to revoke from the system data owner can revoke that particular user and that user cannot access the file shared by the data owner.

1.1 Organization

We organize the rest of this paper as follows.We first review the related work in the literatures in Section II. In Section III, we describe the existing system model. Section IV presents the proposed system model .In Section V concludes this paper.

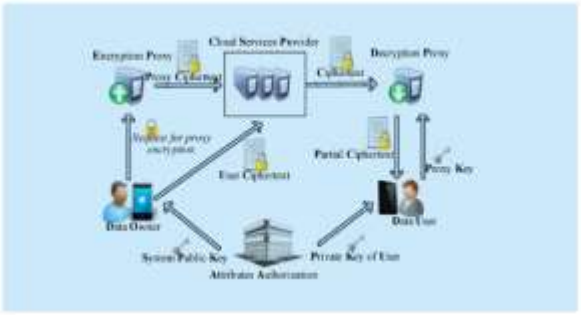
2. Related work

Xiaolong Xu et al.[2] proposed a multi-authority proxy re-encryption scheme with CPABE technique. In this scheme Data owner splits the actual plaintext into two a big block and a small block.The small block is used as a private key to encrypt the big one, and then the encrypted big block will be uploaded to the cloud storage. Wang, Jing, et al.[3] proposed MAVP-FE Scheme.In this scheme every ciphertext is specified with an access policy, a decryptor can access the data if and only if his secret key matches with the access policy.This paper deal with the policy privacy issue and present a mechanism named multi-authority vector policy (MAVP) which provides hidden and expressive access policy for FE. Firstly, each access policy is encoded as a matrix and decryptors can only obtain the matched result from the matrix in MAVP. Junbeom Hur and Dong Kun Noh[4] proposed an Attribute-Based access Control with e_cient Revocation Scheme.The system consists of four kinds of entities, including trusted authority which is a key authority for the managing the key parameters in the system,data owner who owns the data specifies the access policy related to ciphertext,data user who wants to access the data if their access policy matches with that of ciphertext, service provider which is an entity that provides a data outsourcing service. It consists of data servers and a data service manager. Wan, Zhiguo, Jun'E. Liu, and Robert H. Deng.[5] proposed a HASBE access control scheme.In this scheme, a hierarchical attribute-set-based encryption (HASBE) by extending ciphertext-policy attribute-set-based encryption (ASBE) with a hierarchical structure of users is used. Lin, Guoyuan, et al.[6] proposed a MTBAC Scheme based on Mutual trust between Users behaviour and nodes behavior. XuLi and Xingming Sun [7] proposed Image Integrity Authentication Scheme, based on fixed point theory.The data owner transforms an original image into a fixed point image (very close to the original one) of a well chosen transform and sends the fixed point image (instead of the original one) to the receiver; using the same transform, the data user checks the integrity of the received image by testing whether it is a fixed point image and locates the tampered areas if the image has been modified during the transmission. Here all the documents considered as image.This scheme is based GCD transform. Jau-Ji Shen, Ken-Tzu Liu [8] proposed a Image Authentication Technique based on block based staganography.Here the content's authentication code is produced based on the Markov chain. Wang et al.[9] proposed a Biometric Image Authentication Technique.Basedon the concept of Singular value decomposition.Her the scheme makes use of singular values of SVD. Xiaolu Li et al.[10] proposed a Biometric Image Authentication Technique based on chaos and image content to improve the security and secrecy of biometric verification. In this scheme, chaos is used to encrypt the watermark.

3. Existing System

Flexible access control mechanism with outsourcible revocation of users mainly include six communicating parties. Attribute authorization,cloud service provider,data owner,data user,encryption proxyserver and decryption proxy server. .Data owner who possess the data defines the access policies to specified user to share his own message/image documents. Attribute authorization is the only fully trusted third party which is responsible for generating the keys that is used for encryption and decryption. Encryption Proxy (EP), a proxy server for data owner,encrypts files when receives request from DO who have these files.combined encrypted files from data owner and proxy server is stored in the cloud service provider.Decryption Proxy (DP), a proxy server helps data users to decrypt the ciphertext with the proxy key obtained fromthe corresponding data user and converts the ciphertext into partial ciphertext.Data User (DU) is the entity that accesses the confidential data with the private key.. Cloud service provider(CSP) is used mainly for storing user's encrypted data.

Architecture of the existing system in the figure below.



4. Proposed system

In the existing system there is no mechanism for ensuring the integrity and authenticity of the message/documents.So for integrity verification in the proposed system uses a biometric mechanism with the help of handwritten signature of the data owner. From the handwritten signature of the owner can generate one time biokey by the csp .From the biokey and the original message owner can generate a message authentication code that is used to embed/append with in the image/message documents.At the receiver side retrieve the message authentication code and compares with the regenerated authentication code for integrity verification.

4.1 Implementation Details

Figure below shows the architecture of the proposed system implementation.All the user with in the system can register with the CSP using personal details along with the handwritten signature.CSP use the lbp filter mechanism to extract the feature from the handwritten signature and store.This will act as a biokey to generate the message authentication code(MACLESS).When a user wants to upload a message/image document he can login to the system and upload the data.Only the encrypted data is uploaded to the CSP.AES key is generated by the owner itself,by using this can encrypt the data.Also he can contact with the attribute authorization for RSA publickey for the encryption of AES key.Encrypted message and encrypted AES key is combined and store with in the CSP.Before all these encryption happens owner can contact with the CSP to get the biokey for his signature.A MAC-SHA mechanism is used to generate MACLESS from data and biokey.4byte code is gerated.By using DWT with steganography and lsb mechanism each byte from the MACLESS is embed in each region of the image data.For message document append code to the doc .Embedded/Appended data is given for the encryption procedure.A request to the encryption proxy with data can also generate encrypted data by using the AES and RSA mechanism.Also this encrypted data is also stored with in the CSP along with the MACLESS embedded encrypted data. Data owner can share its data to the users based on Access policy.Full permission or partial permission policy is assigned by the owner to the user.An owner can revoke a user from the system by updating the ciphertext along with the removal of access policy.If a user got the shared files from the file owner,he can send a request to decrypt and download that file from the CSP to the decryption proxy.After getting the request decryption proxy contact AA to get the RSA key for encryption proxy result.By using the RSA key generate AES key that is used to regenerate the partial ciphertext.It will send to the data user.By using the RSA public key getting from the AA generate decryption of AES key ,using AES key regenerate the original message/image document from the partial ciphertext..By using the DWT with steganography and lsb retrieval process get each byte of MACLESS from image and combine them to get original MACLESS.Also generate MACLESS from original document and histogram of the data owner.Compare these two MACLESS to verify the integrity.

5. Conclusion

Proposed system promising the integrity and authenticity along with the access control mechanism and outsourcable revocation of data users with the help of a secure one-time message authentication code.MACLESS is generated from the onetime bio key.Biometric mechanism is used to generate one time bio key from the handwritten signatures of the sender. LBP filter mechanism is used to extract the features from the handwritten signature of the data owner.

References

[1] Shungan Zhou, Ruiying Du, Jing Chen, Jian Shen, Hua Deng, and Huanguo Zhang. Facor: Flexible access control with outsourceable revocation in mobile clouds.China Communications,13(4):136–150, 2016

[2] Xiaolong Xu, Jinglan Zhou, Xinheng Wang, and Yun Zhang. Multi-authority proxy re-encryption based on cpabe for cloud storage systems.Journal of Systems Engineering and Electronics, 27(1):211–223, 2016.

[3] Jing Wang, Chuanhe Huang, Kan Yang, Jinhai Wang, Xiaomao Wang,and Xi Chen. Mavp-fe: Multi-authority vector policy functional encryption with efficient encryption and decryption.China Communications,12(6):126–140, 2015.

[4] Junbeom Hur and Dong Kun Noh. Attribute-based access control withefficient revocation in data outsourcing systems.IEEE Transactions on Parallel and Distributed Systems, 22(7):1214–1221, 2011

[5] Zhiguo Wan, Jun'e Liu, and Robert H Deng. Hasbe:a hierarchical attribute-based solution for flexible and scalable access control in cloud computing.IEEE transactions on information forensics and security,7(2):743–754, 2012.

[6] Guoyuan Lin, Danru Wang, Yuyu Bie, and Min Lei. Mtbac: A mutual mtrust based access control model In cloud computing.China Communications, 11(4):154–162, 2014.

[7] Xu Li, Xingming Sun, and Quansheng Liu. Image integrity authentication scheme based on fixed point theory. IEEE Transactions on Image Processing, 24(2):632–645, 2015.

[8] Jau Ji Shen and Ken Tzu Liu. A novel approach by applying image authentication technique on a digital document. In Computer, Consumer and Control(IS3C), 2014 International Symposium on, pages 119–122.IEEE,2014.

[9] De-song Wang, Jian-ping Li, and Xiao-yang Wen. Biometric image integrity authentication based on svd and fragile watermarking. In Image and Signal Processing, 2008. CISP'08. Congress on , volume 5, pages 679–682. IEEE, 2008

[10] Xiaolu Li, Zhi Qi, Zhiqiang Yang, and Jun Kong A novel hidden transmission of biometric images based on chaos and image content. In Education Technology and Computer Science, 2009 . ETCS'09. First International Workshop on, volume 1, pages 21–25. IEEE, 2009.

[11] Zaid Ameen Abduljabbar, Hai Jin, Ali A Yassin, Zaid Alaa Hussien,Mohammed Abdulridha Hussain, Salah H Abbdal, and Deqing Zou.Robust scheme to protect authentication code of message/image documents in cloud computing. In 2016 International Conference on Computing, Networking and Communications (ICNC), pages 1–5. IEEE, 2016