International Journal of Computational Intelligence Research
ISSN 0973-1873 Volume 12, Number 2 (2016), pp. 187-191

http://www.ripublication.com

# Protection of Authentication Code Embedded with in the Message/Image Documents along with Facor Mechanism

**Ms. Jithika.M[1] and Mr. Rijin. I.K[2]**

*[1]Malabar Institute of Technology, Anjarakandy.*
*E-mail: jithikarejin@gmail.com*
*[2]Malabar Institute of Technology, Anjarakandy.*
*E-mail: rijinik@gmail.com*

**Abstract**

Access control mechanism is to provide outsourcable data security.FACOR is a flexible access control mechanism with outsourceble revocation done by the CSP.The time consuming encryption and decryption in the system is outsourced to the encryption/decryption proxy servers.There is an attribute authorisation responsible for key generation for encryption/decryption. Outsourcebale revocation is done by the updation of ciphertext that is stored in the cloud server.Data consumer receives the partial ciphertext from that exact plaintext will be recomputed. In this existing system,proposed a scheme for providing data integrity onetime message authentication code MACLESS is embedded with in the message/image documents. By combining the handwritten signature of the data owner and the data consumer generating a one time bio-key and this can be combine with the MAC-SHA-1.The result is MACLESS ,the authentication code and is hidden in the cover image through LSBs and DWTbased steganography mechanism.Concealing MACLESS with in the documents by usingRC4 method. At the data consumer recomputed MACLESS for data integrity checking.Any environment that uses cloud for the data storage.

**Keywords:** Cloudcomputing,FACOR,MACLESS,bio-key

## INTRODUCTION

Computing based on internet that provides shared processing resources and data to computers and other devices on demand is known as cloud computing.Cloud computing provide enterprises and users to store and process their own data in a third-party environment. It defines three main service models,They areSoftware as a Service (SaaS) .Here the consumer use the providers applicationsthat is running on a cloud infrastructure. Platform as a Service (PaaS).Here the consumer is to move onto the cloud infrastructure, consumer created or acquired applications created using programming languages,libraries, services, and tools supported by the provider. Infrastructure as a Service (IaaS) provided to the consumer is to provision for processing, storage, networks, and other computing resources which can include operating systems and applications.

To provide the security of outsourced data in the cloud platform,access control is one of the key mechanism FACOR [1] is an access control mechanism along with an outsourcable revocation of users .It applies an attribute based encryption scheme for flexible access control .Mainly model include six entities,attribute authorization,cloud service provider,data owner,Data user,2 proxy servers for encryption and decryption.Users outsource the time consuming encryption and decryption to the proxies.Data owner possess the data ,shares the data with other users ,also defines the access policies and encrypts the data with these access policies.Attribute authorization is the only fully trusted third party which is responsible for generating 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. This server is responsible for outsourced encryption . Decryption Proxy (DP), a proxy server helps data users to decrypt the ciphertext with the proxy key obtained from the corresponding data user and transmits the ciphertext into partial ciphertext and undertakes the most time-consuming operations of the whole decryption. Data User (DU) is the entity that accesses the confidential data with the private key,which represents the attributes it owns. Cloud service provider(CSP) is used mainly for storing users' Encrypted data. With CSP, users can share data with others OutSourceable Revocation is done by the CSP. When DU is revoked, there is a need of updation of the ciphertext stored in the cloud to ensure forward secrecy of the system. Figure below shows the FACOR

## RELATED WORK

Xiaolong Xu et al.[3] proposed a multi-authority proxy re-encryption scheme with CPABE technique. Wang, Jing, et al. proposed MAVP-FE Scheme. Junbeom Hur and Dong Kun Noh proposed a Attribute-Based access Control with efficient Revocation Scheme.

## EXISTING SYSTEM

FACOR [1] is an access control mechanism along with an outsourcable revocation of users .Mainly model include six entities,attribute authorization,cloud service provider,data owner,Data user,2 proxy servers for encryption and decryption.Users outsource the time consuming encryption and decryption to the proxies.Data owner possess the data ,shares the data with other users ,also defines the access policies and encrypts the data with these access policies.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. This server is responsible for outsourced encryption . Decryption Proxy (DP), a proxy server helps data users to decrypt the ciphertext with the proxy key obtained from the corresponding data user and transmits the ciphertext into partial ciphertext and undertakes the most time-consuming operations of the whole decryption. Data User (DU) is the entity that accesses the confidential data with the private key,which represents the attributes it owns. Cloud service provider(CSP) is used mainly for storing user's encrypted data.

## PROBLEM DEFINITION

In the existing sytsem, no method is employed to ensure the data integrity and authenticity of the message/image document. Only a flexible access control mechanism with user revocation is implemented. Integrity of message/image document refers to assuring and maintaining the consistency and accuracy of data over its entire life-cycle. Message authentication or data origin authentication is a property that a message has not been modified while in transmission of data and that the receiving party can verify the source of the message.Cryptographic hash functions can be used to ensure the data integrity. Message authentication code can embedd with in the data to ensure the authentication.

## PROPOSED SYSTEM

In the proposed scheme one-time biometric authentcation code MACLESS [2] is used to to ensure message/image document integrity for each user'slogin.This authentication code is actually the combination of key based hash function(MAC-SHA-1) of message/image document and one-time biokey.Proposed scheme uses the advantage of the biometric techniques.The proposed scheme is composed of two phases, namely, configuration and verification. In configuration Cloud service provider,sender and the reciever generate public keys and private keys and shared among each another through a secure channnel mechanism. These keys are used to transmit the encrypted handwritten signature of the sender and the reciever to the CSP. AFter recieving this CSP generates a bio-shared handwritten signature SHS by combining them tocompute the vector of features Rv = Fx(SHS) and the shared key Shk = Fx(SHS).To extract the vector features employs a histogram of LBP(local binary pattern filter).Afterthat CSP encrypts Rv and Shk and transmits them to Sender and Reciever respectively.S and R decrypt the received Rv and Shk. In the verification phase at the sender side generate one-time biometric salt-key.Compute the one-time message authentication code MACLESS by applying keybased hash function on the summation of message/image document and biokey. MACLESS canbe embedded with in the message/image document by using the DWT based steganography mechanism and the RC4 algorithm to hide MACLESS randomly.At the reciever side checks the integrity of the message/image by recomupting the message authentication code MACLESS.If they match we can ensure the integrity and authenticity of the message/image document

## CONCLUSION

Proposed model promising a secure one-time message authentication code to ensure the integrity and authenticityalong with the accesscontrol mechanism. Outsourcable revocation of users is also well maintained in this scheme. Biometric mechanism is used to generate one time bio key from the handwritten signatures of the sender and the receiver.This bio key is used to generate MACLESS the message/image authentication code.The main advantages are attaker may fail to obtain the keys because they depends on the handwritten signature feature extraction.One time bio key leads to one time biometric authentication code.Attacker may not get the bio-shred information because it depends on the combined handwritten signature of the sender and the reciever.

## 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] 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.

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