International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 6, Issue 3, March 2017 **ISSN 2319 - 4847**

SURVEY ON SECURE DATA EXCHANGE USING AUTHENTICATED CIPHERTEXT-POLICY ATTRIBUTED-BASED ENCRYPTION

[#1] Vincy Varghese, [#2] Dr.M.Rajeswari, [#3] Dr.Vince Paul, [#4] Dr.S.Satheeshkumar

[#1] Student, [#2,#4] Associate Professor, [#3] Professor
Department of Computer Science and Engineering
Sahrdaya College of Engineering and Technology, Kodakara, Thrissur

Abstract

In a day to day life, security plays a vital role to protect and authenticate our data from various introducers. This paper focuses on Secure Data Exchange using Authenticated Cipher text-Policy Attributed-Based Encryption.Security is major issue on data sharing system. Different Encryption technologies are used for providing security . Here, ciphertext attribute based encryption along with HMAC process were used. This integrated an authentication and confidentiality feature simultaneously for providing secure data.

Keyword: Authentication, HMAC, MAC, Encryption.

1. INTRODUCTION

Security is the major issues in data sharing system. Secure data is one of the promising challenge in communication. Various techniques are used for providing security. This paper is a survey on secure data exchange using authenticated ciphertext policy attribute based encryption .Different Techniques are used for providing encryption .Encryption and decryption is most commonly used techniques. survey of the above paper giving a complete and comprehensive overview of the two security techniques, CPABE scheme and HMAC process.

The most major security concerns in a communication systems are confidentiality, integrity and authentication. confidentiality "is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes". Data integrity means maintaining and assuring the accuracy and completeness of data over its entire life-cycle. This means that data cannot be modified in an unauthorized or undetected manner. Availability means the information must be available when it is needed.

In communication systems, always occur security related problem .Many techniques were introduced in different papers for providing security. Encryption is the process of converting plain text into ciphertext to prevent unauthorized access. If we send a message to another node, the original message converted to ciphertext using some keys. Encryption is two types, Symmetric and Asymmetric. In Asymmetric, use different keys for encryption and decryption. In Symmetric same key is used for both encryption and decryption. Attribute Based Encryption(ABE) is technique used for encryption. Set of attributes are associated with the private unique key. In attribute-based encryption (ABE) scheme an owner can encrypt the information that can be decoded only by those users, who are eligible to decrypt it. Attribute based encryption ensures the security and access control. Encryption, by itself, can protect the confidentiality of messages, but other techniques are still needed to protect the integrity and authenticity of a message; for example, verification of a message authentication code (MAC) or a digital signature

In cryptography, a message authentication code (MAC) is a short snippet of data used to verify a message— i.e, to affirm that the message originated from the expressed sender (its legitimacy) and has not been changed (here and there known as a tag). The MAC value secures both a message's information trustworthiness and additionally its validness, by permitting verifiers (who likewise have the mystery key) to recognize any progressions to the message content. In cryptography, a keyed-hash message authentication code (HMAC) is a particular sort of message authentication code (MAC) including a cryptographic hash function and a secrete cryptographic key. A digital signature is a scientific plan for showing the authenticity of digital messages or records.

2.LITERATURE REVIEW

R.Roy and M.Chuah [2] Proposed CP_ABE scheme in which encrypted data can only be accessed by authorized nodes. The author mentioned that there are two unique features of the scheme : the incorporation of dynamic attributes where the value of attribute may change over the time and a revocation mechanism.

M.Chuah et. al. [3] described implementation of a late-binding router that supports our security solution. In addition to the incorporation of dynamic attributes and revocation scheme. F.Jing-yi et. al. [7] proposed a new concept, efficient and privacy-preserving attribute-based broadcast encryption (BE) (ABBE) named EP-ABBE. It can reduce the overhead of decryption computation, and protect user privacy by making access policy of cipher text and user's attributes. The author showed that this scheme has three features includes secure, efficient and privacy-preserving

F.Jing-yi et. al. [7] presented a generic attribute based data sharing system based on hybrid mechanism of CPABE and symmetric encryption scheme. It offered constant computation cost and constant size ciphertext. S.Gupta and C.Kumar et. al. [4] proposed security mechanism, Random Electronic Code Book (RECB) combined with permutation functions. This is used for converting the plaintext into ciphertext.RECB contains 16 bit unique random cipher code for each 16 bit of plaintext information. Codebook generated through simple algorithm.

A.Sudarsono and T.Nakanishi [5] presented a technique by which encrypted data can be kept confidential even if the storage server is untrusted and the methods are secure against collusion attacks.

3.DIFFERENT TECHNIQUES

CP_ABE(ciphertext-policy attribute-based encryption)

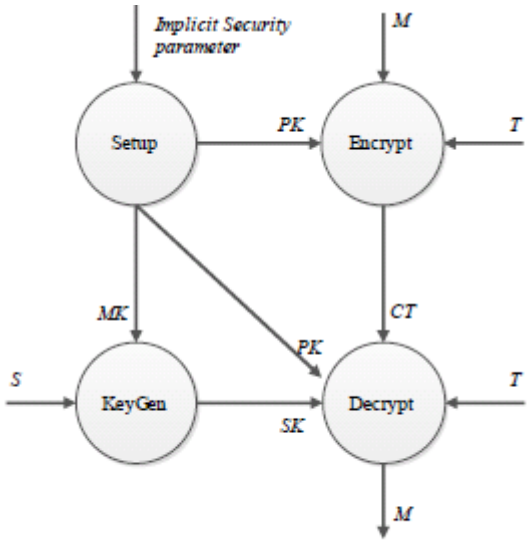
In 2007, J. Bethencourt, A. Sahai, and B. Waters in work Ciphertext-policy attribute-based encryption, in Proceedings of IEEE Symposium on Security and Privacy proposed encryption scheme based on ciphertext-policy attribute-based encryption . Policy to access data not contained in user's private key, and the encrypted data itself (ciphertext). Private key corresponds to a set of attributes. If the attributes contained in the user's private key corresponding to the structure of the ciphertext access, the user can decrypt the dataAlgorithm The algorithm consists of four steps: preliminary steps, encryption, decryption and key generation. Preliminary action is to describe the security settings and access attributes. The output is a public key and a master key. Encryption. The encryption algorithm accepts as input the public key, data to be encrypted, and access structure. The data will be encrypted so that only the user who has the necessary set of attributes, which in turn satisfy the structure of access can decrypt the data. We assume that the encrypted text implicitly contains ***A***. Key generation. Key generation algorithm accept as input a universal key and a set of attributes. The output is a secret key. Decryption. Decryption algorithm accepts as input the public key cipher text and a secret key. If a set of attributes contained in secret key satisfies structure of access, the data will be decrypted. The main feature of the scheme is to facilitate key management and cryptographic access.4 phases,Setup,KeyGen,Encryption and Decryption.

a) Setup (PK,MK): Give a security parameter, this algorithm randomly outputs the public parameters PK and a master key MK which is kept private. PK will be used for encryption and decryption mechanisms, while MK will be operated for generating nodes secret keys

b) KeyGen(PK, MK, S): input public key PK, master key MK and attribute list S like shown in Table I. It outputs a secret key SK for user.

c) Encryption(PK,M,τ): This algorithm is run by all participating nodes who will act as an encryptor. On input a message M, and an access policy τ, and the public key PK, it outputs a ciphertext CT.

d) Decryption(PK,CT, SK): This algorithm is operated by all participating nodes who will act as a decryptor. On input a ciphertext CT, a secret key SK associated with attribute S. If and only if S = τ the message M can be recovered, and error symbol $\perp$ otherwise.



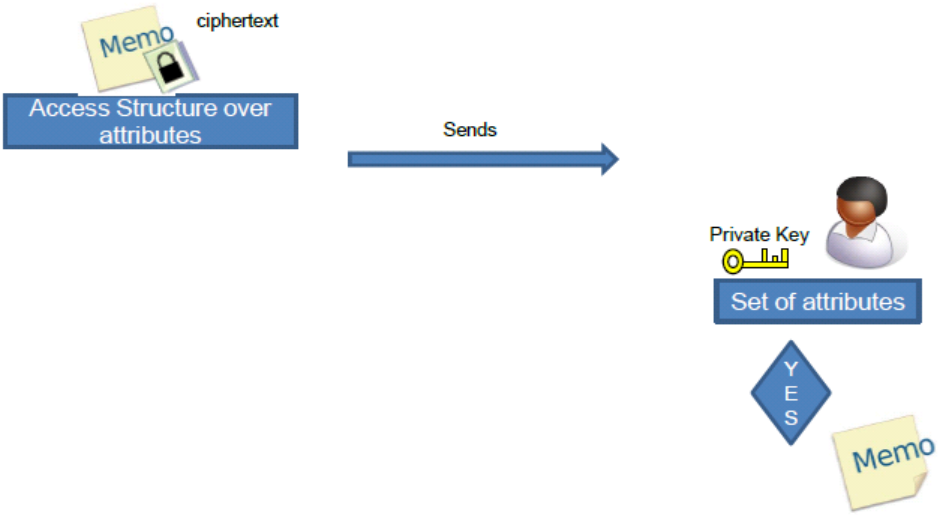
. Overview of CP-ABE scheme phases

CPABE makes it possible to implement many interesting access control mechanisms using cryptography. Traditionally, everyone with the right key can decrypt and thus access the encrypted file. ABE is not that different. However instead of using the public key to encrypt the files, it uses attribute(s) or a key based on attributes to encrypt the files. Ciphertexts not necessarily encrypted to one particular user. Users private keys and ciphertext associated with a set of attributes or a policy over attributes. A "match" between user's private key and the ciphertext decryption is possible.

TABLE I EXAMPLE OF ATTRIBUTES AND THE VALUES [5]

No.	Attributes	Example values
1	Full-name	Firstname Lastname, ...
2	Address	Rose avenue 1-2-3 No.2,...
3	Identity number	AB-12345678,.....
4	Phone number	031-123456,...
5	Gender	Male, Female
6	Place of birth	Surabaya, Tulungagung,...
7	Birthdate	10-04-1993, ...
8	Occupation	Student, Lecturer,...
9	Academic degree	B.S, M.S, Ph.D,....
10	Major	Engineering, science, ...
11	Affiliation	A University, B College
12	Faculty	Engineering, Social,....
13	Department	Information Tech, Multimedia,..
14	Division	IT, Electrical, ...
15	Position	Director, president, ...
16	Location	1st fl D3 building,....

Ciphertext Policy Attribute- Based Encryption



.

2.HMAC(HASH MESSSAGE AUTHENTICATION CODE)

In cryptography, a keyed-hash message confirmation code (HMAC) is a particular sort of message authentication code (MAC) including a cryptographic hash work and a secrete cryptographic key. It might be utilized to all the while confirm both the information honesty and the validation of a message, as with any MAC. Any cryptographic hash function, for example, MD5 or SHA-1, might be utilized as a part of the estimation of a HMAC; the subsequent MAC calculation is named HMAC-MD5 or HMAC-SHA1 as needs be. The cryptographic quality of the HMAC relies on the cryptographic quality of the hidden hash work, the measure of its hash yield, and on the size and nature of the key.

An iterative hash function breaks up a message into blocks of a fixed size and iterates over them with a compression function.

Generated HMAC by the formula

HMAC(M)=H[(k + opad) & H[(k + ipad) & M]]

M=Message

H[]=Hash Function

K=Shared secret key

opad =36hex,repeated as needed

ipad =5chex repeated as needed

& =concatenation operation

+= XOR operation

Use HMAC ,because of its speed and also its library code is widely available. Mac are based on a key that is shared between two parties, if either party's key is compromised, it will be possible for an attacker to create fraudulent messages. ipad and opad are different ,values have been chosen by HMAC designers.

HMAC Algorithm

1.Append zeros to the left end ok k to create a b bit string k+

2.XOR k+ with ipad to produce b bit block si.

3.Append M to si.

4.Apply H to the stream generated in step 3

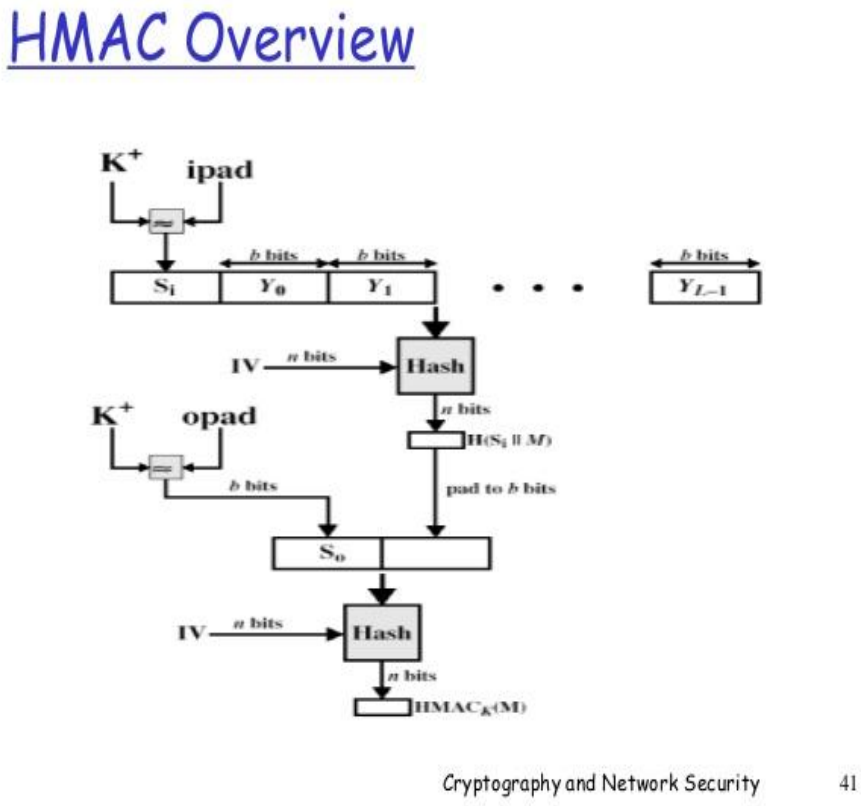
5. XOR k+ with opad to produce the b bit block so.

6. Append the hash result step 4 to so.

7. Apply H to the stream generated in step 6 and output the

Result.

A n-bit hash is a guide from self-assertive length messages to n-bit hash values. A n-bit cryptographic hash is a n-bit hash which is one-way and collision-resistant. Such functions are critical cryptographic primitives utilized for such things as advanced marks and secret word security .The paper utilized SHA 256 as hash capacity. The SHA-256 pressure work works on a 512-piece message square and a 256-piece middle hash esteem. It is basically a 256-piece square figure calculation which scrambles the middle of the road hash esteem utilizing the message hinder as key.SHA 256 is a 256-piece hash and is intended to give 128 bits of security against crash assaults.



4. PROPOSED SYSTEM

Proposed fast hashing function (SHA-512) for HMAC process. The SHA-512 compression function operates on a 1024-bit message block and a 512-bit intermediate hash value. SHA-512 is a variant of SHA-256 which operates on eight 64-bit words. The message to be hashed is first

(1) padded with its length in such a way that the result is a multiple of 1024 bits long, and then

(2) parsed into 1024-bit message blocks M(1);M(2); : ::;M(N).

The message blocks are processed one at a time: Beginning with a fixed initial hash value H(0), sequentially compute

$$H(i) = H(i-1) + CM(i)(H(i-1));$$

Where C is the SHA-512 compression function and + means word-wise mod 264 addition.
H(N) is the hash of M.
It is more cost effective to compute a SHA-512 than it is to compute a SHA-256 over a given size of data. For 64 bit architectures, this would yield a more efficient hashing algorithm, than the current SHA-256.

5. CONCLUSION

The paper addresses the problem of insecurity in data sharing system. The approach reduces the unauthorized access and increases the integrity and confidentiality of the messages. Paper presented a secure data exchange through wireless network using authenticated CP-ABE. The data is attribute based encrypted to satisfy confidentiality feature and it is authenticated to satisfy data authentication simultaneously**.**

REFERENCES

[1] J.Bethencourt, A.Sahai, dan B.Waters, "Ciperthext-policy Attribute-Based Encryption", IEEE Symposium on Security and Privacy,pp.321-334, 2007.
[2] R.Roy and M.Chuah, "Secure Data Retrieval Based on Ciphertext Policy Attribute-Based Encryption (CP-ABE) System for DTNs", Journal of Cryptology, 17(4): pp.297-319,2004.
[3] M.Chuah, S.Roy, and I.Stoev, "Secure Descriptive Message Dissemination in DTNs", Proceeding of MobiOpp'10, 2nd International Workshop on Mobile Opportunistic Networking, pp. 79-85, 2010.
[4] S.Gupta and C.Kumar, "Shared Information Based Security Solution for Mobile Ad Hoc Networks", international Journal of wireless & mobile networks(IJWMN), Vol.2, No.1, February 2010, pp.176-187, 2010
[5] A.Sudarsono and T.Nakanishi, "An Implementation of Secure Data Exchange in Wireless Delay Tolerant Network Using Attribute-Based Encryption", 2nd International Symposium on Computing and Networking (CANDAR 2014), pp. 536-542, Dec. 10-12, Shizuoka, Japan, 2014.
[6] Y.Zhang, D.Zheng, X.Chen, J.Li, and H.Li, "Efficient attribute-based data sharing in mobile clouds", Pervasive and Mobile Computing (2015). http://dx.doi.org/10.1016/j.pmcj.2015.06.009.
[7] F.Jing-yi, H.Qin-long, M.Zhao-feng, and Y.YI-xian, "Secure personal data sharing in cloud computing using attribute-based broadcast
[8] encryption", The Journal of China Universities of Posts and Telecommunications, pp.45-52. 2014.