ATTRIBUTE BASED ENCRYPTION IN MILITARY ENVIRONMENT

Rohit Gurav, Rahul Fulzele, Anand Seshadri, Prof. Pallavi Dhade

BE Computer, Computer Department, Pimpri Chinchwad College of Engineering, Pune, Maharashtra, India
BE Computer, Computer Department, Pimpri Chinchwad College of Engineering, Pune, Maharashtra, India
BE Computer, Computer Department, Pimpri Chinchwad College of Engineering, Pune, Maharashtra, India
Professor, Computer Department, Pimpri Chinchwad College of Engineering, Pune, Maharashtra, India

ABSTRACT

In military network eventualities, it's tough to speak directly between users (e.g., commanders and soldiers) because of irregularity and poor property. In decentralized disrupt tolerant network for military eventualities, info the knowledge the data} must be strictly protected thus as to not leak information by unauthorized access and malicious users. Thereby it's necessary to cypher the shared information to stop the third party. It's expected that commanders might management whether or not the user has authority to decipher the cipher text or not. Besides, it's essential that a key authority that distributes keys to users is decentralized to many authorities for avoiding the invasion from enemy. In CP-ABE, the cipher text is related to the access structure that defines the access policy; the key secrets related to a group of user's attributes. A user is in a position to decipher a cipher text if his attribute satisfy the Cipher text's access structure. Since every cipher text encompasses a nominative access structure, CP-ABE is appropriate for fine grained access management of shared information. There exists a central authority to that several range of native authorities is also assigned. The sender sends the data to the central authority wherever the secret's generated then passed on to the authority. Within the receiver finish the decipherment algorithmic program cross checks the key and verifies for the licensed user. Within the projected system, cipher text attribute based mostly cryptography is being combined with location as associate attribute. A Location based mostly Data- Security System is employed to secure information by applying Encryption-Algorithm and user coordinates. Cryptography means that of economical secure number comparison. The cryptography technology cannot limit the placement of information decipherment. So as to fulfill the demand of a location-dependent approach location-dependent encryption algorithmic program is required. A target latitude/longitude co-ordinate is set first of all. The co-ordinate is incorporated with a random key for encryption. The receiver will solely decipher the cipher text once the co-ordinate receiver is matched with the target co-ordinate.

Keyword: - *Data Encryption, Code breaking, Data encryption standard (DES), Public key cryptosystems, Standards (e.g., DES, PGP, RSA)*

---

1. INTRODUCTION

Attribute-based encoding (ABE) could be a comparatively recent approach that reconsiders the idea of public-key cryptography. In ancient public-key cryptography, a message is encrypted for a selected receiver mistreatment the receiver's public-key. Identity-based cryptography associated particularly identity-based encoding (IBE) modified the normal understanding of public-key cryptography by permitting the public-key to be an impulsive string, e.g.,

the e-mail address of the receiver. ABE goes one step any and defines the identity not atomic however as a group of attributes, e.g., roles, and messages is encrypted with reference to subsets of attributes (key-policy ABE - KP-ABE) or policies outlined over a group of attributes (cipher text-policy ABE - CP-ABE).

The key issue is, that somebody ought to solely be able to decipher a cipher text if the person holds a key for "matching attributes" (more below) wherever user keys area unit forever issued by some trusty party. In cipher text - policy attribute-based encoding (CP-ABE) a user's private-key is related to a group of attributes associated a cipher text specifies an access policy over an outlined universe of attributes inside the system. A user are beer to decipher a cipher text, if and providing his attributes satisfy the policy of the several cipher text. CP-ABE so permits to comprehend implicit authorization, i.e., authorization is enclosed into the encrypted knowledge and solely those who satisfy the associated policy will decipher knowledge. Another nice options is, that users will get their non-public keys when knowledge has been encrypted with reference to policies. Thus knowledge is encrypted while not data of the particular set of users which will be able to decipher, however solely specifying the policy that permits to decipher. Any future users can which will that may} incline a key with reference to attributes specified the policy is glad will then be able to decipher the information. In military network eventualities, it's troublesome to speak directly between users thanks to irregularity and poor property. In redistributed disrupt tolerant network for military eventualities, data the knowledge the data} has got to be strictly protected thus as to not leak information by unauthorized access and malicious users. Therefore by combining CP-ABE with Location encoding the aim of securing the shared confidential knowledge is served. It's necessary to supply a secure and convenient knowledge transmission.

We propose a location-dependent approach for higher knowledge security. The consumer place the coordinates manually in application for encoding. Then our application produce a encrypted file so we tend to send that encrypted file mistreatment email or by any external device to our destination .The consumer solely decipher the cipher text once the coordinate non inheritable from GPS receiver matches with the target coordinate. In keeping with our discussion, the approach will meet the confidentiality, authentication, simplicity and utility of security problems.

2. LITERATURE SURVEY

2.1 Attribute Revocation Attribute Based Encryption Military Networks

This paper, focuses on a CP-ABE scheme which can revoke attribute immediately with no updating user's secret key for attribute revocation. In addition, the length of key and cipher text are fixed. Furthermore the proposed scheme has been compared with other CP-ABE schemes in key size, cipher text size to validate its efficiency.

2.2 Cipher text-Policy Attribute-Based Encryption

A key revocation mechanisms approach in CP-ABE, which is appended an expiration data to each attribute and distribute a new set of keys are distributed to valid users after the expiration. However, in this approach, time lag occurs in the expiration attributes and there is a risk that an unauthorized user can decrypt cipher text when the user changes his attribute frequency.

2.3 Loc-Auth: Location enabled authentication through attribute based encryption

In this paper, a mobile sign on scheme is depicted that benefits from the dynamic relationship between a user's attributes, the service the user wishes to utilize, and location(where the user is, and what services are available there) as an authentication factor. Here Bluetooth Low Energy beacons are demonstrated for location awareness and expressiveness of Attribute-Based Encryption which capture and leverage the described relationship. Bluetooth Low Energy beacons broadcast encrypted messages with encoded access policies. Within range of the beacons, a user with appropriate attributes is able to decrypt the broadcast message and obtain parameters that allow the user to perform a short and simplified login.

2.4 Comparative study of Attribute Based Techniques in Cloud Computing

In this paper multi authority hierarchical attribute based encryption is proposed and it is compared with key policy and cipher text policy attribute based encryption techniques (CP-ABE).Based on NIST statistical tests highest security attribute based encryption algorithm is selected in cloud. NIST tests are performed to test the randomness of binary sequence produced by either hardware and software based cryptographic random or pseudorandom number generator.

Name of the paper	Year published	Remarks	Advantages
Attribute Revocable Attribute-Based Encryption for Decentralized Disruption-Tolerant Military Networks	2015	Cipher text attribute based encryption algorithm	Security of confidential data enhanced.
Location Based Encryption-Decryption Approach for Data Security	2014	Multi authority hierarchical attribute based encryption is proposed	Dynamicity is achieved.
Loc-Auth: Location-enabled authentication through attribute-based encryption	2015	Employing Bluetooth low energy beacons for location awareness & expressiveness of ABE	Login process is short and simplified
Comparative Study of Attribute Based Encryption Techniques	2014	Multi authority hierarchical attribute based encryption is proposed	Less time taking encryption & decryption process

Table 1. Literature Survey

3. PROPOSED METHOD

Attribute based encryption in Military Environment. In the proposed method, by using Cipher text Attribute Based Encryption and location information for encryption of military data communication which helps to increase security of system and authentication of user. The system basically consists of 4 modules- Sender, Key Authorities, Storage Node and Receiver.

In the given scenario, the military network, commander is the sender. This is a one-way communication system, hence only the commander can send a message. Firstly the sender will select a file that is to be sent. Now the selected file is to be encrypted. For this sender will need encryption keys. The key authorities are responsible to generate the keys. Key authorities will generate the keys using the RSA algorithm. The keys will be generated using the attributes of the file and the intended receiver. The attributes which the authorities use are the file name, file size, intended receiver's battalion ID, region ID and location.

For enhancing the security, the key authorities are divided in 4 parts- central, local, personalized and attribute-based. These 4 authorities will generate 4 different keys for encryption. Also the keys that they generate are in a hierarchically interdependent form, i.e. the attribute based key authority cannot generate a key without the personalized key, the personalized key authority cannot generate a key without the local key, the local key authority cannot generate a key without the central key. Hence the final key is a combination of all the four and so it is even more secure.

Once, the encryption is generated and given to the sender, the sender encrypts the file and stores the encrypted file in the storage node. The storage node is responsible to hold the encrypted file. Now the receiver approaches the storage node and demands for access of the required file. The storage node gives the access of the required file to the receiver. This file is in encrypted format. Hence, to decrypt this file the receiver will request for keys to the key authorities. The key authorities will send the keys to the receiver. Once the receiver gets the keys, he can decrypt the file. The file is encrypted using only the intended receiver's attributes, therefore only if the receiver is the intended receiver of that particular file then and then only he will be able to decrypt the file.

4. SYSTEM ARCHITECTURE

The proposed system consists of four components namely- sender, receiver, key authorities and the storage node. These components are responsible to perform the operations of the system. The major operations are:

I) Personalized key generation:

The keys that are required to encrypt the data are generation using this operation. The personalized key generator is one of the key authorities which is responsible for generation of this key.

II) Attribute key generation:

The attribute key is another key used for encryption of the data. It is also generated by oneof the key authorities i.e. Attribute key generator. This key is generated using the receiver's attributes and the file attributes.

III) Attribute revocation:

This operation is carried out at the receiver's end. If only the intended receiver tries to decrypt the file, the file can be decrypted. Only the attributes of the intended receiver can decrypt the file. If the attributes are correct, then and then only the file can be decrypted.

IV) Attribute matching:

If the attributes of the receiver match to the required attributes then the file can be decrypted. This process is called attribute matching.

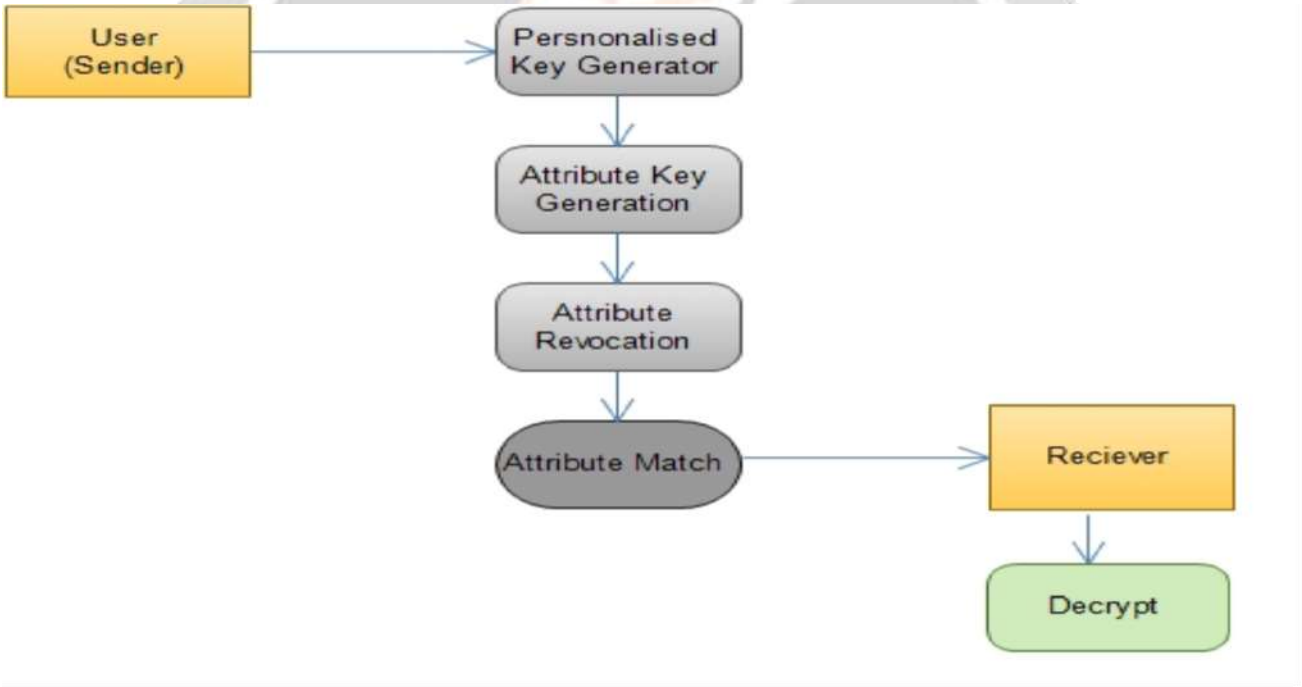

Fig 1: SYSTEM ARCHITECTURE

5. ALGORITHM USED:

The algorithm used in the proposed system is the RSA algorithm discovered by Ron Rivest, Adi Shamir and Leonard Adleman in 1977. Public-key cryptography, also known as asymmetric cryptography, uses two different but mathematically linked keys, one public and one private. The public key can be shared with everyone, whereas the private key must be kept secret. In RSA cryptography, both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. This attribute is one reason why RSA has become the most widely used asymmetric algorithm: It provides a method of assuring the confidentiality, integrity, authenticity and non-reputability of electronic communications and data storage.

Many protocols like SSH, OpenPGP, S/MIME, and SSL/TLS rely on RSA for encryption and digital signature functions. It is also used in software programs -- browsers are an obvious example, which need to establish a secure connection over an insecure network like the Internet or validate a digital signature. RSA signature verification is one of the most commonly performed operations in IT.

The steps for RSA algorithm are:

I) Generate two large prime numbers p and q.
II) Let n=p*q
III) Let m = (p-1)*(q-1); Where m is the totient function
IV) Choose a small number e, co-prime to m, with GCD (m, e) =1; 1<e<m
V) Find d such that de mod m = 1

Publish e and n as the public key.
Keep d and m as the secret key.
Encryption:
Cipher = (message) e mod n
Decryption:
Message = (cipher) d mod n
x and y means the remainder of x divided by y.

6. RESULT:

The snapshot of the GUI is shown below:

Sender GUI:

Fig 2: SENDER

Receiver GUI:

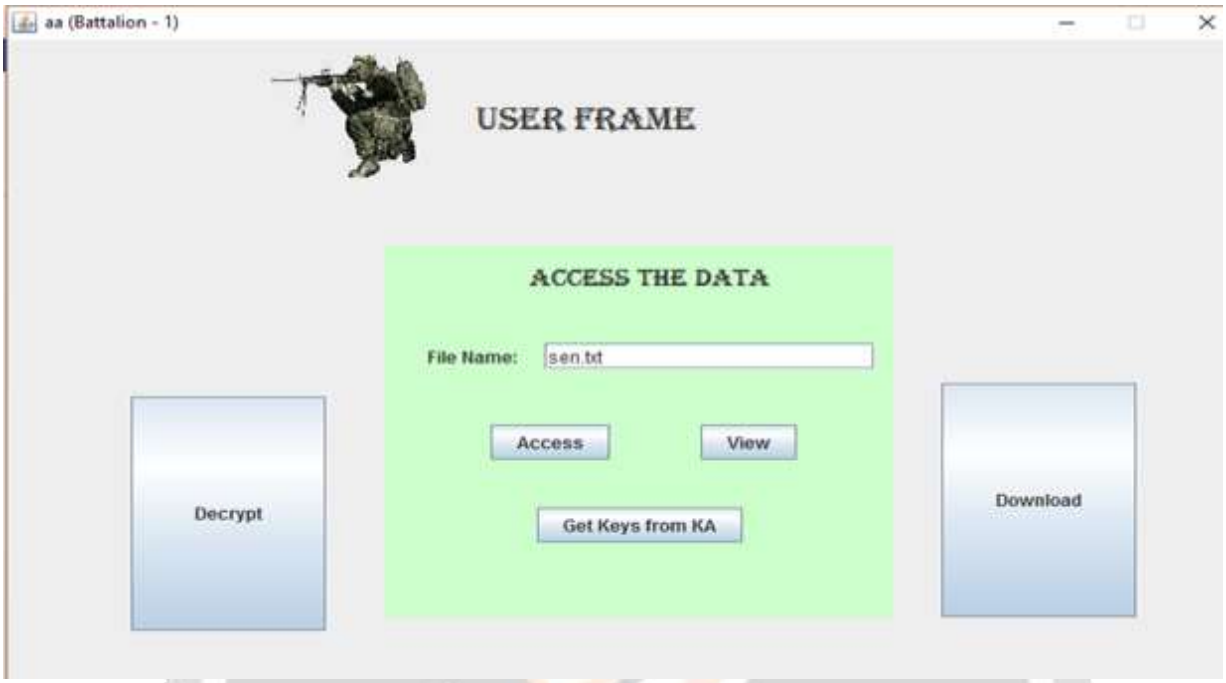

Fig 3: RECEIVER

7. CONCLUSION:

Attribute based encryption is a useful and efficient technique for encryption. The encryption is carried out using the real time attributes of the user which is a very unique and at the same time very safe mechanism. In this paper, we have discussed the use of this encryption technique in a military environment by developing a secure communication system. Here we have used the attributes such as the battalion ID, region ID and location for the encryption. Also the particular file's attributes such as file name and size have been used for encryption.

8. REFERENCES

[1] Attribute Revocation Attribute Based Encryption Military Networks
[2] Cipher text-Policy Attribute-Based Encryption
[3] Loc-Auth: Location enabled authentication through attribute based encryption
[4] Comparative study of Attribute Based Techniques in Cloud Computing
[5] Brown, L. D., Hua, H., and GAO, C. 2003. A widget framework for augmented interaction in SCAPE.
[6] Y.T. Yu, M.F. Lau, "A comparison of MC/DC, MUMCUT and several other coverage criteria for logical decisions", Journal of Systems and Software, 2005, in press.
[7] Spector, A. Z. 1989. Achieving application requirements. In Distributed Systems, S. Mullender Zhiguo Wan, Jun'e Liu, and Robert H. Deng, "HASBE: A Hierarchical
[8] Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing" IEEE Transactions On Information Forensics And Security, Vol. 7, No. 2, April 2012
[9] Eman M.Mohamad, Hatem S.Abdelkader,"Enhahanced data security Model for cloud computing", The 8th International conference on Informatics and system (InFo2012)14-1 May 2012

[10]Affiliation Juan Soto,National Institute of Standards and Technology 1oo bureau Drive,Stop 8930 Gaithersburg"Randomness Testing of Advnced Encryption Standard Candidate Algorithm "
[11]G.Wang, Q. Liu, and J.Wu, "Hierachical attibute-based encryption for fine-grained access control in cloud storage services," in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Chicago,IL, 2010.
[12]Rakesh Bobba, Himanshu Khurana and Manoj Prabhakaran, "Attribute-Sets: A Practically Motivated Enhancement to Attribute-Based Encryption", July 27, 2009
[13] Zhibin Zhou, Dijiang Huang" On Efficient Ciphertext-Policy Attribute Based Encryption and Broadcast Encryption" R.Ostrovsky, A. Sahai, and B. Waters. "Attribute-based encryption with non-monotonic access structures". In Proc. of CCS'06, New York, NY, 2007.
[14]V. Goyal, O. Pandey, A. Sahai, and B. Waters. "Attribute-Based Encryption for Fine-grained Access Control of Encrypted Data". In Proc. of CCS'06, Alexandria, Virginia, USA, 2006.
[15] Ximeng Liu1, Pei-Shan Chung2 and Min-Shiang Hwang," Ciphertext Policy Hierarchical Attribute-Based Solution for Fine Grained Access control of Encrypted Data.International Journal of Network Security vol 16. July 2014
[16] Eman M.Mohamed,Hatern S,Abdelkader, Sherif EI-Etriby,"Enchanced Data Security Model For Cloud Computing,International conference on Informatics and System(Info 2012)14-16 cloud and mobile computing track.