International Journal of Pure and Applied Mathematics
Volume 116 No. 9 2017, 213-217
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

CIPHER TEXT POLICY-ATTRIBUTE BASED ENCRYPTION (CP-ABE) AND DISRUPTION TOLERANT NETWORKING IN CONFIDENTIAL NETWORKS

K.P.Kaliyamurthie
Dean, Department of CSE, Bharath University,Chennai-73.
kpkaliyamurthie@gmail.com

Abstract: Confidential Networks like the networks in the military environment used mobile node for communication, which are then replaced by the storage nodes as the communication through the storage nodes are far more secure than the mobile nodes. Disruptions being an important challenge in the military environment, Disruption-Tolerant military Networks are being used for the communication between the storage nodes. CP-ABE algorithm is used to encrypt the confidential information to overcome the authorization challenges in the storage node, where the decryption could be done when its access policy satisfies with the attribute key. CP-ABE is a semi trusted .The Challenging issue here is to enforce authorization policies to the users who are going to access the secured data. The CP-ABE algorithm is producing some of the issues like attribute Coordination among different users and Key enforcement and key abuse problems. Blow fish is a symmetric block cipher used instead of DSA.In this paper we are combining applying of CP-ABE and Blow fish producing a trusted data retrieval in confidential networks like military networks.

Keywords: CP-ABE,DTN, Blow Fish, Confidential Networks, Storage Nodes, key revocation ,Key Abuse.

1. Introduction

Delay-/Disruption-Tolerant Networking is an overlay architecture intended to operate above the protocol stacks of the distinct ICNs and enable gateway functionality between them through the use of storage capacity, a variety of protocol techniques, replication and parallel forwarding, forward error correction and many other techniques for overcoming communication impairments. Mobile nodes in some challenging network scenarios suffer from intermittent connectivity and frequent partition e.g. battlefield and disaster recovery scenarios. In the above scenarios, an end-to-end path between a source and destination may not always exist where the links between intermediate nodes may be opportunistic, predictable connectivity or periodically connected [8].
To allow nodes to communicate with each other in these extreme network environments recently research community has proposed a new architecture called the Disruption-Tolerant networks (DTN). Typically, the source node's message may need to wait intermediate node substantial amount of time when there is no connection to the destination. After the connection eventually established, the messages is delivered to the destination node. Such regional networks are best described as being isolated from each other[1,2,3].

1.1 Attribute Based Encryption

ABE (Attribute Based Encryption) was first introduced by **Sahai and Waters [2].** It provides a mechanism by which we can ensure that even if the storage is compromised, the loss of information will only be minimal. In order to provide a complex access policy mechanism we need flexible and scalable cryptographic key management algorithms. For improving these disadvantages it is using attribute based encryption hence we employee CP-ABE (cipher text policy – attribute based encryption) technique as a remedy to the above mentioned problem in CP-ABE the recipient can decrypt the data only when the user attribute satisfy the access policy and this can be seen as one-to-many public key encryption and the data owner provides access to many users. In this system the users Private Key is associated with the user attributes and on the other hand the party that is encrypting the data specifying an access policy.

1.2 Challenges In Military Networks

In many challenges occurs in confidential fields like military networks. The confidential data are shared among soldiers in battlefield through mobile nodes. Communications are not reliable through using mobile nodes in extreme network environments. Wireless devices are temporarily disconnected by jamming[4,5], environmental factors and mobility especially when operate in hostile environments. Typically, when there is no end to-end connection between a source and a destination pair, the messages from the source node may need to wait in the intermediate nodes for a substantial amount of time until the connection would be eventually

established. It introduced storage nodes in DTNs where data is stored or replicated such that only authorized mobile nodes can access the necessary information quickly and efficiently [21,22,25]. Many military applications require increased protection of confidential data including access control methods that are cryptographically enforced.

1. 3 Secure Data Retrieval

Cipher text Policy Attribute Based Encryption (CP-ABE) algorithms are used to encrypt a confidential data as a cipher text and enforcing an access policy based on set of attributes. In key generation phase[6,7], it generates a secret key component that it consists of personalized key of each user and multiple attributes. The user wants to retrieve the encrypted data from the storage node when the access policy and attributes that is match then only decrypt the cipher text with its decryption key or secret key using to accessing the confidential data [4]. Otherwise, the user does not allow accessing the confidential information or data from the storage node.

1.4 Blow Fish Cipher

It is a symmetric ,Keyed ,Cryptographic method used as a substitute for DES,DSA algorithms.It can be used as a embedded cryptographic method .It was designed by BRUCE SCHNEIER in 1993 and can be used by any one. The security feature of Blow Fish is tested and proven.

1.5 Introduction to Blowfish

Blowfish is a keyed, symmetric cryptographic block cipher designed by Bruce Schneider in 1993 and placed in the public domain. Blowfish is included in a large number of cipher suites and encryption products, including Splash ID. Blowfish's security has been extensively tested and proven. As a public domain cipher, Blowfish has been subject to a significant amount of cryptanalysis, and full Blowfish encryption has never been broken. Blowfish is also one of the fastest block ciphers in public use, making it ideal for a product like Splash ID that functions on a wide variety of processors found in mobile phones as well as in notebook and desktop computers.Schneier designed Blowfish as a general-purpose algorithm, intended as a replacement for the aging DES and free of the problems associated with other algorithms.

2. Related Work

This section analyzes the various methods available and issues in implementing and achieving a trusted system in Disruption Tolerant military networks.

"Decentralized Attribute Based Encryption" Allison Lewko and Brent Waters, 2010.

In this system describe previous Attribute Based Encryption method collusion resistance when the authority tied together to generate components with user's private key. This system proposed to avoid the collusion resistance by using **multi-authority** system. It describe the system as decentralized because any party can become a authority to generate a public key and issuing private key to different users reflect by their attribute. The authority does not coordinate among the different authorities because it is decentralized systems that not have a central authority. If system has a central authority[8,9], it will globally trustworthy otherwise the system as a risk. It **creates new technique to tie components and prevent between users with different global identifiers from collusion attacks**. It proves the system as secure by using dual system encryption method build bilinear groups of Composite order.

"Secure Data Retrieval in Disruption Tolerant Military Networks" Junbeom Hur and Kyungtae Kang, 2014.

Most of the existing ABE schemes are constructed on the architecture where a single trusted authority has the power to generate the whole private keys of users with its master secret information. Thus, the key escrow problem issues inherent such that the key authority can decrypt every cipher text addressed to users in the system by generating their secret keys at any time. In CP-ABE, the key authority generates private keys of users by applying the authority's master secret keys to users' associated set of attributes. Thus, the key authority can decrypt every cipher text addressed to specific users by generating their attribute keys. If the key authority is compromised by adversaries when deployed in the hostile environments[10,11], this could be a potential threat to the data confidentiality or privacy especially when the data is highly sensitive.

2.1 Our Contribution

In this paper we discussed the CP-ABE algorithm and its strength to overcome the security problems in communicating data in confidential networks.The Advantages of Blow fish Algorithm is combined here to produce keys by Central authority and local authority and transferred to the receiver for example soldier in the case of military networks. It reduces by windows of vulnerability using immediate attribute revocation. Encrypt the confidential data as a cipher text if compromise without access. The data should encrypt to store storage node and when user want to

decrypt the cipher text satisfy the access policy and specified attributes then only access or decrypt the cipher text using a secret key of users[17,18].

2.2 Attribute Based Encryption

Attribute-based encryption is a type of public-key encryption in which the secret key of a user and the ciphertext are dependent upon attributes (e.g. the country in which he lives, or the kind of subscription he has). In such a system, the decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext. A crucial security aspect of Attribute-Based Encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access.

The concept of **attribute-based encryption** was first proposed by Amit Sahai and Brent Waters and later by Vipul Goyal, Omkant Pandey, Amit Sahai and Brent Waters. **Types of Attribute-Based Encryption schemes**There are mainly two types of Attribute-Based Encryption schemes: Key-Policy Attribute-Based Encryption (KP-ABE)[] and Ciphertext-Policy Attribute-Based Encryption (CP-ABE). In KP-ABE, users' secret keys are generated based on an access tree that defines the privileges scope of the concerned user, and data are encrypted over a set of attribute. However, CP-ABE uses access trees to encrypt data and users' secret keys are generated over a set of attribute.Usage:Attribute-based encryption (ABE) can be used for log encryption. Instead of encrypting each part of a log with the keys of all recipients, it is possible to encrypt the log only with attributes which match recipients' attributes. This primitive can also be used for broadcast encryption in order to decrease the number of keys used.

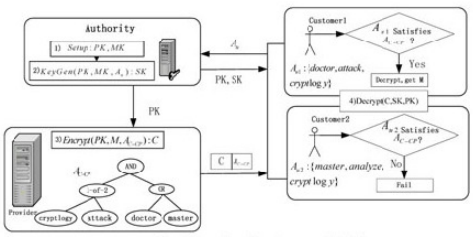

Figure 1. Encryption ,decryption using CP-ABE

2.3 Blow fish encryption

Bruce Scheier designed a encryption algorithm which will eliminate the demerits of normal encryption algorithms like AES,DES and 3 DES and name it as Blowfish in the Year 1993.Blowfish is a symmetric block encryption algorithm designed in consideration with[15,16], **Fast :** It encrypts data on large 32-bit microprocessors at a rate of 26 clock cycles per byte. **Compact:** It can run in less than 5K of memory. **Simple:** It uses addition, XOR, lookup table with 32-bit perands. **Secure:** The key length is variable ,it can be in the range of 32~448 bits: default 128 bits key length. It is suitable for applications where the key does not change often, like communication link or an automatic file encryptor. Unpatented And royality- free.

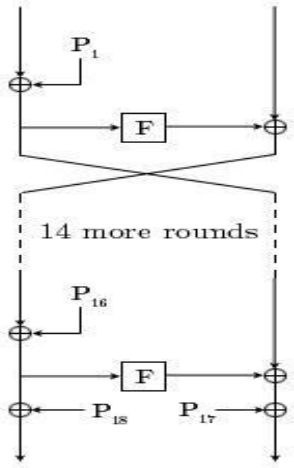

Figure 2. The Feistel structure of Blowfish

2.3.1 Description of Algorithm:

Blowfish symmetric block cipher algorithm encrypts block data of 64-bits at a time.it will follows the feistel network and this algorithm is divided into two parts.

1. Key-expansion
2. Data Encryption

Key-expansion:

Key-expansion will convert a single key into several sub keys like 48 bits into totaling 4168 bytes. Large number of sub keys are used by blow fish. These are generic keys used for any cryptographic functions.

The p-array consists of 18, 32-bit subkeys:

- P1,P2,……,P18

Four 32-bit S-Boxes consists of 256 entries each:

- S1,0, S1,1,……. S1,255
- S2,0, S2,1,…….. S2,255
- S3,0, S3,1,…….. S3,255
- S4,0, S4,1,.....S4,255

Generating the Subkeys**:**

The subkeys are calculated using the Blowfish algorithm:

1. Initialize first the P-array and then the four S-boxes, in order, with a fixed string. This string consists of the hexadecimal digits of pi (less the initial 3): P1 = 0x243f6a88, P2 = 0x85a308d3, P3 = 0x13198a2e, P4 = 0x03707344, etc.

2. XOR P1 with the first 32 bits of the key, XOR P2 with the second 32-bits of the key, and so on for all bits of the key (possibly up to P14). Repeatedly cycle through the key bits until the entire P-array has been XORed with key bits. (For every short key, there is at least one equivalent longer key; for example, if A is a 64-bit key, then AA, AAA, etc., are equivalent keys.)
3. Encrypt the all-zero string with the Blowfish algorithm, using the subkeys described in steps (1) and (2).
4. Replace P1 and P2 with the output of step (3).
5. Encrypt the output of step (3) using the Blowfish algorithm with the modified subkeys.
6. Replace P3 and P4 with the output of step (5).
7. Continue the process, replacing all entries of the P array, and then all four S-boxes in order, with the output of the continuously changing Blowfish algorithm.

In total, 521 iterations are required to generate all required subkeys. Applications can store the subkeys rather than execute this derivation process multiple times.

In summary, cpabe-keygen and cpabe-enc run in a predictable amount of time based on the number of attributes in a key or leaves in a policy tree. The performance of cpabe-dec depends actually increases running time in this case, due to fact that exponentiations are more expensive in G0 than in G1.

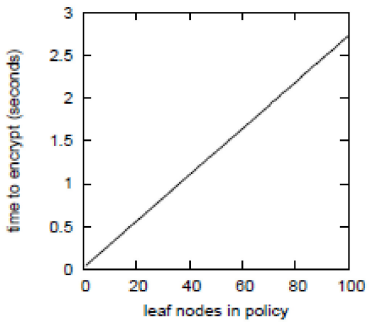

Figure 3. Encryption Time

3. Conclusion

This paper discusses the need of strong attribute based encryption and Blow fish algorithm implementation in the confidential networks using DTN.It discusses about DTN followed by CP-ABE and Blow fish algorithms.Then the concept of implementing these two algorithms in military networks is discussed and various performance measures are evaluated and shown as graphs.By implementing blow fish and CP-ABE as combined methods in confidential networks like military networks the efficiency can be increase with higher level of security.

References

[1]Abdul Shabbir, Anasuri Sunil Kumar (Jan2012) "An Efficient Authentication Protocol for Security in MANETs", IJCCT.
[2]AMSAT http://www.amsat.org.
[3]Abel Joy, Akhila H, Annie Chacko“Survey of Management of PHR by Secure Cipher Text Policy Attribute Based Encryption Scheme”, International Journal of Scientific & Technology Research Vol 3, Issue 4, APR 2014.
[4]DTN research group http://dtnrg.org.
[5]Jin Li, Kui Ren, and Kwangjo Kim “A2BE: Accountable Attribute-Based Encryptionfor Abuse Free Access Control”
[6]John Bethencourt, Amit Sahai and Brent Waters, “Cipher text policy attribute based encryption”
[7]Junbeom Hur and Kyungtae Kang,“Secure Data Retrieval for DecentralizedDisruption-Tolerant Military Network”,IEEE/ACM Transaction in networking VOL. 22, NO. 1, February 2014.
[8]J. Khabbaz, Chadi M. Assi, and Wissam
F. Fawaz “Disruption-Tolerant Networking: “A Comprehensive Survey on Recent Developments and Persisting Challenges Maurice”
[9]J.Jackson “Crypto analysis and security” pg.177-197.
[10]Lewko and B. Waters, “Decentralizing attribute-based encryption,” Cryptology ePrintArchive: Rep. 2010/351, 2010.\
[11]Udayakumar R., Kaliyamurthie K.P., Khanaa, Thooyamani K.P., Data mining a boon: Predictive system for university topper women in academia, World Applied Sciences Journal, v-29, i-14, pp-86-90, 2014.