International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 09, September 2015
Available at http://internationaljournalofresearch.org

Novel ECC Data Security & Privacy Preserving by using TCP-ABE Algorithm

Avula Sandhya[1]& Dr. Shaik Abdul Muzeer[2]
[1]M-Tech Dept. of CSE Megha Institute of Engineering & Technology for Women
[2]Professor & principal Dept. of CSE Megha Institute of Engineering & Technology for Women

ABSTRACT
So, a secure data retrieval scheme is needed for utilizing CP-Attribute based encryption for decentralized DTNs where multiple key ascendant entities manage their attributes independently. But the main drawback is that the updating of attributes is not so efficient and high intricacy.Here we verbalize over several encoding techniques for access control and secure data retrieval in Disruption- tolerant network environments. Some of the most intriguing issues in this assumption are the enforcement of approve policies and the policy updating for secure data retrieval. Secure data retrieval plays vital role in all communication environments. To communicate between nodes in the network data should transfer and any one can retrieve it securely. Disruption- tolerant network (DTN) technologies are considered to be sanctioning nodes to communicate with each other in the extreme networking environments. It stores and forward scheme by utilizing auxiliary storage nodes. Since the data is sensitive that one needs to consider the security policies of cryptographic solution like encoding techniques.In order to surmount the above cited quandaries I am proposing an incipient technique Trust predicated Cipher Text-Policy Attribute Predicated Encryption for reducing involution and withal to ameliorate the security in DTN.The concept of attribute-predicated encryption is a promising approach that full fills the requisites for secure data retrieval in DTN. The subsisting system involves cipher text-policy attribute-predicated encryption presentation, which provides a scalable way of encrypting informationthis that the encrypted defines the attribute put that the decrypted needs to process for decrypting the cipher text. However, the quandary of applying CP-ABE in decentralized DTN results in several security and privacy challenges with regards to the attribute annulment, key escrow, and categorization of attributes issued from different ascendant entities.

Keywords: CP-Attribute based encryption; Cipher text-policy attribute-predicated encryption**;** Disruption- tolerant network

1 Introduction

Advancement in technology and the quest for efficacious communication have led to the revelation of networks that are delay/disruption tolerant where some of the posits on which today's Internet was built no longer hold. These networks ranging from marine networks, mobile ad-hoc networks, wireless sensor networks, military tactical networks to deep-space networks all share a prevalent quandary. This prevalent quandary is their inability to sustain communication in the face of constraints like intermittent connectivity, high/variable delay, asymmetric data rates, high error rates and heterogeneity. To address this quandary, the Delay/Disruption Tolerant Networking (DTN) [1],

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 09, September 2015
Available at http://internationaljournalofresearch.org

[2] was proposed and the overlay network approach [3] was considered the most opportune. Its emergence opens incipient areas of research in security which includes key management, Denial of Accommodation (DoS) attacks, anonymity and privacy, access control amongst others. Access control is the main focus of this paper.

Many military applications require incremented auspice of confidential data including access operate methods that are cryptographically imposed. In many cases, it is desirable to provide differentiated access accommodations. In a network communication between two hosts should be encrypted to enhance security. There are variants of encryption algorithms utilized for transferring the data securely.

2. Related Work

2.1 ABE for Different Policies

ABE is genuinely a generalization of IBE (identity-predicated encryption [4]): in an identity-predicated encryption system, cipher texts are associated with only one attribute (the identity). The Attribute based encryptionsystem of Sahai-Waters [5] was proposed as a fuzzy identity-proclaimed encryption schema, which sanctioned for some error tolerance around the culled identity. In more recent terminology, it would be reported because a key-policyAttribute Based Encryptionschema that approves for threshold policies. Key-policy denotes that the encryptoronly gets to label a cipher text on a set of attributes. The ascendancy culls a policy for each utilizer that decides which cipher texts he can decrypt. A threshold policy system would be one in which the ascendancy designates an attribute set for the utilizer, and the utilizer is approved to decrypt when the overlap among this set and the set associated with a special cipher text is above a threshold.

Goyal et al. Proposed a key-policy-Attribute Based Encryptionsystem which fortifies whatever monotonic access formula lying of AND, OR, or threshold gates. A structure for Key Policy-ABE schema with nonmonotonic access structures (which additionally include NOT gates, i.e. negatively charged constraints in a key's access formula) was proposed by Ostrovsky, Sahaiplus Waters. All of these systems are characterized as key-policy Attribute based encryption since the access structure is designated in ye private key, as the attributes are acclimatized to report the ciphertexts. The functions of the ciphertexts and keys are turned in the ciphertext-policy Attribute based Encryption introduced by Bethencourt, Sahai and Waters [2], in that the ciphertext is encrypted access policy culled by an encryptor but akey is just engendered with veneration to an attributes set. The security of their system is indicated in the generic group pattern. Recently, [8] proposed CP-Attribute Based Encryption constructions connoted on a few different pairing posits which work for whatever access policy that can be expressed in conditions of an LSSS matrix. In such paper, we will appear only at the Key-Privacy-Attribute Based Encryption setting. We will visually study some the simple threshold, and the more puzzled monotonic access structure instance, and will build a construction predicated on the same postulations as Sahaipl us Waters and Goyal et al.[9]. Some non-monotonic access structures plus the ciphertext policy schemes require much more vigorous posits, and very different techniques, so we will not conceive these types in our work.

2.2 Problem Statement

In proposed System CP-Attribute based encryptionsystem for secure information retrieval in decentralized DTNs. Each local ascendancy effects partial personalized and attribute key

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 09, September 2015
Available at http://internationaljournalofresearch.org

components to a utilizer by performing secure 2PC protocol with the central ascendancy. Each attribute key of a utilizer can be updated individually plusinstantly. Thus, the measurability and protection can be enhanced in the proposed scheme. Since the first CP-ABE scheme proposed by Bethencourt et al. [10], dozens from CP-Attribute based encryption schemes have been proposed [12], [11]–[13]. The subsequent CP-ABE schemes are mostly motivated by more rigorous security proof in the standard model. Nevertheless, most of the systems failed to reach the quality of the Bethencourt et al.'s system, which reported an efficient system that was expressive in that it approved an encrypt or to express an access predicate in terms of any monotonic formula over attributes. Therefore, in this section, we formulate a variation of ye CP-Attribute based encryption algorithm partially predicated on (but not constrained to) Bethen court et al.'s construction in rate to enhance the quality of the access control policy in lieu of building an incipient CP-Attribute based encryptionsystem from scratch.

CP-Attribute based encryption is utilized to engender a private key of utilizer predicated on their attribute keys. Every time when a utilizer enters or abstracts from certain group then immediate key revocation is done. Updating attribute is not so efficient for every changes and it engenders high computation intricacy and communication cost.

3.Proposed Architecture

3.1 Trust based Cipher Text-Policy (ABE)

Secure data retrieval scheme is needed for utilizing CP-Attribute based encryption for decentralized Disruption Tolerant Networking's where multiple key ascendant entities manage their attributes independently. But the main drawback is that the updating of attributes is not so efficient and high involution. In order to surmount the above cited quandaries here proposing an incipient technique Trust predicated CP-Attribute based encryption, for reducing involution and additionally to amend the security in Disruption Tolerant Networking. Here data encryption and decryption implemented by elliptical curve digital signature algorithm and for key generation we used Diffie–Hellman key generation method.

3.2 ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic curve cryptosystems were invented by Neal Koblitzplus Victor Miller [15] in 1985. They can be looked at as elliptic curve analogues of the older discrete logarithm cryptosystems in which the subgroup of Zp * is replaced by the group from points on an elliptic curve over a finite field. Ye mathematical infrastructure for the surety of elliptic curve cryptosystems is ye computational intractableness from the elliptic curve discrete logarithm quandary. Elliptic curve discrete logarithm quandary is a relative of discrete logarithm cryptography. An elliptic curve E over Zp as in Figure 1 is defined in the Cartesian coordinate system by an equation of the form: y 2 = x 3 + ax + b (8) where a, b ε Zp, and 4a3 + 27b2 ≠0 (mod p), together with a special point O, called the point at illimitability. The set E (Zp) consists of all points (x, y), x ε Zp, y ε Zp, which gratify the defining equation, together with O. Each value of a and b gives a dissimilar elliptic curve. The public key is a point on the curve plus the private key is a desultory number. The public key is obtained by multiplying the private key with an engenderer point G in the curve. The definition of groups and finite fields, which are fundamental for the construction of elliptic curve cryptosystem are discussed in next subsections.

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 09, September 2015
Available at http://internationaljournalofresearch.org

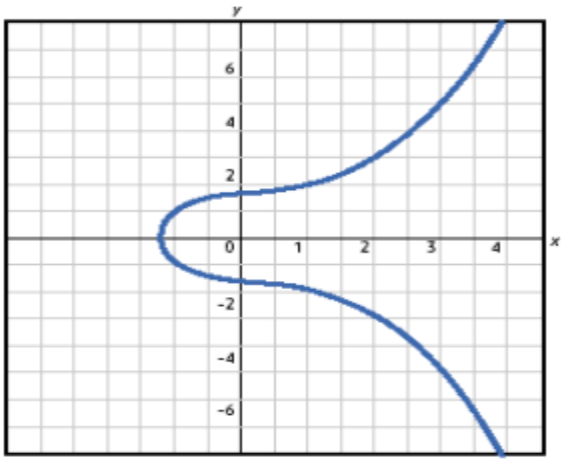


Figure 1. An Elliptic Curve

Advantages of ECC:

Thus, the ECC offered remarkable advantages over other cryptographic system.

1. It provides more preponderant security for a given key size.
2. It provides efficacious and compact implementations for cryptographic operations requiring more minuscule chips.
3. Due to more minuscule chips less heat generation and less power consumption.
4. It is mostly felicitous for machines having low bandwidth, low computing potency, less recollection.
5. It has more facile hardware implementations. So far no drawback of ECC had been reported.

3.3 Diffie–Hellman key generation

The Diffie–Hellman key replace algorithm solves the following dilemma. Alice and Bob want to allocate a secret key for use in a symmetric cipher, but their only betokens of communication is unsafe. Every piece of data that they replace is observed by their opponent Eve. How is it possible for Alice and Bob to apportion a key without making it available to Eve? At first glance it appears that Alice and Bob face an infeasible task. It was a brilliant perceptivity of Diffie and Hellman that the arduousness of the discrete logarithm quandary for F ∗ p provides a possible solution. The first step is for Alice and Bob to concur on an immensely colossal prime p and a nonzero integer g modulo p. Alice and Bob make the values of p and g public erudition; for example, they might post the values on their web sites, so Eve kens them, additionally. For sundry concludes to be talked over later, it is best if they optate g such that its order in F ∗ p is an astronomically immense prime.

The following step is for Alice to pick a secret integer a that she does not reveal to anybody, while at the same time Bob picks an integer b that he holds secret. Bob and Alice use their secret integers to compute

A ≡ g a (mod p) (Alice computes this) and B ≡ g b (mod p) | {z }(Bob computes this)

They next replace these calculated values, Alice sends A to Bob and Bob sends B to Alice. Observe that Eve gets to optically discern ye values of A plus B, since they are sent out over the dangerous communication channel. Conclusively, Bob plus Alice again usage their privy integers to compute

A1 ≡ B a (mod p) (Alice computes this) and B1 ≡ A b (mod p) (Bob computes this) .

The measures that they compute, A0 and B0 severally, are really the same,

since A1 ≡ B a ≡ (g b) a ≡ g ab ≡ (g a) b ≡ A b ≡ B1 (mod p).

This mutual value is their replaced key. The Diffie–Hellman key replace algorithm is summarized in Table 2.1.

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 09, September 2015
Available at http://internationaljournalofresearch.org

Public Parameter Creation	
A trusted party chooses and publishes a (large) prime p and an integer g having large prime order in $\mathbf{F}_p^*$.	
Private Computations	
Alice	**Bob**
Choose a secret integer a. Compute $A \equiv g^a \pmod p$.	Choose a secret integer b. Compute $B \equiv g^b \pmod p$.
Public Exchange of Values	
Alice sends A to Bob $\longrightarrow$ A	
B $\longleftarrow$ Bob sends B to Alice	
Further Private Computations	
Alice	**Bob**
Compute the number $B^a \pmod p$.	Compute the number $A^b \pmod p$.
The shared secret value is $B^a \equiv (g^b)^a \equiv g^{ab} \equiv (g^a)^b \equiv A^b \pmod p$.	

Table 2.1: Diffie–Hellman key exchange

4. Implementation

4.1 Diffie-Hellman key exchange using Elliptic Curve (DHECC)

An elliptic curve E over the finite field Fp is given through an equation of the form

Y 2 = X3 + aX + b,a,b ϵFp, and − (4a3 + 27b2) ≠ 0

Please note that as verbally expressed in the commencement of the section, the "=" should be superseded by a "≡" in the above definition. Another remark is that when we verbalize about partial derivatives we mean the "formal partial derivate" which can be defined (optically discern beginning of this section) over an arbitrary field. Suppose two communication parties, Alice and Bob, want to concur upon a key which will be later utilized for encrypted communication in conjunction with a private key cryptosystem. They first fine-tune a finite field Fq, an elliptic curve E defined over it and a base point B ϵ E (with high order). To engender a key, first Alice culls an arbitrary a ϵ Fq (of high order) which she keeps secret. Next she calculates aB ϵ E which is public and sends it to Bob. Bob does the same steps, i.e. he culls an arbitrary integer b (secret) and calculates bB which is sent to Alice. Their secret mundane key is then P = abB ϵ E.

An elliptic curve E over the field F is a smooth curve in the so called "long transform" Y 2 + a1XY + a3Y = X3 + a2X 2 + a4X + a6, aiϵ F

We let E(F) denote the set of points (x, y) ϵ F2 that slake this equation, along with a "point at infinity" denoted O. Recollect that smooth designates that there is no point in E(F) where both partial derivatives vanish. The definition given above is valid for any field. But in cryptography we are only intrigued with finite fields. Considering only finite fields we get an "easier" equation. Two finite fields are of particular interest. The finite field Fp with p ϵ P elements, because of it's structure, and the finite field Fqm with q = pr Elements, since setting p = 2 the arithmetic in this field will be apposite for implementations in hardware. For generation a shared secret between A and B utilizing ECDH, both have to concur up on EC domain arguments. Both end have a key pair consisting of a private key d(a desultorily culled integer less then n, where n is the order of the curve) and public key Q= d*G (G is the engenderer point). Let (dA,QA) be the private-public key pair of A and (dB,QB) be the private-public key of B.

1. The end A Computes KA= (XA, YA) = dA * QB
2. The end B Computes KB= (XB, YB) = dB * QA
3. Since dA * QB = dAdBG= dBdAG = dB * QA . Therefor KA= KB and hence XA =XB
4. Hence the shared secret is KA. Since it is practically impossible to find the private key dA or dB from the public key KA.

5. Conclusion

DTN technologies are becoming prosperous solutions in military applications that sanction wireless contrivances to communicate with to each one and access the confidential data reliably

by exploiting external storage nodes. CP – Attribute based encryption is a scalable cryptographic solution to the access control and secure data retrieval issues. In the subsisting system, an efficient and secure data retrieval method utilizing CP-Attribute based encryption is utilized for decentralized Distributed Tolerant networks where multiple key ascendant entities manage their attributes independently. The innate key escrow quandary is resolved this that ye confidentiality of the stored data is ensured even under the bellicose environment where key ascendant entities might be compromised or not plenarily trusted. In integration, the fine-grained key revocation can be done for each attribute group. But the drawback in this method is less trade off between the computational intricacy and security. So, in the proposed system incipient technique Trust predicated CP-Attribute based Encryption [17], for reducing involution and withal to amend the security in Distributed Tolerance Networks. Here data encryption and decryption implemented by elliptical curve digital signature algorithm and for key generation we used Diffie–Hellman key generation method.

6. References

[1.] Farrell, S., Cahill, V.: Delay- and Disruption-Tolerant Networking. Artech House (2006), ISBN 1596930632.

[2.] Cerf, V., Hooke, A., Torgerson, L., Durst, R., Scott, K., Fall, K., Weiss, H.: Delay-Tolerant Networking Architecture. IETF RFC 4838, April 2007.

[3.] Fall, K.: A Delay-Tolerant Network Architecture for Challenged Internets. SIGCOMM, August 25-29, 2003.

[4.] Adi Shamir. Identity-Based Cryptosystems and Signature Schemes. In CRYPTO, pages 47–53.Springer, 1984.

[5.] AmitSahai and Brent Waters. Fuzzy Identity-Based Encryption. In EUROCRYPT, volume 3494 of LNCS, pages 457–473. Springer, 2005.

[6.] VipulGoyal, OmkantPandey, AmitSahai, and Brent Waters. Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. In Computer and Communications Security, pages 89–98. ACM, 2006.

[7.] RafailOstrovsky, AmitSahai, and Brent Waters. Attribute-Based Encryption with Non-Monotonic Access Structures. In Computer and Communications Security, pages 195–203, 2007.

[8.] Brent Waters. Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization. Cryptology ePrint 2008/290.

[9.] VipulGoyal, OmkantPandey, AmitSahai, and Brent Waters. Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. In Computer and Communications Security, pages 89–98. ACM, 2006.

[10.] AmitSahai and Brent Waters.Fuzzy Identity-Based Encryption. In EUROCRYPT, volume 3494 of LNCS,pages 457–473. Springer, 2005.

[11.] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, “Mediated ciphertext-policy attribute-based encryption and its

application," in *Proc. WISA*, 2009, LNCS 5932, pp. 309–323.

[12.] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in *Proc. ACM Conf. Comput. Commun. Security*, 2007, pp. 456–465.

[13.] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute-based encryption," in *Proc. ICALP*, 2008, pp. 579–591.

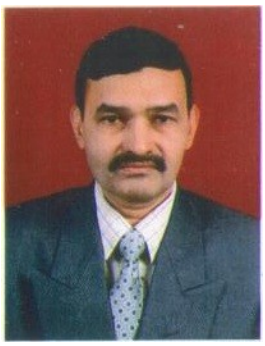
[14.] Koblitz, N., 1987. Elliptic curve cryptosystems. Mathematics of Computation 48, 203-209.

[15.] Miller, V., 1985. Use of elliptic curves in cryptography.CRYPTO 85.

[16.] Certicom ECC Challenge. 2009. Certicom Research.

[17.] S. Roy andM. Chuah, "Secure data retrieval based on ciphertext policy attribute-based encryption (CP-ABE) system for the DTNs," Lehigh CSE Tech. Rep., 2009.

Author Profile



Dr.Shaik Abdul Muzeer
Professor & Principal
Megha institute of Engineering & Technology for Women

Dr.S.A.Muzeer, at present working as a principal of Megha institute of engineering & Technology has completed his PG and P.HD in Electronics & Communication Engineering and published around 25 Papers in National & International Journals. His area of research is Digital signal processing and Bio-medical engineering