International Journal for Modern Trends in Science and Technology
Volume: 02, Issue No: 11, November 2016
ISSN: 2455-3778
http://www.ijmtst.com

Attribute Based Encryption - A Cryptographic Frame Work in a Shared Medium among Multiple Clients

P.Venkata Hari Prasad[1] | Dr.K.Gangadhara Rao[2] | Dr.B.Basaveswara Rao[3]

[1]Associate Professor, Department of CSE, DIET | Research Scholar, Acharya Nagarjuna University, Guntur, India.
[2]Associate Professor, Department of CSE, Acharya Nagarjuna University, Guntur, India.
[3]Department of CSE, Acharya Nagarjuna University, Guntur, India.

To Cite this Article
P.Venkata Hari Prasad, Dr.K.Gangadhara Rao and Dr.B.Basaveswara Rao, "Attribute Based Encryption - A Cryptographic Frame Work in a Shared Medium among Multiple Clients", *International Journal for Modern Trends in Science and Technology*, Vol. 02, Issue 11, 2016, pp. 224-229.

ABSTRACT

Steady Size Figure content Policy Attribute Based Encryption is a practical cryptographic framework to get entrance control of information that is shared between more than one client. In CCABE, each user has characteristics and related imparted information are encoded utilizing access control structures on rundown of qualities. A client can send encrypted cipher text to another user in any broadcasting medium. A valid user is one whose properties in the mystery key must fulfill the approach then just the user can decrypt the cipher text. But CCPABE is highly overhead when pairing operations are usually applied. Broadcasting message through the network requires less overhead and must decrypt the message within time. CCPABE approach which included in this study which performs well under the specified message size. Experimental results show that this approach performs constant time complexity, when encryption and decryption operations are performed.

Keywords—*Constant cipher text, Attribute based encryption, pattern policy, storage overhead, encryption and decryption.*

I. INTRODUCTION

Today for a couple of affiliations they have to store up their huge amount of data. Framework stockpiling suppliers are giving the advantages for these relationships as you need it. In un trusted stockpiling data servers are not allowed to take in the substance of delicate data, nor would they have the capacity to be relied on upon to maintain data access procedures. To keep data mystery to data servers, the data proprietor scrambles data before exchange. Customer access is yielded by having the data unraveling key(s). Exactly when this kind of cryptographic based access control arrangement gives security protection on data, there are moreover a couple of essential troubles identified with the arrangement layout (Shucheng Yu., 2010).

Trait based encryption, starting late made one-to-various open key cryptography, has discovered the chance to approve the extend access systems for endless scale structures. In ABE, information is connected with traits. Access strategies, characterized on qualities, are upheld inside the encryption system. Not the same as routine broadcast encryption, ABE offers the capacity to encode data without watchful dominance in the beneficiary set. From this

viewpoint the thought of ABE is about related to Role-Based/Attribute-Based Access Control and suitable for limitless scale applications.

In ABE, a customer puzzle key is described over properties and it doesn't have the adjusted correspondence using any particular customer. To ensure against key abuse attacks, we can play the same trap in ABE, as backstabber, after for an anomalous state view. In any case, concealed methodologies got by existing swindler taking after structures just can't be direct joined with ABE, in light of the fact that, authorities are addressed autonomously in conventional show encryption, while it is commonly not in ABE. A novel decision is needed for securing against key strikes for ABE. In doing accordingly, the absolute best test is the best approach to profitably direct after activities without being perceived through the suspected customers (Shucheng Yu., 2010).

In modern cryptography, the security of cipher is heavily depending on the secrecy of one's cryptographic key utilized by the cipher. Obviously, one of the most secure techniques to do this is to have the key in a single well-guarded location. However, after the "well-guarded" location is compromised, the system fails completely. Hence, the additional extreme would be to distribute the secret at multiple locations. However, this type de-centralized approach raises the vulnerability to failure and also makes the work of these, very potential attackers a lot simpler. Additionally, in the real world, the users and the key distributor would possibly not trust one another. Secret sharing then, feels like a good cope with such problems. In mystery imparting, a mystery is dispersed and imparted over an extensive variety of clients.

There are several important properties and security issues in CCP-ABE, such as the efficiency of cipher text-size, the expressiveness of decryption policy and the chosen cipher text security. The length of cipher text is a mainly concerned issue, since; the efficiency of bandwidth is very important factor in the communication networks. In mostly proposed CCP-ABE, the size of cipher texts depended on the number of traits in the entrance structure. The expressiveness of the entrance structure is also an important property of CCP-ABE, because if the scheme has more expressiveness then it can be supported more flexible access control. At the same time, the chosen cipher text security is mainly concerned security issue of CCP-ABE.

In a few circulated frameworks, a client ought to really have the capacity to get to information any, time a client has a certain scope of characteristics. The main system for upholding such arrangements is as a rule to contract a trusted server to collect the far reaching information and control access approaches. Nonetheless, if any trusted framework putting away the imparted information is bargained, likely the privacy of a given information will definitely be traded off. For giving secured access control on encoded information CPABE can be used. By utilizing this system scrambled information can undoubtedly be kept private maybe if the capacity framework is untrusted; additionally, these systems are secure against diverse plot assaults. Existing ABE based capacity frameworks provides the encrypted information what's more, incorporated arrangements with indicated client keys; though in our framework ascribes are used to clarify a client's security certifications, and an outsider scrambling information depicts a strategy for who can unscramble.

Figure content Policy Attribute Set Based Encryption is one of the type of CP-ABE, in which dissimilar to existing Cipher content Policy Attribute Based Encryption plans that speak to client properties for being solid starting in keys, sorts out client characteristics into your recursive set based structure and permits clients to force dynamic requirements concerning how, those credits may be consolidated to fulfill a strategy. In the following CP-ABE plan, unscrambling keys just bolster client properties that are composed legitimately for being single set, so clients are just ready to utilize every conceivable blend of characteristics in a solitary set issued on their keys to fulfill arrangements. To battle with this trouble, figure content strategy property set-based encryption happens. ASBE is an augmented system for CP-ABE which arranges, client characteristics directly into a recursive set structure.

II. Related Work

Within a key-approach quality based encryption (V. Goyal et al., 2006) system, cipher texts are named from the sender by utilizing an assortment of graphic traits, while client's private mystery is issued by the trusted trait power catches the strategy (alluded to as the entrance structure) that determines which sort of figure messages the fundamental component can unscramble. KP-ABE plans run well with organized associations with

principles about, who may read specific records. Common uses of KP-ABE incorporate secure scientific examination and target show. Fig. 1 demonstrates the structural planning of the information imparting framework, which comprises of the accompanying framework elements:

1. Key era focus: It is a key power that produces open and mystery parameters for CPABE. It is accountable for issuing, disavowing, and overhauling quality keys for clients.
2. Data putting away focus: It is a substance that gives an information imparting administration. It is responsible for controlling the gets to from outside clients to the putting away information and giving comparing substance administrations.
3. Data proprietor: It is a customer who claims information, and wishes to transfer it into the outside information putting away habitat for simplicity of offering or for expense sparing. A data proprietor is responsible for describing access course of action, and approving it in solitude data by scrambling the data under the methodology before passing on it.
4. User: It is a substance who needs to get to the information. If a customer has, a plan of properties satisfying the passageway methodology of the encoded data, and is not prevented in any from claiming the considerable property groups, then he will have the ability to unscramble the figure message and get the data.

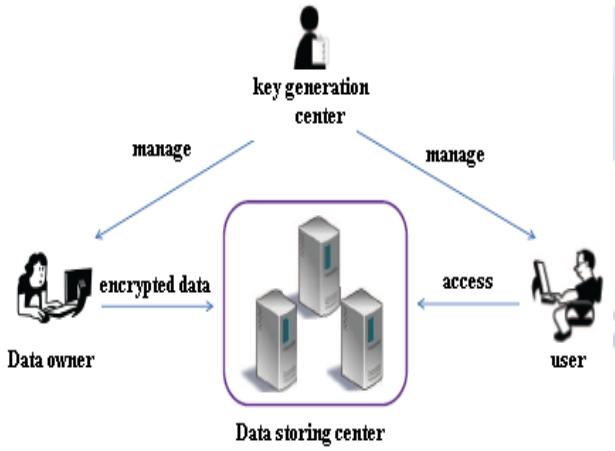


Fig: 2.1. Demonstrates the building design of the information offering framework

Nishide et al., (Delerablée C et al., 2007) expanded the plan into bolster strategy mystery. Goyal et al. gave the first standard model development of CP-ABE plan that could bolster flexible strat (Chase M., 2007). Cheung and Newport gave the essential model for development of CP-ABE plan. While their plan upheld both negative and positive traits it was really solely for approaches with single AND entryways.

III. A FRAME WORK OF PATTERN BASED ENCRYPTION ALGORITHM

Let u = {a1,a2… .. ak} be the Set of properties in the framework. Every ai has three qualitie a_i^+ denotes the user has a_i , a_i^- denotes the user does not have a_i , a_i^* denotes either a_i^+ or a_i^- [4].

Bilinear Maps:

Blending uses bilinear guide capacity E : , where C0 and C1 are two multiplicative cyclic gatherings with p substantial prime request.

Properties:

Bilinearity:

$$E(A^p, B^q) = E(A,B)^{pq}, \forall A, B \in C_0, \forall p, q \in Z_p^*$$

Nondegeneracy:

E (g,g) $\neq 1$ where g is generator of C_0

Algorithm steps:

This plan comprises of four central calculations:

Setup Function:

Input: Number of attributes k.

Output: Public key and Master Key.

Setup function takes number of attributes k as input and returns Public and Master key as output. Encryption function uses Public key and for private key, generation master key will be used.

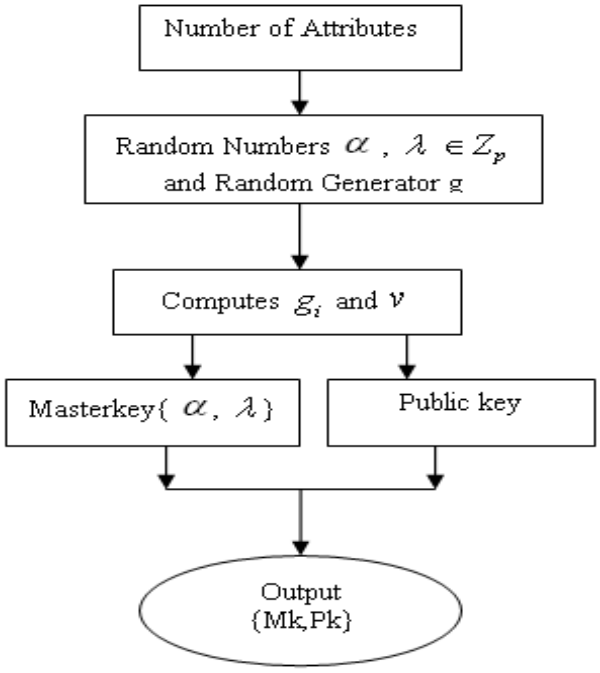


Fig: 3.1. Flow chart for public key and master key generation

Key Generation Function:
Input: Public key, Master Key and Attribute List
Output: Private Key.
The Key Generation procedure takes general society key, the expert key and the client's trait list as data .This capacity returns private key of the client as yield.

Encryption Function:
Input: Public key, Policies and Message.Output: Cipher text

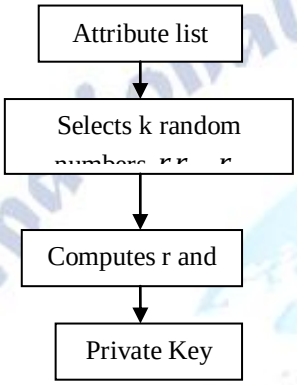


Fig: 3.2 Flow chart for private key generation

The Encrypt calculation takes the general population key, access strategy and the message M as data. The calculation gives ciphertext as yield, such that, just a client with trait rundown fulfilling the entrance strategy can decode the message.

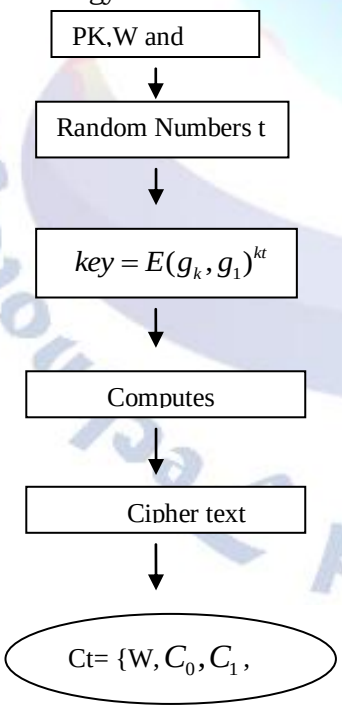


Fig: 3.3. Flow chart for encryption the text

Decryption Function:
Input: Public, Private Key and Cipher text.
Output: Message.

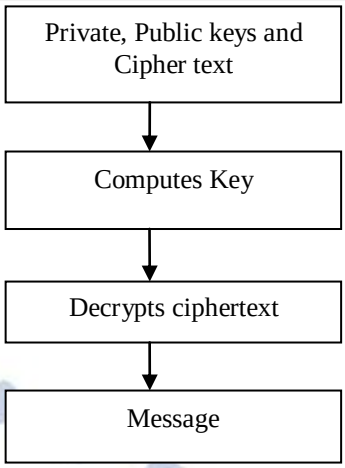


Fig: 3.4. Flow chart for decryption

The Decryption capacity takes people in general key, the private key of the client and the figure message as data. It gives back the plaintext M if a client list approach fulfills with the characteristic rundown.

IV. EXPERIMENTAL RESULTS

"All examinations were performed with the courses of action IntelCore prosser PR(TM)2 CPU 2.13GHz, 2 Giga Byte RAM, and the working system stage is Microsoft Windows XP Professional (SP2)".

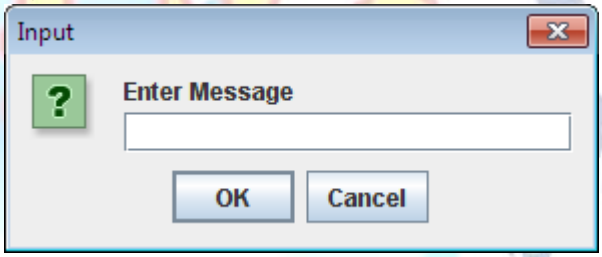


Fig:4.1 Enter Message to Encrypt using Proposed approach

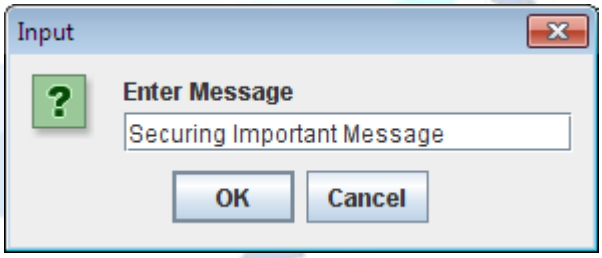


Fig: 4.2. Entered the message

Intermediate Result during Encryption and Decryption:
GENERATD PUBLIC KEY
730750818665451621361119245571504901405
97655961717005681
PRIVATE KEY INFORMATION :
cn:student1
Dept:CSE
sysadmin:csedept
uid:student1
Key Generation : 6.671 SECS

```
//end to keygen
//Executing encryption
ENCRYPTIONKEY=
{x=19950256062608947345878639899194504532147742516572502261828616071514724006665329752849477391829932008391113158089911841516141841002676342407190865540367 16,
y=41815802891228509744971018708059942231931685283127339324214008111935399257160980251567778180373003085054632217164791562695740671190612868285636882403507 92}
Encryption process : 4.324 SECS
//end of encryption
//Executing decryption
DECRYPTION KEY =
{x=19950256062608947345878639899194504532147742516572502261828616071514724006665329752849477391829932008391113158089911841516141841002676342407190865540367 16,
y=41815802891228509744971018708059942231931685283127339324214008111935399257160980251567778180373003085054632217164791562695740671190612868285636882403507 92}
Decryption process: 1.811 SECS
//end of decryption
```

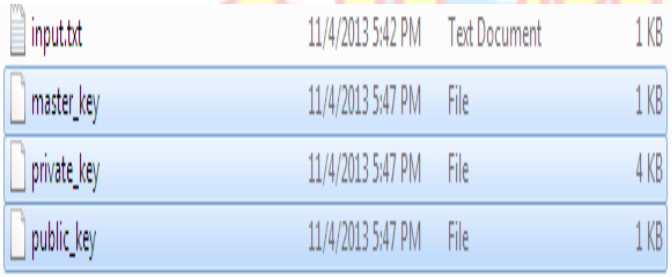
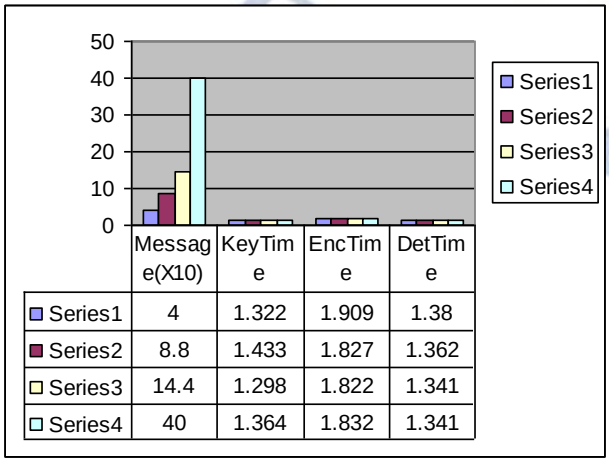
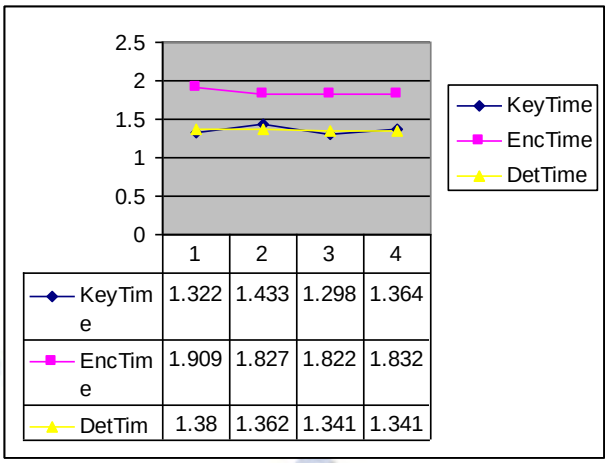


Fig: 4.3 Generated the keys

Performance Analysis: Graph 1 and 2 shows the comparison between Message in bytes with the Constant time for sending and Receiving:



	Message(X10)	KeyTime	EncTime	DetTime
Series1	4	1.322	1.909	1.38
Series2	8.8	1.433	1.827	1.362
Series3	14.4	1.298	1.822	1.341
Series4	40	1.364	1.832	1.341



	1	2	3	4
KeyTime	1.322	1.433	1.298	1.364
EncTime	1.909	1.827	1.822	1.832
DetTim	1.38	1.362	1.341	1.341

Fig: 4.4. The comparison between Message in bytes with the Constant time for sending and Receiving

V. CONCLUSION

In this study consistent Ciphertext Policy Attribute Based Encryption is tested with different message bytes. An experimental result shows that this system suffers communication overhead and storage overhead, when the message bytes size is increased during the broadcast mechanism. Also message security during the broadcasting does not give trust to the authorized users. An experimental result shows constant time display for the constant size message. In future this system can be improved by introducing secured encryption and compression mechanism for this constant based Ciphertext Policy Attribute Based Encryption technique.

REFERENCES

[1] Yu, Shucheng, et al. "Attribute based data sharing with attribute revocation." *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*. ACM, 2010.

[2] Goyal, Vipul, et al. "Attribute-based encryption for fine-grained access control of encrypted data." *Proceedings of the 13th ACM conference on Computer and communications security*. Acm, 2006.

[3] Zhang, Qiang, et al. "Megabits secure key rate quantum key distribution." *New Journal of Physics* 11.4 (2009): 045010.

[4] Delerablée, Cécile. "Identity-based broadcast encryption with constant size ciphertexts and private keys." *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, Berlin, Heidelberg, 2007.

[5] Chase, Melissa. "Multi-authority attribute based encryption." *Theory of Cryptography Conference*. Springer, Berlin, Heidelberg, 2007.