Journal of Science and Technology (JST)
Volume 3, Issue 2, March - April 2018, PP 11-17
www.jst.org.in *ISSN: 2456 - 5660*

Pattern Based Homomorphic Encryption Technique for Minimizing Computation and Communication Overhead

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

[1]*Associate Professor,CSE Dept,DIET, Research Scholar,, Acharya Nagarjuna University*
[2]*Associate Professor, Dept. of CSE, Acharya Nagarjuna University*
[2]*Dept. of CSE, Acharya Nagarjuna University*

Abstract: *Securing private information and distribution plays a vital role in distributed environment against the unauthorized users. Server information can be distributed to the authorized users based on the user's identity. Traditional identity based attack which breaks the user's identity and privacy during the communication process. Existing attribute based encryption and decryption process relay on policy tree structure and number of attributes in the setup phase. Due to identity based attacks, data communication within or outside the network changed or spoofed. Network communication cost increases as the number of users within the network increases. In order to overcome identity based attacks, a new pattern based user's identity or policy structure was implemented in this paper. In this work, each attributes along with user's policies are defined in the form of patterns. Each pattern has three parts with three operations namely policy AND, policy OR and policy ANY. During set up phase and encryption phase each user's profile is constructed in the form of patterns. Proposed pattern based mechanism minimizes the policy search space and decryption time during data communication. Experimental result shows that proposed approach completely protects against the identity attacks by minimizing the communication and storage overhead.*

Keywords - *Policy protection, data privacy, pattern policy, storage overhead, encryption and decryption.*

I. INTRODUCTION

A broadcast encryption scheme is used whenever an source person wants to send messages to several receivers using an unsecured network channel. This type scheme actually allows the broadcaster to go with dynamically a subset of privileged users in the set of all possible authorized receivers and to send a cipher text, readable only by the privileged users. This sort of schemes is helpful in various real time applications such as the documents sharing within the LAN and internet or broadcast of multimedia content. Many schemes have also been suggested to solve this problem regarding communication overhead. The first phase applies to almost fixed sets of authorized users. In this case the encryption process is efficient but modifying the set of privileged users entails the sending of causing long message. In the second phase, setting is intended for day-to-day self-management of very large or minimal sets of privileged users. Schemes develop for that purpose allow one to change without payment the desirable of privileged users however the size of the encryption grows linearly when using the size of the desirable of revoked users[1].

Ciphertext-Policy Attribute-Based Encryption addresses some communication overheads. This system identifies a user with a set of attributes instead of its identity. A person would be able to decrypt personal files, given that his/her attributes satisfy the access policy associated with the ciphertext as shown in fig 1. Encrypt messages will specify through an access tree structure a policy. Decryption users access policy tree structure to decrypt the message. The most ideal advantage of CPABE over public key cryptography is less overhead for your key management infrastructure. Inside a scenario exactly where the private key associated with a user is compromised, then the files that could be decrypted making use of the attributes of that specific user will be compromised. This ensures better security in CPABE, when compared with Symmetric Key Encryption. In CP-ABE, data is encrypted dictated by access structure in a way that just those whose attributes satisfy this structure, can decrypt the answer. Unauthorized users are unfit to decrypt the ciphertext even if they are able to collide[2-3].

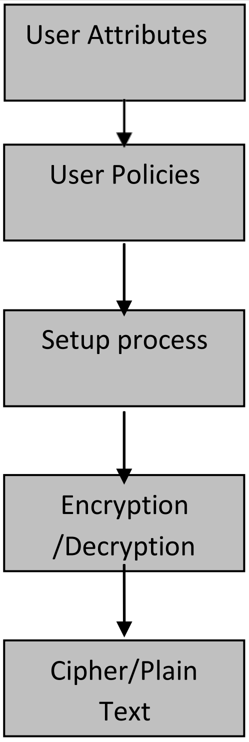


Fig 1 Basic Attribute Based Encryption and Decryption

II. RELATED WORK

Sahai and Waters in the paper [2] proposed an idea of Attribute-Based Encryption. Two types of ABE schemes are introduced: One is Key-Policy ABE schemes and the other is Ciphertext Policy ABE schemes [2,3]. In Key-Policy ABE schemes[7], a ciphertext is associated with a multitude of attributes and a user secret key is involved with an access structure. User who has secret key can decrypt the cipher-text if the user's attributes associated with the cipher-text satisfies the policy access structure associated with the secret key. A related work to KP-ABE serves as a method of key search on encrypted data . In CPABE the purpose is reversed. A ciphertext is associated with the access structure and of course the user secret secret is involved with particular attributes. User who has secret key can decrypt the ciphertext if the attributes connected with the secret key satisfy the access structure related with the ciphertext.

The efficiency of those schemes can only be proved when few users are revoked, yet the binary tree structure presented in [4-5] together with its following improvements may be designed to characterize teams of users by attributes: for instance, the left subtrees of one's internal nodes on a given level may refer to users with the use of a given attribute, and the right subtrees to users with this attribute missing. The access policy is defined using the content, and attributes are utilized to build decryption keys handed to users. These ciphertext-policy attribute-based encryption schemes have direct applications for broadcast: the access policy defines specific privileged users. With a relevant distribution of attributes, any privileged users might be described by an access policy.

Attribute Computation Scheme: Non-interactive Attribute computation enables a computationally source client to outsource the computation associated with a function to one or maybe more users. The workers return the answer of one's function evaluation and also a noninteractive proof the fact that the computation of a given function was accepted out correctly. As they schemes deal with outsourcing of general computation problems and certainly preserve the privacy of input data, they might be used to outsource decryption in ABE systems. However, the schemes proposed being used fully homomorphic encryption system being a building block, and as a consequence the overhead of these schemes is at the moment too large to remain practical. This provides input and output privacy yet data modification that happened in cloud couldn't be identified.

Revocation of some authorized user especially hard to accomplish efficiently in CP-ABE that is usually addressed by extending attributes with expiration dates or by an authority distributing keys with expiration dates [6]. In some cases, a tree of revocable attributes may have to become maintained and a trusted party granted to validate the revocation statuses of users; the control access could be system-wide or maybe more fine-grained. A revocation process using linear sharing and binary tree techniques, where each user is associated which includes an identifier on any revocation tree, is one example. The problem this particular general approach within the mobile context is the idea that it a change in mobile users required to incur the communication amount of continually requesting new keys, while wireless communication always remains expensive. Also, the data owner is typically a mobile user as well, and in consequence the owner cannot effectively manage access control on demand for additional users on account of its transient connectivity. Revocation for data outsourcing purposes has been proposed that relies upon stateless key distribution and access control toward the attribute level, but requirements trusted authority and encumbers the data owner utilizing a pairing operation [7], a cryptographic function that's very computationally expensive.

III. PROPOSED APPROACH

Setup Process: In this process, two set of lists are taken as input namely policies list, user's attribute list. Each policy list is partitioned into three parts one is AND operator, second one is OR operator and the third is ANY operator. Each pattern is partitioned with its length delimiter and then flag and pattern hash is calculated.

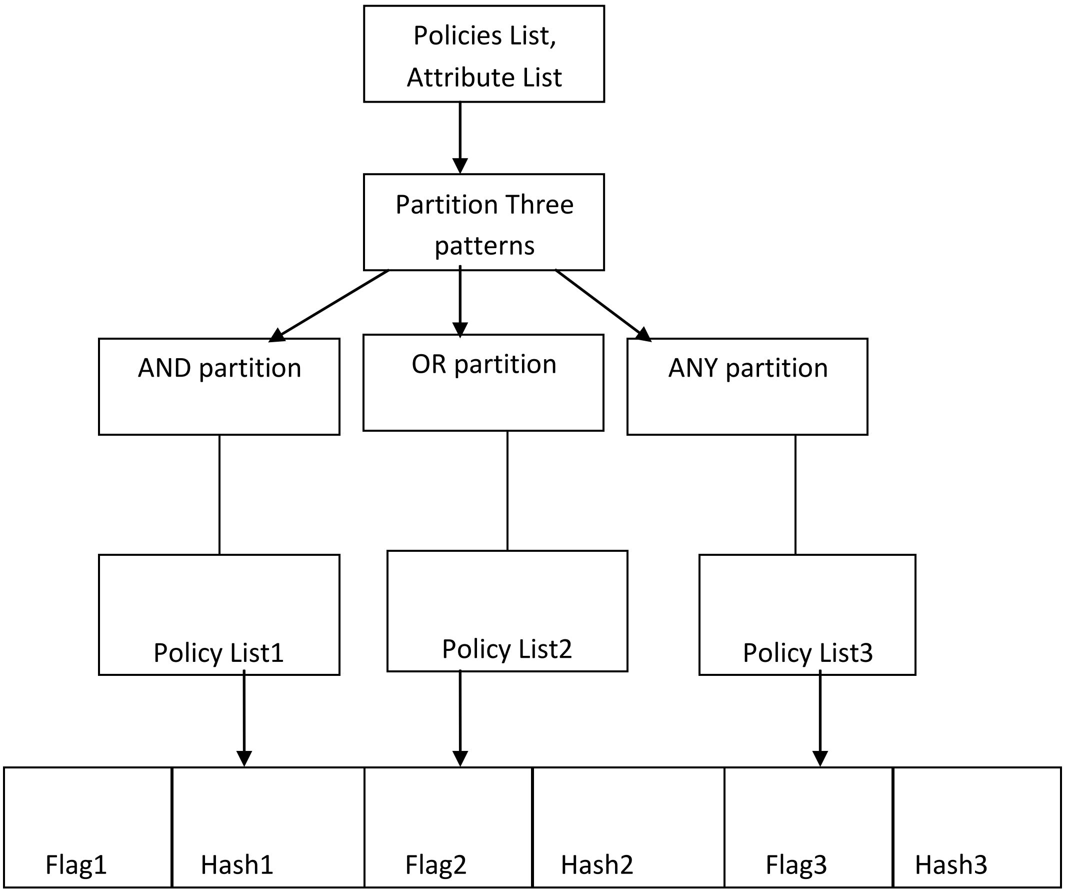


Fig 2. User policy structure definition

Encryption Process:

Input: Public key, Policy Patterns, Message;

Procedure:

Public Key :={ $S', g_p, g_q, g_r, G_\alpha, G_\beta, G_\gamma$, H'_1, H'_2, H'_3; };

Calculations:

$C_0 = g_p^{S'}$;

$C'_0 = g_p^{(\alpha+\beta+\gamma)}$; Where $\alpha, \beta, \gamma \in G_\alpha, G_\beta, G_\gamma$;

$C_{1,i} = g_p^{H'_2+H'_3} . g_p^{H'_1+\alpha}$ i:=0……pat1.length;

$C_{2,j} = g_p^{H'_1+H'_3} . g_p^{H'_2+\beta}$ j:=0……pat2.length;

$C_{3,k} = g_{p}^{H'_1+H'_2} . g_{p}^{H'_3+\gamma}$ k:=0…..pat3.length;

Cipher Text CT={ Tp, H'_1, H'_2, H'_3,M.e($Enc(M_1 + M_2)$,Enc($M_1 . M_2$)),{ $C_{1,i}, C_{2,j}, C_{3,k}$ },C};

Decryption Process:

Input: CipherText

Decryption:= M. $e(g_p, g_p)^{S'(\alpha+\beta+\gamma)}$ /e(C,D*A)

:= M. $e(g_p, g_p)^{S'(\alpha+\beta+\gamma)}$ /e($g_p^{S'}, g_p^{\alpha} . g_p^{\beta+\gamma}$)

:= M. $e(g_p, g_p)^{S'(\alpha+\beta+\gamma)} / e(g_p^{S'}, g_p^{\alpha+\beta+\gamma})$

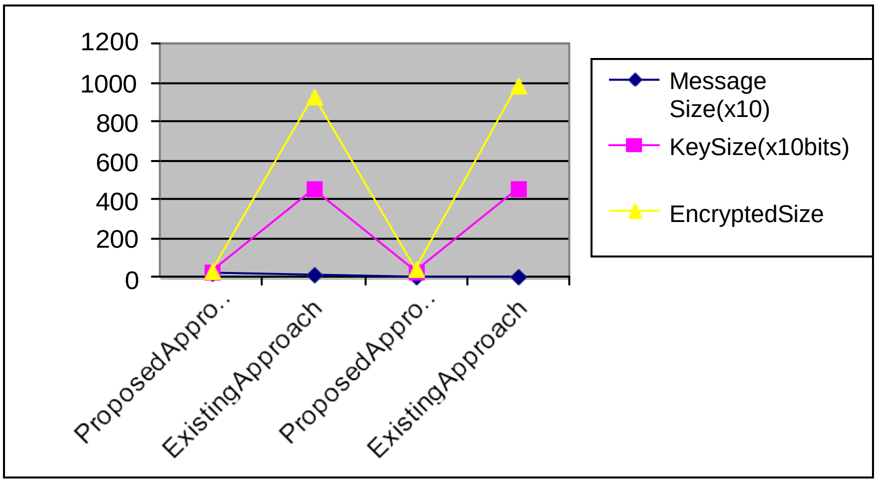
:= M. $e(g_p, g_p)^{S'(\alpha+\beta+\gamma)} / e(g_p, g_p)^{S'(\alpha+\beta+\gamma)}$

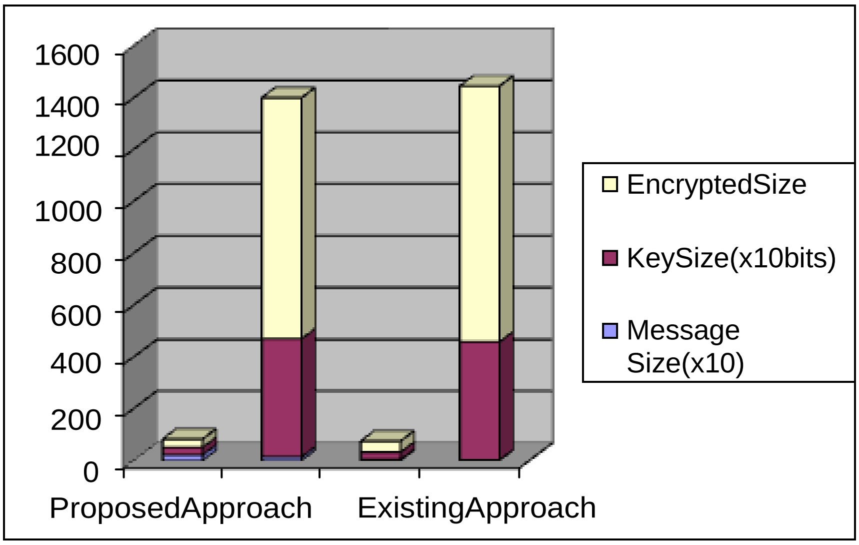
:= M

IV. RESULTS

COMMUNICATION OVERHEAD:

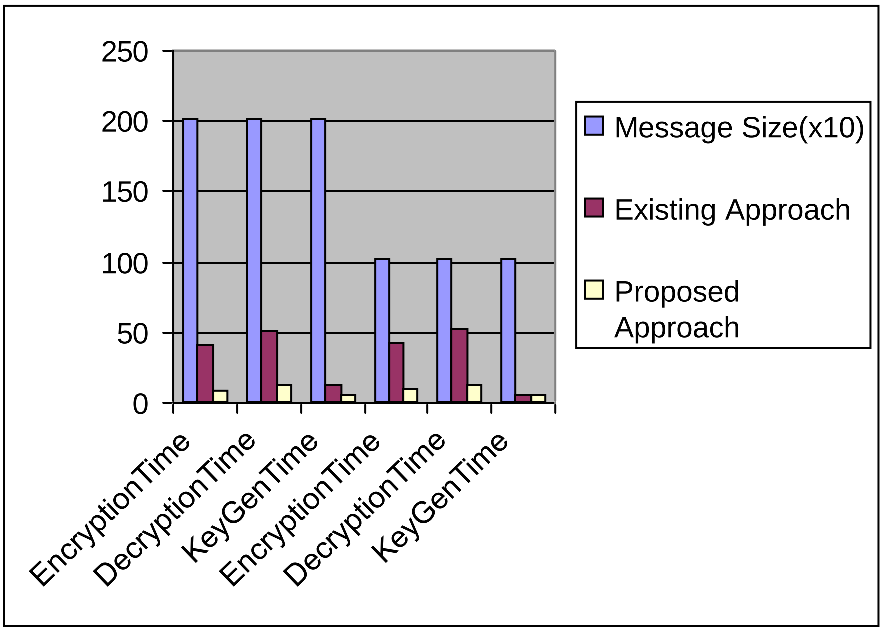
	Message Size(x10)	KeySize(x10bits)	EncryptedSize
ProposedApproach	22.8	28.7	32
ExistingApproach	14.8	456.6	930
ProposedApproach	4.88	28.7	42
ExistingApproach	3.88	456.6	986



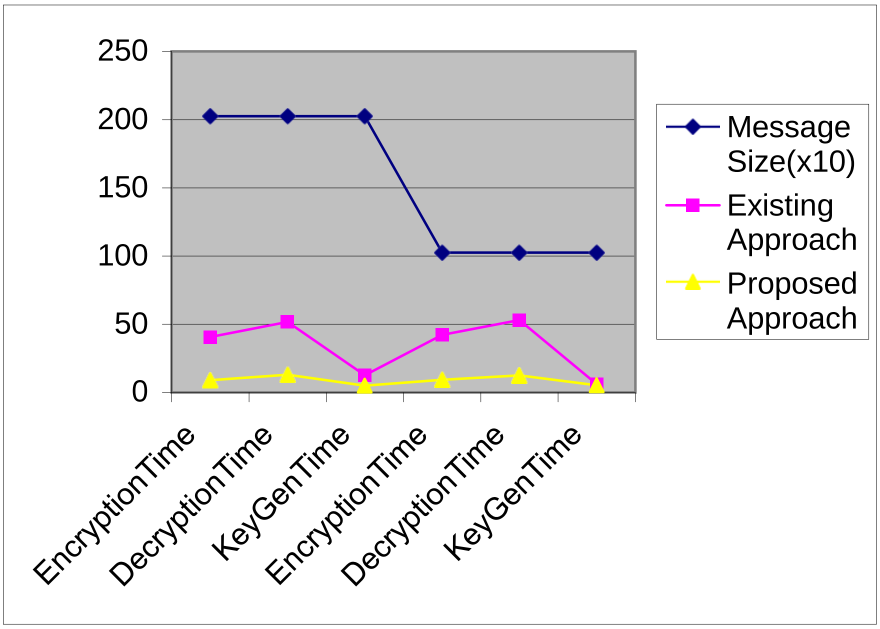


COMPUTATIONAL OVERHEAD

	Message	**Existing**	**Proposed**
	Message Size(x10)	**Existing Approach**	**Proposed Approach**
EncryptionTime	202.4	40.5	8.9
DecryptionTime	202.4	51.6	12.92
KeyGenTime	202.4	12.4	4.99
EncryptionTime	102.4	42	9.24
DecryptionTime	102.4	53	12.5
KeyGenTime	102.4	5.99	5.34



Bar Graph :Message Encryption and Decryption Computation in Proposed and Existing System



Line Graph: Message Encryption and Decryption Computation in Proposed and Existing System

V. CONCLUSION

In this paper, a secured identity attack resistance based encryption and decryption model is proposed. This model successfully works against identity type of attacks. This model takes linear constant time at encryption and decryption process. Present model minimizes the Communication overhead and storage overhead during the broadcasting messages. Experimental results are executed on different message sizes with different policies. Finally, proposed approach outperforms well compare to existing models in terms of time and overhead is concern.

REFERENCES

[1] RAKESH BOBBA, OMID FATEMIEH, FARIBA KHAN, ARINDAM KHAN, CARL A. GUNTER, HIMANSHU KHURANA, and MANOJ PRABHAKARAN,Attribute-Based Messaging: Access Control and Confidentiality, ACM Transactions on Information and System Security, Vol. 13, No. 4, Article 31, : December 2010.

[2] Nuttapong Attrapadung, Javier Herranz, Fabien Laguillaume, Benoˆıt Libert, Elie de Panafieu, and Carla R`afols, "Attribute-Based Encryption Schemes with Constant-Size Ciphertexts", PKC 2011.

[3] Fugeng ZENG, Chunxiang XU,Attribute-based Signature Scheme with Constant Size Signature, Journal of Computational Information Systems 8: 7 (2012) 2875–2882.

[4] V.Abinaya, IIV.Ramesh,Attribute Based Mechanism Using Cipher Policy Verification, International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014).

[5] Peifung E. Lam, John C. Mitchell,Declarative Privacy Policy: Finite Models and Attribute-Based Encryption, ACM 978-1-4503-0781-9/12/01.

[6] Qinyi Li, Hu Xiong, Fengli Zhang,"An Expressive Decentralizing KP-ABE Scheme with Constant-Size Ciphertext", International Journal of Network Security, Vol.15, No.3, PP.161-170, May 2013.

[7] John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-policy attribute-based encryption. In Proceedings of the 2007 IEEE Symposium on Security and Privacy, SP '07, pages 321–334.