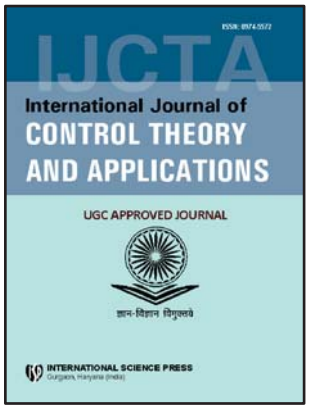


International Journal of Control Theory and Applications

ISSN : 0974-5572

© **International Science Press**

Volume 10 • Number 33 • 2017

Fine Grained and Filtered Access Control Policies in Distributed Host Based Storage

Syamala Saisree. Mallubhotla[a] and Manna Sheela Rani. Chetty[b]

[a]*Research Scholar, Department of Computer Science Engineering, K L University, Guntur, Andhra Pradesh, INDIA.*

E-mail: syamalamallubhotla71@gmail.com

[b]*Professor, Department of Computer Science Engineering, K.L. University, Guntur, Andhra Pradesh, INDIA.*

E-mail: sheelarani_cse@kluniversity.in

Abstract: Distributed Host based data storage is an advanced and empirical concept in present days for out sourcing of data in Host based. Distributed file storage requires Clients trust on their required data which is given to service provider of the Host based computing. Because of increasing security and protection concerns in out sourced data in Host based storage, traditionally several approaches like Feature Related Encryption (FRE) have been proposed to provide access specified control based on Client activity in out sourced distributed environment. This schema follows symmetric key approaches to provide security in Host based computing. Symmetric key approach is not suitable for supporting authorization effectively because, it uses single key for encryption and decryption. Presently authors focus on centralized approaches for proving security using single key distribution center. A new decentralized grained access control approach is required for privacy on data storage that supports anonymous authentication. In this paper we propose and develop an approach *i.e*. Filtered Based Hierarchal Access Control Mechanism (FBHACM) to achieve fine grained, flexible and scalable access control in Host based computing for secure distributed Host based storage. Our proposed approach is not only perform scalable due to its pyramid structure, it also share effective and flexible access control in supporting on FRE, it also assigns for Client expiration time and revocation which is efficient than existing schemas. Our experimental results show effective data share in distributed environment with feasible data retrieval with access permissions in distributed computing.

Keywords: *Host based Computing, Feature Related Encryption. Flexible, Access Control, Pyramid Structure, Distributed Host based Storage.*

1. INTRODUCTION

Host based computing is a casual keyword for the delivery of hosted services over web service which includes computer resources. Different companies enable Host based computing to compute resources as utility to maintaining Host based infrastructures with relevant network services in network. Based on services of distributed computing, following modules are as follows:1. Individual Data Outsourcing 2. Elasticity with Flexibility 3. Client Services by Paying Money. These 3 services can be public, private and hybrid. Private

services are outcome from business which maintain data centers to applications used Clients in data storage. Private Host based services achieve connivance, preserving management control and security. In public Host based model, middle service provider achieves and outcome Host based service over web service provider. These services are sold on demand and usage on Host based computing, customers pay for CPU operations, storage and bandwidth of clients consuming. Based on application usage in real time Host based environments like IBM, HCL and other distributing events shows efficient advantages in real time applications.

Figure 1: Distributed Host based Infrastructure Framework

As shown in figure 1, distributed Host based computing refers to configure, manipulate applications on web with application processes. If offers online data storage, infrastructure and application outsourcing in Host based . It offers development and service models for manipulate applications in distributed storage system [2][3]. Recently Host based file storage is an emerging concept in implementation of distributed Host based computing, Clients concerns about privacy of data storage that impacts Host based computing from different operations. These concerns are complicated from sensible data in public Host based. It is maintained by unfavorable CLOUD SERVICE PROVIDER. Feature Based Encryption follows primitive security from untrusted Clients while data sharing in Host based . Still now there are two kinds of FRE approaches were proposed to provide security in Host based : Key Policy based FRE (KP-FRE) and Encrypted text Policy FRE (CP-FRE). In KP-FRE, access control policy is assigned in secure format in terms of private key with sequential storage of Host based data, where as CP-FRE follows security as private key in terms of Encrypted text [5]. By preferring these conditions FRE gives privacy & way for data Client to distribute out sourced data to untrusted data storage service provider instead of described and feasible server with specified large amount of Clients in Host based computing.

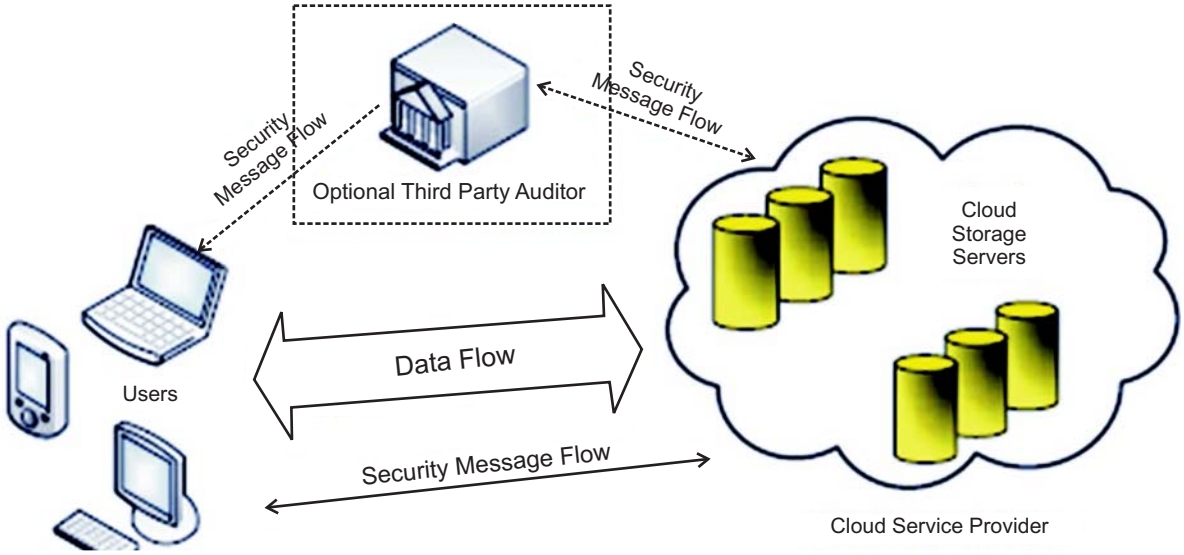


Figure 2: Ensuring data storage security in distributed Host based computing

Consider the effective disadvantage of FRE is communication with computational cost while decoding with decryption phase in data sharing. Procedure of ensuring secure file storage environment as shown in figure 2. FRE needs to increase efficiency, introduce outsourced Anonymizationmity FRE which provides outsourcing intensive computed task during decryption phase to CLOUD SERVICE PROVIDER without producing data or primitive keys, was introduced in [6][7]. For example, in mobile Host based application development; data collecting nodes as mobile devices or sensors has limited computation ability to complete encryption and decryption stages with residual execution of data sharing to protect sensitive data in public Host based . Therefore computational storage intensive tasks performed by resource constrained Client's data sharing Host based computing. Beyond that decryption is heavy complex task while number private keys used in data sharing from group of Clients then it may overload while features authority in Host based data storage. So, we propose to develop Filtered Based Hierarchal Access Control Mechanism (FBHACM) for access control in Host based computing. FBHACM enhances the Encrypted text policy Feature based encryption for data prediction and secure storage with hierarchical or pyramidal structure of system Clients presentation to achieve scalable, flexible and fine grained access control procedure in real time distributed environment. Contributions of proposed work as follows:

1. We show how FBHACM coming from FRE with pyramid structure to improve scalability, flexibility while at the same time extends the properties of fine grained access control of Feature set based encryption (ASBE).
2. Demonstrate and implement full-fledged fine grained access control based on FRE, This schema supports for pyramid based structure with Client grant and revoke, file creation, file forwarding, file deletion in distributed Host based data storage.
3. Formalize the security of our proposed approach based on CP-FRE schema with computational performance of application data sharing in distributed environment.
4. Implement FBHACM and then conduct comprehensive experiments in terms of performance evaluation that demonstrate FBHACM gives satisfactory performance with reduced complexity.

Paper Organization: Section 2 describes related work with literature review on security in Host based computing. Section 3 describes Feature based encryption procedure for providing privacy to data sharing in Host based computing with architectural implementation. Section 4 formal to implement Scalable Feature Based Encryption implementation with design. Section 5 discusses experimental evaluation with comparative results to decrease computational overhead to provide security in Host based computing. Section 6 concludes overall conclusion of providing security using FBHACM with decrease of computational overhead in Host based computing.

2. BACKGROUND RELATED WORK

In this, we review the process of feature centered protection and also provide brief summary of the feature set centered protection and also we analyze current accessibility management schemas depending on feature centered protection.

K.,X.Jia,K.Ren, and B. Zhang [4] This document explains information accessibility management which is a highly efficient approach so that the details protection in the reasoning. Despite, because of details freelancing and untrusted reasoning web servers, the details accessibility management becomes a examining problem in allocated storage frameworks.

W.- G. Tzeng [5], This document shows recommend efficient and protected (string) unaware transfer (OT1n) programs for any n _ 2. We set up our OT1 n strategy from central cryptographic techniques straight. The receiver's decision is truly protected and the secret of the unclosed expert information relies upon on the solidity of the decisional Diffie-Hellman problem. S. Yu, C. Wang, K. Ren, and W. Lou[11] This document represents Personal Health Record (PHR) is a creating patient-driven model of wellness data trade, which is frequently contracted to be put away at an outsider, for example, reasoning providers [11]. However, there have been wide protection problems as individual wellness data could be provided to those outsider web servers and to unapproved events.

A. joicy, [1] This document current a novel kind of cryptographic strategy, which encourages any pair of customers to provide securely and to validate each other's represents without trading personal or open important factors, without keeping key indices , and without using the companies of an outsider [12]. The program expect the existence of reliable key era concentrates, whose only objective is to give every customer a personalized amazing card when he first be a part of the organize.

A. Sahai and B. Rich waters,[4] This document current another sort of Identity-Based Encryption (IBE) strategy that we contact Unclear Identity-Based Encryption. In Unclear IBE we see a way of life as set of informative features. A Unclear IBE strategy considers a personal key for a personality, ω, to deEncrypted a Encrypted text scrambled with a personality, ω_ , if and just if the individualities ω and ω are near each different as calculated by the "set cover" separating measurement [13].

V. Goyal, O. Pandey, A. Sahai, and B. Rich waters,[3][4] This document shows As more sensitive details is shipped and put away by outsider places on the Internet, there will be a need to scribe details put away at these locations. One issue with development details is that it can be specifically allocated just at a coarse-grained level (*i.e.*, giving another collecting your personal key). We build up another cryptosystem for fine-grained discussing of secured details that we contact Key-Policy-Feature-Based Encryption (KPFRE) [7].

By and by, the agreement utilized the cover up strategy and in this way leaded to spilling of personal details. Atallah and Li analyzed the problem of handling the modify separating between two successions and showed a highly efficient conference to securely delegate collection connection with two web servers. Moreover, Ben and Atallah maintained to the point of protected freelancing for generally appropriate direct statistical computations. In fact, the suggested conferences required the expensive functions of homomorphic protection. Atallah what's more, Frikken further focused on this problem and provided improved conferences considering the expected incapable secret covering doubt [8][9]. These days, Wang et al. provided efficient

elements for protected freelancing of straight development computation. We take note of that however a few programs have been knowledgeable about securely delegate sorts of expensive computations, they are not appropriate for keeping in mind FRE computational expense of exponentiation at customer side. To achieve this purpose, the traditional technique is to use server-helped techniques. Be that as it may, past jobs are found to quickening the rate of exponentiation using untrusted web servers. Straightforwardly using these systems in FRE will not perform efficiently. Another technique may be to guide delayed wide freelancing process or giving computation in light of completely homomorphism protection or Client-friendly proof structure. In any case, Gentry has revealed that notwithstanding for incapable protection factors on “”bootstrapping”” function of the homomorphic protection, it would take no less than 30 a few moments on an top level machine [10]. In this way, regardless of the fact that the protection of the details and generate can be stored by using these general techniques, the computational expense is still tremendous and unfeasible.

3. SECURE HOST BASED STORAGE WITH FRE

In this section, we discuss about outsourced FRE and its procedure implementation and design. Secure data outsourcing is an emerging concept in real time Host based data sharing. Conventionally propose FRE with Anonymization Feature control and Anonymization Feature control-F to allow Host based service providers to provide access privileges and control Clients based on their identity and knower information in out sourced Host based as shown in figure 3.

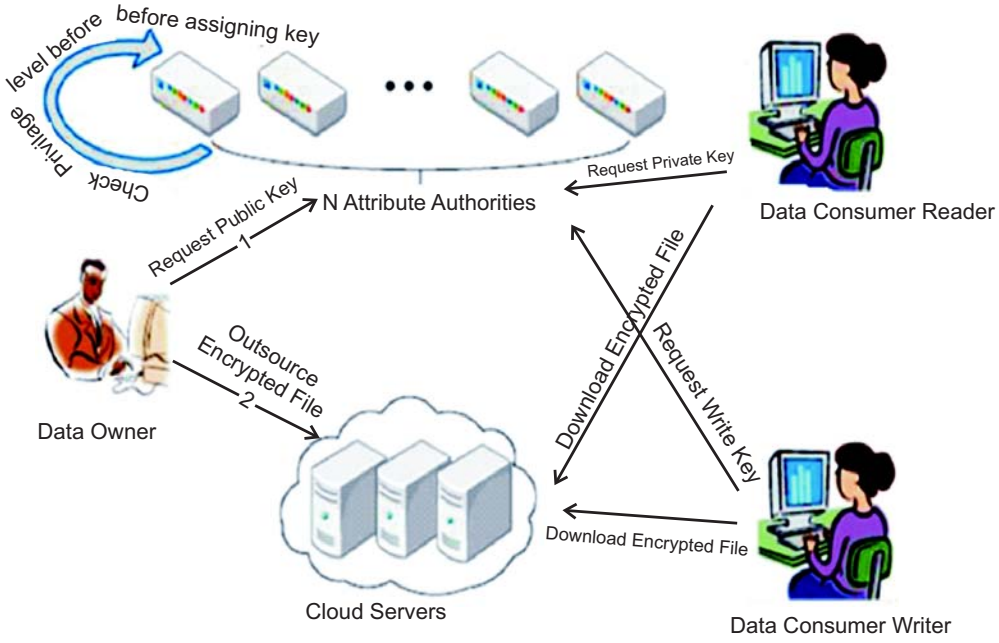


Figure 3: Anonymization and Anonymization Control-F implementation procedure

This schema is able to provide Client’s privacy against single Client authority in possibility of individual founded information [1]. Partially data enclosed with Anonymization Feature Control and no information in Anonymization Feature Control-F then multi authority based encryption achieves Anonymization Control sequences. Following steps are helpful for development of Anonymization Control F-measure in outsourced data in Host based computing.

1. **Registration with Community Authentication :** Specifically more number of peoples were registered to contribute their working procedure in Host based data sharing and also add some more friends for uploading, downloading required files.

2. **Feature Based Encryption :** Utilizing for every node encrypts information store. After encrypted information and again the re-encoded the same information is utilizing for fine-grain idea utilizing client information transferred. The quality in feature based protection has been proposed to secure the distributed storage with FRE [20][21][22]. In such encryption conspire, a character is seen as an arrangement of illustrative features, and decoding is conceivable if a decrypt or's personality has a few representations with the one indicated in the encrypted text.
3. **Multi Authority :** This group-authority collaborative system is displayed in which every Client has its Client id and they can cooperate with every key generator (authority) utilizing different code representations. We will probably accomplish a group-authority CP-FRE which accomplishes the privacy as characterized above; assurances the security of Data Consumers" personality data [7][8] [14]; and endures dependent attacks on the authorities to process individual security concerns. Anonymization Feature Control-F directly measures privacy of Anonymization Feature Control but extra computational communication overhead is incurred by oblivious transfer data in distributed Host based environment. Supporting Client revocation is an emerging concept in real time Host based application development.

4. SYSTEM DESIGN AND IMPLEMENTATION

Procedures of Host based computing under consider five following steps: Host based Service Provider, Client's Data, Data Consumers based o their Features, Domain Authorities with Features and Trusted Authority for Clients.

1. **System Design:** As depicted in fig 4, CLOUD SERVICE PROVIDER controls overall Host based to provide information with security and storage service. Data entrepreneurs secure their information in terms of data files and then store them into Host based for information discussing into other information customers.

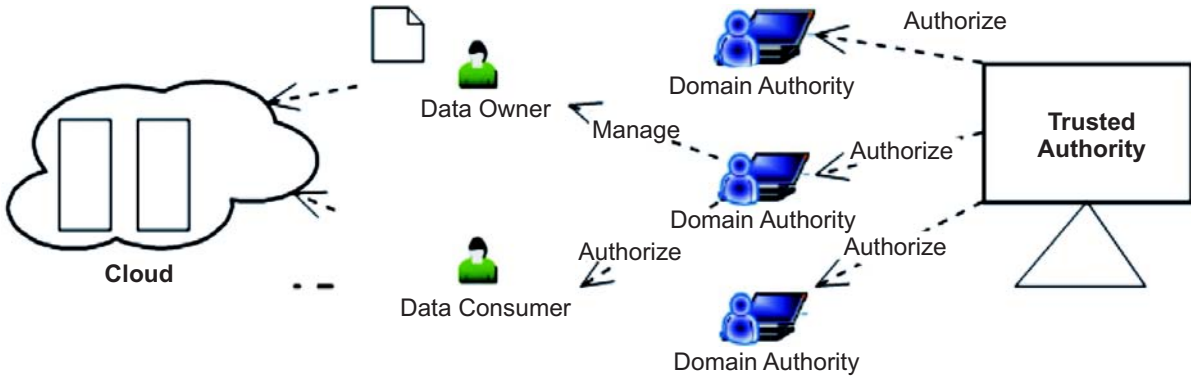


Figure 4: Proposed Approach Implementation Procedure

To access their data files information customers decrypt information submitted from information entrepreneurs. Each information owner or information consumer administrated by sector power, Domain power managed by reliable sector power provider [15][19].

2. **FBHACM schema Implementation:** The suggested FBHACM schema totally expands FRE to handle chart structure of the program customers shown in figure 5. Remember suggested approach program design comprises multiple sector regulators, reliable regulators with numerous customers corresponding to information consumers and information owners. Trusted regulators maintain, managing and spread program factors with master private important factors as well as approve parent sector regulators. So sector power is responsible for assigning secrets of subordinate regulators at each level of description with feasible reflection of information based on its sector.

Main operations of FBHACM are as follows: we are ready to develop following steps to implement scalable access control environment to share Client's data into different domain authorities.

System Setup, Domain Authority, Client Grant, File Creation, Client Revocation, File Access and File Deletion. Procedure of developing these steps achieved as follows:

System Setup: Host based distributed environment trusted authority achieves implementation procedure to create public key (PK) parameters and Victim Key (VK_0). PK will store data as public to visible data to all persons in same time VK_0 will be secret to data sharing. Setup $d = 2 \rightarrow$ (PK, VK0), where d is depth measure of key structure store in procedure. Implementation procedure selects bilinear group B of unique order p with generator g and then random exponents $\delta, \gamma_i \in Z_p$, $A_i\{1, 2\}$. To support generated key design with proper structure of depth d and i is the range from 1 to d. The procedure for PK and VK_0 is as follows:

$$\begin{aligned} PK &= (B, g, h_1 \\ &= g^n, f_1 \\ &= g^{\frac{1}{n}} \\ h_2 &= g_n, \\ f_2 &= g^{1/n}, e(g, g)\delta) \\ VK_0 &= (\gamma_1, \gamma_1, g^{\delta}) \end{aligned}$$

Main Level Domain permission Authority: Main Feature domain authority conceive with unique representation *i.e.* ID and recursive Feature set $Z = \{C_0, C_1, C_2, C_3, \ldots C_m\}$ where $C_i = \{c_0, c_1, c_2, \ldots\ldots c_m\}$ with $a_{i,j,}$ it is being able to generate *jth* Feature in C_i and n_i being presentation of all the Features in C_i then create Domain Authority(DA) as follows:

$$\begin{aligned} VK_i &= Z, D \\ &= g^{\frac{(\delta + g\{\mu\}}{\gamma_1}}, \\ D_{i,j} &= g^{\gamma_i^{\{m\}}} . H(C_{i,j})^{\gamma_{i,j}^{\{m\}}}, \\ \tilde{D}'_{i,j} &= g^{\gamma_{i,j}^{\{\mu\}}} \text{ for} \rightarrow (0 \le i \le m), (1 \le j \le n_i) \\ E_i &= g^{\frac{(\gamma^{\{\mu\}} + \gamma_i^{\{m\}})}{\gamma_2}} \text{ for} \rightarrow (1 \le i \le m)) \end{aligned}$$

In the above victim key reflection E_i is for interpretation from $r^{\{\mu\}}$ of C_i at the converting components E_i and E_i' can be used in decryption process.

Client Grant: When customers signify as u and new subordinate sector power denoted as DA_{i+1} wants to be a part of in to system for giving authorization to other customer present immediately reasoning data discussing with possible connections created by managing the domain authority. Create Client using victim key proceeding Feature set using create domain authority procedure with secret key as follows:

$$\begin{aligned} VK_{i+1} &= (\tilde{Z}, \tilde{D} = D. f_1^{\tilde{\gamma}\{\mu\}}, \tilde{D}_{i,j} = D_{i,j} . g_1^{\tilde{\gamma}\{\mu\}} . H(C_{i,j})\gamma_{i,j}^{\{\mu\}} \\ \tilde{D}_{i,j} &= \tilde{D}_{i,j} . g^{\gamma_{i,j}^{\{\mu\}}} \text{for} \rightarrow C_{i,j} \in \tilde{Z} \\ \tilde{E}_i &= E_i . f_2^{\tilde{\gamma}\{m\} + \tilde{\gamma}_i^{\{\mu\}}} \text{for} \rightarrow C_i \in \tilde{Z} \end{aligned}$$

The newly generated secret key VK_{i+1} for key structure $\tilde{\mathbb{C}}$, it is equivalent received key from trusted authority.

Data file Creation: To guard information saved on the reasoning, a information proprietor first encrypts information and then stores the secured information on the reasoning. Before posting file into reasoning prepared by information proprietor as follows: Pick file exclusive id, arbitrarily select symmetrical information security using Encryption and then decrypt with Decryption process, describes shrub accessibility framework [18][19].

Client Revocation: Whenever there is a person to be suspended, the system must make sure the suspended customer cannot connect to the associated information any more. One way to resolve this problem is to re-encrypt all the associated information used to be utilized by the suspended customer, but we must also ensure that the other Clients who still can get rights to these information can accessibility them properly. FBHACM gets the advantage of FRE in efficient customer cancellation.

File Deletion: Encrypted information can be removed only at the demand of the information proprietor. To remove an secured computer file, the information proprietor delivers the file's exclusive ID and its trademark on this ID to the reasoning. Only upon successful confirmation of the information proprietor and the demand, the reasoning removes the information file.

5. EXPERIMENTAL SETUP

In this section, we analyze theoretical computation of complexity of proposed schema at each operation. Then we implement an FBHACM based on CP-FRE and also defines series of experiments to evaluate performance of our proposed schema with comparison of outsource Anonymizatio FRE. Theoretical implementation already discussed in above section with feasible implementation.

Performance Evaluation: We have implemented multi level FBHACM based on CP-FRE which is pair based cryptography. Experimental setup conducted on laptop with I3 processor 4GB RAM running Windows Operating system successfully. It's implementation as follows:

FBHACM Setup: Generates a public key PK and Victim key operates VK_0.

FBHACM Key Gen: Generates key structure using PK and VK_0, usually supported depth of key structure maintain in between 1 and 2.

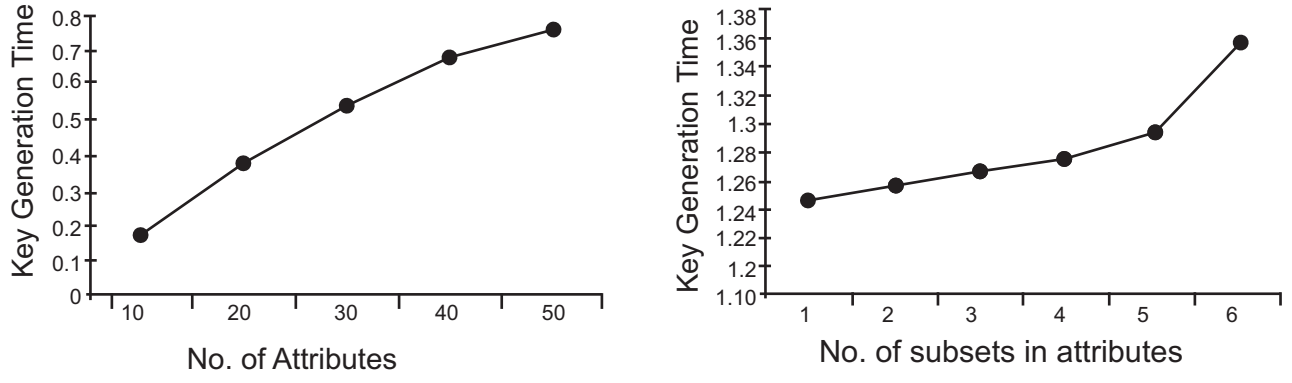


Figure 5: Tests on system setup and top-level sector power allow. (*a*) Top-level sector power allow (the variety of subsets in the key framework is 1); (*b*) top-level sector power allow (the count of features in the key framework is 50)

FBHACM-KeyDel: In Domain authority, some parts are private keys to new Clients in DA_{i+1} in its domain presentation. Delegated key is equivalent to generated private keys by Root Authority in data access control.

FBHACM KeyUp: Firstly generate PK with Features; while Clients decide to change PK in data sharing then usually generates updated PK with new Features.

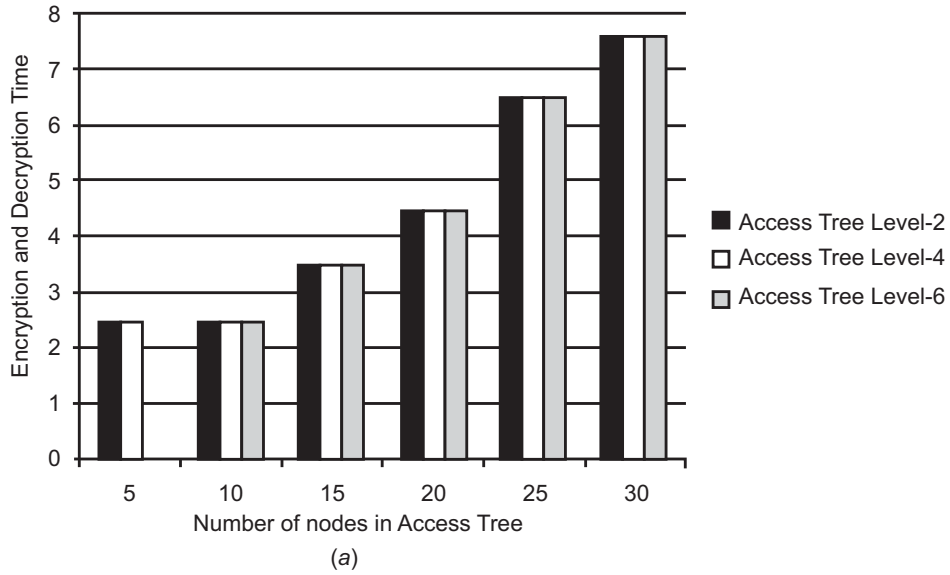
FBHACM Enc: Do encryption on files under an access tree policy specified in developed procedure.

FBHACM Dec: Using private keys and then decrypts a file.

Following figure shows proposed system setup to maintain key structure using different parameters with respect to time. This figure achieves only performance of proposed approach only because of drawback in FRE as suitable maintenance of privates key with their depths.

Performance *w.r.t* to Maintain Key Structure with different paradigms *i.e*, they are key generation time with number of Features and second one is key generation time with subset of Features.

This procedure performed with command line FBHACM-KeyGen is determined by the variety of subsets and features in the key framework creation. This process is conducted only one sub set present in key framework, expenses previously improved based on variety of features improved. Practical implementation of key update, data encryption and decryption assigned based on Features added to the domain authority.



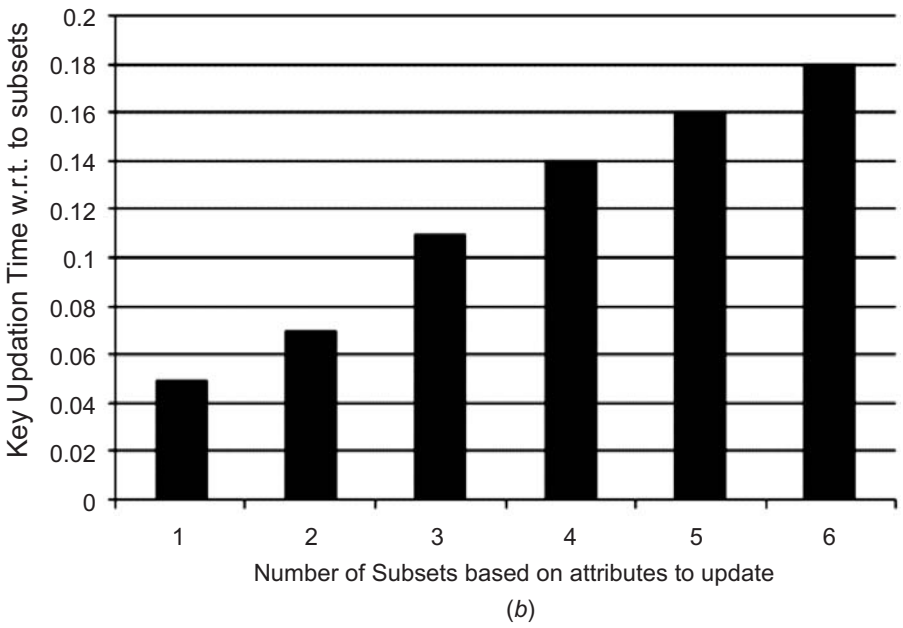


Figure 6: Experiments setup on file encryption & decryption, (*a*) Encrypt/Decrypt file operations based on access tree based on Features (*b*) key update generation time with sub set Features achieved in access tree operations

Client revocation basically consists two operations i.e. Key Update with new features (Features) and Data Encryption/Decryption; Key update is generalized with KeyUp command in FBHACM for operations effective utilization. Domain authority assigns new Features to the Client authority; O (1) is the average time complexity in new Features added to subset of private keys analyzed with subsets. FBHACM-Rec is used to encrypt and decrypt file with different access tree levels in real time application development. Procedure for key update and file encryption and decryption shown in figure 6 with subset Features and newly added features by domain authority. We can see effective performance of proposed approach with representative Features in real time Host based development.

6. CONCLUSION

In this paper, we implement FBHACM scheme for realizing the flexible, scalable and dependable feature access control in distributed Host based environment with computational implementation. The FBHACM incorporates pyramid structure of systematic Client's implementation by improving outcome delegation procedure to FRE. FBHACM not only supports relevant features due to flexibility feature set combinations with data client removable revocation because of multiple analyzed features with newly added features to upload file. Finally our proposed schema conducted theoretical and practical experimental setup and evaluation, it shows efficiency in Client revocation and computational overhead with existing schemas.

REFERENCES

[1] M. Suriyapriya1, A. Joicy, "Attribute Based Encryption with Privacy Preserving In Clouds", International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: 2 Issue: 2, 231-236, 2015.

[2] C. Wang, Q. Wang, K. Ren, N. Cao and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing", *IEEE T. Services Computing*, vol. 5, no. 2, pp. 220–232, 2012.

[3] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in *IEEE INFOCOM*. , pp. 441–445, 2010.

[4] A. Sahai and B. Waters, "Fuzzy identity based encryption," in Proc. Acvances in Cryptology—Eurocrypt, 2005, vol. 3494, LNCS, pp. 457–473.

[5] S. Kamara and K. Lauter, "Cryptographic cloud storage," in *Financial Cryptography Workshops*, ser. Lecture Notes in Computer Science, vol. 6054. Springer, pp. 136–149, 2010.

[6] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-based authentication for cloud computing," in *CloudCom*, ser. Lecture Notes in Computer Science, vol. 5931. Springer, pp. 157–166, 2009.

[7] A.-R. Sadeghi, T. Schneider, and M. Winandy, "Token-based cloud computing," in *TRUST*, ser. Lecture Notes in Computer Science, vol. 6101. Springer, pp. 417–429, 2010.

[8] R. K. L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B. S. Lee, "Trust cloud: A framework for accountability and trust in cloud computing," HP Technical Report HPL-2011- 38. Available at http://www.hpl.hp.com/techreports/2011/HPL-2011- 38.html.

[9] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," in *ACM ASIACCS*, pp. 282–292, 2010.

[10] D. F. Ferraiolo and D. R. Kuhn, "Role-based access controls," in *15th National Computer Security Conference*, 1992.

[11] D. R. Kuhn, E. J. Coyne, and T. R. Weil, "Adding attributes to role-based access control," *IEEE Computer*, vol. 43, no. 6, pp. 79–81, 2010.

[12] M. Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multiowner settings," in *SecureComm*, pp. 89–106, 2010.

[13] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in *ACM ASIACCS*, pp. 261–270, 2010.

[14] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in *ACM CCS*, , pp. 735–737, 2010.

[15] F. Zhao, T. Nishide, and K. Sakurai, "Realizing fine-grained and flexible access control to outsourced data with attribute-based cryptosystems," in *ISPEC*, ser. Lecture Notes in Computer Science, vol. 6672. Springer, pp. 83–97, 2011.

[16] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed access control in clouds," in *IEEE TrustCom*, 2011.

[17] S. Ruj, M. Stojmenovic and A. Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds", *IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, pp. 556–563, 2012.

[18] S. Jahid, P. Mittal, and N. Borisov, "EASiER: Encryption-based access control in social networks with efficient revocation," in *ACM ASIACCS*, 2011.