International Journal of Research in Advent Technology, Special Issue, March 2019
E-ISSN: 2321-9637
International Conference on Technological Emerging Challenges (ICTEC-2019)
Available online at www.ijrat.org

Experimental Study Of User Revocation And Dynamic Operations Over Cloud Server

M.A. Chakravarthi, M.Tech, (PhD) [1], B.Ravali, K.Mounisha, K.Hemanth kumar, M.Prathysusha [2]
[1] *Associate Professor, Department of CSE, Tirumala Engineering College, Narasaraopet, Guntur, Andhra Pradesh.*
[2]*Pursuing B.Tech Final year, Department of CSE, Tirumala Engineering College, Narasaraopet, Guntur, Andhra Pradesh.*
[1]*me.chakravarty@gmail.com,* [2]*bayyanaravali29@gmail.com, mounishakondapati98@gmail.com , kannahemanthkumar1700@gmail.com , prathyusha61@gmail.com*

Abstract: In this paper we identify challenges associated with cloud-based security system and possible provide solutions to understand existing research work conducting compressive review on different access control mechanisms and the extended HCP-ABE framework consists of four entities Data owner (DO), Data User (DU), Cloud service provider (CSP) and Attribute Authority (AA), a Data owner outsource sensitive document to the cloud and define a set of policies over encrypted data, Attribute authority manages attributes of different users and issues token keys, data user can download any document from the cloud but for decryption user policies should satisfy the ciphertext then only it converts if not it won't. In this paper providing possible solutions for data confidentiality, integrity, efficient user revocation and dynamic operations over cloud data. The experimental result shows the proposed scheme reduced 15 % time complexity and the contributions in this thesis unique and considered as extended methods to improve data security and to support efficient user revocation and dynamic data operations.
Keywords: HCP-ABE, CP-ABE, Access control policy ACP.

1. INTRODUCTION

In today Internet has grown to be persistent in daily livelihood furthermore Cloud computing is a rising model where computing resources offered over the Internet as scalable, on-demand (Web) services. An association deploy internet service needs to use enormous amounts of money on infrastructure needs to serve feasible users which is not a problem for large venture but when it comes to Small and Medium Enterprises or Enterprises affordability becomes a huge factor with the huge infrastructure come problems like machines failure, hard drive noises, software bugs, etc. Here might be a big problem for such a community. Cloud Computing is the ultimate solution to this problem. Rather than buying, installing and operating its own systems, an organization can rely on a cloud provider to do this for them. Cloud Computing key market leaders like Google, Amazon and Microsoft etc, these providers introduce new operating and business models that allow customers to pay for the resources they completely use, instead of making tremendous upfront investments. Cloud computing is a paradigm where resources or services (Infrastructure, platform, software and database) delivered over the internet, and it provides computing power to computing infrastructure, application and business process can be accessed as a service wherever and whenever you need them. Cloud-deployed in four ways private, public, hybrid and community cloud, due to flexibility and services many of the users are migrating to the cloud to avoid the local burden, once data outsourced to the cloud any user can access but due to security issues, the outsourced data must encrypt before placing to the cloud. In existing most of the research work focused on key management issues and static access policies but due to user dynamic the access control mechanism should design for proactive strategies. To support dynamic access control and operations Homomorphic ciphertext policy-Attribute based encryption (HCP-ABE) scheme intended. The purposed HCP-ABE consists of five fundamental algorithms, and each algorithm having the specific functionality they are Setup, Key generation, Encryption, Decryption and Update Encrypt, firstly Public key (PK), Master key (MK) are generated for this input as implicit parameters. Secondly, secret key (SK) created based on user attributes for this required PK; thirdly, Plaint text converted into an unreadable mode to do this PK, Access list AL and Access structure AS are needed. Fourthly Cipher text transformed into the plain text to do this secret key (SK) is necessary. Finally, dynamic operations (update, delete and append) on encrypted data to accomplish this ciphertext CT required.

2. IMPLEMENTATION

The Figure 6.1 shows the Engineering College hierarchy structure with the different departments depends on upon the nature of the work and authorization level of each user. The access policies can be created and managed by system authorities according to the nature of the documents uploaded into the cloud. Consider the role of various

employees denoted with the notations as the Board of Directors (BOC), Administration officer (AO), Principal, CSE Dept, ECE dept and EEE department; these departments upload various documents to the cloud. The hundreds or thousands of access control policies that can be easily created and maintained by system authorities using cuckoo filter data structure. The purpose of using a cuckoo filter is to alleviate the storage problem and role explosion issues which usually faced in role-based access control techniques. The following are the sample access control policies which are managed by the system authorities.

ACP_1 = (role = "BOD", {< overall college activities>, < Revenue details}
ACP_2 = (role = "AO", {<set and monitor the college student fee details >, <View production reports>}
ACP_3= (role = "Principal", {< monitor each department activities>})

ACP_4 = (role ="CSE", {<Control CSE department activities >})

ACP_5 = (role ="ECE", {<Control ECE department activities >})

ACP_6 = (role ="EEE", {<Control EEE department activities >})

$ACP_{7=}$ (role ="Assistant professor", {<Monitor student details >})
$ACP_{8=}$ (role ="Lab assistant", {<Monitor book details>})

The system authority generates the RSA keys and access token for each policy. The access token is unique for each subgroup, and it is maintained in a cuckoo hash table, further, the token mapped with each subgroup users. As per example, the first ACP says that the board of directors can monitor the administration activities and revenue details. The ACP_2 intended for presidents who can set and monitor the organizational goals and view production reports and general managers can monitor various department details as shown in ACP_3. The remaining ACP's are related to monitoring the documents related to different departments by various department employees. The CP-ABE scheme can be applied to the group the members and further identify the users for subgroups according to the access control policies. Then the user can access the file based on the token issued by the system authority.

3. ANALYSIS OF EXPERIMENTAL RESULTS

The algorithm of HCP-ABE scheme setup () and key_generation () are made before initiation of communication. We observed that optimized HCP-ABE scheme took less time complexity when compared to existing access control schemes. The overhead of 15% more time in optimized scheme is attributed to the fact that it involved pre-computation phase where some to cpu intensive values are computed beforehand.

HCP-ABE Encryption and Decryption: We have assessed the performance for new and existing algorithms with revoked user-list size of 1,000 to 10,000, we observed that optimized HCP-ABE scheme implementation took 20% less time compared to existing Access controls. We observed that optimized HCP-ABE scheme exhibited better performance with larger datasets.

***Attribute Based Cryptosystem KeyGen and Setup*:** The time required for pre-computation phase for optimized ABE scheme was 200 milliseconds and was constant even with increasing number of records. The ABE setup took 68 ms and ABE-OPT required 40 ms which excludes the pre-computation phase time, KeyGen took 819 milliseconds and 661 milliseconds for ABE and optimized ABE algorithms respectively.

Attribute Based Cryptosystem Operations: We observed that optimized ABE has taken 40% less time when assessed with datasets of size 2,000 to 20,000 which is due to optimizations we have performed to base implementation.

Average Computation Time of various phases of file Upload.

File Size (KB)	Total Time (Sec)	Data Transmission Time (Sec)	Encryption Time (Sec)	Key Management (Sec)
1	0.0474	0.0344	0.011	0.002
10	0.0641	0.0431	0.017	0.004
50	0.0962	0.0682	0.022	0.006
100	0.1331	0.0711	0.055	0.007
1000	0.1705	0.0845	0.077	0.009

Table 1 Average Computation Time of various phases of file Upload.

In table 1 Average time calculated for different file size (in kb) for this parameters are considered time taken to encrypt the data, for key management and data transmission to cloud storage.

Average Computation of various phases of file Download

File size (KB)	Total time (sec)	Data Transmission (sec)	Encryption time (sec)	Key management (sec)
1	0.06	0.038	0.021	0.001
10	0.087	0.046	0.037	0.004
50	0.165	0.058	0.052	0.055
100	0.193	0.061	0.065	0.067
1000	0.26	0.074	0.097	0.089

Table 2 Average Computation of various phases of file Download

In table 2 Average time calculated for file decryption from the cloud server, to this few parameters are considered like total time is taken for downloading the file from the cloud server and of different sizes.

In fig 1 and 2 denotes average computation time to complete the file upload and file download with different file sizes.

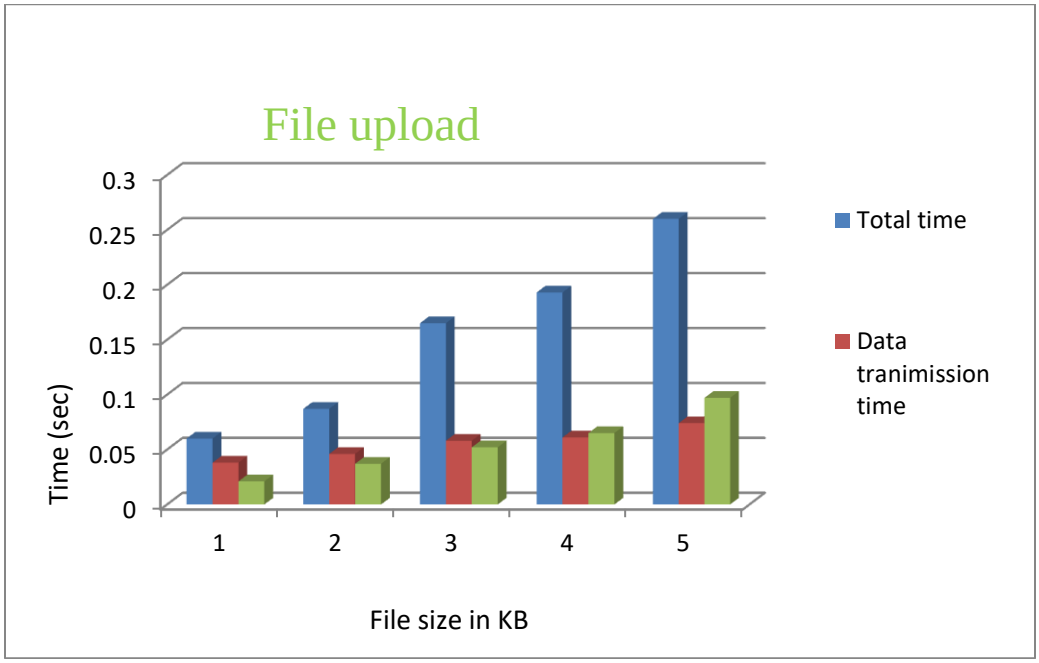

Figure 1 Average computation time for File Upload

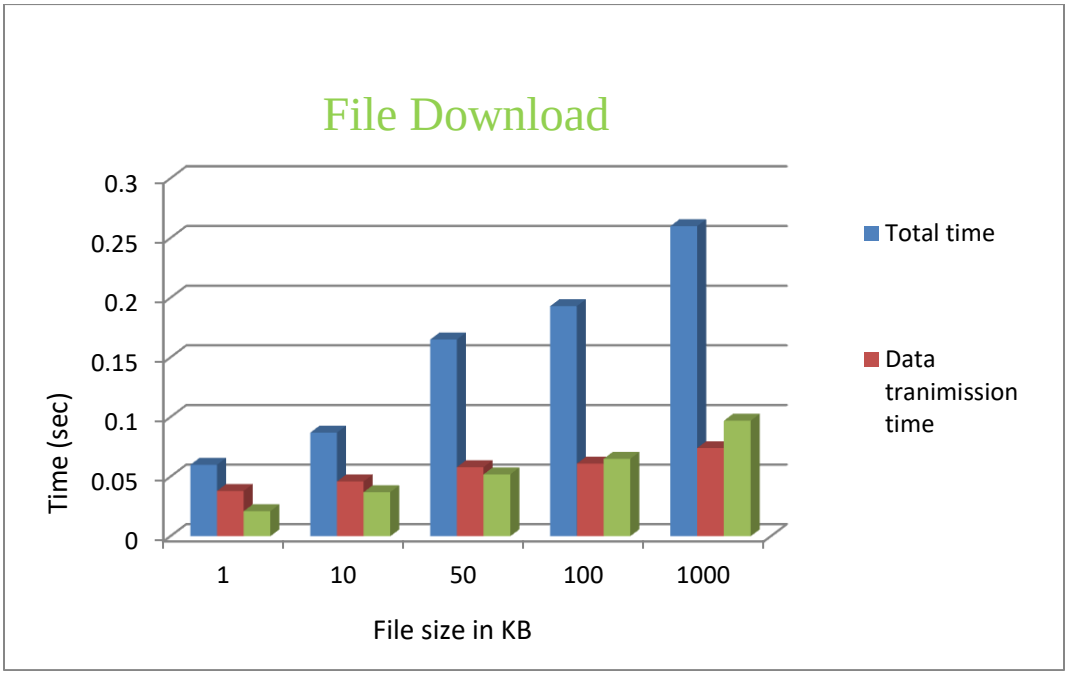

Fig 2Average computation time for File Download.

Fig 1 and 2 describes file upload and download operations on a cloud server with HCP-ABE and CP-ABE

4. CONCLUSION

In this the proposed HCP-ABE framework implemented and shown detailed discussion with each use case. First a scenario is taken from engineering college where different organizations are formed if any user wants to share a document for intended users then get the public key from attribute authority and encrypt the document under access policy then upload to the cloud. In order to download file user must have secret key and which internally consist policy. the experiment conducted windows platform with 3-GB RAM 3.10 GZ CPU, Microsoft IDE visual studio 2013 to this Telerik test studio plug-in used. The performance analysis shows better than existing CP-ABE scheme. Finally HCP-ABE scheme has proven efficient and maintains secure in terms user policies. The average time calculated for file uploads and download operations on cloud server for this different parameters and different file sizes are considered.

REFERENCES

[1] Alofi Shane Black & Tony Sahama, 2014, "eHealth-as-a-Service (eHaaS): The industrialisation of health informatics, a practical approach", e-Health Networking, Applications and Services (Healthcom), P: 555-559.

[2] Cheng-Yi Yang &Chien-Tsai Liu, 2013, "Developing IHE-Based PHR Cloud Systems", Social Computing (SocialCom), 2013 International Conference on, PP: 1022-1025.

[3] Danwei Chen; et.al, 2014, "Securing patient-centric personal health records sharing system in cloud computing", ISSN: 1673-5447, Volume: 11, Issue: 13, PP: 121-127.

[4] Eung-Hun Kim; et.al, 2006, "Web-Based Personal-Centered Electronic Health Record for Elderly Population", Distributed Diagnosis and Home Healthcare, 2006. D2H2. 1st Transdisciplinary Conference on, PP: 144-147.

[5] Fabian Prasser; et.al, 2018, "A Scalable and Pragmatic Method for the Safe Sharing of High-Quality Health Data", ISSN: 2168-2194, Volume: 22, Issue: 2, PP: 611-622.

[6] Florian Daniel; et.al, 2011, "Beyond Health Tracking: A Personal Health and Lifestyle Platform", ISSN: 1089-7801, Volume: 15, Issue: 4, PP: 14-22.

[7] George Hsieh &Rong-Jaye Chen, 2012, "Design for a secure interoperable cloud-based Personal Health Record service", PP: 472-479.

[8] LinkeGuo; et.al, 2015, "Verifiable privacy-preserving monitoring for cloud-assisted mHealth systems", Computer Communications (INFOCOM), 2015 IEEE Conference on, ISSN: 0743-166X, PP: 1026-1034.

[9] M. Poulymenopoulou; et.al, 2014, "A virtual PHR authorization system", ISSN: 2168-2194, Biomedical and Health Informatics (BHI), 2014 IEEE-EMBS International Conference on, PP: 73-76.
[10] Pieter Van Gorp; et.al. (2012) "Addressing health information privacy with a novel cloud-based PHR system architecture", ISSN: 1062-922X, PP: 1841-1846.
[11] Weiwei Jiang; et.al, 2011, "Individual Self-Service Electronic Health Records: Architecture, Key Technologies and Prototype System", (CyberC), 2011 International Conference on, PP: 574-579.
[12] Yang Yang; et.al, 2017, "Lightweight Sharable and Traceable Secure Mobile Health System", ISSN: 1545-5971, Volume: PP, Issue: 99, PP: 1-1.