ISSN NO: 9726-001X
Volume 11 Issue 02 May 2023

JOURNAL OF CURRENT SCIENCE

EXPERIMENTAL STUDY OF USER REVOCATION AND DYNAMIC OPERATIONS OVER CLOUD SERVER

Dr.G Kishore Kumar , Mr.P Viswanatha Reddy , Mrs.G S Gowthami Kumari
Associate Professor[1],Assistant Professor[2,3]
Department of CSE,
Viswam Engineering College (VISM) Madanapalle-517325 Chittoor District, Andhra Pradesh, India

ABSTRACT: - ***We would recognize problems in the Cloud-based protection environment and will offer strategies for understanding the current research work on different access management frameworks and the expanded HCP-ABE architecture consists of four Data Owner (DO), Data Consumer (DU), Cloud Service Provider and Attribute Authority (AA), Data Owner outsource sensate. This paper offers potential alternatives for secrecy, honesty, effective user revocation and complex cloud storage operations. The experimental findings indicate a 15% reduction in the sophistication of the schema and the inputs to this study are special and considered to be expanded approaches to enhance data protection and to facilitate effective user revocation and interactive data operations.***
Keywords: HCP-ABE, CP-ABE, ACP Access Check Regulation.

I. INTRODUCTION

Cloud compute ring is an increasing paradigm in which computational capabilities available on the Internet as elastic, on-demand (Web) platforms become more persistent in everyday livelihood. An association that utilizes internet resources has to use huge quantities of capital for technology to support viable customers, not an issue for major enterprises but in the affordability of small to medium-sized firms or companies the enormous system has a number of challenges, such as computer breakdown, hard drive sounds, program glitches etc. For such a group, this may be a huge concern. The ultimate solution to this problem is cloud computing. An organization can rely on a cloud provider to do this instead of purchasing, installing and running its own systems. Cloud computing main industry players such as Google, Amazon and Microsoft etc., these vendors develop innovative company and organizational structures that permit consumers to compensate for their whole services, not make massive upfront expenditures. Cloud computing is a paradigm where resources or services (infrastructure, platform, software and databases) supplied over the web can be accessed as a service wherever, and when you are in need of, computing power in the field of computing infrastructure, application and business processes. Because of its versatility and resources, many people move to the cloud in four way, individually, publicly, hybrid and in group clouds to avoid local pressures until data is outsourced to the cloud to every consumer, however due to protection concerns outsourced data must be secured until being put in the cloud. Much of the recent literature centered on key management problems and rigid access protocols, but the Access Control mechanism can design constructive solutions because of the usage complexities. Help for dynamic access control and operations the policy-attribute-based encoding homographic cipher text (HCP-ABE) scheme is planned. The HCP-ABE includes five basic algorithms, each of which has the specific functionality of configuring, key generation, encryption, decryption and update encryption, firstly public key (PK) and master key (MK) as implicit parameters for this input. Second, secret key (SK) for this appropriate PK is generated based on user attributes. Third, the Plaint Text translated into an unreadable mode, AL Access List and AS Access Framework are needed. Fourthly, the text translated into a simple text is required for this hidden key (SK). Finally, dynamic (update, delete, and attach) operations for encrypted data are needed to carry out this CT cipher text.

I.

ISSN NO: 9726-001X
Volume 11 Issue 02 May 2023

II. IMPLEMENTATION

The organizational arrangement of the Engineering College with the various divisions depends on the essence of the job and authorization standard of each customer in Figure 6.1. Access policies may be developed and handled in compliance with the existence of documents submitted into the cloud by the device authorities. Consider the role of various staff identified with the ratings as Board of Directors (BOC), Administrative Officer (AO), Principal, CSE Dept, ECE dept, EEE department and various cloud documents for these departments. The hundreds or thousands of access control rules that device authorities can build and manage easily using the cuckoo filter data structure. The aim of using a cuckoo filter is to reduce storage problems and problems of role explosion that usually arise in solitary access control techniques.

The below are the example access management procedures that the machine authorities handle.

ACP1 = (role = "BOD," {< college overall activities>, < income details}

ACP2 = (role = AO), {<sets student fee information and tracking >, <Production reports>}

ACP3= (role = key, {< track each operation of a department >})

ACP4 = (role = "CSE," {<Control CSE activities>}) [translation]

ACP5 = (role = "ECE," {< Monitor ECE operation department >})

ACP6 = (role = "EEE," {< EEE control operation >})

ACP7= (role = "assistant teacher," {< student monitor information >})

ACP8= (role="Lab wizard," {<Details of the monitor book>})

For each policy, the system authority generates the RSA keys and access token. The access token is special for each subgroup and holds the token mapped for each individual in a cuckoo hash table, moreover. The first ACP specifies, for example, that the management board should track management operations and revenue information. The ACP2 for presidents who can set and track their corporate priorities and display production reports and general managers can monitor separate departmental information as seen in the AAC3. The remaining ACPs are related to the monitoring by various department employees of documents relating to different departments. The CP-ABE can be applied to the members group and the users for subgroups can be identified further according to the access control policies. The consumer will then view the file on the basis of the device authority token.

III. ANALYSIS OF EXPERIMENTAL RESULTS

The HCP-ABE scheme setup () and key generation () algorithms are generated before contact is started. We noticed that the streamlined HCP-ABE system took less time relative to current access control schemes. The 15 percent improvement in streamlined scheme is due to the fact that there was a pre-computation stage in which certain cup-intensive values are determined in advance.

HCP-ABE Encryption and Decryption: We measured the efficiency of new and existing algorithms in the user lists with revoked dimensions from 1,000 to 10,000, and found the streamlined implementation of HCP-ABE in comparison to established access controls was 20 percent lower in time. We noticed that the configured HCP-ABE scheme demonstrated increased results for larger data sets.

ISSN NO: 9726-001X
Volume 11 Issue 02 May 2023

Eigen and Configuration Attributes Dependent Cryptosystem: The pre-computing process period needed for optimized ABE schemes was 200 milliseconds, with increasing records. The set-up of ABE took 68 ms and ABE-OPT required 40 ms, except the pre-computation period, 819 milliseconds and 661 milliseconds, respectively for ABE and optimized ABE algorithms.

Attribute Dependent Cryptosystem Operations: We found that streamlined ABE took around 40% less time when tested with dataset sizes between 2,000 and 20,000, which was the product of our base implementation optimizations.
Total computing period for separate file upload stages.

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 Total computing period for separate file upload stages.

The average time measured in Table 1 is the time taken to encrypt the data, to handle main issues and to migrate data to cloud storage for various file size (in kb).

Average Computation with separate file phases 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 with separate file phases Download

Table 2 Average time to decrypt a file from the cloud server, to these few criteria is known to have taken the whole time to retrieve the file of various sizes from the cloud server.

Figures 1 and 2 display an average period for finishing the upload and download of the file of varying file sizes.

ISSN NO: 9726-001X
Volume 11 Issue 02 May 2023

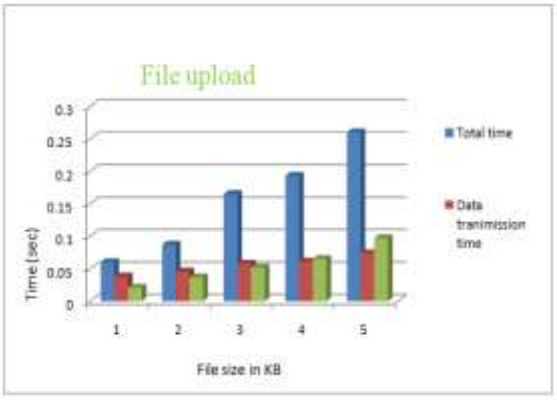
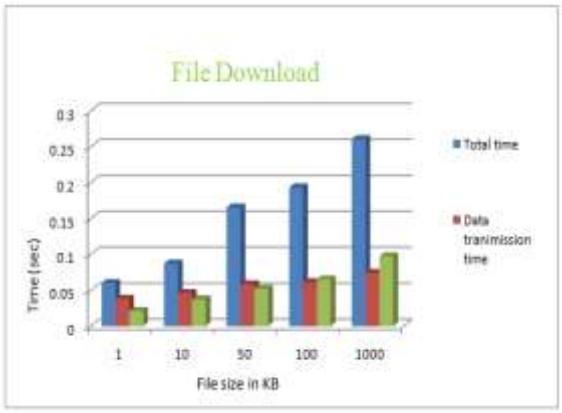


Figure 1 Normal file transfer computation period



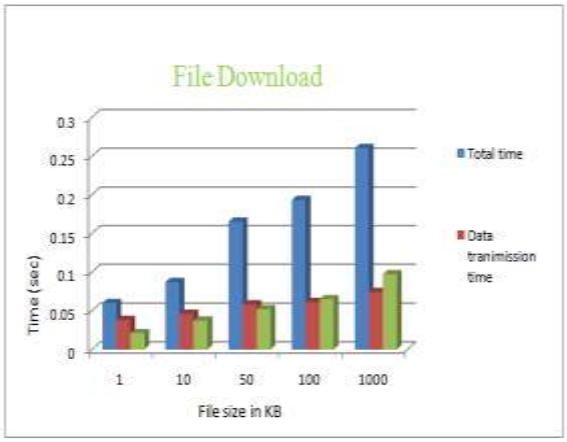


Fig 2 Average File Download Estimation Period.
Figure 1 and 2 define uploading and copying file operations on an HCP-ABE and CP-ABE cloud server.

IV. Conclusion

In this sense, the suggested HCP-ABE system was applied and thorough debate for each implementation case was illustrated. First, an engineering college is used to build various organizations whenever a person chooses to exchange a document with expected users and then get the public key of the attribute authority and encrypt the document under the access protocol, then upload to the cloud. To download the file consumer must have a hidden key and a policy that is internal. Windows application experiment with RAM 3.10 GZ CPU 3-GB, Microsoft IDE Visual Studio 2013 used with this telluric research studio plug-in. The output review illustrates more than the new

CP-ABE method. Finally, HCP-ABE has proved successful and holds user policy safe. The average time for file uploads and downloads on the cloud service is considered for these multiple criteria and file sizes.

REFERENCES

1. *Aloft Shane Black & Tony Sahara, 2014, "health-as-a-Service (eras): The industrialization of health informatics, a practical approach", e-Health Networking, Applications and Services (Healthcom), P: 555-559.*
2. *Cheng-Yi Yang & Chine-Tsai Liu, 2013, "Developing IHE-Based PHR Cloud Systems", Social Computing (SocialCom), 2013 International Conference on, PP: 1022-1025.*
3. *Dawned 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. *Keung-Hun Kim; et.al, 2006, "Web-Based Personal-Centered Electronic Health Record for Elderly Population", Distributed Diagnosis and Home Healthcare, 2006. D2H2. 1st Tran disciplinary Conference on, PP: 144-147.*
5. *Fabian Presser; 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. *Florien 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. *Linked Goo; et.al, 2015, "Verifiable privacy-preserving monitoring for cloud-assisted health 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", (Cyber), 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.*