IMPLEMENTING SECURE DATA ACCESS CONTROL USING CP-ABE

[1]Rajeswari, [2]Vinitha R, [3]Rabubieyya Aiiysha Zahra, [4]Greeshma N

[1]Sr. Asst. Professor, [2]B.E Student, [3]B.E Student, [4]B.E Student

[1-4]Department of Information Science and Engineering

[1-4]New Horizon College of Engineering, Bangalore, Karnataka, India

ABSTRACT: In cloud, an effective way to ensure security is using Data Access Control. But, data access control becomes a very challenging issue in cloud storage systems due to untrusted cloud servers and data outsourcing. To overcome this problem multi-authority Attribute Based Encryption is employed. In this different sets of attributes along with the corresponding decryption keys are issued to users by the attribute authorities. Ciphertext Policy Attribute Based Encryption (CP-ABE) is a promising cryptographic technique based on these attributes. A user is able to decrypt a ciphertext if and only if his attributes satisfy the ciphertext access structure in which each user is associated with a set of attributes and the data is encrypted using access structures. However, attribute revocation becomes cumbersome for this scheme. The proposed solution enables the multi-authority to revoke user attributes with minimal effort. By uniquely integrating the technique of proxy re-encryption and CP-ABE, attributes can be revoked with minimal effort. This enables the authority to delegate the most laborious tasks to proxy servers.

IndexTerms **-** Access Control, Ciphertext, Attribute Based Encryption, proxy servers, cryptography

I. INTRODUCTION

Cloud Computing is one of the major development in computer history [3]. Advantages of utilizing distributed storage incorporate more noteworthy availability, higher dependability, fast arrangement and more grounded insurance, to give some examples. In spite of the said benefits, this worldview likewise delivers new difficulties on information get to control, which is a basic issue to guarantee information security. The Cloud Computing model consists of five characteristics, there delivery models, and four deployment models [11]. Since distributed storage is worked by cloud specialist co-ops, who are for the most part outside the put stock in space of information proprietors, the customary access control strategies in the Client/Server show are not reasonable in distributed storage condition. The information gets to control in distributed storage condition has accordingly turned into a testing issue. Cloud Computing defined five essential characteristics of Cloud Computing as on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service [10]. To address the issue of information, get to control in distributed storage, there have been many plans proposed, among which Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is viewed as a standout amongst the most encouraging procedures. A notable component of CP-ABE is that it awards information proprietors coordinate control in view of access approaches, to give adaptable, fine grained and secure access control for distributed storage frameworks. In CP-ABE plans, the entrance control is accomplished by utilizing cryptography, where a proprietor's information is encoded with an entrance structure over traits, and a client's mystery key is named with his/her own particular properties. Just if the properties related with the client's mystery key fulfil the entrance structure, can the client unscramble the comparing ciphertext to get the plaintext.

The main contributions of this work can be summarized as follows:

- To address the single-point execution bottleneck of key conveyance existed in the current plans, we propose a strong and proficient heterogeneous structure with single CA (Central Authority) and different AAs (Attribute Authorities) for open distributed storage. The overwhelming heap of client authenticity confirmation is shared by various AAs, every one of which deals with the all-inclusive quality set and can freely total the client authenticity check, while CA is in charge of computational errands. To the best of our insight, this is the primary work that proposes the heterogeneous access control system to address the low proficiency and single-point execution bottleneck for distributed storage.
- We reproduce the CP-ABE plan to fit our proposed structure and propose a strong and high-productive access control plot, in the interim the plan still jam the fine granularity, adaptability and security highlights of CP-ABE.
- Our scheme includes an auditing mechanism that helps the system trace an *AA*'s misbehavior on user's legitimacy verification.

II. EXISTING SYSTEM

Despite the mentioned benefits, this paradigm also brings forth new challenges on data access control, which is a critical issue to ensure data security. Since cloud storage is operated by cloud service providers, who are usually outside the trusted domain of data owners, the traditional access control methods in the Client/Server model are not suitable in cloud storage environment. The data access control in cloud storage environment has thus become a challenging issue.

Disadvantages

- It is hard to find the responsible authority if mistakes have been made or malicious behaviors have been implemented in the process of secret key generation and distribution.

- Weak point on security makes this straightforward idea hard to meet the security requirement of access control for public cloud storage.

III. PROPOSED SYSTEM

To address the issue of information, get to control in distributed storage, there have been many plans proposed, among which Cipher text Policy Attribute-Based Encryption (CP-ABE) is viewed as a standout amongst the most encouraging systems. A notable element of CP-ABE is that it awards information proprietors coordinate control in view of access strategies, to give adaptable, fine-grained and secure access control for distributed storage frameworks. In CP-ABE plans, the entrance control is accomplished by utilizing cryptography.

Advantages

- The conspire jelly the fine granularity, adaptability and security highlights.
- Scheme incorporates an inspecting instrument that enables the framework to follow an AA's rowdiness on client's authenticity confirmation.
- A powerful and effective heterogeneous system with single CA (Central Authority) and different AAs (Attribute Authorities) for open distributed storage.

IV. SYSTEM STUDY

SYSTEM REQUIREMENTS:

Hardware Requirements:

System	:	Intel i3 2.1 GHZ
Memory	:	4GB.
Hard Disk	:	40 GB.
Monitor	:	15 VGA Colour.
Mouse	:	Logitech.

Software Requirements:

Operating System	:	Windows 7 / 8.
Language	:	JAVA / J2EE
Database	:	MySQL
Tool	:	NetBeans, Navicat.

V. SYSTEM ARCHITECTURE

The design arrangement methodology is worried about working up a major fundamental framework for a system. It incorporates perceiving the genuine parts of the structure and exchanges between these fragments. The starting design strategy of perceiving these subsystems and working up a structure for subsystem control and correspondence is called development demonstrating plot and the yield of this diagram methodology is a depiction of the item basic arranging. The proposed engineering for this framework is given underneath. It demonstrates the way this framework is planned and brief working of the framework.

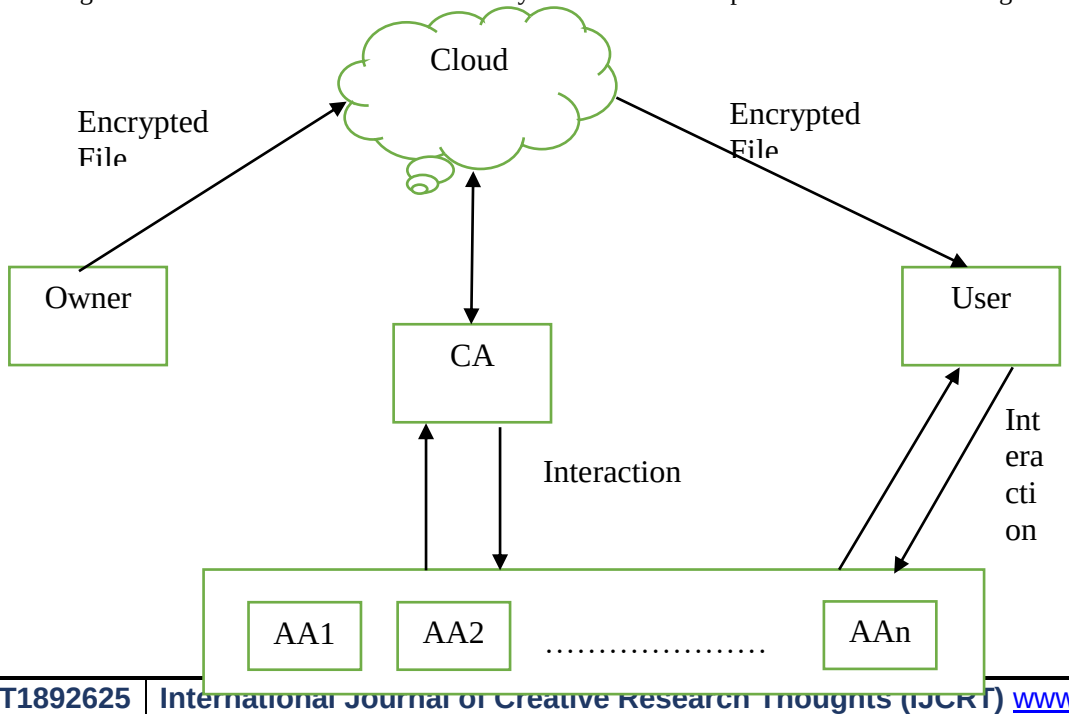


Fig.1: System Architecture

VI. **Modules and description**

The framework model of our plan comprises of five substances: a focal expert (CA), different trait specialists (AAs), numerous information proprietors (Owners), numerous information purchasers (Users), and a cloud specialist co-op with various cloud servers (here, we specify it as cloud server.).

•The central authority (CA)

The CA is the director of the whole framework. It is in charge of the framework development by setting up the framework parameters and producing open key for each trait of the all-inclusive property set. In the framework introduction stage, it allots every client a one of a kind Uid and each property expert a remarkable Aid. For a key demand from a client, CA is in charge of creating mystery keys for the client based on the got middle of the road key related with the client's authentic qualities checked by an AA. As a head of the whole framework, CA has the ability to follow which AA has mistakenly or noxiously confirmed a client and has allowed ill-conceived characteristic sets.

•The attribute authorities (AAs)

The AAs are in charge of performing client authenticity check and producing halfway keys for authenticity confirmed clients. Dissimilar to a large portion of the current multi-specialist plans where every AA deal with a disjoint trait set separately, our proposed plot includes numerous experts to share the obligation of client authenticity check and every AA can play out this procedure for any client autonomously. At the point when an AA is chosen, it will check the clients' true-blue properties by physical work or verification conventions and produce a middle of the road key related with the qualities that it has authenticity confirmed. Middle key is another idea to help CA to create keys.

• The data owner (Owner)

The data owner (Owner) characterizes the entrance approach about who can gain admittance to each document and scrambles the record under the characterized strategy. Above all else, every proprietor scrambles his/her information with a symmetric encryption calculation. At that point, the proprietor details get to approach over a trait set and encodes the symmetric key under the strategy as per open keys acquired from CA. From that point forward, the proprietor sends the entire encoded information and the scrambled symmetric key (indicated as figure content CT) to the cloud server to be put away in the cloud.

• The data consumer (User)

The data consumer (User) is allotted a worldwide client character Uid by CA. The client has an arrangement of characteristics and is outfitted with a mystery key related with his/her property set. The client can unreservedly get any intrigued encoded information from the cloud server. In any case, the client can decode the encoded information if and just if his/her quality set fulfills the entrance approach installed in the scrambled information.

• The cloud server

The cloud server gives an open stage to proprietors to store and offer their encoded information. The cloud server doesn't lead information get to control for proprietors. The encoded information put away in the cloud server can be downloaded uninhibitedly by any client.

VII. **ALGORITHM**

ADVANCED ENCRYPTION STANDARD:

The more well-known and generally received symmetric encryption calculation liable to be experienced these days is the Advanced Encryption Standard (AES). It is found no less than six time quicker than triple DES.

A substitution for DES was required as its key size was too little. With expanding figuring power, it was viewed as helpless against comprehensive key hunt assault. Triple DES was intended to beat this disadvantage however it was discovered moderate.

The highlights of AES are as per the following –

- Symmetric key symmetric square figure
- 128-bit information, 128/192/
- Stronger and speedier t
- Provide full particular and configuration points of interest
- Software implementable in C and Java

Provides platform for share

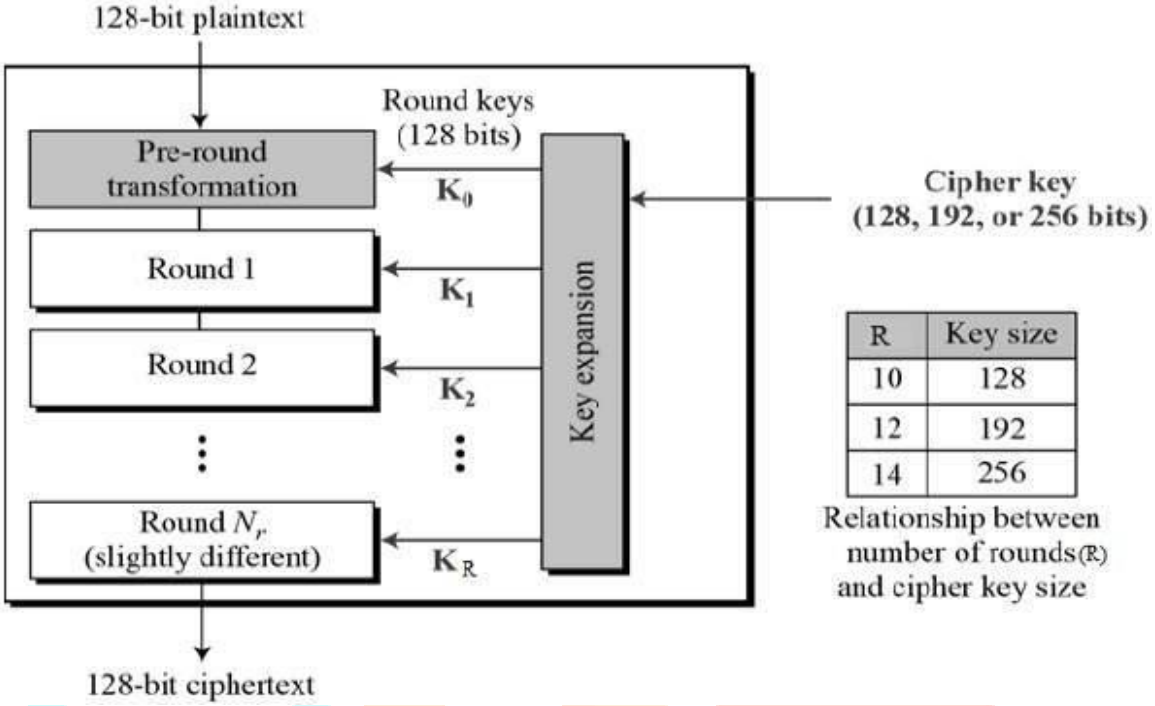
Operation of AES:

AES is an iterative as opposed to Feistel figure. It depends on 'substitution– change arrange'. It includes a progression of connected activities, some of which include supplanting contributions by particular yields (substitutions) and others include rearranging bits around (changes).

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix −

Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

The schematic of AES structure is given in the following illustration.



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

Fig.2: Advanced Encryption Standard(AES)

Encryption Process:

Here, we restrict to description of a typical round of AES encryption. Each round comprise of four sub-processes.

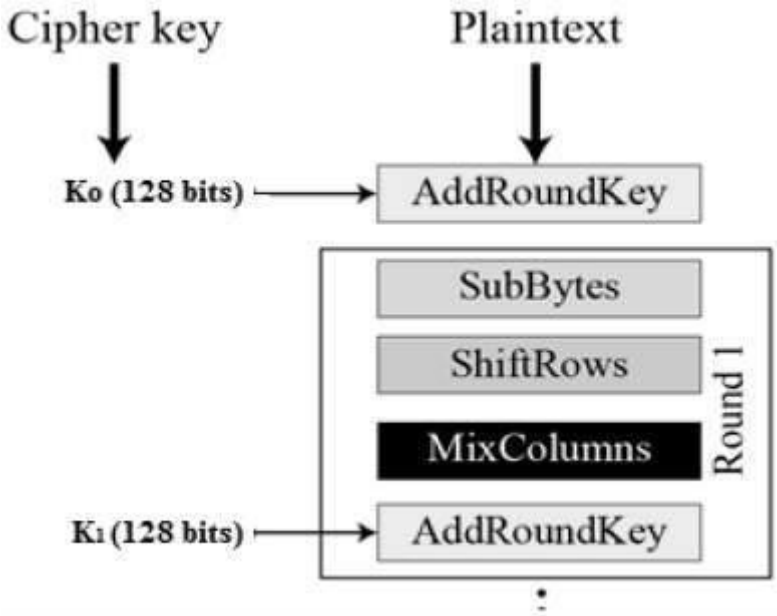


Fig.3: Encryption Process

VIII. **SOFTWARE TESTING**

Testing is a critical stage in the improvement life cycle of the item. This is, where the rest of the mistakes, assuming any, from every one of the stages are distinguished. Subsequently testing plays out an extremely basic part for quality confirmation and guaranteeing the dependability of the product.

Amid the testing, the program to be tried was executed with an arrangement of experiments and the yield of the program for the experiments was assessed to decide if the program was executing not surprisingly. Blunders were found and adjusted by utilizing

the beneath expressed testing steps and redress was recorded for future references. Along these lines, a progression of testing was performed on the framework before it was prepared for execution.

It is the procedure used to help recognize the rightness, culmination, security, and nature of created PC programming. Testing is a procedure of specialized examination, performed in the interest of partners, i.e. expected to uncover the quality-related data about the item regarding setting in which it is planned to work. This incorporates, however isn't restricted to, the way toward executing a program or application with the purpose of discovering errors.

TEST CASES:

User Test Case 1	
Test Case Name	User Registration
Input	User Details
Expected Outcome	Registered Successfully
Result	As Expected
Status	Successful

User Test Case 2	
Test Case Name	User Authentication
Input	User ID & Password
Expected Outcome	Logged In Successfully
Result	As Expected
Status	Successful

User Test Case 3	
Test Case Name	Privileged User Login
Input	PID & Password
Expected Outcome	Logged In Successfully
Result	As Expected
Status	Successful

User Test Case 4	
Test Case Name	Encryption Key Request
Input	Username & Filename
Expected Outcome	Key Request Sent Successfully
Result	As Expected
Status	Successful

User Test Case 5	
Test Case Name	File Request
Input	Username & Filename
Expected Outcome	File Request Sent Successfully
Result	As Expected
Status	Successful

User Test Case 6	
Test Case Name	Attribute Authority-View Key Request
Input	ID & Key Request
Expected Outcome	Key Request sent to Central authority
Result	As Expected
Status	Successful

User Test Case 7	
Test Case Name	Generate Key(CA)
Input	EKey, User Attribute
Expected Outcome	Private Key Generated & sent to user successfully
Result	As Expected
Status	Successful

User Test Case 8	
Test Case Name	Upload File
Input	File & Encryption Key
Expected Outcome	File Encrypted & Uploaded at the server successfully
Result	As Expected
Status	Successful

User Test Case 9	
Test Case Name	Private key Request(User)
Input	Filename & User ID
Expected Outcome	Private Key request sent successfully
Result	As Expected
Status	Successful

User Test Case 10	
Test Case Name	Download File
Input	Filename & Private Key &User ID
Expected Outcome	File Decrypted and downloaded successfully
Result	As Expected
Status	

User Test Case 11	
Test Case Name	Add Attribute Authority
Input	Attribute authority details
Expected Outcome	Attribute Authority Details Added Successfully
Result	As Expected
Status	Successful

User Test Case 12	
Test Case Name	Remove Attribute Authority
Input	Attribute Authority ID
Expected Outcome	Attribute Authority Details Removed Successfully
Result	As Expected
Status	Successful

IX. **RESULT AND OUTPUT**

Figure 4 shows that the admin who is the privileged user(P-user) has logged in successfully.

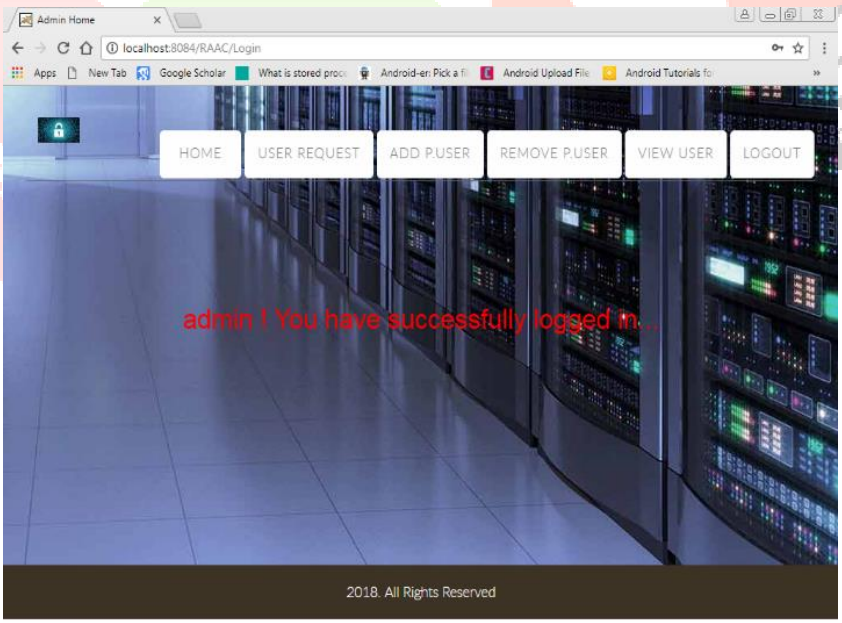


Fig.4: add P-user

Figure 5 shows that the user who needs to access data has been successfully logged in. The user can be of two types user and owner. Owner is the one who uploads his file and requests for encryption whereas user is the one who needs the access of the file which has been encrypted.

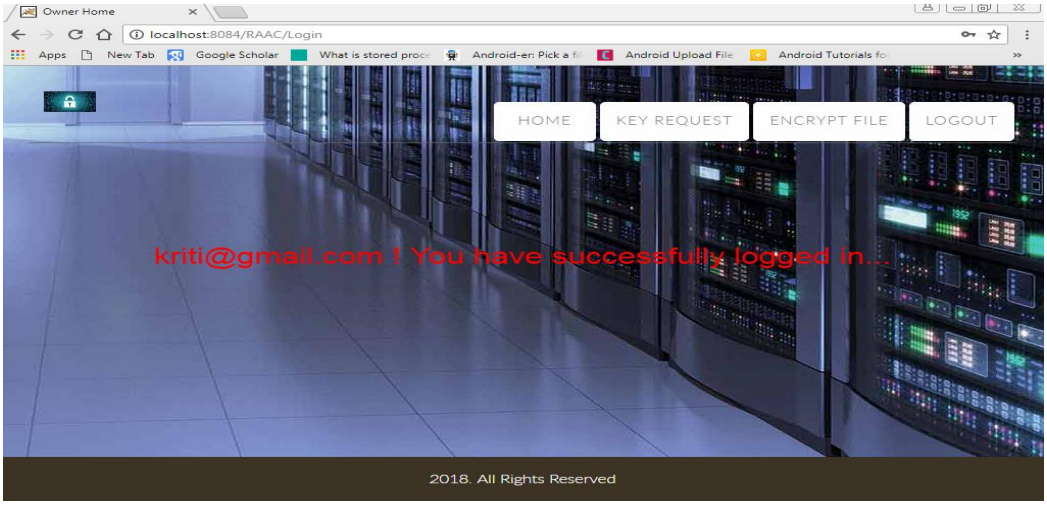


Fig.5: Log in success

Figure 6 shows the page of which a user is successfully logged out.

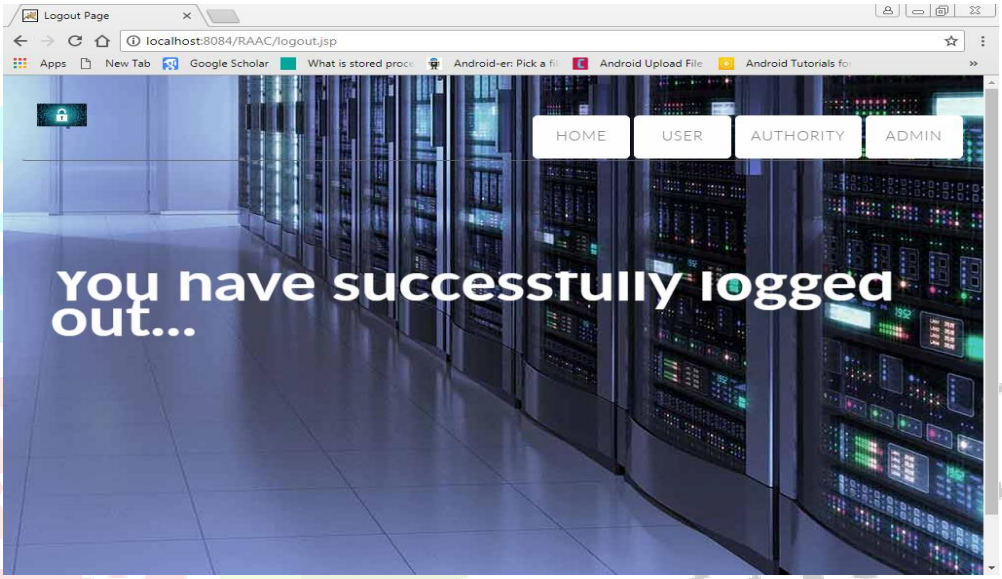


Fig.6: Logged Out

Figure 7 shows the registration page where the new user has to register to the page when he is using it for the first time. Once the user is registered next time he can directly login and continue the operation.

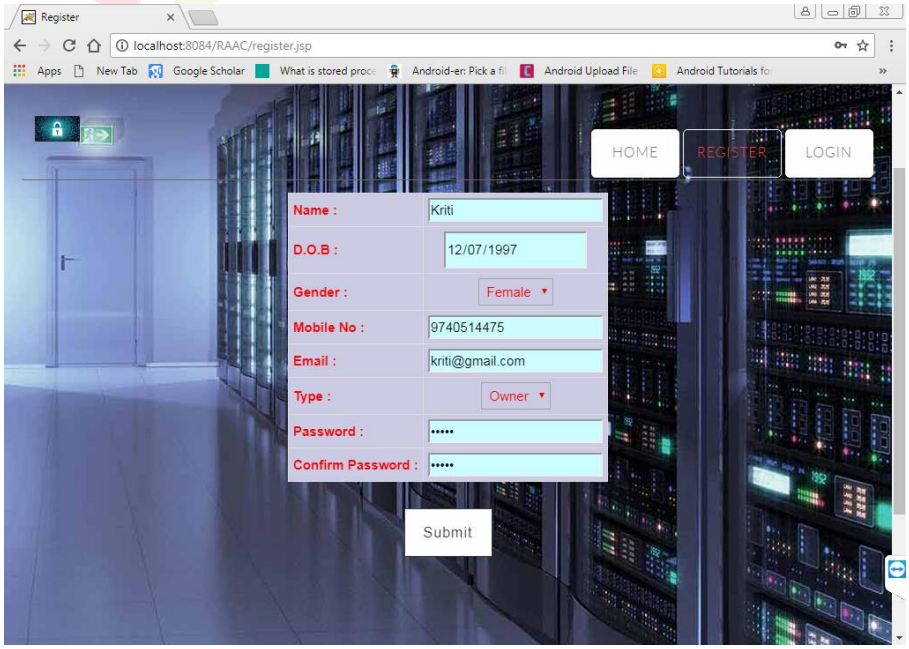


Fig.7: Register

Figure 8 shows that the user with mail id amulya@gmail.com has successfully registered. And now when she whats to access or upload any file she can directly login by specifying her username and password which generated at the time of registration.

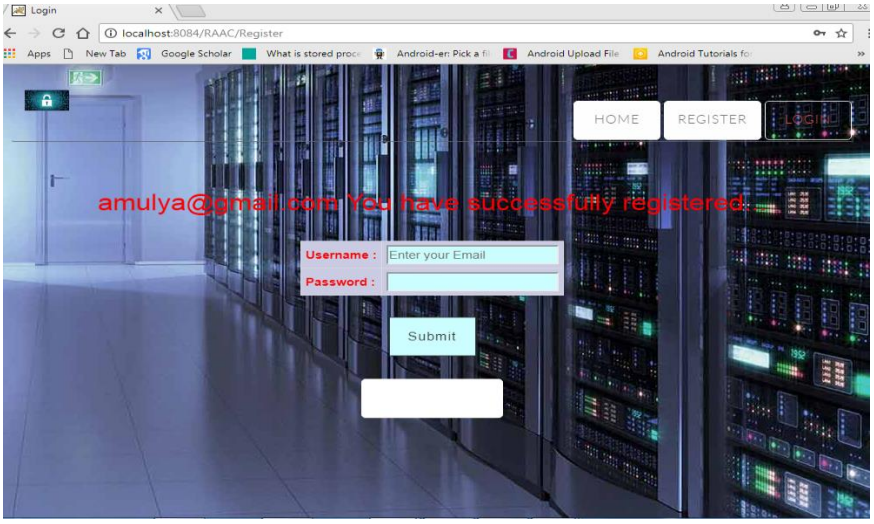


Fig.8: Register Success

Figure 9 shows the users who are already registered to the database along with their details like ID, Name of the user, Email address and mobile number of the corresponding user.

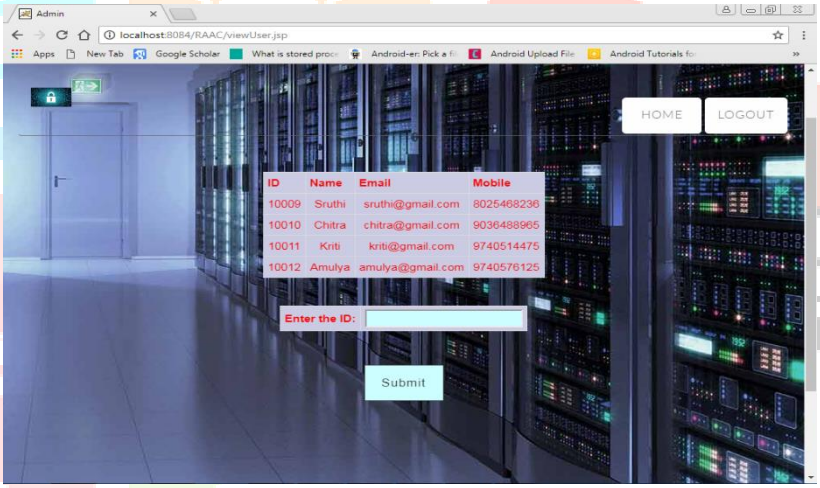


Fig.9: View

Figure 10 shows the download page where the users can download the file which is required by clicking the download link.

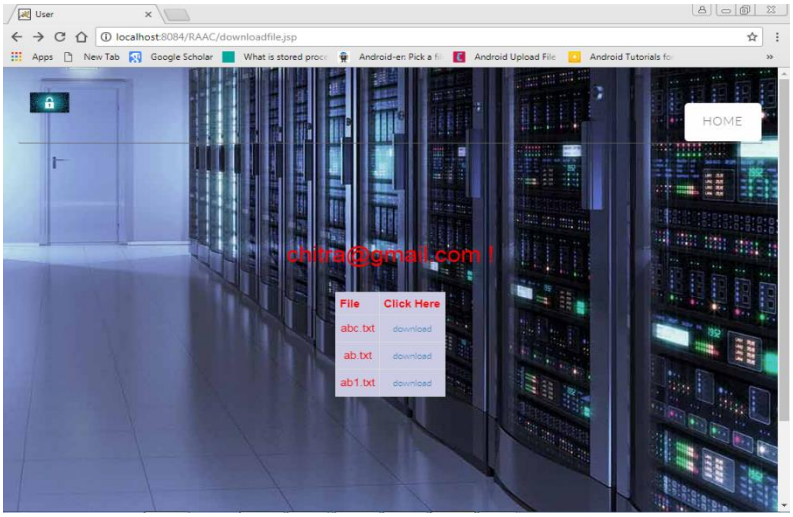


Fig.10: Download

X. CONCLUSION

In this paper, we proposed a new framework, named RAAC, to eliminate the single-point performance bottleneck of the existing CP-ABE schemes. By effectively reformulating CP-ABE cryptographic technique into our novel framework, our proposed scheme provides a fine-grained, robust and efficient access control with one-CA/multi-AAs for public cloud storage. Our scheme employs multiple AAs to share the load of the time-consuming legitimacy verification and standby for serving new arrivals of user's requests. We also proposed an auditing method to trace an attribute authority's potential misbehavior. We conducted detailed security and performance analysis to verify that our scheme is secure and efficient. The security analysis shows that our scheme could effectively resist to individual and colluded malicious users, as well as the honest-but-curious cloud servers. Besides, with the proposed auditing & tracing scheme, no AA could deny its misbehaved key distribution.

REFERENCES

[1] Wg Cdr Nimit Kaura, Lt Col Abhishek Lal-Survey Paper on Cloud Computing Security. International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), 2017.

[2] Prof.(Dr.) Pradeep Kumar Sharma, Prof.(Dr.) Premala Shankar Kaushik, Payal Jain, Shivangi Agarwal, Kamlesh Dixit – Issues and Challenges of Data Security in a Cloud Computing Environment. Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), 2017.

[3] Akshay A Nayak, Sridhar.N.K, Poornima G R, Dr. Shivashankar – Security Issues in Cloud Computing and its Counter Measure. International Conference On Recent Trends in Electronics Information Communication Technology, 2017.

[4] Ayman M. EI – Zoghby, Marianne A. Azer – Cloud Computing Privacy Issues, Challenges and Solutions. International Conference on Computer Engineering and Systems (ICCES), 2017.

[5] S.Rajeshwari, R.Kalaiselvi-Survey of data and storage security in cloud computing. In proceedings of the IEEE International Conference on Circuits and systems (ICCS), PP.76-81,2017.

[6] Prachi Garg, Dr. Sandeep Goel, Dr. Avinash Sharama – Security Technology for Cloud Computing Environment. International Conference on Computing, Communication and Automation (ICCCA), 2017.

[7] Anil Barnwal, Satyakam Pugla, Rajesh Jangade Various Security Threats and their Solution in Cloud Computing International Conference on Computing Communication and Automation (ICCCA), 2017.

[8] Gaurav Jain, Vikas Sejwar – Improving the Security by using Various Crypto GraphicTechniques in Cloud Computing. International Conference on Intelligent Computing and Control Systems (ICICCS), 2017.

[9] G. Shanmugasundaram, V.Aswini, G.Suganya – A Comprehensine review on Cloud Computing Security. International conference on Innovations in information Embedded and Communication system (ICIIECS), 2017.

[10] Kanagavalli Rangasami, Vagdevi S – Comparative study of Homomorphic Eneryption methods for secured data operations in Cloud Computing. International Conference on Electrical, Electronics, Communication, Computer and optimization Techniques (ICEECCOT), 2017.

[11] Ting-ting yui, Ying-guo zhu- Research on Cloud Computing and Security. International Symposium on distributed Computing and Applications to Business, Engineering and Science, 2012.

[12] Mutum Zico Meetei- Cloud Computing and Security Measure. International Congress on Image and Signal processing (CISP), 2013.

[13] P. Mell and T. Grance, "The NIST definition of cloud computing," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. 800-145, 2011.

[14] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 9, pp. 2546–2559, Sep. 2016.

[15] Z. Fu, X. Sun, S. Ji, and G. Xie, "Towards efficient content-aware search over encrypted outsourced data in cloud," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr. 2016, pp. 1–9.

[16] K. Xue and P. Hong, "A dynamic secure group sharing framework in public cloud computing," *IEEE Trans. Cloud Comput.*, vol. 2, no. 4, pp. 459–470, Oct. 2014.

[17] Y. Wu, Z. Wei, and R. H. Deng, "Attribute-based access to scalable media in cloud-assisted content sharing networks," *IEEE Trans. Multimedia*, vol. 15, no. 4, pp. 778–788, Jun. 2013.

[18] J. Hur, "Improving security and efficiency in attribute-based data sharing," *IEEE Trans. Knowl. Data Eng.*, vol. 25, no. 10, pp. 2271–2282, Oct. 2013.

[19] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 7, pp. 1214–1221, Jul. 2011.

[20] J. Hong, K. Xue, W. Li, and Y. Xue, "TAFC: Time and attribute factors combined access control on time-sensitive data in public cloud," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2015, pp. 1–6.