A Light weight Secure Data Sharing Scheme in Cloud Computing

THESIS SUBMITTED IN PARTIAL FULFILLMENT OF REQUIREMENTS
FOR THE AWARD OF THE DEGREE OF

Master of Technology
in
Computer Science Engineering

Under the esteemed guidance of
Mr. Manoj Kumar
(Associate Professor)
Computer Science and Engineering
Delhi Technological University

Submitted By-
Chirag Chawla
(Roll No. - 2K16/CSE/03)

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

DELHI TECHNOLOGICAL UNIVERSITY

SESSION: 2016-2018

DECLARATION

We hereby declare that the thesis work entitled "**A Light weight Secure Data Sharing Scheme in Cloud Computing**" which is being submitted to Delhi Technological University, in partial fulfilment of requirements for the award of degree of Master of Technology (Computer Science Engineering) is a bonafide report of thesis carried out by me. The material contained in the report has not been submitted to any university or institution for the award of any degree.

Chirag Chawla
2K16/CSE/03

CERTIFICATE

This is to certify that Chirag Chawla (2K16/CSE/03) has completed the thesis titled "**A Light weight Secure Data Sharing Scheme in Cloud Computing**" under my supervision in partial fulfilment of the MASTER OF TECHNOLOGY degree in Computer Science Engineering at DELHI TECHNOLOGICAL UNIVERSITY.

Supervisor

Mr. Manoj Kumar

Associate Professor

Department of Computer Science and Engineering

Delhi Technological University

Delhi -110042

ABSTRACT

Ciphertext Policy – Attribute Based Encryption is used to share the data securely as it is a challenge because it is an emerging encryption technology and can be very useful used over the cloud platform. The CP-ABE scheme has been implemented over the setup of a typical university architecture and gives the fine grained access for it. The documents that are sent to the data users by the data owners are encrypted first with the ABE encryption and following the access control structure on that document and then it can be decrypted when the data users wants them and only for those users the file will be decrypted whose attributes will be matched according the access control structure. The satisfaction of the attributes will only gives the permission to the data user to view the file. Experimental setup has been made and it is shown how the file is encrypted according to the file access policy and then the decryption setup is made for the data users. Also the encryption/decryption depends on the number of attributes, size of the file and the type. The ABE encryption can be implemented over the cloud and it can be very useful for the data owners. The user will only be access to the data only if its credentials or attributes are matched. The method doing this that was implanting the server with this and be made but we are compromising as we cannot trust the servers. So by our technique the data can be kept over the server confidentially as it is trusted or not. By CP-ABE the trust factor of the servers are also solved as we are not depending on them by this.

ACKNOWLEDGEMENT

I am very thankful to Mr. Manoj Kumar (Associate Professor, Computer Science Eng. Dept.) and all the faculty members of the Computer Science Engineering Dept. of DTU. They all provided immense support and guidance for the completion of the project undertaken by me.

I would also like to express my gratitude to the university for providing the laboratories, infrastructure, testing facilities and environment which allowed me to work without any obstructions.

I would also like to appreciate the support provided by our lab assistants, seniors and peer group who aided me with all the knowledge they had regarding various topics.

Chirag Chawla
M. Tech. in Computer Science Engineering
Roll No. 2K16/CSE/03

TABLE OF CONTENTS

DECLARATION i

CERTIFICATE ii

ABSTRACT iii

ACKNOWLEDGEMENT iv

LIST OF FIGURES AND TABLES vii

ABBREVIATIONS viii

CHAPTER 1: INTRODUCTION ……..…….…....1-7

1.1 Overview ……..……..…….....2-5

1.1.1 CP-Attribute Based Encryption …….…….…….3-5

1.2 Motivation Study ……..…….....5-6

1.3 Problem Statement …….…….....6-7

1.4 Organisation of Thesis …….……7

CHAPTER 2: LITERATURE REVIEW ……..…….....8-13

2.1 Related work ……..……..…….....13

CHAPTER 3: RESEARCH METHODOLOGY ……..……..….14-19

3.1 Description of CP-ABE ……..……..….14-15

3.1.1 Setup Steps …….….14-15

3.2 Construction ……..……...…….……16

3.3 Advancement in Work …….....17-19

3.3.1 AES…….16

3.3.2 RSA …….....17-19

CHAPTER 4: IMPLEMENTAION AND RESULTS ……20-33

4.1 Implementation …….……20-24

4.2 Results and Discussion …….……24-27

4.3 Screenshots …….……..28-35

CHAPTER 5: CONCLUSION AND FUTURE WORK…….…….……...36-37
5.1 Summary …….…..…….…….....36
5.2 Future Work ……..…….…….....37

REFERENCES ……..…….……...…...38-40

LIST OF FIGURES AND TABLES

Figure 1.1: Conventional Public Key Cryptographic System …….....2
Figure 1.2: Attribute Based Encryption System …….....4
Figure 1.3: CP-ABE Example Scheme ……..…….....5
Figure 3.1: Data Access Control CP-ABE ……..…….15
Figure 3.2: AES Structure …….……...18
Figure 3.3: RSA ……...19
Figure 4.1: Typical Role Hierarchy of Academic Employees in University …….……20
Figure 4.2: Tree Structure of Access policy ……22
Figure 4.3: Access policy ……..…24
Figure 4.4: No. of Attributes vs Key Generation Time ……25
Figure 4.5: No. of Attributes vs Encryption Time ……25
Figure 4.6: No. of Attributes vs Decryption Time ……25
Figure 4.7: Size of File vs Encryption Time …….……26
Figure 4.8: Size of File vs Decryption Time …….……26
Figure 4.9 Screenshots ……28

Table 4.1: Attribute List of Employees ……...……23
Table 4.2: Environment of Performance Measurement ……..24

ABBREVIATIONS

ABE : Attribute Based Encryption

CP-ABE: Ciphertext Policy Attribute Based Encryption

KP-ABE: Key Policy Attribute Based Encryption

GPK: Global Public Key

PRK: Private Key

CT: Cipher Text

MSK: Master Secret Key

AES: Advanced Encryption Standard

CHAPTER 1

INTRODUCTION

In the present paperless workplaces numerous vital reports required by a few people must be shared on companywide servers. One and all of the conspicuous necessities in this situation is that each archive ought to be available to just couple of clients who are approved to get to it. For instance, if a college stores reports of the considerable number of offices at a focal server, any workforce of any division can get to any archive. Encryption is one method for putting away and transmitting information in an incomprehensible shape. Established strategies for secret key based or customary open key cryptography based arrangement requires every client to have the same number of passwords or open/private key matches the same number of documents he/she all as will needs to get to. Property Based Encryption (ABE), first introduced by Sahai and Waters inthis upsetopen key cryptography by permitting credit set of client to beopen key rather a of than irregular string. Further, a variation of ABE as CP-ABE conspire, first proposed by Bethencourt et al. It by can be utilized to givea more proficient access control component contrasted with ordinary open key cryptographic encryption. In this approacha message is scrambled under an entrance arrangement and unscrambling is fruitful just if decryptor's of and property set related with his/her private key meets the entrance strategy prerequisite. Fine-grained get to control for giving diverse access rights to an arrangement of clients or individual clients over secure scrambled documents is conceivable utilizing this strategy.

In this work, we have proposed Ciphertext Policy-Attribute Based Encryptionof (CP-ABE) based a answer for fine grained get to control of college records, where specific sharingis required for critical archives put away on a focal area for transferring the imprints by each staff of specific subject. Dissimilar of a tom watchword based framework, where every client requires knowing watchword of each record it needs to access, here just a single mystery key for each client is required. Likewise, while out in the open key cryptography based

arrangement, each archive must be scrambled different circumstances for mystery access by numerous clients, in CP-ABE based arrangement record should be encoded just once. The proposed CP-ABE strategy give fine grained get to control of informationrs by having just a single basic open key and single private forevery client.In our usage various leveled information get to is additionally conceivable. In this paper, CP-ABE has been executed for proposing cryptographic security to shared records for characteristic based access by clients. can perform on document composes like .docx, .pptx, .xls and the .pdf file .

1.1 Overview

In this work, we give the first development of a ciphertext-arrangement quality based encryption (CP-ABE) to address this issue, and give the first development of such a plan. In our framework, a client's private key will be related with a subjective number of characteristics communicated as strings. Then again, when a gathering scrambles a message in our framework, they indicate a related access structure over properties. A client might have the capacity to decode a figure content if that client's qualities go through the figure content's entrance structure. At a numerical level, get to structures in our framework are depicted by a mono-tonic "access tree", where hubs of the entrance structure are made out of edge entryways and the leaves portray properties. We take note of that AND entryways can be built as n-of-n limit doors or potentially entryways as 1-of-n edge doors. Besides, we can deal with more mind boggling access controls.

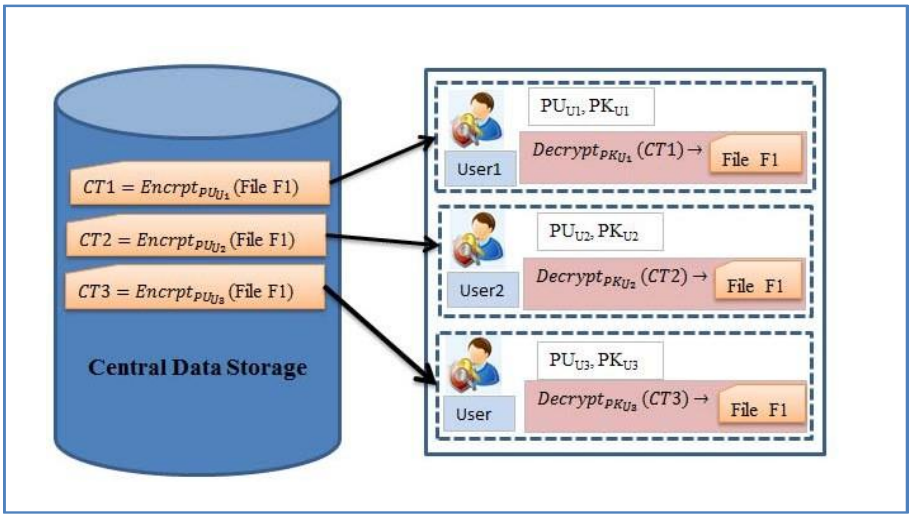

Fig.1.1. Conventional Public key Cryptographic System

1.1.1 CIPHERTEXT POLICY ATTRIBUTE BASED ENCRYPTION

A. Attribute based Encryption(ABE)

Property based encryption strategy is a kind of open key cryptography where any client is related to of set properties e.g. name, id, division, assignment and so on. An ordinary open key cryptographic framework utilizes two keys; an open key known to everybody and a private or mystery key known just to the beneficiary of the message. At the point when a User1 needs to send a safe message to User2, he/she utilizes User2's open key to encode the message. User2 at that point utilizes her private key to unscramble it. The traditional open key cryptographic planisappeared in Figure 1. Assume that an information proprietor needstostore a document File 1 in scrambled frame on the focal information stockpiling so it can be gotten to by just User1, User2 and User3. It scrambles the File1 with the PRU1, PRU2and PRU3 (open keys of User3, User2 and User1) and produce three distinctive ciphertext record CT1: (1), CT2: (1) and CT3: (1). Ciphertext document CT1 can be unscrambled by just User1's private key PRU1, CT2 can be decoded by just User2's private key PRU1 and CT3 can be unscrambled by just User3's private key PRU1.

In Attribute Based Encryption, worldwide open key (GPK) is normal for every one of the clients. Private Key (PRK) of every client is extraordinary and issued from a focal confided in specialist. Each client scrambles the document with the Global Public Key and unscramble the record with his/her own particular private key related with set of characteristics. The Attribute based Encryption conspire is appeared in Figure 2. Assume that an information proprietor needs to store a document File1 in scrambled shape on the focal information stockpiling and the record can be gotten to by just User3 and User2 , User1. It encodes the File1 with the Global Public Key GPK and creates a ciphertext document CT: (1). The ciphertext document CT can be unscrambled utilizing distinctive client's private key related with the set of qualities.

Henceforth, if there are 'n' clients in the framework at that point to give fine grained get to control utilizing traditional open key cryptography will create 'n' diverse cyphertext documents ant '2n' while keys quality based encryption strategy will produce a solitary cyphertext record and '1+n' keys. Along these lines, both cyphertext stockpiling and encryption time are spared.

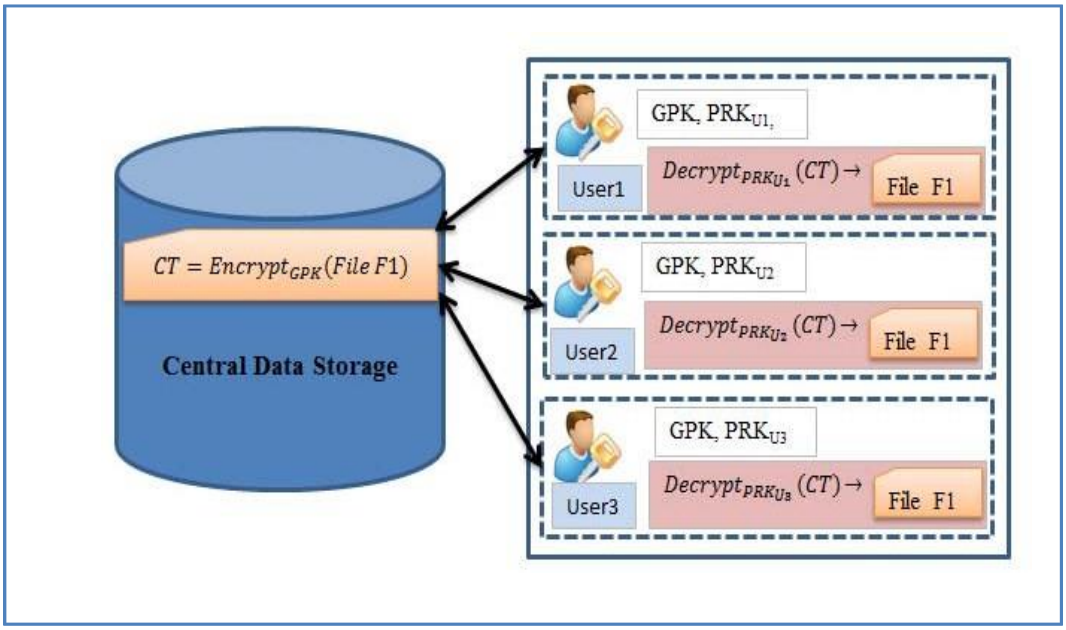

Fig.1.2. Attribute Based Encryption System

B. Ciphertext Policy Attribute Based Encryption (CP-ABE)

In CP-ABE, worldwide open key is normal for every one of the clients.Private key and of every client is related with an arrangement of qualities and at the season of encryption get to strategies are characterized over properties utilizing consistent administrators [5]. A tree get to structure is determined for get to conditions where interior hubs are consistent administrators and outer hubs are distinctive properties. A ciphertext document can be gotten to by just those clients whose properties indicated at the season of key age fulfill the entrance structure. Access conditions are sensible formulae manufacture utilizing values determined in characteristic rundown joined with rationale administrators. The rationale administrators can be utilized to characterize the entrance conditions, for example, OR, AND and n of t edge gate(where t out of n properties must be coordinated in the entrance conditions). Accordingly, AND administrator is n of n edge door as well as administrator is 1 of n edge entryway. A client can just unscramble a ciphertext in the event that he/she holds a key for coordinating characteristics. Record get to the condition is characterized by installed at document to the season of encryptions. Fig. 3 demonstrates a case of

ABE-CP conspire. Information proprietor scrambles the message X below the entrance approach T. Clients unscramble their cyphertext CT and if clients' trait sets and fulfill their T.

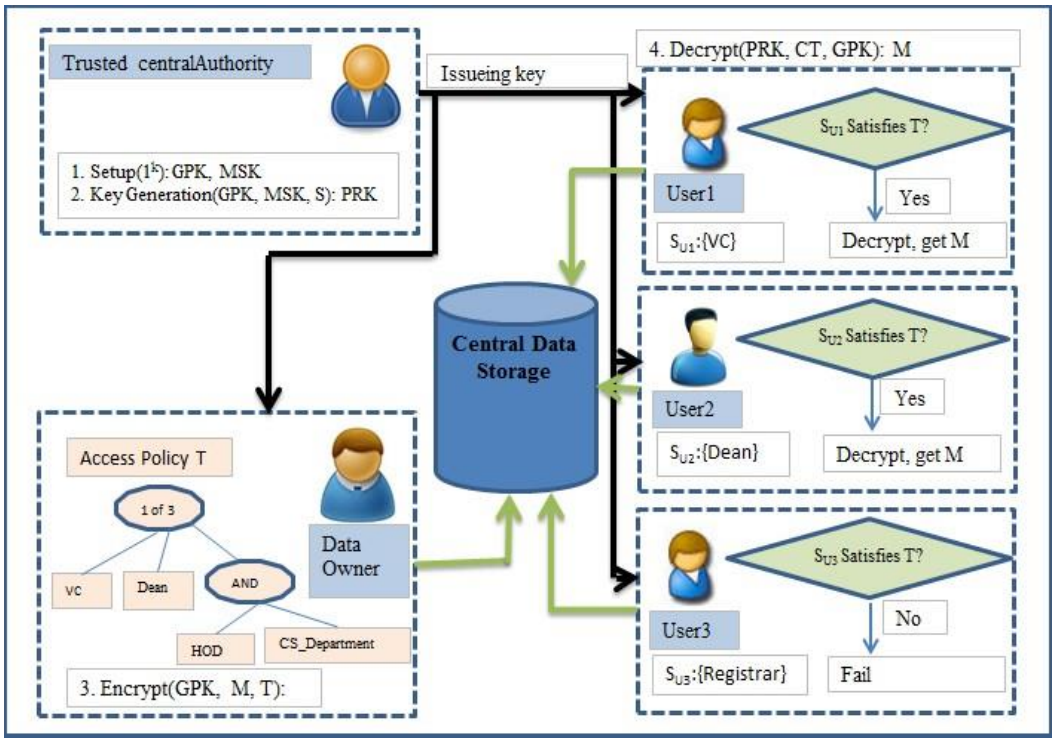

Fig.1.3. ABE-CP example scheme

1.2 Motivation Study

In conventional public key cryptographic systems we have to encypt the file many times for the different users and also the users have to maintain many passwords for the different files and also many pairs of public/ private key pairs for the different files. It was a very hectic scenario for the administrator to deal with all the users so in the need of this it came up with the idea of the attribute based encryption[1]. In the Attribute based encryption we don't need to encrypt the same file several times instead we encrypt the file according to the user. The capacity to amass describes into sets and to outline arrangements that can specifically confine the decoding key to

utilize credits having a place with a similar set is an intense element more than one may understand at first. In this area we outline its flexibility by tackling different issues in various settings which did not have any sensibly effective arrangements preceding this.

The expressive intensity of a CP-ABE plot is given by the class of inquiries into this table the plan can bolster. For example, BSW CP-ABE [2] bolsters a substantial class of such questions. One test to expand the expressive power is widen this class. Nonetheless, there is another essential measurement in which the expressive intensity of CP-ABE plan can be enhanced, by supporting a more broad class of characteristic tables. The above portrayal of CP-ABE required that every client ID shows up in just a single column in the table. (At the end of the day, the client ID must be a "superkey" in the trait table.) obviously, a table can be compelled to have this property, yet prompting extensive blow ups in the quantity of planned properties that a client gets or the measure of the outlined approach. Then again, a CP-ASBE plan can specifically bolster a table with different lines per client: properties in each line is given as a different set.

1.3 Problem Statement

Attribute Based encryption enables the sender to encode the message without getting the general population key testament. Capacity to scramble information with an open key without endorsements now and again is an answer of the issue. For instance, the client A can send an encoded message to the beneficiary B without PKI or when the beneficiary isn't associated at the season of transmission. Identity is seen as an arrangement of engaging traits utilizing characteristic based encryption. A client with a mystery key ω can unscramble information scrambled with general society key ω', if and just if ωand ω' contrast marginally. The limit of unimportance of contrasts is set by some metric d. Expecting the sender needs to scramble the report for all clients who have a particular arrangement of properties. For instance, the leader of the transport armada needs to pass on data in an encoded frame to drivers. For this situation, the information is scrambled with the property of the shape: {"bus armada", "Head", "driver"}. Anybody with these characteristics, can unscramble this information. The upside of this calculation is that the scrambled record can be transmitted over an open correspondence channel or put away on an unprotected server. Hypothetically the characteristic can be any data. It is

essential that the characteristic was indistinguishable from the subject or the protest which it is doled out or have a place with. As to the subjects nature of characteristics accomplished either physically or using specialized, hierarchical and other safety efforts. As for data assets it is accomplished by cryptographic strategies.

For adjustable approval in distributed computing and for getting to control and keeping up information secure by disposal processing cost and to accomplishes security against picked plaintext assault a framework is created called Cipher-content Policy Attribute-based Encryption (CP-ABE) and adaptable legitimacy, under the k-multi-direct Decisional Diffie-Hellman presumption are utilized to guarantee the information secrecy and the undeniable nature of appointment on untrustworthy cloud servers. The fundamental witticism of our task is for accomplishing access control and keeping information secret by decreasing figuring cost and to accomplish security against picked plaintext assaults with a specific end goal to demonstrate the effectiveness of the proposed work.

1.4 Organisation of Thesis

The thesis has been organised in various chapters as follows :

- Chapter 1 tells about the introduction part and gives the overview of the work done and it gives the brief idea of the project work.
- Chapter 2 gives an overview of the related work of the study that is what is the various research works have been done in this area and how all those work helped in evolution of our study.
- Chapter 3 gives the summarized research methodologies used in this thesis including overview of the recommended framework and the description of ABE system.
- Chapter 4 tells the final implementation of the work done and the results of that.
- Chapter 5 Concludes the proposition and explains the future work which can be done to improve the system further.
- Finally, all the references used in the research have been mentioned.

CHAPTER - 2

LITERATURE REVIEW

In [1] : By moving information stockpiling and preparing from lightweight cell phones to ground-breaking and brought together processing stages situated in mists, Cloud Mobile Computing (MCC) an extraordinarily improve an ability of the cell phones. In any case, when information proprietors outsource delicate information to portable cloud for sharing, the informationis outside of their confided in space and canpossibly be conceded to untrusted parties which incorporate the specialist co-ops. Information security and adaptable access control have turned into the most squeezing requests for MCC. To address this issue, we plan a safe and light weight information get to control plot in light of Ciphertext-PolicyAttribute based Encryption (CP-ABE) calculation, which can ensure the secrecy of outsourced information and provide fine grained information get the control for MCC. Their plan can clearly enhance the general framework execution by incredibly lessening the calculation overheads in encryption and unscrambling tasks, give adaptable and expressive information get to control approach, and in the mean time empower information proprietors to safely outsource the greater part of the calculation overheads at cell phones to cloud servers. The security and execution assessment demonstrate than you plan will secured, exceedingly proficient byand appropriate for light and weight cell phones.

In [2] : In a few appropriated frameworks a client should just have the capacity to get to information if a client groups a specific arrangement of cre-dentials or properties. At present, the main strategy for upholding such strategies is to utilize a confided in server to store the information and intercede get to control. Be that as it may, if any server putting away the information is endangered, at that point the confidentiality of the information will be imperiled. In this paper we introduce a framework for acknowledging complex access control on scrambled information that we call Ciphertext-Policy Attribute-Based Encryption. By utilizing our procedures encoded information can be kept confidential regardless of whether the stor-age

server is untrusted; besides, our techniques are secure against plot assaults. Past Attribute-Based Encryption frameworks utilized ascribes to depict the encoded information and incorporated arrangements with client's keys; while in our framework credits are utilized to portray a client's certifications, and a gathering scrambling information stop digs a strategy for who can unscramble. Along these lines, our meth-ods are adroitly nearer to conventional access control strategies, for example, Role-Based Access Control (RBAC). Likewise, we give a usage of our sys-tem and give execution estimations.

In [3] : With the ubiquity of distributed computing, cell phones can store/recover individual information from anyplace whenever. Thusly, the information security issue in portable cloud turns out to be increasingly extreme and avoids facilitate improvement of versatile cloud. There are significant investigations that have been led to enhance the cloud security. Nonetheless, the greater part of them are not appropriate for portable cloud since cell phones just have restricted figuring assets and power. Arrangements with low computational overhead are in extraordinary requirement for versatile cloud applications. The paper is proposed by a lightweight data that can sharing by plan (LDSS) by the versatile parallel computing. It embraces CP-ABE, an entrance control innovation utilized as a part of typical cloud condition, however changes the structure of access control tree to make it reasonable for portable cloud situations. LDSS moves a huge segment of the computational escalated get to control tree change in CP-ABE from cell phones to outside intermediary servers. Besides, to lessen the client disavowal cost, it acquaints quality depiction fields with actualize lethargic renouncement, which is a prickly issue in program based CP-ABE frameworks. The exploratory outcomes demonstrate that LDSS can adequately decrease the overhead on the cell phone side when clients are sharing information in versatile cloud situations.

In [4] : Ciphertext-strategy property based encryp-tion (CP-ABE) is an exceptionally encouraging encryption method for secure information partaking with regards to distributed computing. Information proprietor is permitted to completely control the entrance strategy related with his information which to be shared. In any case, ABE-CP is restricted to a potential security hazard that is known as key escrow issue, whereby the mystery keys of clients must be issued by a confided in key specialist. Furthermore, a large portion of the current CP-ABE plans can't bolsiter characterstic by the discretionary state and though this we of return to quantity

information based sharing and plan with a specific end goal to settle their key nescrow issues of in addition enhance their expressivenes and traits, so their subsequent plan by the all most well disposed their parallel computer applicationss. We propose an enhanced two-party key issuing convention that can ensure that neither key specialist nor cloud specialist co-op can bargain the entire mystery key of a client separately. In addition, we present the idea of trait with weight, being given to improve the outflow of property, which can not just stretch out the articulation from parallel to discretionary state, yet additionally help the many-sided quality of access strategy. Accordingly, both capacity cost and encryption many-sided quality for a ciphertext we calmed. The execution investigation and the security evidence demonstrate that the proposed conspire can accomplish efficient and secure information partaking in distributed computing.

In [5] : The fast development of distributed computing as a recently discovered innovation and numerous hazy security issues in it cause numerous difficulties. These difficulties are indicated in specialist organization's cloud servers and transmission forms. Likewise, this paper shows a model in light of independent information and key cloud servers and a customer based information encription benefit our expanding their unwavering quality at distributed computer conditions. In the proposed show, the key age process is done in a different cloud application and open and private keys are put away in key cloud servers. Additionally, the encryption and unscrambling forms are done in customer side by an administration that named "information encryption benefit". By aplying them encription framework as similar report our and finished in breaking down their qualities our shortcomings our seven famous unbalanced encryption key calculation (RSA-unique, Small-e RSA, Small-d RSA, MERA, RSA-E, and E-AMRSA) as indicated by time, key size and security parameters. These calculations were quickly depicted and re developed in a similar circumstance for the re-enactment procedure to examine the execution by customer required information encription benefit. Moreover, their scrutiny investigation were finished an exploring them execution for portrayed calculations again their famous assaults: Brute-Force, Mathematics, and Timing-Attack. As indicated by them outcomes RSA-E in their must fitting calculation from utilizing as a part of customer based information encryption benefit by accomplishing increasing speed, precision, and security in this administration in view of similarity issues in a customer side administration.

In [6] : In view of direct mystery sharing and computerized signature, another multi-specialist quality based encryption conspire is proposed. In our plan, a mark on a client's character is installed in the client's private key. The outsider can straightforwardly follow the personality of the proprietor of the private key as indicated by the released private key, and can confirm the accuracy of the client's character freely. In addition, numerous specialist focuses mutually create the private key of the client, which viably takes care of the security issue existing in an expert focus. The capacity execution investigation comes about demonstrate that our plan is exceptionally reasonable for distributed computing condition.

In [7] : Distributed computing is a model on which association and people can work with application from anyplace on the planet on request. The real issue of distributed computing is saving classification and uprightness of information in information security. The essential answer for this issue is encoding cloud information. Security in distributed computing being one of the great research point. Numerous systems have been proposed on property based encryption strategies. In this paper multi expert various leveled trait based encryption is proposed and it is contrasted and key strategy and figure content arrangement property based encryption methods. In view of NIST factual test most noteworthy security trait based encryption calculation is chosen in cloud.

In [8] : With the ongoing reception and dispersion of the information sharing worldview in disseminated frameworks, for example, online interpersonal organizations or distributed computing, there have been expanding requests and worries for conveyed information security. A standout amongst the most difficult issues in information sharing frameworks is the authorization of access strategies and the help of arrangements refreshes. Ciphertext strategy quality based encryption (CP-ABE) is turning into a promising cryptographic answer for this issue. It empowers information proprietors to characterize their own entrance arrangements over client properties and authorize the strategies on the information to be disseminated. Nonetheless, the favorable position accompanies a noteworthy downside which is known as a key escrow issue. The key age focus could unscramble any messages routed to particular clients by creating their private keys. This isn't reasonable for information sharing situations where the information proprietor might want to make their private information just open to assigned clients. Likewise, applying CP-ABE in the information sharing framework acquaints another test with respect with

the client disavowal since the entrance strategies are characterized just finished the characteristic universe. Along these lines, in this investigation, we propose a novel CP-ABE conspire for an information sharing framework by misusing the normal for the framework engineering. The proposed conspire highlights the accompanying accomplishments: 1) the key escrow issue could be understood by without escrow key issuing convention, which is built utilizing the protected two-party calculation between the key age focus and the information putting away focus, and 2) fine-grained client denial per each characteristic should be possible as a substitute encryption which exploits the specific trait aggregate key circulation over the ABE. The execution and security examinations show that the proposed plot is effective to safely deal with the information dispersed in the information sharing framework.

In [9] : As more touchy information is shared and put away by outsider locales on the Internet, there will be a need to scramble information put away at these destinations. One disadvantage of encoding information, it as is that it can be specifically shared just at a coarse-grained level (i.e., giving another gathering your private key). We build up another cryptosystem for fine-grained sharing of encoded information that we call Key-Policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, ciphertexts are marked with sets of properties and private keys are related with air conditioning cess structures that control which ciphertexts a client can unscramble. We showthe pertinence of our con-struction to sharing of review log for the a data and communicate encryption. Our of the all development underpins assignment of private keys which subsumes Hierarchcal Identity Based Encryption .

In [10] : Over and over, property based encryption has been appeared to be the common cryptographic device for building different sorts of contingent access frameworks with extensive applications, however the arrangement of such frameworks has been moderate. A focal issue is the absence of an encryption plot that can work on touchy information productively and, in the meantime, gives includes that are essential practically speaking.

This paper proposes the principal completely secure ciphertext-approach and key-strategy ABE plans in view of a standard presumption on Type- III blending gatherings, which don't put any confinement on strategy write or on the other hand qualities. We actualize our plans alongside a few other noticeable ones utilizing the Charm library, and exhibit that they perform better on all parameters of intrigue.

In [11] : Distributed computing passes on everything as an administration over the web bolsters client request, for instance arrange, programming framework, stockpiling, equipment, programming, and assets. Advantages of distributed storage are simple access implies access as far as anyone is concerned wherever, in any case, whenever, versatility, strength, cost proficiency, and high unwavering quality of the information. So every last association is moving its information to the cloud, implies it utilizes the capacity benefit gave by the cloud supplier. So there is a need to ensure that information against unapproved access, adjustment or foreswearing of administrations on and so forth. To anchor the Cloud implies secure the medicines (computations) and capacity (databases facilitated by the Cloud supplier). In this paper we study diverse security issues to cloud and distinctive cryptographic calculations adoptable to better security for the cloud.

In [12] : For the vital reason of protection, a few distributed storage encryption patterns have been anticipated to anchor the data from those that don't approach. Every single such plan accept that distributed storage suppliers are secure and can't be hacked. Be that as it may, by and by, a few experts could force distributed storage providers to frame open client mysteries and private data. This paper shows an Attribute-Based access to the media inside the cloud wherever it utilizes figure ciphertext policy Attribute-Based encryption (CP-ABE) strategy to make relate get to administration dole out a key to each client characteristic and scrambles the data bolstered the suitably dispersed keys to a cloud is regularly encoded comparing framework.

CHAPTER - 3

Research Methodology

This chapter first describes the description of the Encryption Attribute Based Cipher text system our then their architecture of them Attribute based encryption system. The setup environment after that in the next chapter the implementation is explained.

3.1 Description of CP-ABE

Ciphertext-approach property based encryption (CP-ABE) - has swung to be an essential encryption innovation as to handle the test of secure information sharing. In a CP-ABE, client's mystery of key is portrayed by a characteristic set, and ciphertext is a related with an entrance structure. DO is to be permitted to define get to structure over the universe of traits. A client can unscramble an given ciphertext just if his/her quality set matches the entrance structure over the ciphertext. Utilizing a CP-ABE framework a specifically into a cloud application that may yield some open issues. Right off the bat, all clients' mystery keys should be issued by a completely confided in key specialist (KA). This brings a security hazard that is known as key escrow issue. By knowing and the mystery key of a framework client, the KA can decode all the client's ciphertexts, and to which a remains altogether against to the will of the client. Furthermore, the expressiveness an of quality set is another worry. To the extent we know, the greater part of the current and CP-ABE plans can just to depict parallel state over characteristic, for instance, "1 - fulfilling" and "0 - not-fulfilling", but rather not managing self-assertive state trait.

3.1.1 Setup steps of CP-ABE :

• Setup (1k): GPK, MSK

This procedure takes a security parameter k as input and generates a global public key (GPK) and a master secret key (MSK). MSK, GPK are used by admin for key generatio

n of each user. GPK is also known to every user and used in encryption and decryption procedure.

• Key-generation(GPK ,MSK ,S): PRK

This procedure takes input global public key (GPK), master secret key (MSK) an d set of attributes S of a user as input and produces a secret key for that par ticular user. The admin generates the private key (PRK) for everyuser in the system.

• Encryption(GPK, M, T): CT

This procedure is used to encrypt a file M under the specified decryption policy T using GPK and generates ciphertext, CT. Any user in the system can encrypt the file by spec ifying access conditions so that only the users whose attributes match with access policy can decrypt the file. Policy can be defined using relational operators like‘’, ‘<=’, ‘>=’, and ‘=’, specifically on the numerical attributes.

• Decryption(PRK, CT, GPK): M

This procedure inputs PRK, CT, GPK. If user’s set of attributes, S satisfy the access pol icy T, then file CT is decrypted by PRK and generated file M can be accessed by the user.

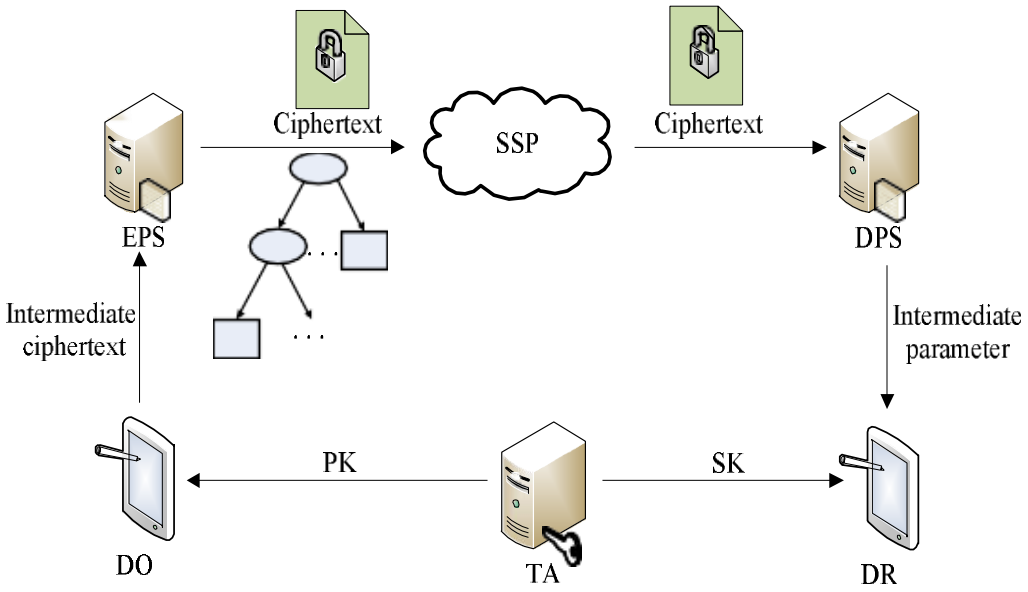

Fig.3.1. Data Access control CP-ABE

3.2 Construction

The shown CP-ABE system the private keys are held with a set P of descriptive attributes. When the client will encrypt a message, he will specify the access policy by using an access structure of the tree, T. The internal nodes represent logic operators or threshold gate. If an internal node x has n children numbered as 1 to n then threshold value t of this node will be 1<=t<=n. If t=1 then threshold gate works as OR operator and if t=n then threshold gate works as AND operator. The external node z represents the attribute value ,att_val associated with that node $G\ X\ G\ \rightarrow G$ for pairing operations where G,G are two cyclic groups of prime order p.

ABE is constructed as follows :

1. Setup : This procedure generates master secret key MSK as $(\beta, g\alpha)$ and global public key GPK as (G, g, h, f, e(g, g)). Where α,β are two random integers .

2. Key Generation : This will generate the private key PRK for every user and according to the set of attributes S as follows :

$$\text{PRK=D} = g^{(\alpha+i)/\beta},$$
$$\forall s \in S: D_s = g^i . H(s)^{i_s}, D'_s = g^{i_s}$$

3. Encrypt : By using this procedure the file we have to encrypt will be done under the access tree structure T. For every node x in the tree whether inside or outside in the tree T a polynomial will be chosen in the drop down manner and by start will be taken from the root node of T ans also assign the degree of the tree and with each of the node x which will be equal to K-1.

A random no will be chosen to set q(0)=n from the root node and chooses d so as to define the polynomial p.

$$q_x(0) = q_{\text{parent(x)}}^{\text{index(x)}}$$

4. Decrypt : This algorithm will be start by the simply calling of the Decrypt node function (PRK,CT,roots) for the access tree T of the root node in that. Now if the policies that are defined in the encryption if they will be met then the file will be decrypted means if the attributes S if they are satisfied we can retrieve our file.

R= DecryptNode(CT,PRK,root).

3.3 Advancement in work :

The advancement we can define as what we have modified in our proposed structure. As when we were doing or implementing the CP-ABE we were using the AES algorithm to encrypt our data. But now we will use the RSA algorithm to propose our new work. We choose RSA as the new encryption algorithm because we want to go for a light weight encryption algorithm than the previous one and also our performance should increase. So we choose RSA to be implemented in place of AES algorithm. I will be presenting the comparison between the two as first we should see the comparison between the two as how they works and then we will be showing the final outcomes or the results of our compared data. Firstly the AES algorithm as follows:

A. Symmetric Key Algorithm :

The most vital and the basic sort of the encryption is the symmetric key encryption. Symmetric-key of the calculations are those calculations which utilize a similar key for both encryption and decoding. Henceforth the key is kept mystery. Symmetric calculations have the benefit of not devouring excessively of processing force and it works with fast in encryption. Symmetric-key calculations are isolated into two kinds: Block cipher and Stream cipher. In block cipher input is taken as a square of plaintext of settled size contingent upon the kind of a symmetric encryption calculation, key of settled size is connected on to square of plain content and after that the yield square of the same measure as the square of plaintext is acquired. In Case of stream cipher one piece at any given moment is encoded. Some mainstream Symmetric-key calculations utilized as a part of distributed computing incorporates: Data Encryption Standard (DES), Triple-DES, and Advanced Encryption Standard (AES).

3.1.1 Advanced Encryption Standard (AES) :

Advanced Encryption Standard is a symmetric- key block cipher published as FIPS-197 in the Federal Register in December 2001 by the Institute of National Technologies and Standard (NIST). AES is a non-Feistel cipher. AES encrypts data with block size of 128-bits. It uses 10, 12, or fourteen rounds. Depending on the number of rounds, the key size may be 128, 192, or

256 bits as shown in figure 3. AES operates on a 4×4 column major order matrix of bytes, known as the state.

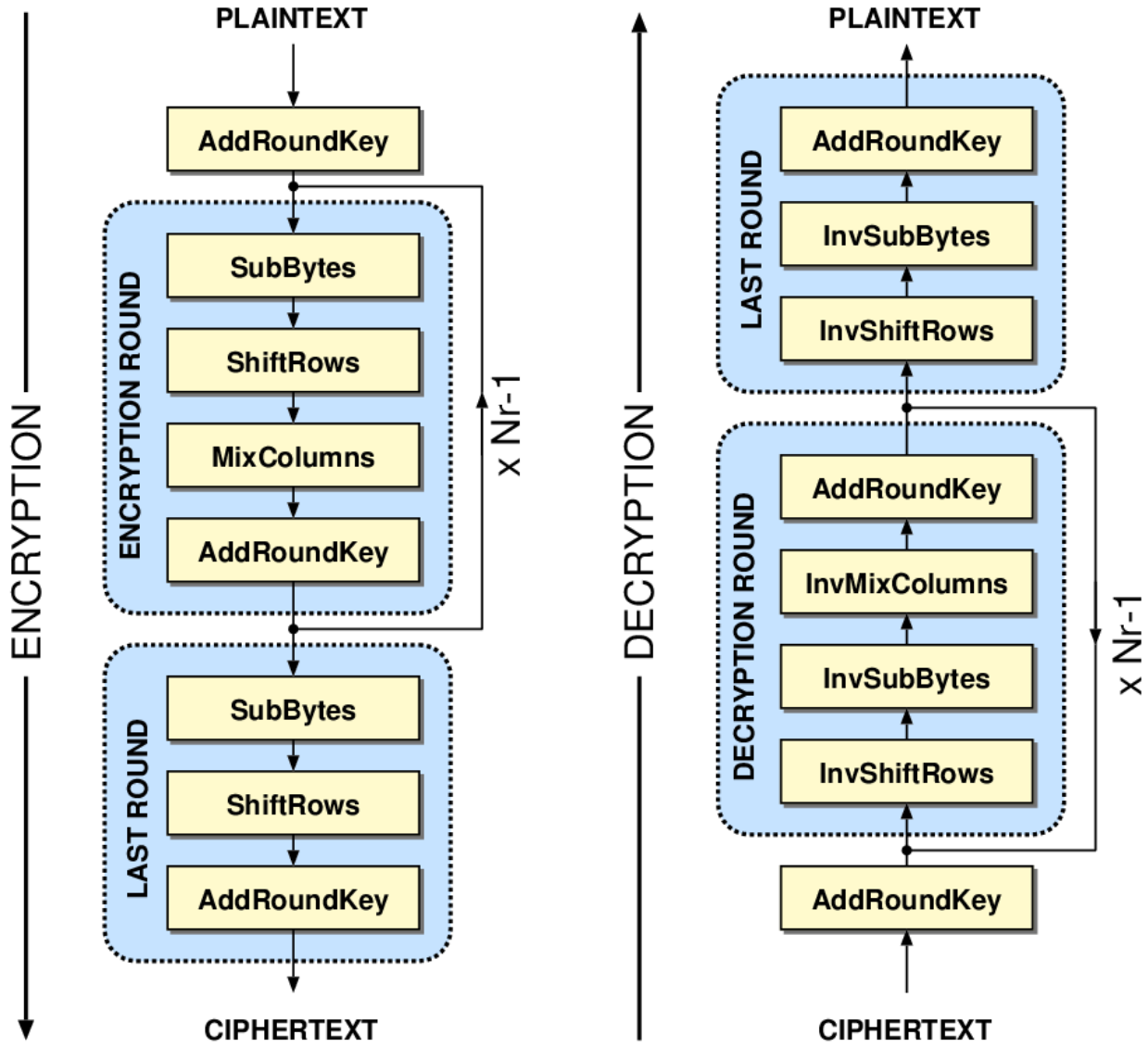

Fig.3.2. AES Structure

B. Asymmetric Key Algorithm :

Asymmetric-key algorithms are those algorithms that use different keys for encryption and decryption. The two keys are: Private Key and Public Key. The Public key is used by the sender for encryption and the private key is used for decryption of data by the receiver. In cloud

computing asymmetric-key algorithms are used to generate keys for encryption. The most common asymmetric-key algorithms for cloud are: RSA, IKE, Diffie-Helman Key Exchange.

3.2.2 RSA :

RSA cryptosystem realize the properties of the multiplicative Homomorphic encryption. Ronald Rivest, Adi Shamir and Leonard Adleman have invented the RSA algorithm and named after its inventors. RSA uses modular exponential for encryption and decryption. RSA uses two exponents, a and b, where a is public and b is private. Let the plaintext is P and C is ciphertext, then at encryption C = Pa mod n. And at decryption side P = Cb mod n. n is a very large number, created during key generation process.

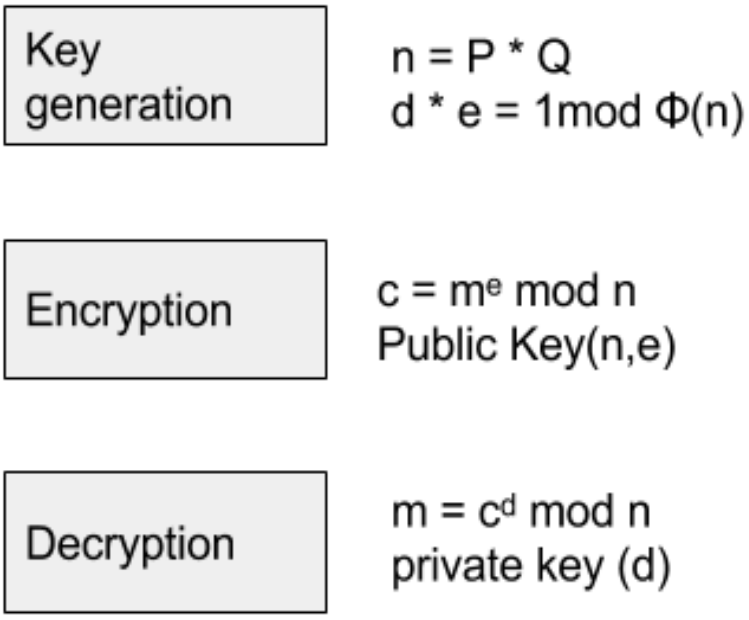

Fig. 3.3 RSA Structure

CHAPTER - 4

Implementation and Results

We have taken example of a university, where records are stored at a central area say Location1. Every faculty of all the departments can get to this data. Assumed hierarchy systemof scholastic representatives in university is given in Fig. 7.

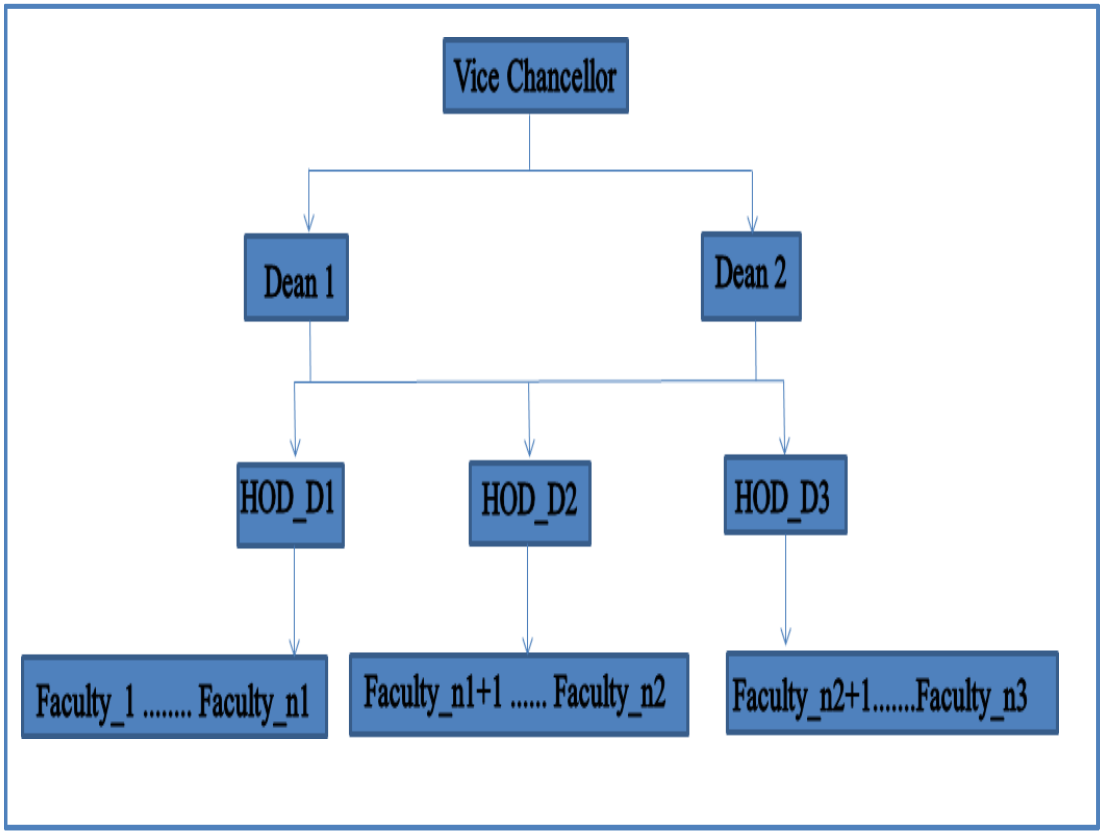

Fig.4.1. Typical Role hierarchy of Academic Employees in University

Presently assume a record named Subject1_D1_B5_Sem2_Lab_Marks_EVEN_2017.doc is put away on a neighborhood server'Location1'. Here Subject1 is subject name, D1 is the department, B5 is clump 5 and Sem 2 is II semester. This is the imprints document which is classified and ought to be gotten to by just by staff related with this cluster. As document is put away on regular server, it can be gotten to by everybody. Secret word insurance can be utilized to shield document access from unapproved client yet watchword based utilization has operational troubles as talked about earlier. There is a need to store the record in scrambled frame to such an extent that it is available to just approved clients of that specific file.We have proposed Ciphertext Policy-Attribute based encryption (CP-ABE) based answer for Fine Grained Access Control of college marks data.

We need to force the conditions that either workforce (as it were Teacher or Associate Professor or Assistant Professor) having a place with Department D1 or HOD, instructing the subject Suject1 (Lecture, instructional exercise or Lab of B5 group) or a hypothesis/lab organizer of this subject or accountable for Subject1 in EVEN semester 2017 or a responsible for second Semester D1 2017 or an Responsible for D1 2017 can get to this record as it were. Additionally, all these can get to this document till end of EVEN semester 2017 yet HOD of D1depatment, Dean and VC can get to the document after that too.

The file access structure of access policy of this example is given in fig 8.

The entrance tree is utilized to descript an entrance approach that indicates which mix of traits can decode the ciphertext. Let tree T whose root hub is r speak to the entrance strategy. Each inward hub of T is a rationale administrator, for example, "AND", "OR" and "OF", while each leaf hub speaks to a trait. A characteristic can be any expressive string that characterizes, orders, or comments on the client, to which it is appointed. As indicated by the possibility of mystery sharing, every hub of the entrance tree speaks to a mystery. In the encryption expression, we have to top-down recursively dole out a mystery to every hub. While in the unscrambling expression, we have to base up recuperate the mystery of the root hub. A character can be any expression string that characterizes, orders, or comments on the client, to which is to be appointed on the database. The university data access policy we have to define so that it can be accessed according to the rule and we can apply on the data set of that university easily. The query applied on data set can be easily fetched.

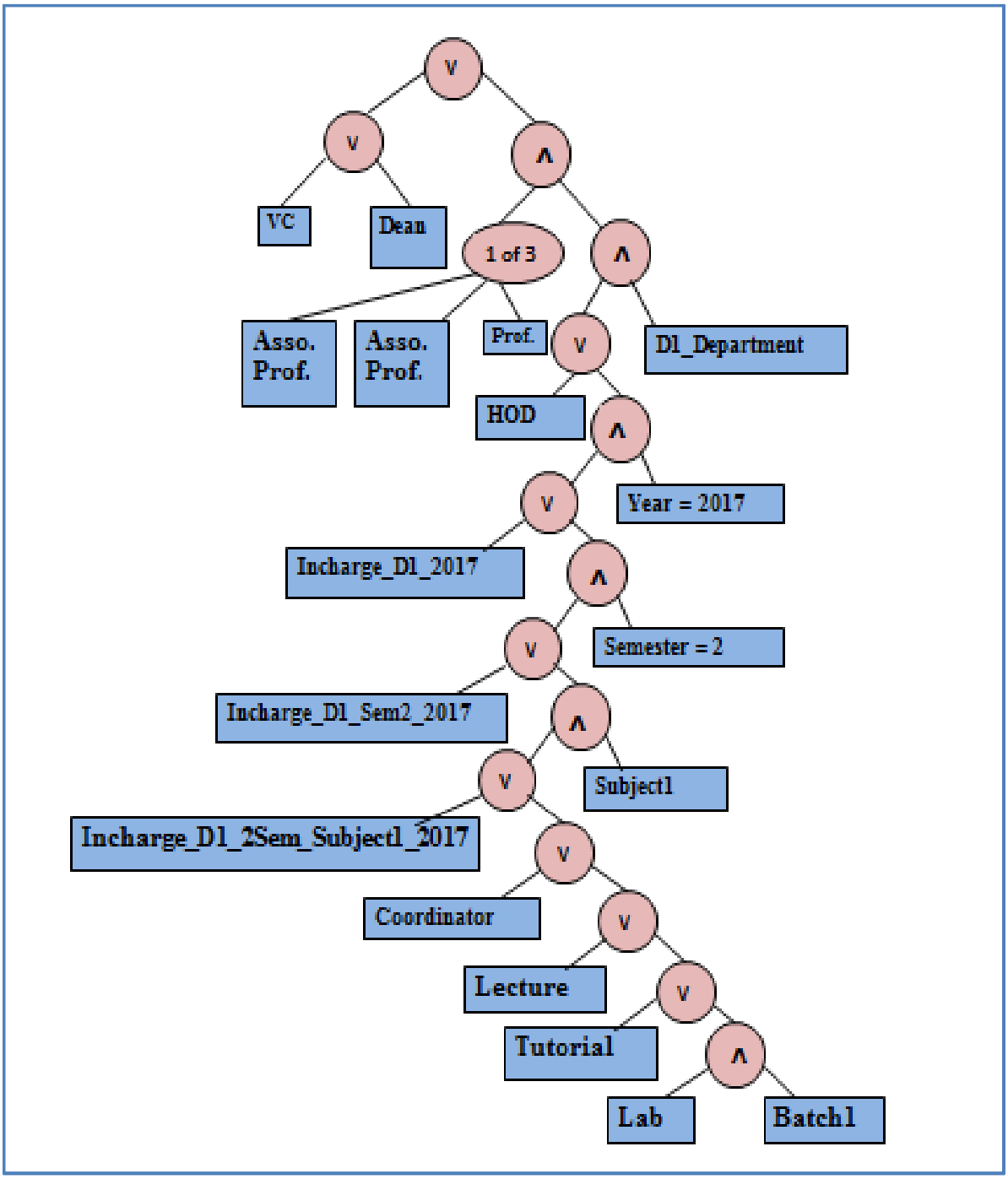

Fig.4.2. Tree Structure of Access policy

There are different properties of every representative, the document can be gotten to by just those representatives whose properties esteems fulfill the entrance conditions. Trait rundown of representatives are appeared in Table I. These credit esteems are utilized to produce private keys of every client.

Name	Designation	Department	ID	Role	Subject	Batch	Semester	Year
Faculty1	Assistant Professor	D1 Department	'ID = 1554'	Lecture	Subject1	Batch1	'Semester = 2'	'Year = 2017'
Faculty2	Assistant Professor	D1 Department	'ID = 1550'	Tutorial	Subject1	Batch6	'Semester = 2'	'Year = 2017'
Faculty3	Assistant Professor	D1 Department	'ID = 1535'	Lab	Subject1	Batch5	'Semester = 2'	'Year = 2017'
Faculty4	Associate Professor	D1 Department	'ID = 1249'	Coordinator Theory	Subject1		'Semester = 2'	'Year = 2017'
Faculty5	Professor	D1 Department	'ID = 1211'	HOD				
Mgmt1			'ID = 1201'	VC				
Faculty6	Professor	D1 Department	'ID = 1210'	In-charge D1 2017				'Year = 2017'
Faculty7	Associate Professor	D1 Department	'ID = 1220'	In-charge D1 2Sem 2017				'Year = 2017'
Faculty8	Associate Professor	D2 Department	'ID = 1230'	Incharge D1 2Sem SDFII 2017	Subject1		'Semester = 2'	'Year = 2017'
Faculty9	Assistant Professor	D1 Department	'ID = 1560'	Lab	Subject5	Batch5	'Semester = 2'	'Year = 2017'

TABLE 4.1: ATTRIBUTE LIST OF EMPLOYEES

Our usage utilizes cpabe library for ABE setup, key age, encryption and decoding tasks and PBC library for matching based cryptographic tasks. Setup strategy produces the Global Public Key (GPK) what's more, Master Secret Key (MSK) record. These GPK and MSK are utilized to produce the private key of every client. To create private key of a client his/her's qualities are used as info. Presently, to store a record on Location1 in encoded shape, get to strategy must be implemented on the information with the encryption charge. Access arrangement is set of conditions spoke to in intelligent formulae on properties joined with logical operators. One case of access arrangement is given in the Fig. 9.

(VC or (Dean and Academic) or
(1 of(Professor,AssociateProfessor , Assistant_Professor) and (D1_Department and (HOD or ((Incharge_D1_2017 or (Incharge_D1_2Sem_2017 or ((Incharge_D1_2Sem_SDFII_2017 or Coordinator or Lecture or Tutorial or (Lab and B5)) and Subject1) and Semester =2)) and Year=2017)))))

Fig.4.3. Access Policy

For utilizing Subject1_D1_B5_Sem2_Lab_Marks_EVEN_2017.doc put away on Location1, client needs to unscramble the document utilizing his/her private key U issued by focal expert in light of his arrangement of qualities S. Document would be accurately decoded utilizing his key, if client's qualities coordinate the entrance arrangement, T, determined in scrambled document.

4.2 Results and Discussion

From execution assessment of ABE-CP based encription furthermore, decoding, a few trials were performed on sham clients, their arrangement of qualities and shifting record sizes. All examinations were done in condition defined in Table II. We have investigated the execution of the key age, encryption and unscrambling tasks with regard to varying number of properties. The outcomes are appeared in Figures 10-12.

CPU	Intel Core i5 CPU@2.70GHz
RAM	8 GB
OS	Windows OS 8
Compiler	NetBeans
Language	Java
External Library	GMP, OpenSSL, TEPLA

TABLE 4.2:ENVIRONMENT OF PERFORMANCE MEASUREMENT

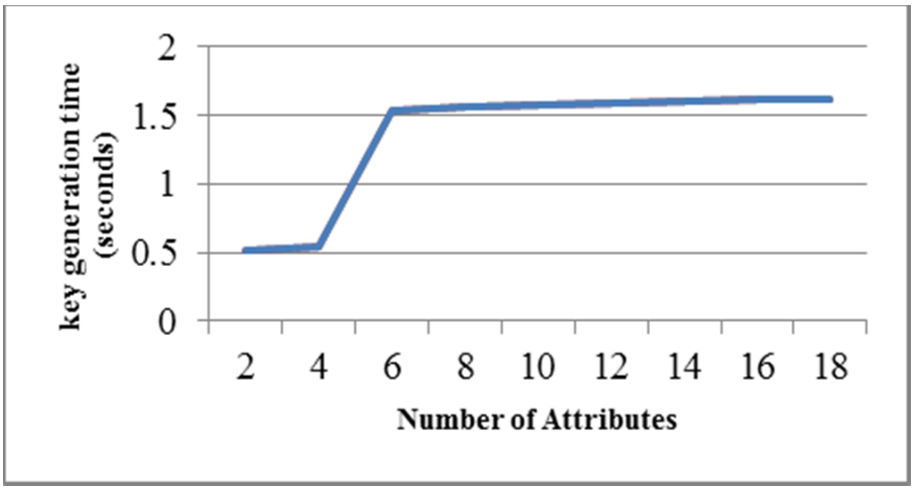

Fig.4.4. No. of attributes vs Key generation time

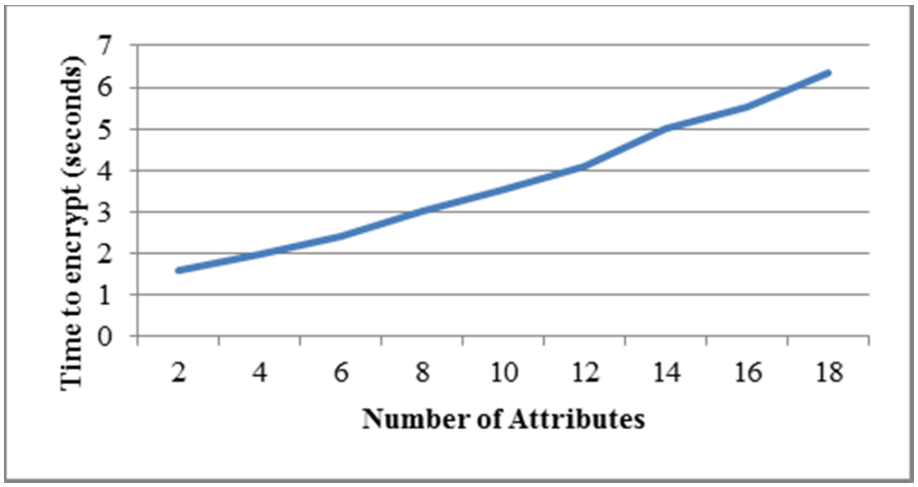

Fig.4.5. No. of attributes vs Encryption time

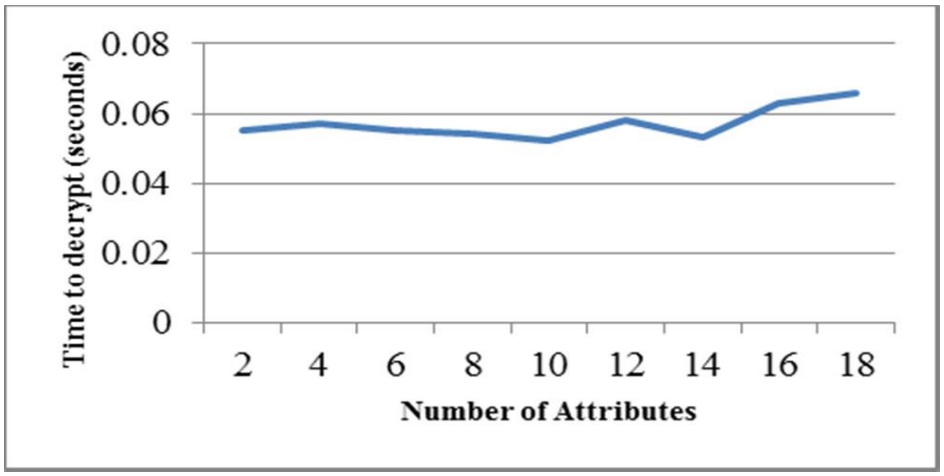

Fig.4.6. No. of attributes vs Decryption time

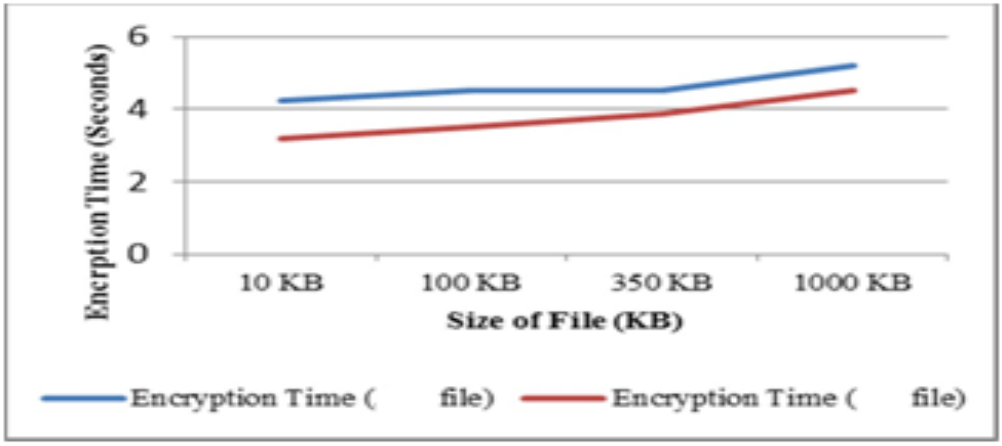

Fig.4.7. Size of file vs Encryption time

Fig.4.8. Size of file vs Decryption time

In Fig. 10, genuine calculation time of mystery key age calculation into the ABE-CP conspire them deference changing of number traits from describing every client. The key age time is same when number of qualities is between 2 to 4. The key age time increments quickly in straight way for number of ascribes from 4 to 6. On expanding the quantity of characteristics further, key age time additionally increments yet slowly. This apparently irregular key age time on expanding number of traits related with mystery key is because of arbitrary qualities α, β, is an ∈ ZΓ utilized as and part of exponentiation. Overall, key age time differ straightly with number of characteristics. As appeared in Fig. 8, encryption time too slowly and directly

increments with increment in number of qualities utilized in indicating access strategy. Be that as it may, this straight reliance isn't extremely unmistakable in unscrambling times. The unscrambling time rely upon the specific access trees and set of qualities included. More number of examinations comes about more decoding time. We ran decoding system on same ciphertext encoded under same access strategy to a however changing diverse clients' private key. Fig. 9 demonstrates that unscrambling time and a isn't dependant just on number of characteristics yet additionally on the particular access arrangement of the ciphertext and the characteristics related with the private key. We have likewise our a dissected the execution of the encryption tasks by expanding the measure of different kinds of record like .docx,.pptx, xls .pdf and so forth. The outcomes can be to are appeared in figure 10 and11.Figure 10 demonstrates that the execution of encryption methodology is better for .xls document than .doc record since .xls record contain less data than .doc record like design and header information and encryption time is around following the direct association with record and to estimate for both kind of document. Figure 11 analyzes and the execution of .pdf and .ppt record. .ppt document takes more encryption time than .pdf on the grounds that .ppt record header furthermore, design contain more data than .pdf record. Encryption time increments directly by expanding the record measure.

4.3 Screenshots

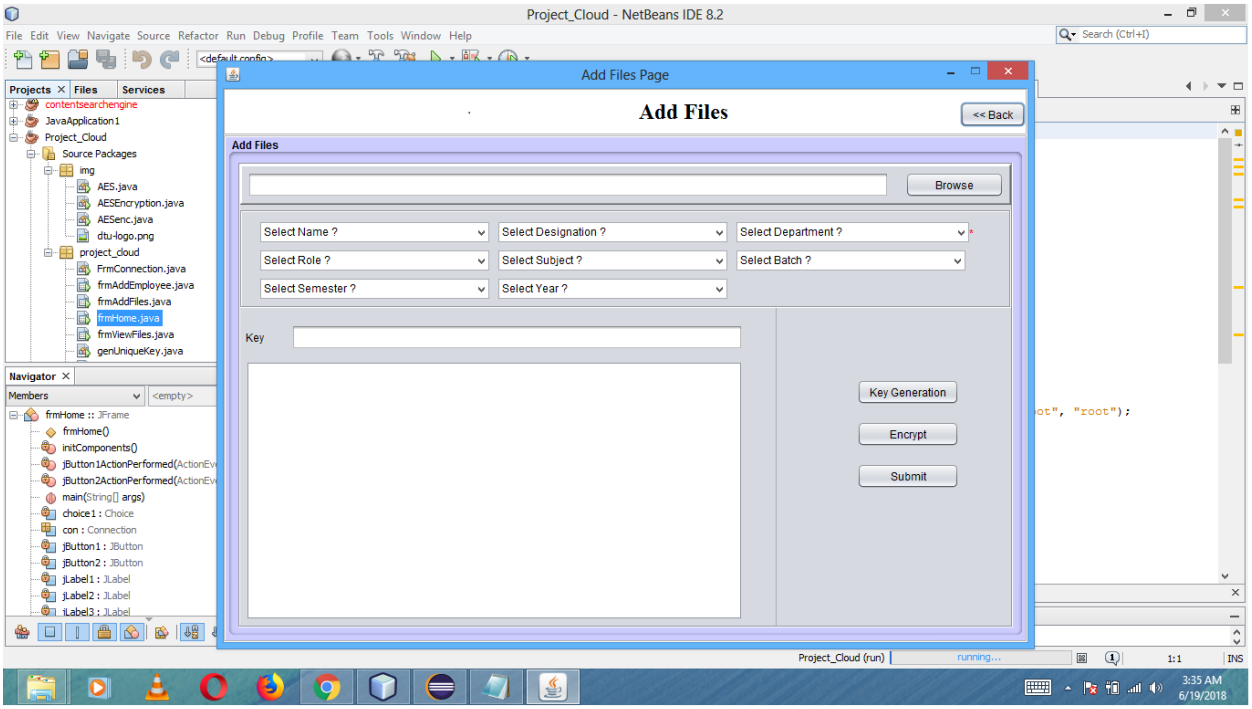

Fig. 4.3.1 Add Files

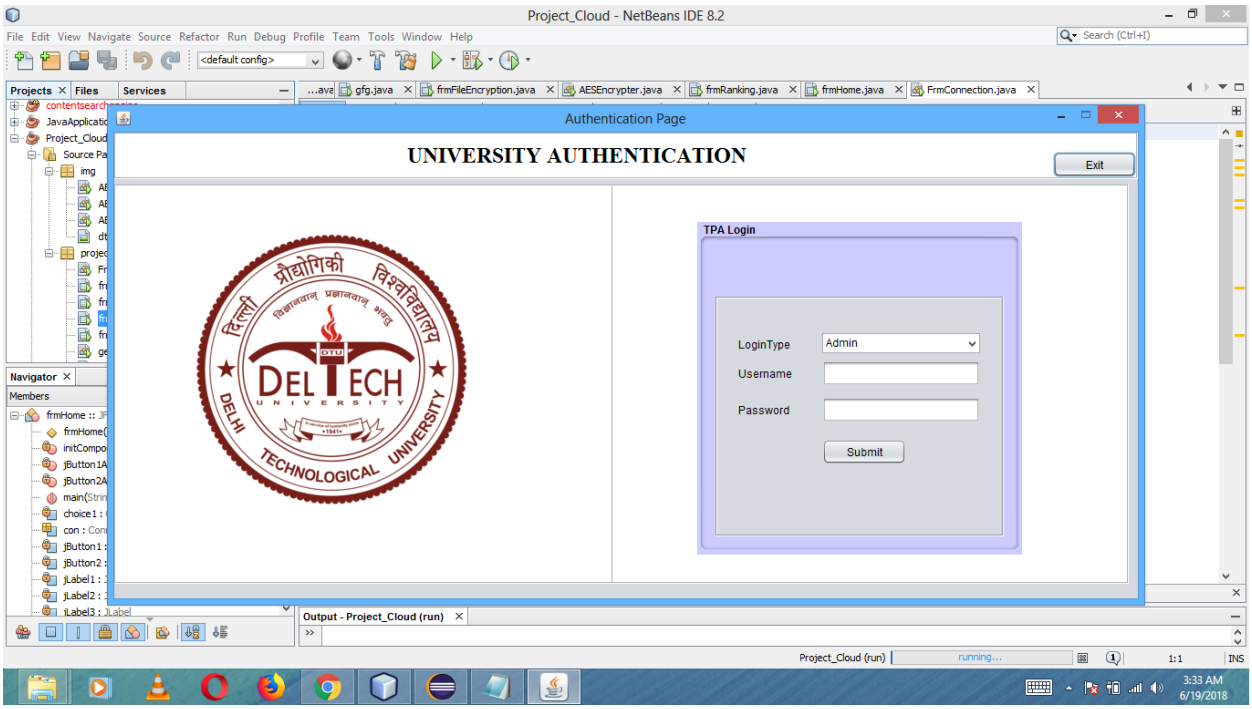

Fig.4.3.2 Admin Login

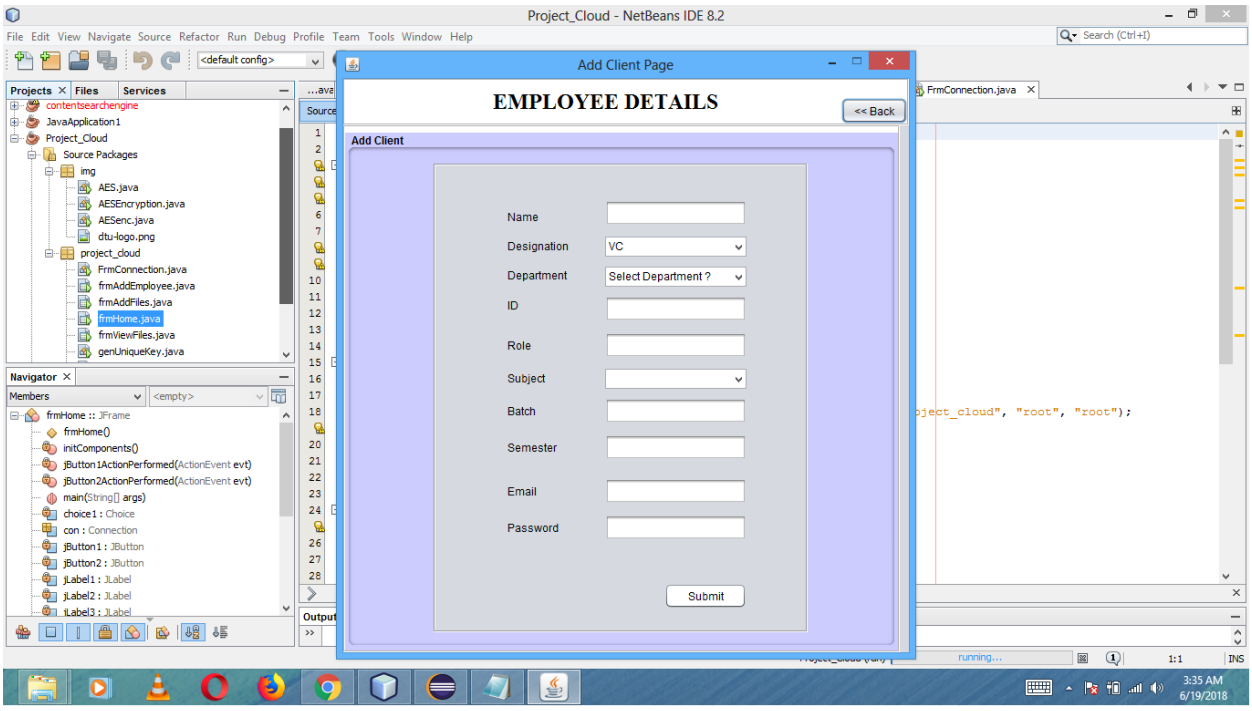

Fig.4.3.3 Employee Details

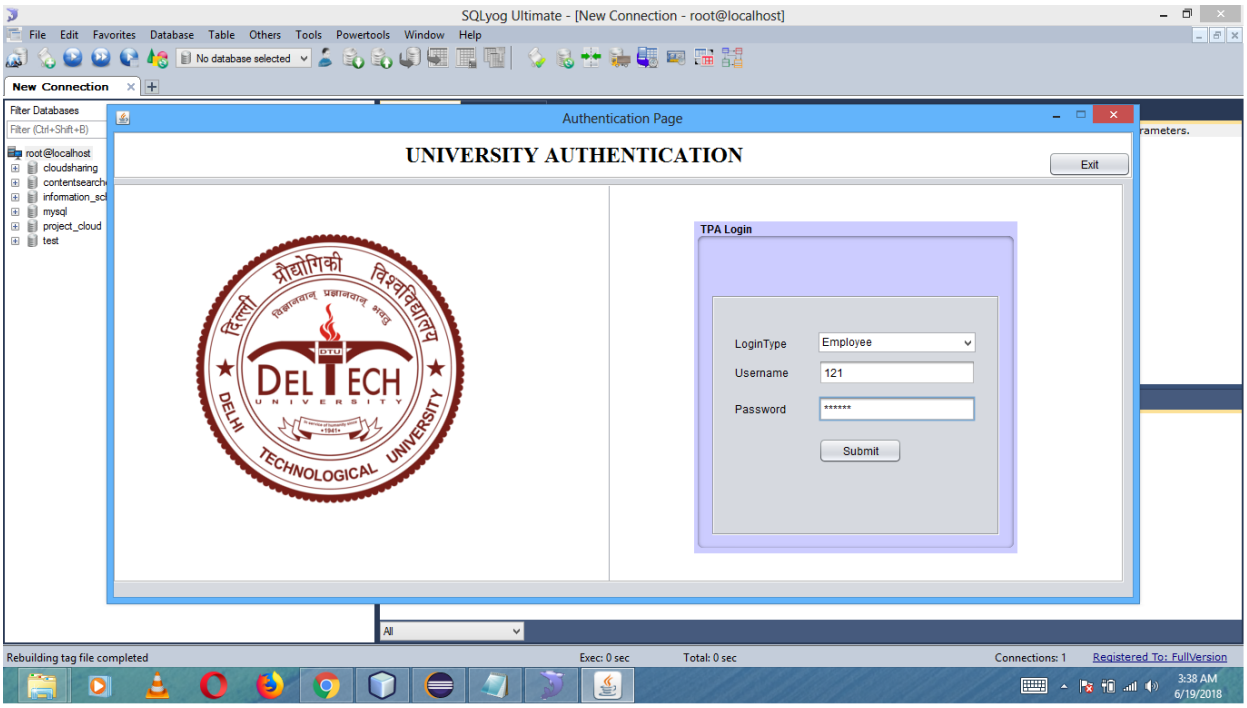

Fig.4.3.4 Employee Login

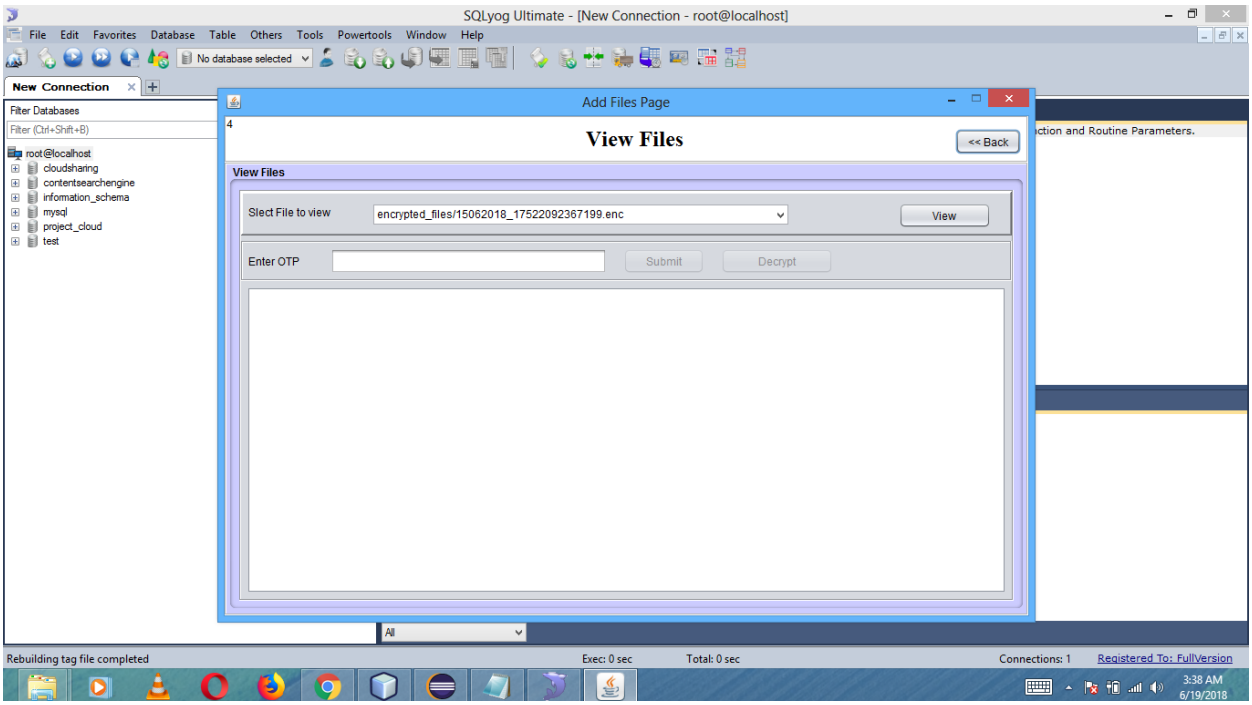

Fig.4.3.5 View Files

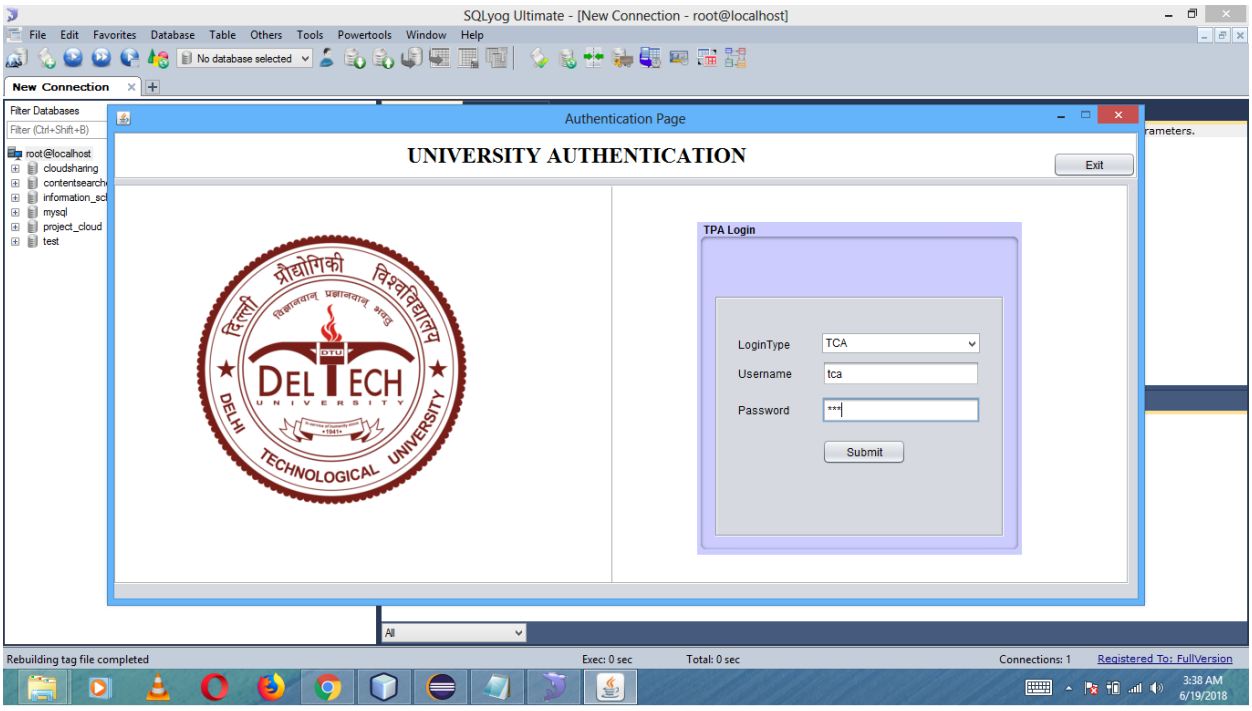

Fig 4.3.6 TCA Login

CHAPTER - 5

Conclusion and Future Work

A CP-ABE based fine grained access control of documents has been presented into an university scenario. Documents can be stored at central location and still accessible to only those users whose attribute values satisfy the access policy. It has been found to be an efficient cryptographic solution as compared to traditional public key cryptography, as far lesser number of keys and encrypted documents need to be created. The work can be further extended to support CP-ABE based partial encryption and decryption of documents.

We discussed the challenges of securely storing and sharing data in MCC. To solve this problem, we proposed a secure and lightweight data access control scheme named CP-ABE, which can preserve the confidentiality of outsourced data and meanwhile achieve fine-grained data access control efficiently in MCC. Compared with previous works, CP-ABE has significant advantages. Firstly, the overall system performance can an is improved obviously by greatly reducing the computation overheads in encryption and decryption phrases. Secondly, there is as no special restrictions on access policy tree, which provides expressive and flexible data access control. Lastly, mobile devices can easily complete the data processing operations by outsourcing most of the computation operations to proxy servers located in cloud. For future work, we will realize dynamic attribute revocation in CP-ABE to get better control over access privilege.

5.2 Future Work

The limitation of the approach proposed, is that it requires updating the secret key of a user. Currently we assume that only TCA can add/delete/update the attributes. In future, we can consider the Multi authority based setup to deal with the issue. We can apply this updating feature to user revocation, group signature, etc. and may get better understanding of protocol. Currently TCA can change any attribute but in future, we can divide into static and dynamic such that TCA can update only dynamic attributes. Our current work is focus on this.

In the future, it would be interesting to consider attribute-based encryption systems with different types of expressibility. While, Key-Policy ABE and Ciphertext-PolicyABE capture two interesting and complimentary types of systems there certainly exist other types of systems. The primary challenge in this line of work is to find a new systemswith elegant forms of expression that produce more than an arbitrary combination of techniques.

One limitation of our system is that it is proved se- cure underthe generic group heuristic. We believe an important endeavor would be to prove asystem secure under a more standard and non-interactive assumption. This type of work would be interesting even if it resulted in a moderate loss of efficiency from our existing system.

References

[1] Vipul Goyal, Omkant Pandey,Amit Sahai,Brent Waters, “Attribute-Based Encryption forFine-Grained Access Control of Encrypted Data, Proceedings of the 13th ACM conference on Computer and communications security, Pages 89-98, Alexandria, Virginia, USA — October 30 - November 03, 2006.

[2] John Bethencourt, Amit Sahai, and Brent Waters, “Ciphertext-Policy Attribute-BasedEncryption”,28th IEEE Symposium on Security and Privacy (Oakland) , May 2006.

[3] Keisuke Hasegawa, Naoki Kanayama, Takashi Nishide, Eiji Okamoto, “ Software Library for Ciphertext/Key-Policy Functional Encryption with Simple Usability”, Journal of Information Processing, Vol.24, No.5, 764-771, Sep. 2016.

[4] Myong H. Kang, Joon S. Park, and Judith N. Froscher. Access control mechanisms for inter-organizational workflow. In SACMAT '01: Proceedings of the sixth ACM symposium on Access control models and technologies, pages 66-74, New York, NY, USA, 2001. ACM Press. Proceedings of 2017 Tenth International Conference on Contemporary Computing (IC3), 10-12 August 2017, Noida, India

[5] Rita Gavriloaie, Wolfgang Nejdl, Daniel Olmedilla, Kent E. Seamons, and Marianne Winslett. No registration needed: How to use declarative policies and negotiation to access sensitive resources on the semantic web. In ESWS, pages 342-356, 2004.

[6] Ting Yu and Marianne Winslett. A united scheme for resource protection in automated trust negotiation. In IEEE Symposium on Security and Privacy, pages 110-122, 2003.

[7] Jiangtao Li, Ninghui Li, and William H. Winsborough. Automated trust negotiation using cryptographic credentials. In ACM Conference on Computer and Communications Security, pages 46-57, 2005.

[8] Hugh Harney, Andrea Colgrove, and Patrick Drew McDaniel. Principles of policy in secure groups. In NDSS, 2001.

[9] Patrick Drew McDaniel and Atul Prakash. Methods and limitations of security policy reconciliation. In IEEE Symposium on Security and Privacy,pages73-87,2002.

[10] J. Bethencourt, A. Sahai, and B. Waters, ``Ciphertext-policy attribute based encryption," in Proc. IEEE SP, Oakland, CA, USA, May 2007,pp.321-334.

[11] Zhijie Wang, Dijiang Huang, Yan Zhu, Bing Li, Chun-Jen Chung, "Efficient Attribute-Based Comparable Data Access Control", IEEE Transactions On Computers, Vol. 64, No. 12, December 2015.

[12] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. EUROCRYPT, 2005, vol. 3494, pp. 457–473.

[13] L. Ibraimi, Q. Tang, P. Hartel and W. Jonker, "Efficient and provable secure ciphertext-policy attribute-based encryption schemes," Lecture Notes in Computer Science, Berlin Heidelberg: Springer, pp.1-12, 2009.

[14] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," Proc. 14th ACM Conf. Computer and communications security, 2007, pp. 456-465.

[15] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," Proc. ACM Conf. Computer and Comm. Security, 2006, pp. 89-98.

[16] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models," Computer, vol. 29, no. 2, pp. 38-47, 1996.

[17] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, Ā Scalable secure file sharing on untrusted storage," Proc. 2nd USENIX Conf. File Storage Technol, 2003, pp. 29–42.

[18] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi and P. Samarati, "Over-encryption: management of access control evolution on outsourced data," Proc. 33rd Int. Conf. Very Large Data Bases, 2007, pp. 123–134.

[19] L. Ibraimi, M. Petkovic, S. Nikova and W. Jonker, "Mediatedciphertext-policy attribute-based encryption and its application," Information Security Applications. Berlin Heidelberg: Springer, pp. 309-323, 2009.

[20] G. Wang, Q. Liu, J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," Proc. 17th ACM conference on Computer and communications security, 2010, pp. 735-737.

[21] M. Chase, "Multi-authority attribute based encryption," Theory of Cryptography, Berlin Heidelberg: Springer, pp. 515-534, 2007.

[22] V. Božovis, D. Socek, R. Steinwandt and V. I. Villányi, "Multi- authority attribute-based encryption with honest-but-curious central authority," International Journal of Computer Mathematics, vol. 89, no. 3, pp. 268-283, 2012.

[23] R. Ostrovsky, A. Sahai and B.Waters, "Attribute-based encryption with non-monotonic access structures," Proc. 14th ACM conference on Computer and communications security, 2007, pp. 195-203.

[24] V. Goya, A. Jain, O. Pandey and A. Sahai. "Bounded ciphertext policy attribute based encryption," Automata, Languages and Programming, Berlin Heidelberg: Springer, pp. 579-591, 2008.

[25] A. J. Menezes, P. C. Van Oorschot, S. A. Vanstone, "Handbook of applied cryptography," CRC press, 1996.