CIPHER TEXT-POLICY ATTRIBUTE-BASED ENCRYPTION AND WITH DELEGATION EMERGES IN CLOUD COMPUTING

KODEDALA CHAND BEE[1], C S MAHABOOBBEE[2], T PADMA[3]

[1]M.Tech Scholar, ST.MARK Educational Institution Society Group Institutions.
[2,3] Assistant Professor, ST.MARK Educational Institution Society Group Institutions.

ABSTRACT: We propose a new design for large-scale multimedia content protection systems. Our design leverages cloud infrastructures to provide cost efficiency, rapid deployment, scalability, and elasticity to accommodate varying workloads. The proposed system can be used to protect different multimedia content types, including 2-D videos, 3-D videos, images, audio clips, songs, and music clips. The system can be deployed on private and/or public clouds. Our system has two novel components: (i) method to create signatures of 3-D videos, and (ii) distributed matching engine for multimedia objects. The signature method creates robust and representative signatures of 3-D videos that capture the depth signals in these videos and it is computationally efficient to compute and compare as well as it requires small storage. The distributed matching engine achieves high scalability and it is designed to support different multimedia objects. We implemented the proposed system and deployed it on two clouds: Amazon cloud and our private cloud. Our experiments with more than 11,000 3-D videos and 1 million images show the high accuracy and scalability of the proposed system. In addition, we compared our system to the protection system used by YouTube and our results show that the YouTube protection system fails to detect most copies of 3-D videos, while our system detects more than 98% of them. This comparison shows the need for the proposed 3-D signature method, since the state-of-the-art commercial system was not able to handle 3-D videos.

1 INTRODUCTION

Cloud computing is the utilization of registering belongings (gear and programming) that are conveyed as an administration over a method (in general the internet). The title originates from the basic utilization of a cloud-formed picture as a deliberation for the unpredictable base it involves in framework graphs. Disbursed computing depends far off firms with a consumer's data, programming and computation. Disbursed computing entails gear and programming assets made available on the web as supervised outcast corporations. These businesses more commonly present access to forefront programming applications and top quality frameworks of server PCs.

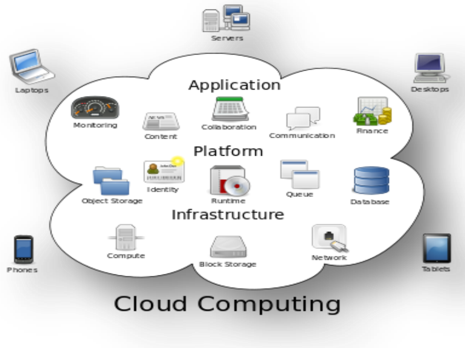


Fig 1.1 Structure of Cloud Computing

1.2 Working of Cloud Computing

The objective of distributed computing is to apply fashioned supercomputing, or sophisticated processing energy, usually utilized by way of military and exploration offices, to participate in many trillions of calculations every 2nd, in client organized purposes, for example, money related portfolios, to carry personalized knowledge, to give expertise stockpiling or to affect mammoth, immersive computer diversions.

Characteristics and Services Models

The salient characteristics of cloud computing founded on the definitions supplied by way of the country wide Institute of requisites and Terminology (NIST) are outlined below:

- On-demand self-carrier: A customer can unilaterally provision computing capabilities, corresponding to server time and community storage, as wanted routinely without requiring human interaction with each and every provider's provider.
- Large community access: Capabilities are on hand over the network and accessed through typical mechanisms that promote use with the aid of heterogeneous thin or thick customer systems (e.G., mobile telephones, laptops, and PDAs).
- Useful resource pooling: The provider's processing assets are pooled to serve more than a few customers utilising a multi-inhabitant model, with various physical and digital property swiftly distributed and reassigned with the aid of curiosity.

There is a feeling of subject autonomy in that the customer for essentially the most phase has no manage or learning over the specific subject of the gave property nevertheless could have the capacity to examine subject at a bigger amount of deliberation (e.G., nation, state, or server farm). Illustrations of assets incorporate stockpiling, making ready, reminiscence, system data switch capability, and digital machines.

Services Models

Cloud Computing comprises three exclusive provider items, namely Infrastructure-as-a-provider (IaaS), Platform-as-a-provider (PaaS), and application-as-a-service (SaaS). The three provider models or layer are accomplished with the aid of an end person layer that encapsulates the end person perspective on cloud services. If she accesses a carrier on the applying layer, these tasks are most likely looked after by using the cloud service supplier.

1.3 Advantages of Cloud Computing

1. Attain economies of scale increase quantity yield or efficiency with less participants. Your fee every unit, task or object falls..
2. Reduce spending on science infrastructure. . Maintain up simple access to your data with negligible forthright spending. Pay as you go (week after week, quarterly or each year), in light of curiosity.
3. Globalize your workforce on the affordable. Persons international can get to the cloud, if they've an internet organization.
4. Four. Streamline strategies. Get more work executed in much less time with less individuals.
5. Reduce capital costs. There's no compelling reason to spend gigantic money on gear, programming or authorizing fees.
6. Reinforce accessibility. You may have admittance at something time, at any place, making your lifestyles so much easier!
7. Display initiatives extra quite simply. Stay within spending plan and in entrance of consummation method durations.
8. Much less personnel training is required. It takes much less contributors to accomplish extra chip away at a cloud, with a negligible expectation to absorb understanding on gear and programming issues

1.4 Area of Research

Attribute based encryption sahai and waters proposed the notation of attribute based encryption. The focused on policies across multiple authorities and issue of what expression could achieve the strongest form of expression is Boolean formula in ABE system. Which still for from being able to expresses access control in the form of any program or circuit. Actually there still remains two problems the first one is there have no construction for realizing CP-ABE for general circuits. The other is related to the efficiency, since the existing circuits ABE scheme just a bit encryption one thus it is apparently still remaining a pivotal open problem to design an efficient circuit CP-ABE scheme.

The first ABE with outsourcing decryption scheme to reduce the computation cost during decryption. After that proposed the definition of ABE with verifiable outsourced decryption. They seek to gurantee the correctness of the original cheaper text by using a commitment. However since the data owner generates a commitment without any secret value.

2. PROPOSED WORK AND ANALYSIS

In this chapter discussion about Existing System, Disadvantages of the Existing System and Techniqes used in Proposed System Advantages Proposed System and system Architecture.

2.1 Existing System

The servers could be wont to handle and calculate varied information consistent with the user's demands. As applications move to cloud computing platforms, ciphertext-policy attribute-based encryption (CP-ABE) and verifiable delegation (VD) square measure used to make sure the information confidentiality and also the verifiability of delegation on dishonest cloud servers. The increasing volumes of medical images and medical records, the healthcare organizations place a massive quantity of knowledge within the cloud for reducing data storage prices and supporting medical cooperation. There are 2 complementary forms of attribute primarily based secret writing. One is key-policy attribute-based secret writing (KP-ABE) and the alternative is ciphertext-policy attribute-based encryption (CPABE).

2.1.1 Disadvantages of Existing System

- The cloud server might tamper or replace the information owner's original ciphertext for malicious attacks, and then respond a false transformed ciphertext.
- The cloud server might cheat the approved user for value saving. Though the servers may not respond an accurate reworked ciphertext to AN

unauthorized user, he could cheat AN approved one that he/she isn't eligible.

2.2 Proposed System

We first off gift a circuit ciphertext-policy attribute-based hybrid secret writing with verifiable delegation theme. General circuits are used to specific the strongest variety of access management policy. the proposed theme is well-tried to be secure primarily based on k-multilinear Decisional Diffie-Hellman assumption. On the other hand, we implement our theme over the integers. During the delegation computing, a user could validate whether or not the cloud server responds a correct reworked ciphertext to assist him/her decipher the ciphertext straightaway and properly.

2.2.1 Advantages of Proposed System

- The generic KEM/DEM construction for hybrid encodeion that will encrypt messages of discretional length.
- They seek to guarantee the correctness of the initial ciphertext by employing a commitment.
- We give the anti-collusion circuit CP-ABE construction in this paper for the rationale that CPABE is conceptually nearer to the standard access management strategies.

2.3 System Architecture

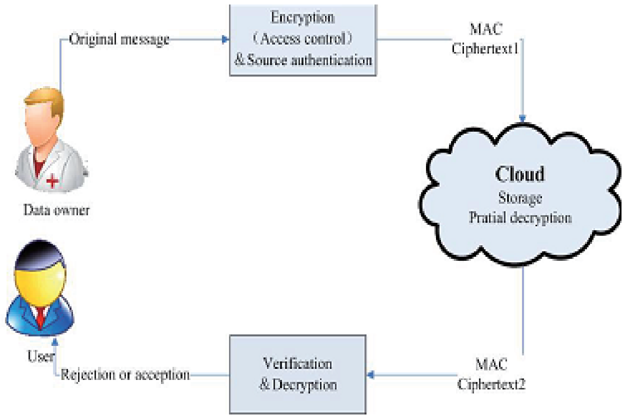


Fig 2 System Architecture

Data owner send the original message in the form of encryption format. It is cipher text. It is not a readable format. Receive the message to the user through cloud storage. If verification is yes then message can be readable and decryption the message. If key is send user can open the file otherwise not open the file. If verification is no then message cannot readable.

2.4 System Study

2.4.1 Feasibility Study

The achievability of the mission is dissected in this stage and business proposition is evolved with an especially wide association for the project and some rate gauges. Amid framework examination the probability investigation of the proposed framework is to be completed. That is to guarantee that the proposed framework is just not a weight to the group. For possibility examination, some comprehension of the giant prerequisites for the framework is principal.

Three key considerations involved in the feasibility analysis are

- Economical Feasibility
- Technical Feasibility
- Social Feasibility

2.4.2 Economical Feasibility

This learns is accomplished to assess the financial influence that the framework can have on the organization. The measure of believe that the group can fill the revolutionary work of the framework is limited. The consumptions must be legitimized. For this reason the created framework too throughout the economic allowance and this used to be attained to in gentle of the fact that the vast majority of the advances utilized are uninhibitedly accessible. Just the tweaked items must be received.

2.4.3 Technical Feasibility

This learn is done to assess the specialized attainability, that's, the specialized requirements of the framework. Any framework created must now not have an attraction on the obtainable specialized assets. This will prompt levels of popularity on the available specialised assets. This may occasionally immediate phases of repute being set on the consumer. The created framework have to have a humble necessity, as just negligible or invalid changes are needed for actualizing this framework.

3. IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

3.1 Modules

- Attribute Authority
- Cloud Server
- Data owner
- Data Consumer

3.1.1 Attribute Authority

Authority will have to offer the key, as per the user's key request. Every users request can have to be raised to authority to induce access key on mail. There are 2 complementary forms of attribute-based secret writing. One is key-policy attribute-based secret writing (KP-ABE) and the alternative is ciphertext-policy attribute-based encryption (CPABE). In a KP-ABE system, the decision of access policy is created by the key distributor rather than the encipherer, which limits the usefulness and usability for the system in sensible applications.

3.2 Cloud Server

Cloud server will have the access to files that square measure uploaded by the information owner Cloud server needs to decipher the files offered underneath their permission. Furthermore information user can have to decipher the info to access the initial text by providing the individual key. File has been decrypted successfully and provided for shopper.

3.2.1 Data Owner

Data owner can have to register initio to induce access to the profile. Data Owner can transfer the file to the cloud server in the encrypted format. Random encryption key generation is happening whereas uploading the file to the cloud. Encrypted file will be hold on the cloud.

3.2.2 Data Consumer

Data shopper can be initio raise for the key to the Authority to verify and decipher the enter the cloud. Data shopper will access the file primarily based on the key received from mail id. As per the key received the consumer will verify and decipher the info from the cloud.

4. RESULTS

In this chapter the software requirements and the hardware requirements that are necessary to execute the extraction pattern are specified. The graphical user interface that the user or performs while utilizing the CP-ABE and verifiable delegation are discussed.

4.1 System Requirements

Hardware Requirements

➢	System	:	Pentium IV 2.4 GHz.
➢	Hard Disk	:	40 GB.
➢	Monitor	:	15 VGA Colour.
➢	Ram	:	512 Mb.

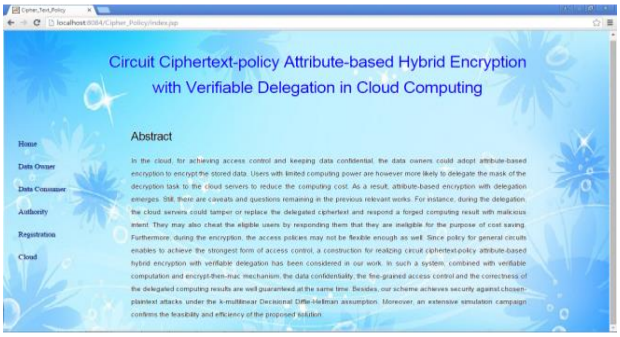
Software Requirements

➢	Operating system	:	Windows XP/7.
➢	Coding Language	:	JAVA/J2EE
➢	IDE	:	Netbeans 7.4
➢	Database	:	MYSQL

4.2 Execution Results

In this section it describes the entity disambiguity. In this section each and every screen shot has been presented and The graphical user interface that the user or performs while utilizing the CP-ABE and verifiable delegation are discussed.

4.2.1 Home Page



Circuit Ciphertext-policy Attribute-based Hybrid Encryption with Verifiable Delegation in Cloud Computing

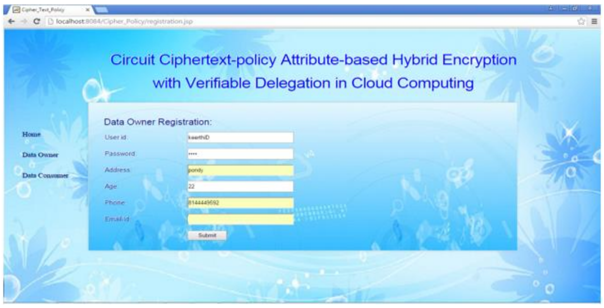
Abstract

In the cloud, for achieving access control and keeping data confidential, the data owners could adopt attribute-based encryption to encrypt the stored data. Users with limited computing power are however more likely to delegate the mask of the decryption task to the cloud servers to reduce the computing cost. As a result, attribute-based encryption with delegation emerges. Still, there are caveats and questions remaining in the previous relevant works. For instance, during the delegation, the cloud servers could tamper or replace the delegated ciphertext and respond a forged computing result with malicious intent. They may also cheat the eligible users by responding them that they are ineligible for the purpose of cost saving. Furthermore, during the encryption, the access policies may not be flexible enough as well. Since policy for general circuits enables to achieve the strongest form of access control, a construction for realizing circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation has been considered in our work. In such a system, combined with verifiable computation and encrypt-then-mac mechanism, the data confidentiality, the fine-grained access control and the correctness of the delegated computing results are well guaranteed at the same time. Besides, our scheme achieves security against chosen-plaintext attacks under the k-multilinear Decisional Diffie-Hellman assumption. Moreover, an extensive simulation campaign confirms the feasibility and efficiency of the proposed solution.

Fig 3 Home Page

This screen describes about the registration of data owner, data consumer , authority , data owner registration , cloud.

4.2.2 Data Owner Registration



Circuit Ciphertext-policy Attribute-based Hybrid Encryption with Verifiable Delegation in Cloud Computing

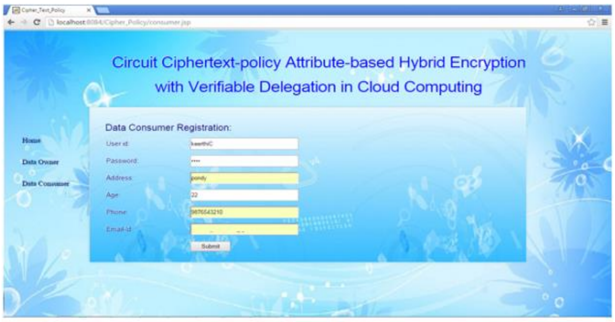
Data Owner Registration:

User id	keerthiD
Password	****
Address	pondy
Age	22
Phone	8144449692
Email id	

Fig 4 Data Owner Registration

This screen describes about the data owner registration form with the following fields like userid, password, age, mail id etc.

4.2.3 Data Consumer Registration



Circuit Ciphertext-policy Attribute-based Hybrid Encryption with Verifiable Delegation in Cloud Computing

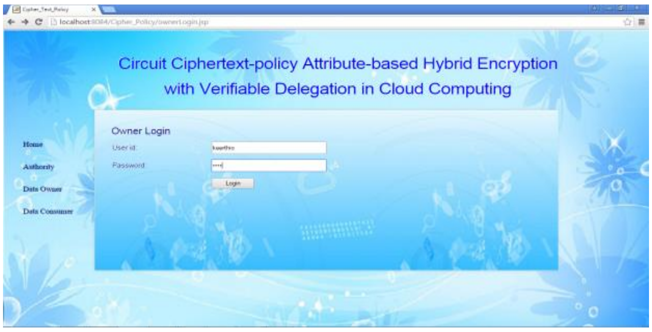
Data Consumer Registration:

User id: keerthiC
Password: ****
Address: pondy
Age: 22
Phone: 9876543210
Email-id:

Fig 5 Data Consumer Registration

This screen describes about the data consumer registration form with the following fields like userid, password, age, mail id etc.

4.2.4 Owner Login



Circuit Ciphertext-policy Attribute-based Hybrid Encryption with Verifiable Delegation in Cloud Computing

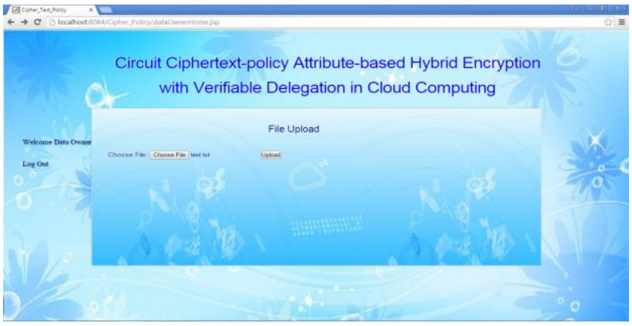
Owner Login

User id: keerthio
Password: ****

Fig 6 Owner Login

This screen tells about the data owner login with the required fields. User id and password for owner login page.

4.2.5 File Upload



Circuit Ciphertext-policy Attribute-based Hybrid Encryption with Verifiable Delegation in Cloud Computing

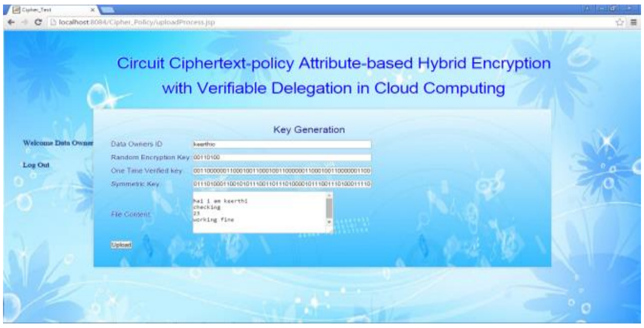
File Upload

Choose File: text.txt

Fig 7 File Upload

This screen tells about the file upload. Owner upload the file through the cloud storage . File is encryption format . file cannot be readable.

4.2.6 Key Generation



Circuit Ciphertext-policy Attribute-based Hybrid Encryption with Verifiable Delegation in Cloud Computing

Key Generation

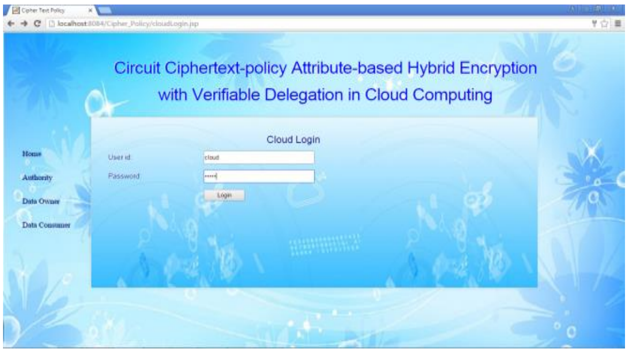
Data Owners ID: keerthio
Random Encryption Key: 00110100
One Time Verified key: [illegible]
Symmetric Key: [illegible]
File Content:

```
hai i am keerthi
checking
23
working fine
```

Fig 8 Key Generation

The above figure explains the consumer send the key to the authority. And send the request of the key. Authority access the key and permit to login.

4.2.7 Cloud Login



Circuit Ciphertext-policy Attribute-based Hybrid Encryption with Verifiable Delegation in Cloud Computing

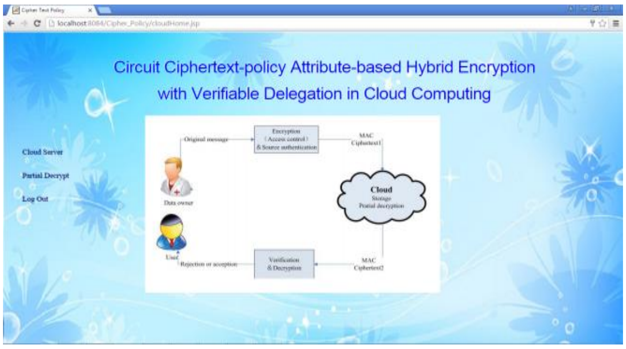
Cloud Login

User id: cloud
Password: *****

Fig 9 Cloud Login

The above figure show that owner login into the system. Owner is upload the file.after that cloud login into the system . to access the file upload by the owner.

4.2.8 Cloud Home

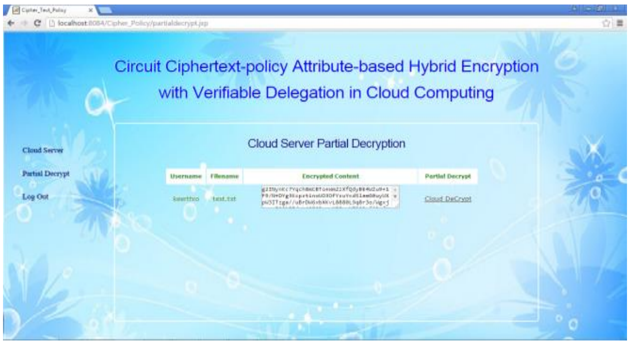


Circuit Ciphertext-policy Attribute-based Hybrid Encryption with Verifiable Delegation in Cloud Computing

Fig 10 Cloud Home

The above figure show that cloud home fields are the cloud server, partial decrypt, logout.

4.2.9 Partial Decrypte Text File Page



Circuit Ciphertext-policy Attribute-based Hybrid Encryption with Verifiable Delegation in Cloud Computing

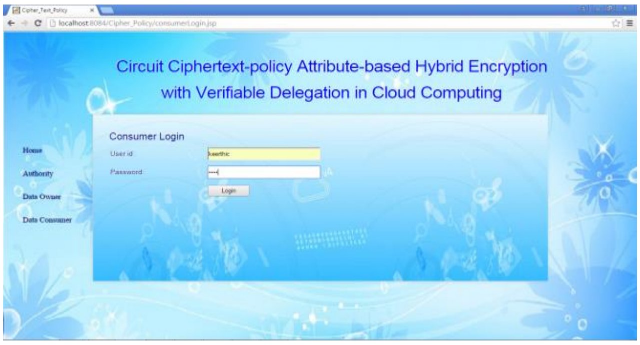
Cloud Server Partial Decryption

Username	Filename	Encrypted Content	Partial Decrypt
keerthio	test.txt	[illegible]	Cloud DeCrypt

Fig 11 Partial Decrypte Text File Page

The above figure shows that file is partial decryption. It is readable format. Cloud activities are partial decryption.

4.2.10 Consumer Login



Circuit Ciphertext-policy Attribute-based Hybrid Encryption with Verifiable Delegation in Cloud Computing

Consumer Login

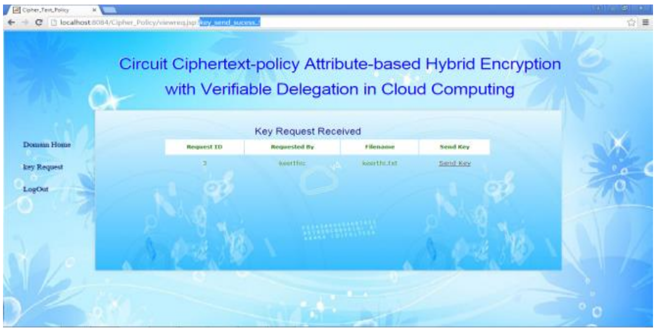
User id: keerthic

Password: ••••

Fig 12 Consumer Login

The above figure show that consumer login required field user id and password. Consumer send the key to the authority . and request the file to the authority.

4.2.11 Authority Send Key



Circuit Ciphertext-policy Attribute-based Hybrid Encryption with Verifiable Delegation in Cloud Computing

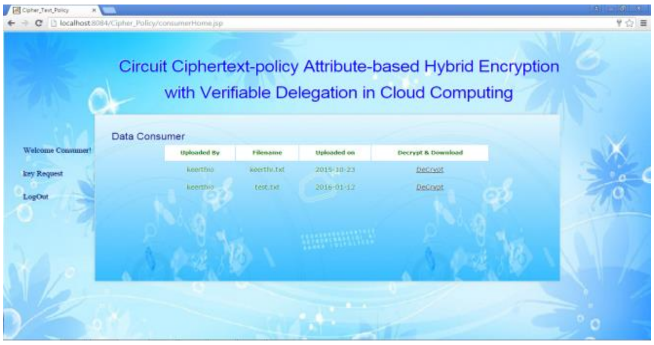
Key Request Received

Request ID	Requested By	Filename	Send Key
3	keerthic	keerthic.txt	Send Key

Fig 13 Authority Send Key

The above figure shows that consumer send the key to authority. And key request of the file to the authority. The key not a readable format.

4.2.12 Verifiable Data Consumer



Circuit Ciphertext-policy Attribute-based Hybrid Encryption with Verifiable Delegation in Cloud Computing

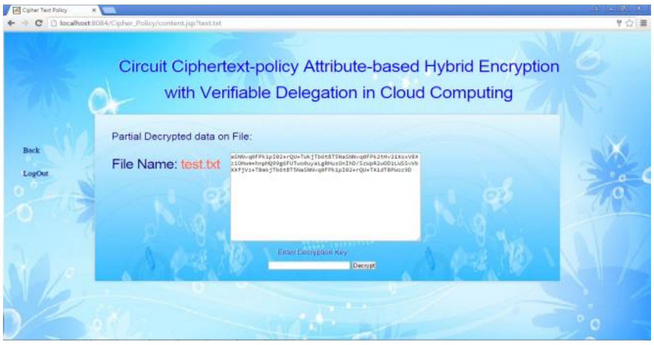
Data Consumer

Uploaded By	Filename	Uploaded on	Decrypt & Download
keerthio	keerthi.txt	2015-10-23	DeCrypt
keerthio	test.txt	2016-01-12	DeCrypt

Fig 14 Verifiable Data Consumer

The above figure shows that data consumer upload the file by owner , upload file name , upload date, decrypt the file

4.2.13 Partial Decrypted data on File



Circuit Ciphertext-policy Attribute-based Hybrid Encryption with Verifiable Delegation in Cloud Computing

Partial Decrypted data on File:

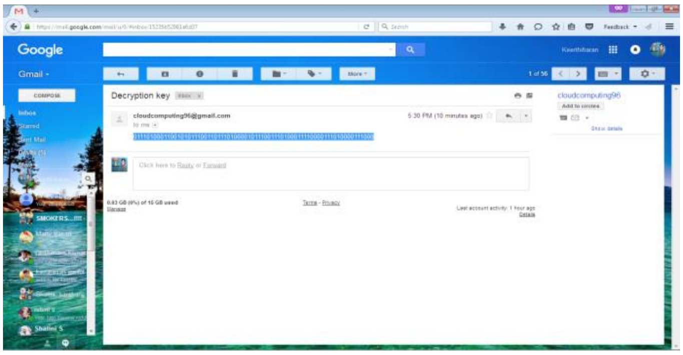
File Name: test.txt

Enter Decryption Key

Fig 15 Partial Decrypted data on File

The above figure show that cloud partial decrypt data of the file. And file is readable format.

4.2.14 Key Send Mail



Decryption key

cloudcomputing96@gmail.com

to me

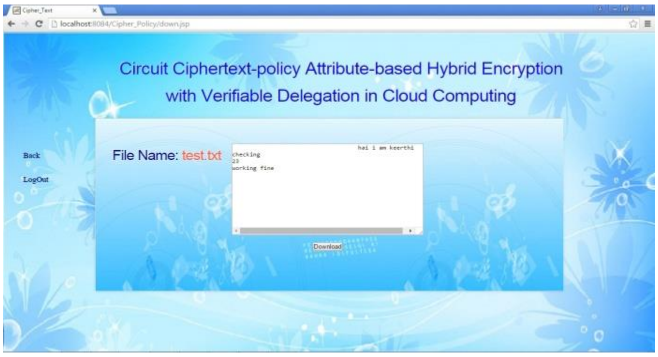
5:30 PM (10 minutes ago)

0.63 GB (4%) of 15 GB used

Fig 16 Key Send Mail

The above figure show that the cloud send the decryption key to mail. And key is readable format.

4.2.15 File View



Circuit Ciphertext-policy Attribute-based Hybrid Encryption with Verifiable Delegation in Cloud Computing

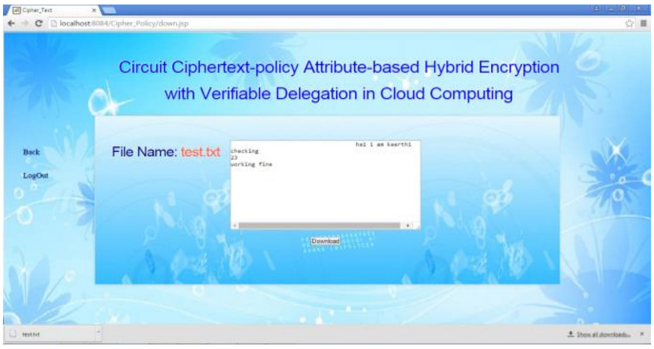
File Name: test.txt

```
                                        hai i am keerthi
checking
23
working fine
```

Fig 17 File View

The above figure show that file view by the authority. Consumer sends the key, request of the key to the mail.

4.2.16 File Download



Circuit Ciphertext-policy Attribute-based Hybrid Encryption with Verifiable Delegation in Cloud Computing

File Name: test.txt

```
                                        hai i am keerthi
checking
23
working fine
```

Fig 18 File Download

The above figure show the file download by the authority. Decryption the file. File view by authority.

CONCLUSION

To the best of our knowledge, we first off gift a circuit cipher text-policy attribute-based hybrid secret writing with verifiable delegation theme. General circuits are used to specific the strongest variety of access management policy. Combined verifiable computation and encrypt-then-mac mechanism with our ciphertext policy attribute-based hybrid encryption, we may delegate the verifiable partial decoding paradigm to the cloud server. In addition, the proposed theme is well-tried to be secure primarily based on k-multilinear Decisional Diffie-Hellman assumption. On the other hand, we implement our theme over the integers. The costs of the computation and communication consumption show that the theme is sensible within the cloud computing. Thus, we may apply it to guarantee the info confidentiality, the fine-grained access control and the verifiable delegation in cloud.

A circuit cipher text-policy attribute-based hybrid encryption with verifiable delegation scheme is presented, circuits are used to state the secure type of access control policy. Certifiable computation and encrypt-then-mac mechanism are combined with ciphertext-policy attribute-based hybrid encryption and assign the verifiable partial decryption paradigm to the cloud server. The expenses of the computation and communique consumption show that the scheme is useful in the cloud computing.

REFERENCES

1] A. Shamir, “Identity-based cryptosystems and signature schemes,” in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 1985, pp. 47–53.

[2] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2005, pp. 457–473.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proc. 13th CCS, 2006, pp. 89–98.

[4] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute based encryption,” in Proc. IEEE SP, May 2007, pp. 321–334.

[5] M. Chase, “Multi-authority attribute based encryption,” in Theory of Cryptography. Berlin, Germany: Springer-Verlag, 2007, pp. 515–534.