Cryptographically Enforced Dynamic Access Control

Masula Anusha[1], K. Charan Theja[2]
[1]P.G. Scholar, [2]Guide, Head of the Department
[1,2] BRANCH:CSE(Mtech)
[1,2] Geethanjali College Of Engineering And Technology
Email id: [1]masulaanusha@gmail.com, [2]charantheja.kp2628@gmail.com

Abstract:

Secure cloud storage, which is an arising cloud administration, is intended to ensure the classification of reevaluated information yet in addition to give adaptable information admittance to cloud clients whose information is out of actual control. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is viewed as one of the most encouraging methods that might be utilized to make sure about the assurance of the administration.

In any case, the utilization of CP-ABE may yield an unavoidable security penetrate which is known as the abuse of access accreditation (for example decryption rights), due to the natural "win big or bust" decryption highlight of CP-ABE. In this paper, we research the two principle instances of access accreditation abuse: one is on the semi-believed authority side, and the other is in favor of cloud client. To alleviate the abuse, we propose the main responsible power and revocable CP-ABE based cloud storage framework with white-box recognizability and evaluating, alluded to as CryptCloud+. We likewise present the security investigation and further exhibit the utility of our framework by means of examinations.

Keywords: access control, cloud, revocation

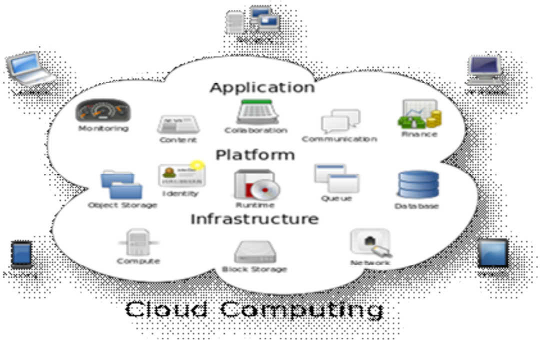
Introduction

What is cloud computing?

Cloud computing is the utilization of computing assets (equipment and programming) that are conveyed as a help over an organization (normally the Internet). The name comes from the regular utilization of a cloud-formed image as a reflection for the unpredictable foundation it contains in framework charts. Cloud computing depends far off administrations with a client's information, programming and calculation. Cloud computing comprises of equipment and programming assets made accessible on the Internet as overseen outsider administrations. These administrations regularly give admittance to cutting edge programming applications and top of the line organizations of worker PCs.

How Cloud Computing Works?

The objective of cloud computing is to apply customary supercomputing, or elite computing power, typically utilized by military and examination offices, to perform many trillions of calculations for every second, in purchaser situated applications, for example, monetary portfolios, to convey customized data, to give information storage or to control enormous, vivid PC games.



Structure of cloud computing

The cloud computing utilizes organizations of enormous gatherings of workers commonly running minimal effort buyer PC innovation with specific associations with spread information preparing errands across them. This shared IT framework contains enormous pools of frameworks that are connected together. Frequently, virtualization strategies are utilized to boost the intensity of cloud computing.

Attributes and Services Models:

The remarkable attributes of cloud computing dependent on the definitions gave by the National Institute of Standards and Terminology (NIST) are plot beneath:

- On-request self-administration: A purchaser can singularly arrangement computing abilities, for example, worker time and organization storage, varying consequently without requiring human connection with each specialist co-op's.

- Broad network access: Capabilities are accessible over the organization and gotten to through standard components that advance use by heterogeneous slight or thick customer stages (e.g., cell phones, PCs, and PDAs).

- Resource pooling: The supplier's computing assets are pooled to serve various buyers utilizing a multi-occupant model, with various physical and virtual assets powerfully appointed and reassigned by shopper interest. There is a feeling of area freedom in that the client by and large has no control or information over the specific area of the gave assets yet might have the option to determine area at a more significant level of reflection (e.g., nation, state, or server farm). Instances of assets incorporate storage, handling, memory, network transfer speed, and virtual machines.

- Rapid versatility: Capabilities can be quickly and flexibly provisioned, sometimes consequently, to rapidly scale out and quickly delivered to rapidly scale in. To the purchaser, the capacities accessible for provisioning frequently seem, by all accounts, to be limitless and can be bought in any amount whenever.

- Measured administration: Cloud frameworks naturally control and upgrade asset use by utilizing a metering capacity at some degree of deliberation fitting to the kind of administration (e.g., storage, handling, transfer speed, and dynamic client accounts). Asset utilization can be overseen, controlled, and announced giving straightforwardness to both the supplier and purchaser of the used assistance.

1) Sedasc: Secure information partaking in clouds
Creators: Mazhar Ali, Revathi Dhamotharan, Eraj Khan, Samee U. Khan,
Athanasios V. Vasilakos, Keqin Li, and Albert Y. Zomaya

Cloud storage is a utilization of clouds that frees associations from building up in-house information storage frameworks. Notwithstanding, cloud storage offers ascend to security concerns. If there should be an occurrence of gathering shared information, the information face both cloud-explicit and regular insider dangers. Secure information dividing between a gathering that counters insider dangers of genuine yet noxious clients is a significant examination issue. In this paper, we propose the Secure Data Sharing in Clouds (SeDaSC) approach that gives: 1) information classification and trustworthiness; 2) access control; 3) information sharing (sending) without utilizing register concentrated reencryption; 4) insider danger security; and 5) forward and in reverse access control. The SeDaSC approach encodes a document with a solitary encryption key. Two diverse key offers for every one of the clients are produced, with the client just getting one offer. The ownership of a solitary portion of a key permits the SeDaSC philosophy to counter the insider dangers. The other key offer is put away by a confided in outsider, which is known as the cryptographic worker. The SeDaSC system is material to customary and portable cloud computing conditions. We execute a working model of the SeDaSC strategy and assess its exhibition dependent on the time devoured during different activities. We officially confirm the working of SeDaSC by utilizing significant level Petri nets, the Satisfiability Modulo Theories Library, and a Z3 solver. The outcomes end up being empowering and show that SeDaSC can possibly be adequately utilized for secure information partaking in the cloud.

2) Iot-based enormous information storage frameworks in cloud computing: Perspectives and difficulties
Creators: Hongming Cai, Boyi Xu, Lihong Jiang, and Athanasios V. Vasilakos.
Web of Things (IoT) related applications have arisen as a significant field for the two specialists and analysts, mirroring the size and effect of information related issues to be settled in contemporary business associations particularly in cloud computing. This paper initially gives a utilitarian system that recognizes the securing, the board, preparing and mining regions of IoT huge information, and a few related specialized modules are characterized and depicted regarding their key qualities and capacities. At that point flow research in IoT application is investigated, additionally, the difficulties and openings related with IoT large information research are recognized. We additionally report an investigation of basic IoT application distributions and examination themes dependent on related scholastic and industry distributions. At long last, some open issues and some ordinary models are given under the proposed IoT-related examination system.

3) jpbc: Java matching based cryptography
Creators: Angelo De Caro and Vincenzo Iovino
It has been as of late found that some cyclic gatherings that could be utilized in Cryptography concede an exceptional bilinear blending map that acquaints additional structure with the gathering. Bilinear matching guides were first used to break cryptosystems (see, for instance,) and later it was understood that the additional structure could be abused to fabricate cryptosystems with additional properties. Boneh and Franklins character based encryption conspire is the most renowned early illustration of what could be accomplished utilizing bilinear guides. From that point onward, a plenty of cryptosystems have been planned utilizing bilinear guides. No full and unreservedly accessible execution of matching based cryptography was accessible until this work. Late

proposition miss the mark concerning this objective as either their source code isn't accessible or in light of the fact that they uphold a restricted scope of elliptic bend. In addition, neither one of executes preprocessing that is essential to lessen the calculation time. In this work, we present jPBC a Java port of the PBC library written in C. jPBC gives a full biological system of interfaces and classes to rearrange the utilization of the bilinear guides in any event, for a non-cryptographer. jPBC upholds various kinds of elliptic bends, preprocessing which can speedup the calculation essentially and it is prepared for the versatile world. Additionally a benchmark examination among jPBC and PBC has been performed to quantify the hole between the two libraries. Moreover jPBC has been benchmarked on various Android portable stages.

4) Enabling semantic inquiry dependent on theoretical diagrams over scrambled rethought information

Creators: Zhangjie Fu, Fengxiao Huang, Xingming Sun, Athanasios Vasilakos, and Ching-Nung Yang

As of now, accessible encryption is an intriguing issue in the field of cloud computing. The current accomplishments are principally centered around watchword based inquiry plans, and practically every one of them rely upon predefined catchphrases separated in the periods of list development and question. In any case, watchword based pursuit plans overlook the semantic portrayal data of clients' recovery and can't totally coordinate clients' hunt aim. Thusly, how to plan a substance based hunt plan and make semantic inquiry more viable and setting mindful is a troublesome test. In this paper, unexpectedly, we characterize and tackle the issues of semantic inquiry dependent on reasonable graphs(CGs) over scrambled re-appropriated information in clouding computing (SSCG).We initially utilize the productive proportion of "sentence scoring" in content synopsis and Tregex to separate the most significant and rearranged theme sentences from reports. We at that point convert these rearranged sentences into CGs. To perform quantitative count of CGs, we plan another strategy that can plan CGs to vectors. Next, we rank the returned results dependent on "text synopsis score". Besides, we propose a fundamental thought for SSCG and give an altogether improved plan to fulfill the security assurance of accessible symmetric encryption (SSE). At last, we pick a genuine world dataset – ie., the CNN dataset to test our plan. The outcomes got from the test show the viability of our proposed conspire.

5) KSF-OABE: re-appropriated attribute-based encryption with catchphrase scan work for cloud storage

Creators: Jiguo Li, Xiaonan Lin, Yichen Zhang, and Jinguang Han

Cloud computing turns out to be progressively famous for information proprietors to re-appropriate their information to public cloud workers while permitting proposed information clients to recover these information put away in cloud. This sort of computing model carries difficulties to the security and protection of information put away in cloud. Attribute-based encryption (ABE) innovation has been utilized to configuration fine-grained admittance control framework, which gives one great strategy to settle the security issues in cloud setting. Notwithstanding, the calculation cost and ciphertext size in most ABE plans develop with the unpredictability of the entrance policy. Reevaluated ABE (OABE) with fine-grained admittance control framework can to a great extent diminish the calculation cost for clients who need to get to encoded information put away in cloud by re-appropriating the hefty calculation to cloud service provider (CSP). Notwithstanding, as the measure of encoded records put away in cloud is getting exceptionally tremendous, which will thwart proficient inquiry preparing. To manage above issue, we present another cryptographic crude called attribute-based encryption plot with rethinking key-giving and reevaluating decryption, which can actualize catchphrase search work (KSF-OABE). The proposed KSF-OABE plot is demonstrated secure against picked plaintext assault (CPA). CSP performs incomplete decryption task appointed by information client without knowing the slightest bit about the plaintext. Besides, the CSP can perform encoded catchphrase search without knowing the slightest bit about the watchwords installed in secret entrance.

MODULES:

- Data Owner
- Data User
- Semi-trusted authority
- Auditor
- Cloud Server and Encryption Module

EXISTING SYSTEM:

- In a CP-ABE based cloud storage system, for example, organizations (e.g., a university such as the University of Texas at San Antonio) and individuals (e.g., students, faculty members and visiting scholars of the university) can first specify access policy over attributes of a potential cloud user.
- Authorized cloud users then are granted access credentials (i.e., decryption keys) corresponding to their attribute sets (e.g., student role, faculty member role, or visitor role), which can be used to obtain access to the outsourced data.
- As a robust one-to-many encryption mechanism, CP-ABE offers a reliable method to protect data stored in cloud, but also enables fine-grained access control over the data.

DISADVANTAGES OF EXISTING SYSTEM:

- The leakage of any sensitive student information stored in cloud could result in a range of consequences for the organization and individuals (e.g., litigation, loss of competitive advantage, and criminal charges).
- The existing CP-ABE based cloud storage systems fail to consider the case where access credential is misused.

PROPOSED SYSTEM:

- Seeking to mitigate access credential misuse, we propose CryptCloud+, an accountable authority and revocable CPABE based cloud storage system with white-box traceability and auditing.
- Specifically, in our work, we first present a CP-ABE based cloud storage framework. Using this (generic) framework, we propose two accountable authority and revocable CP-ABE systems (with whitebox traceability and auditing) that are fully secure in the standard model, referred to as ATER-CP-ABE and ATIR-CPABE, respectively. Based on the two systems, we present the construction of CryptCloud+
- Access credentials for individual traced and further determined to be “compromised” can be revoked.

ADVANTAGES OF PROPOSED SYSTEM:

- To the best of our knowledge, this is the first practical solution to secure fine-grained access control over encrypted data in cloud.
- Users who leak their access credentials can be traced and identified.
- A semi-trusted authority, who (without proper authorization) generates and further distributes access credentials to unauthorized user(s), can be identified.

This allows further actions to be undertaken (e.g. criminal investigation or civil litigation for damages and breach of contract).

- ❖ An auditor can determine if a (suspected) cloud user is guilty in leaking his/her access credential.

MODULES DESCSRIPTION:

Data Owner:

In the first module, we develop the Data Owner Module. In this module, data owner has the option of File Upload, File View, Trace Request and Trace Results. This module helps the owner to register those details and also include login details. This module helps the owner to upload his file with encryption algorithm. This ensures the files to be protected from unauthorized user. Data owner has a collection of documentsthat he wants to outsource to the cloud server in encrypted form while still keeping the capability to search on them for effective utilization. Data Owners (DOs) encrypt their data under therelevant access policies prior to outsourcing the (encrypted)data to a public cloud (PC).PC stores the outsourced (encrypted) data from Dosand handles data access requests from data users(DUs)

Data User:

This module includes the user registration login details.This module is used to help the client to search the file using the multiple key words concept and get the accurate result list based on the user query. The user is going to select the required file and register the user details and get activation code in mail email before enter the activation code. After user can download the Zip file and extract that file.Data users are authorized ones to access the documentsof data owner. With *t* query keywords, theauthorized user can generate a trapdoor *TD* accordingto search control mechanisms to fetch *k* encrypted documentsfrom cloud server. Then, the data user can decryptthe documents with the shared secret key.Authorized DUs are able to access (e.g. downloadand decrypt) the outsourced data.

Semi-trusted authority:

Semi-trusted authority (STA)generates system parametersand issues access credentials (i.e., decryptionkeys) to DUs.

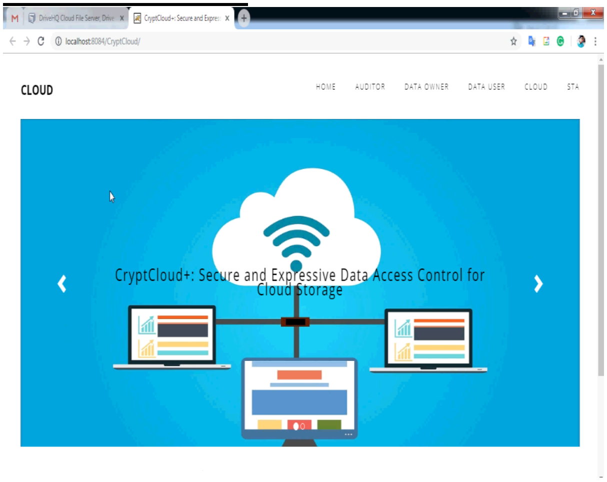
Auditor:

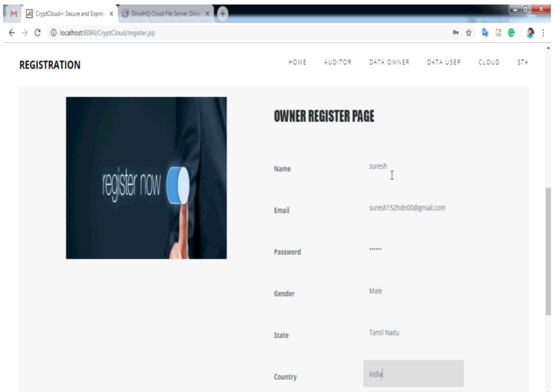
Auditor (AU) is trusted by other entities, takescharge of audit and revoke procedures, and retursthe trace and audit results to DOs and DUs. In this module, auditor has the options of File details, User Request & Trace Request details.

Cloud Server and Encryption Module:

This module is used to help the server to encrypt the document using RSA Algorithm and to convert the encrypted document to the Zip file with activation code and then activation code send to the user for download.Cloud serverstores the encrypted document collectionfor dataowner. Upon receiving the trapdoor *TD* from the datauser, the cloud server executes search, and finally returns the corresponding collection of top-*k* ranked encrypted documents. Besides, upon receivingthe update information from the data owner, the serverneeds to update and document collection *C*according to the received information.The cloud server in the proposed scheme is consideredas "honest-but-curious", which is employed by lots ofworks on secure cloud data search

SCREEN SHOTS


DriveHQ Cloud File Server, Drive
CryptCloud+: Secure and Expres
localhost:8084/CryptCloud/
CLOUD
HOME
AUDITOR
DATA OWNER
DATA USER
CLOUD
STA
CryptCloud+: Secure and Expressive Data Access Control for Cloud Storage



localhost:8084/CryptCloud/register.jsp

REGISTRATION

OWNER REGISTER PAGE

Name: suresh

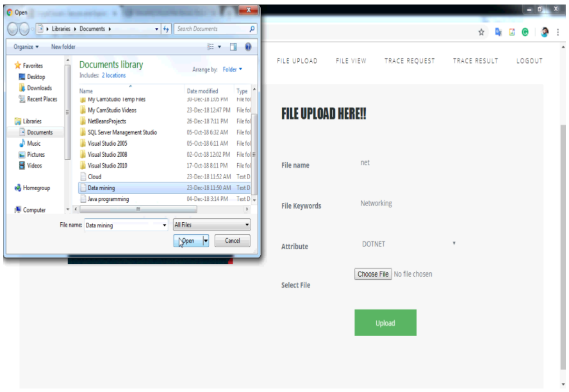
Email: suresh152hdn00@gmail.com

Password: ......

Gender: Male

State: Tamil Nadu

Country: India



Organize ▾ New folder

Libraries ▸ Documents ▸

Documents library
Includes: 2 locations

Name	Date modified	Type
My CamStudio Temp Files	30-Dec-18 1:05 PM	File fol
My CamStudio Videos	23-Dec-18 12:47 PM	File fol
NetBeansProjects	26-Dec-18 7:11 PM	File fol
SQL Server Management Studio	05-Oct-18 6:32 AM	File fol
Visual Studio 2005	05-Oct-18 6:11 AM	File fol
Visual Studio 2008	02-Oct-18 12:02 PM	File fol
Visual Studio 2010	17-Oct-18 8:11 PM	File fol
Cloud	23-Dec-18 11:52 AM	Text D
Data mining	23-Dec-18 11:50 AM	Text D
Java programming	04-Dec-18 3:14 PM	Text D

File name: Data mining — All Files

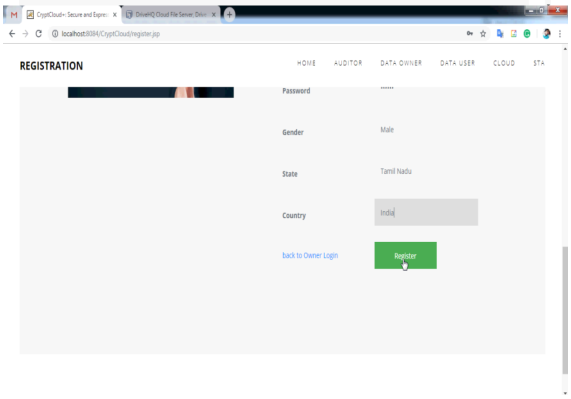
FILE UPLOAD HERE!!

File name: net

File Keywords: Networking

Attribute: DOTNET

Select File: Choose File No file chosen



localhost:8084/CryptCloud/register.jsp

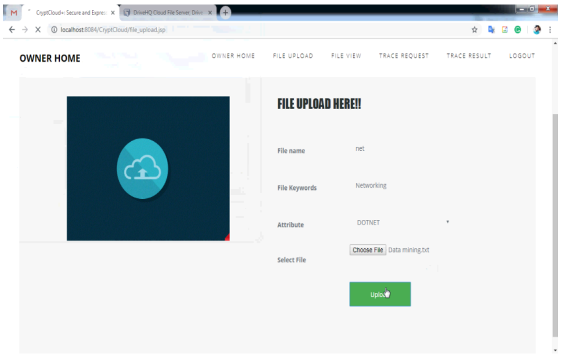
REGISTRATION

Password: ......

Gender: Male

State: Tamil Nadu

Country: India



localhost:8084/CryptCloud/file_upload.jsp

OWNER HOME

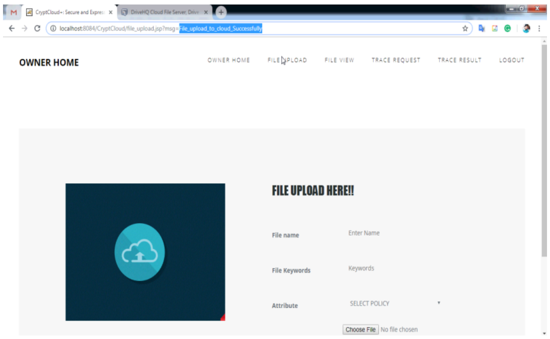
FILE UPLOAD HERE!!

File name: net

File Keywords: Networking

Attribute: DOTNET

Select File: Choose File Data mining.txt



localhost:8084/CryptCloud/file_upload.jsp?msg=file_upload_to_cloud_Successfully

OWNER HOME

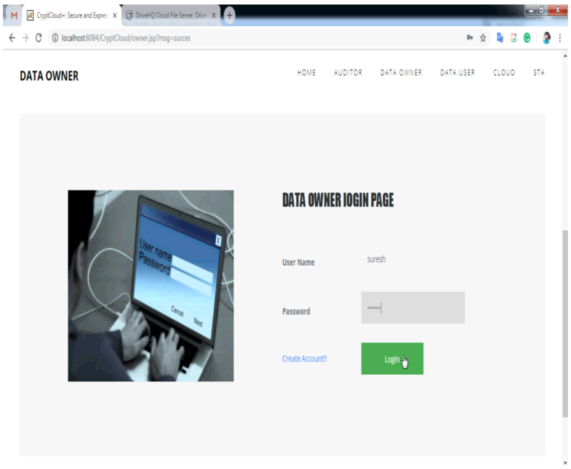
FILE UPLOAD HERE!!

File name: Enter Name

File Keywords: Keywords

Attribute: SELECT POLICY

Choose File No file chosen



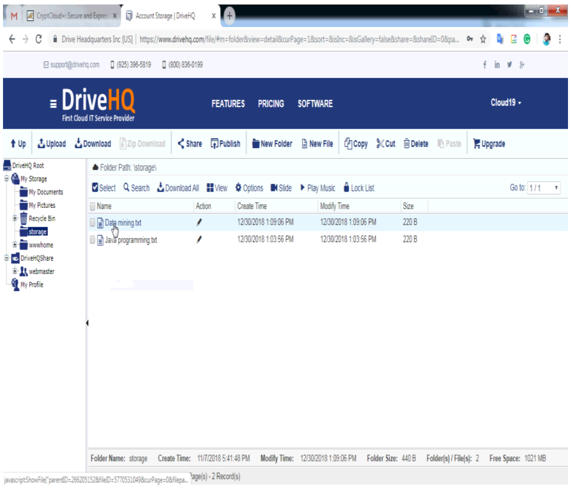
localhost:8084/CryptCloud/owner.jsp?msg=succes

DATA OWNER

DATA OWNER lOGIN PAGE

User Name: suresh

Password: .....



Drive Headquarters Inc [US] | https://www.drivehq.com/file/#m=folder&view=detail&curPage=1&sort=&isInc=&isGallery=false&share=&shareID=0&pa...

support@drivehq.com (925) 396-5819 (800) 836-0199

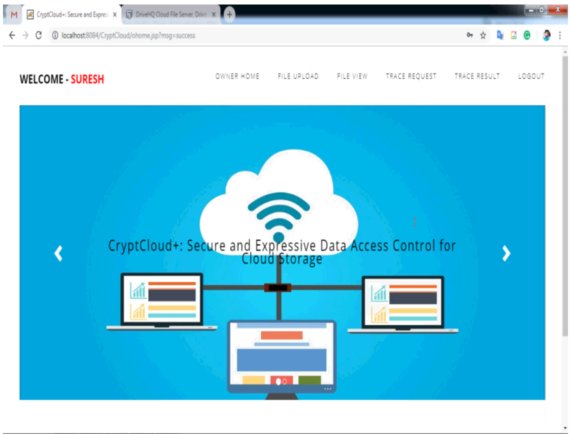
Folder Path: \storage\

Name	Action	Create Time	Modify Time	Size
Data mining.txt		12/30/2018 1:09:06 PM	12/30/2018 1:09:06 PM	220 B
Java programming.txt		12/30/2018 1:03:56 PM	12/30/2018 1:03:56 PM	220 B

Folder Name: storage Create Time: 11/7/2018 5:41:48 PM Modify Time: 12/30/2018 1:09:06 PM Folder Size: 440 B Folder(s) / File(s): 2 Free Space: 1021 MB

Page(s) - 2 Record(s)

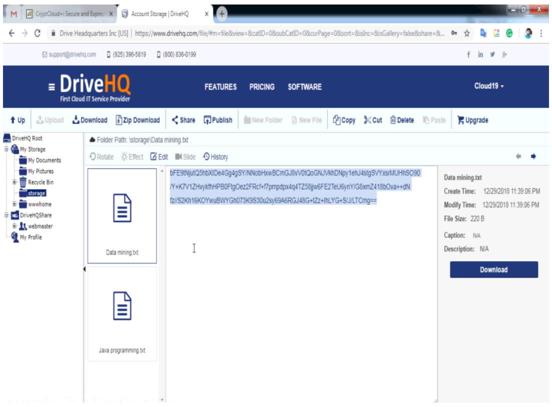
javascript:ShowFile("parentID=266205152&fileID=5770531049&curPage=0&filepa...



localhost:8084/CryptCloud/ohome.jsp?msg=success

WELCOME - SURESH

CryptCloud+: Secure and Expressive Data Access Control for Cloud Storage



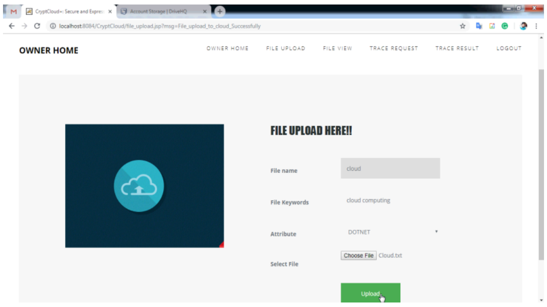
Drive Headquarters Inc [US] | https://www.drivehq.com/file/#m=file&view=&catID=0&subCatID=0&curPage=0&sort=&isInc=&isGallery=false&share=&...

support@drivehq.com (925) 396-5819 (800) 836-0199

Folder Path: \storage\Data mining.txt

bFE9tNjutQ5hbXIDe4Gg4gSY/NNobHxwBCmGJ8vV0tQoGNJVkhDNpy1ehJ4stgSVYxsrMUHhSO90
/Y+K7V1ZHvykfhHPB0FtgOez2FRcf+f7pmpdpx4q4TZ58jjw6FE2TeU6ynY/G8xmZ418bOva++dN
fz//S2Kh16KOYwuBWYGh073K9S30u2sy69A6RGJ48G+tZz+lhLYG+S/J/LTCmg==

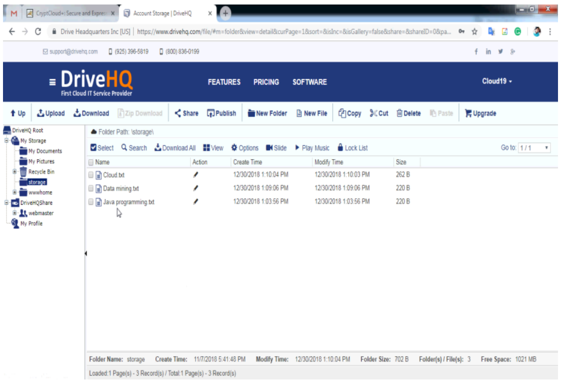
Data mining.txt
Create Time: 12/29/2018 11:39:06 PM
Modify Time: 12/29/2018 11:39:06 PM
File Size: 220 B
Caption: N/A
Description: N/A



localhost:8084/CryptCloud/file_upload.jsp?msg=File_upload_to_cloud_Successfully

FILE UPLOAD HERE!!

File name: cloud
File Keywords: cloud computing
Attribute: DOTNET
Select File: Cloud.txt



Drive Headquarters Inc [US] | https://www.drivehq.com/file/#m=folder&view=detail&curPage=1&sort=&isInc=&isGallery=false&share=&shareID=0&pa...

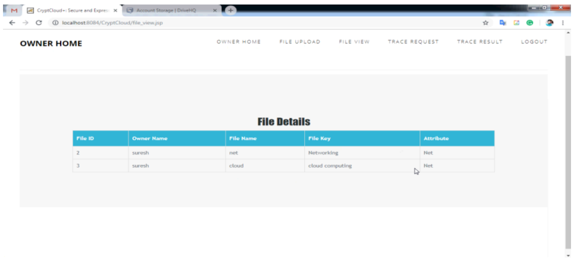
support@drivehq.com (925) 396-5819 (800) 836-0199

Folder Path: \storage\

Name	Action	Create Time	Modify Time	Size
Cloud.txt		12/30/2018 1:10:04 PM	12/30/2018 1:10:03 PM	262 B
Data mining.txt		12/30/2018 1:09:06 PM	12/30/2018 1:09:06 PM	220 B
Java programming.txt		12/30/2018 1:03:56 PM	12/30/2018 1:03:56 PM	220 B

Folder Name: storage Create Time: 11/7/2018 5:41:48 PM Modify Time: 12/30/2018 1:10:04 PM Folder Size: 702 B Folder(s) / File(s): 3 Free Space: 1021 MB

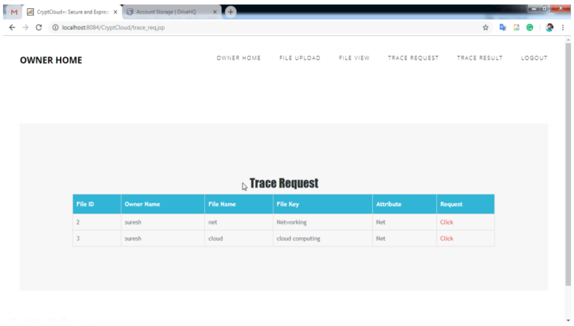
Loaded:1 Page(s) - 3 Record(s) / Total:1 Page(s) - 3 Record(s)



localhost:8084/CryptCloud/file_view.jsp

File Details

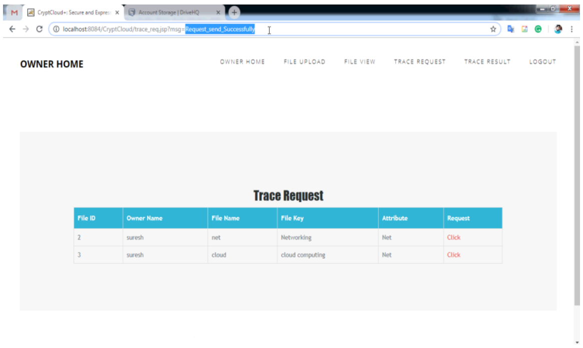
File ID	Owner Name	File Name	File Key	Attribute
2	suresh	net	Networking	Net
3	suresh	cloud	cloud computing	Net



localhost:8084/CryptCloud/trace_req.jsp

Trace Request

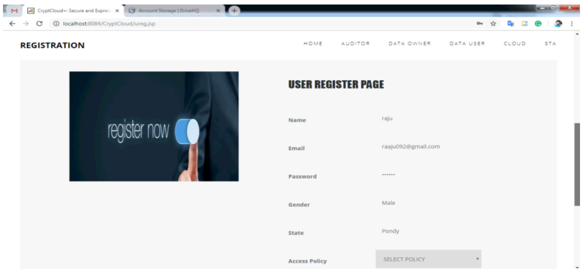
File ID	Owner Name	File Name	File Key	Attribute	Request
2	suresh	net	Networking	Net	Click
3	suresh	cloud	cloud computing	Net	Click



localhost:8084/CryptCloud/trace_req.jsp?msg=Request_send_Successfully

Trace Request

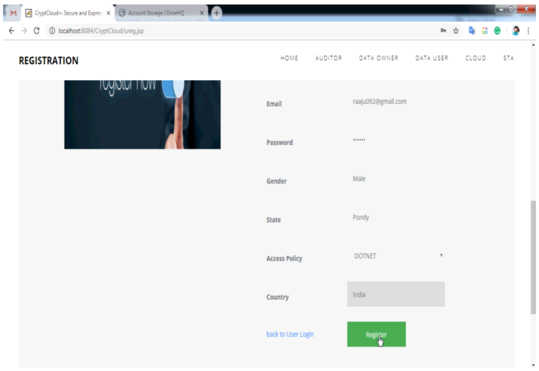
File ID	Owner Name	File Name	File Key	Attribute	Request
2	suresh	net	Networking	Net	Click
3	suresh	cloud	cloud computing	Net	Click



localhost:8084/CryptCloud/ureg.jsp

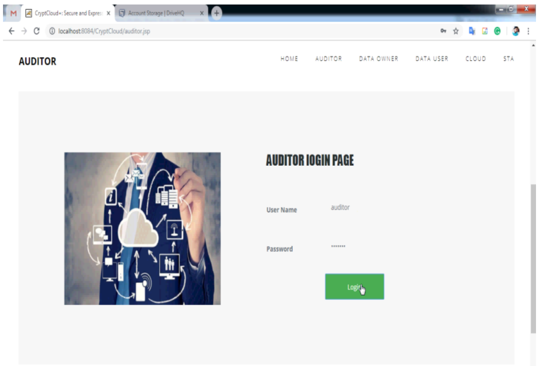
USER REGISTER PAGE

Name: raju
Email: raaju092@gmail.com
Password: ••••••
Gender: Male
State: Pondy
Access Policy: SELECT POLICY



localhost:8084/CryptCloud/ureg.jsp

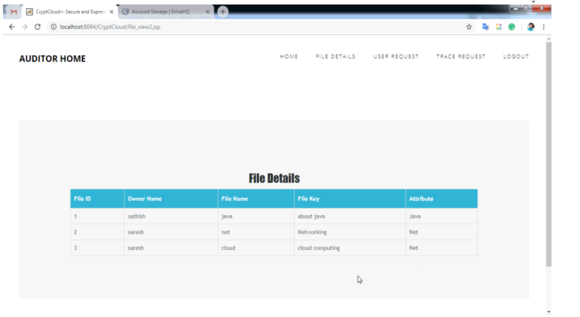
Email: raaju092@gmail.com
Password: ••••••
Gender: Male
State: Pondy
Access Policy: DOTNET
Country: India



localhost:8084/CryptCloud/auditor.jsp

AUDITOR lOGIN PAGE

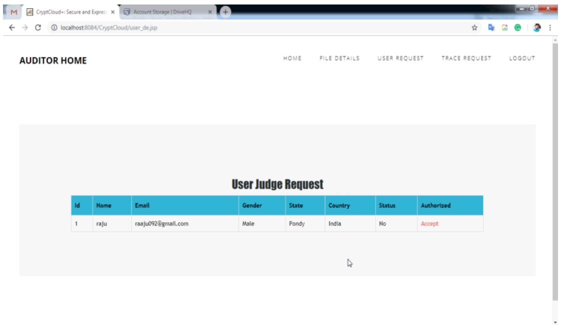
User Name: auditor
Password: •••••••



localhost:8084/CryptCloud/file_view2.jsp

File Details

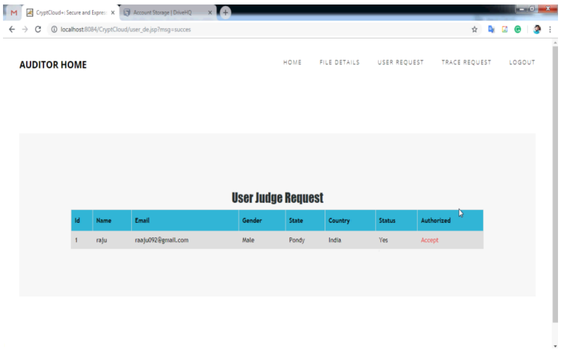
File ID	Owner Name	File Name	File Key	Attribute
1	sathish	java	about java	Java
2	suresh	net	Networking	Net
3	suresh	cloud	cloud computing	Net


localhost:8084/CryptCloud/user_de.jsp

AUDITOR HOME

User Judge Request

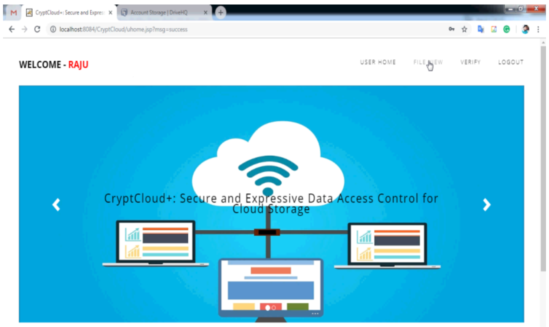
Id	Name	Email	Gender	State	Country	Status	Authorized
1	raju	raaju092@gmail.com	Male	Pondy	India	No	Accept


localhost:8084/CryptCloud/user_de.jsp?msg=succes

AUDITOR HOME

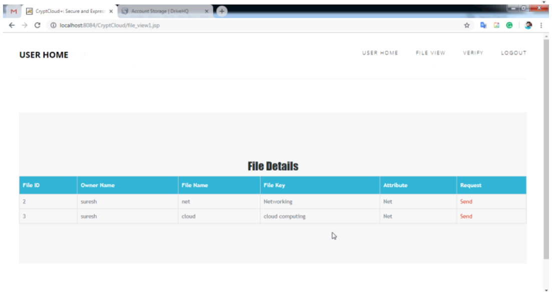
User Judge Request

Id	Name	Email	Gender	State	Country	Status	Authorized
1	raju	raaju092@gmail.com	Male	Pondy	India	Yes	Accept


localhost:8084/CryptCloud/uhome.jsp?msg=success

WELCOME - RAJU

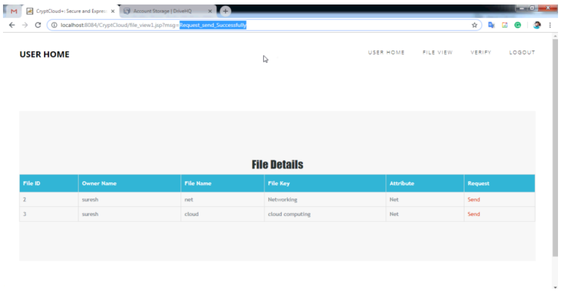
USER HOME
FILE VIEW
VERIFY
LOGOUT
CryptCloud+: Secure and Expressive Data Access Control for Cloud Storage


localhost:8084/CryptCloud/file_view1.jsp

USER HOME

File Details

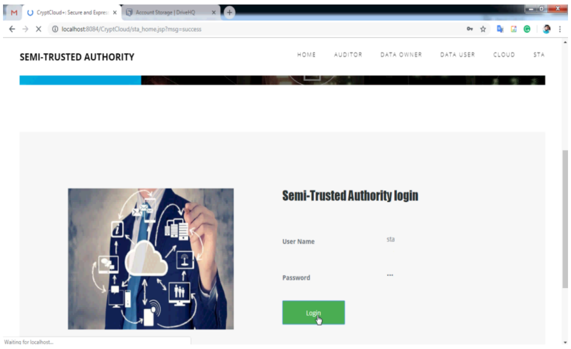
File ID	Owner Name	File Name	File Key	Attribute	Request
2	suresh	net	Networking	Net	Send
3	suresh	cloud	cloud computing	Net	Send


localhost:8084/CryptCloud/file_view1.jsp?msg=Request_send_Successfully

USER HOME

File Details

File ID	Owner Name	File Name	File Key	Attribute	Request
2	suresh	net	Networking	Net	Send
3	suresh	cloud	cloud computing	Net	Send

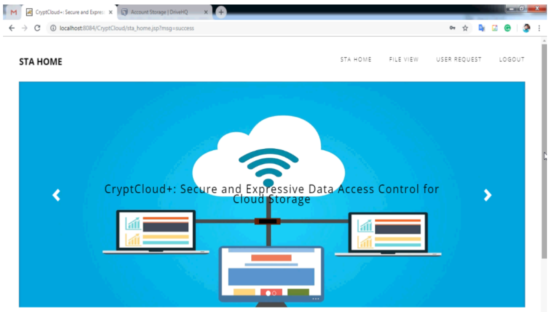

localhost:8084/CryptCloud/sta_home.jsp?msg=success

SEMI-TRUSTED AUTHORITY

Semi-Trusted Authority login

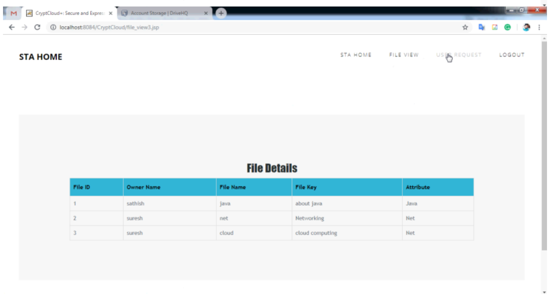
User Name: sta

Password: ***


localhost:8084/CryptCloud/sta_home.jsp?msg=success

STA HOME

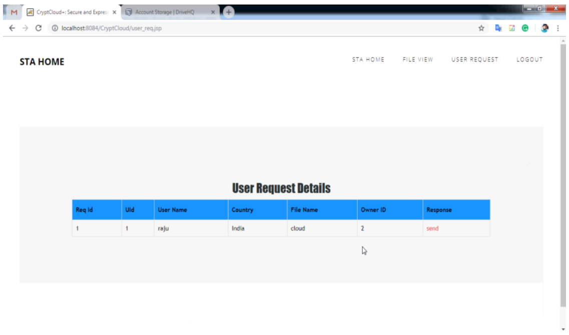
STA HOME
FILE VIEW
USER REQUEST
LOGOUT
CryptCloud+: Secure and Expressive Data Access Control for Cloud Storage


localhost:8084/CryptCloud/file_view3.jsp

STA HOME

File Details

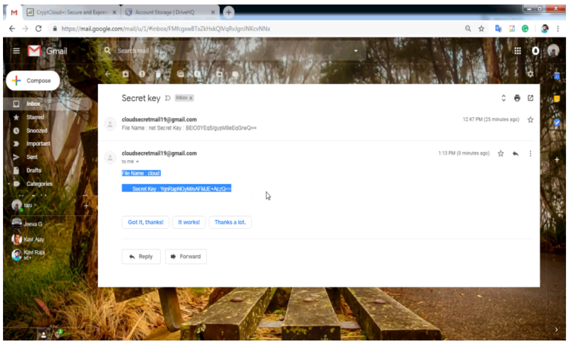
File ID	Owner Name	File Name	File Key	Attribute
1	sathish	java	about java	Java
2	suresh	net	Networking	Net
3	suresh	cloud	cloud computing	Net


localhost:8084/CryptCloud/user_req.jsp

STA HOME

User Request Details

Req Id	UId	User Name	Country	File Name	Owner ID	Response
1	1	raju	India	cloud	2	send


https://mail.google.com/mail/u/1/#inbox/FMfcgxwBTsZkHxkQlVqRvJgnJNKcvNNx

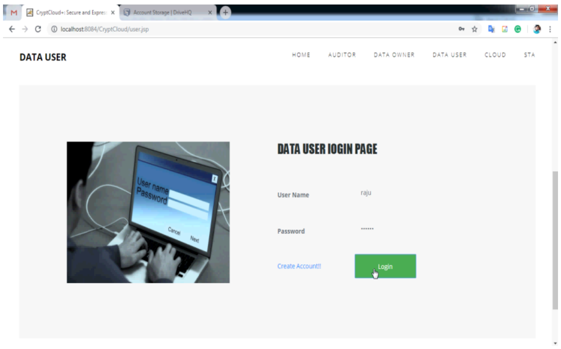
Secret key Inbox

cloudsecretmail19@gmail.com 12:47 PM (25 minutes ago)
File Name : net Secret Key : BEIO0YEqS/gypM8eEqGrwQ==

cloudsecretmail19@gmail.com 1:13 PM (0 minutes ago)
to me

File Name : cloud

Secret Key : YgnRapNGyM/eAFMJE+AczQ==

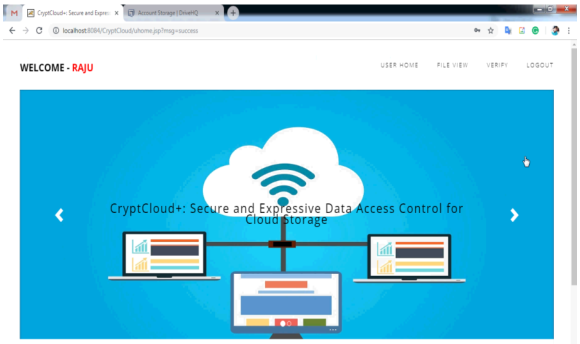

localhost:8084/CryptCloud/user.jsp

DATA USER

DATA USER IOGIN PAGE

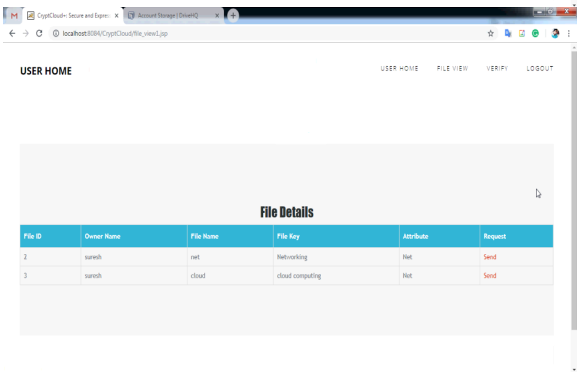
User Name: raju

Password: ••••••


localhost:8084/CryptCloud/uhome.jsp?msg=success

WELCOME - RAJU

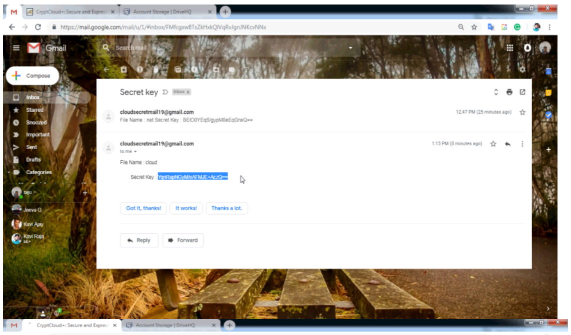
CryptCloud+: Secure and Expressive Data Access Control for Cloud Storage


localhost:8084/CryptCloud/file_view1.jsp

USER HOME

File Details

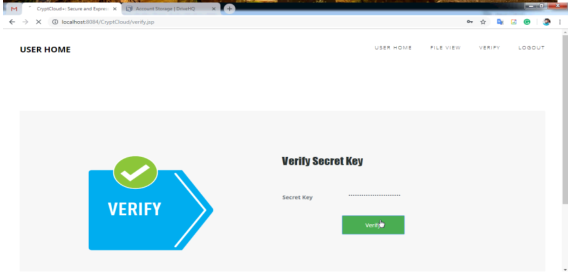
File ID	Owner Name	File Name	File Key	Attribute	Request
2	suresh	net	Networking	Net	Send
3	suresh	cloud	cloud computing	Net	Send


https://mail.google.com/mail/u/1/#inbox/FMfcgxwBTsZkHxkQlVqRvJgnJNKcvNNx

Secret key

cloudsecretmail19@gmail.com — 12:47 PM (25 minutes ago)
File Name : net Secret Key : BEIO0YEqS/gypM8eEqGrwQ==

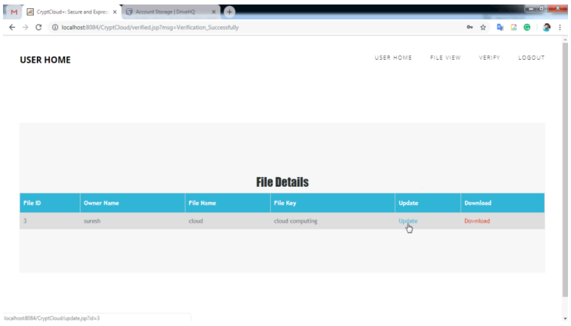
cloudsecretmail19@gmail.com — 1:13 PM (0 minutes ago)
to me
File Name : cloud
Secret Key : YqnRapNGyMeAFMJE+AczQ==


localhost:8084/CryptCloud/verify.jsp

USER HOME

Verify Secret Key

Secret Key: ••••••••••••••••••••••••

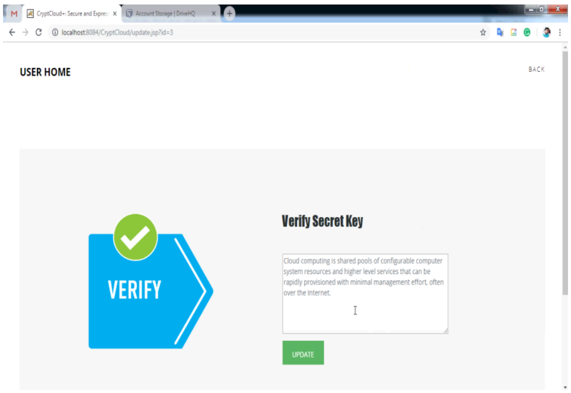

localhost:8084/CryptCloud/verified.jsp?msg=Verification_Successfully

USER HOME

File Details

File ID	Owner Name	File Name	File Key	Update	Download
3	suresh	cloud	cloud computing	Update	Download

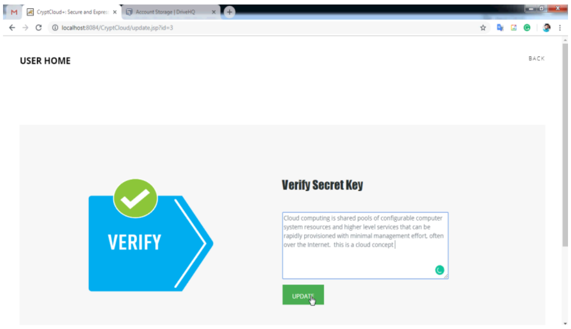
localhost:8084/CryptCloud/update.jsp?id=3


localhost:8084/CryptCloud/update.jsp?id=3

USER HOME

Verify Secret Key

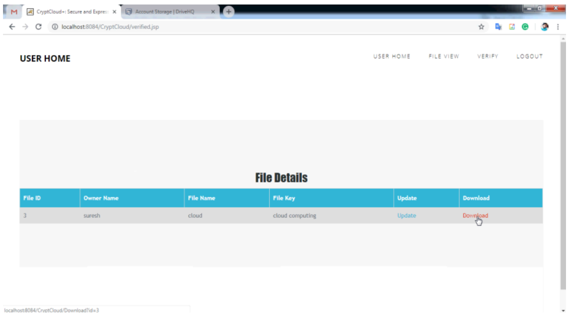
Cloud computing is shared pools of configurable computer system resources and higher level services that can be rapidly provisioned with minimal management effort, often over the Internet.


localhost:8084/CryptCloud/update.jsp?id=3

USER HOME

Verify Secret Key

Cloud computing is shared pools of configurable computer system resources and higher level services that can be rapidly provisioned with minimal management effort, often over the Internet. this is a cloud concept

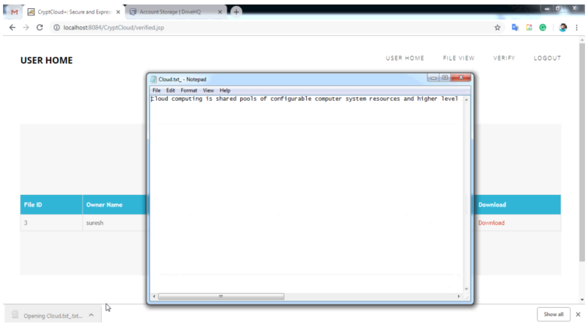

localhost:8084/CryptCloud/verified.jsp

USER HOME

File Details

File ID	Owner Name	File Name	File Key	Update	Download
3	suresh	cloud	cloud computing	Update	Download

localhost:8084/CryptCloud/Download?id=3


localhost:8084/CryptCloud/verified.jsp

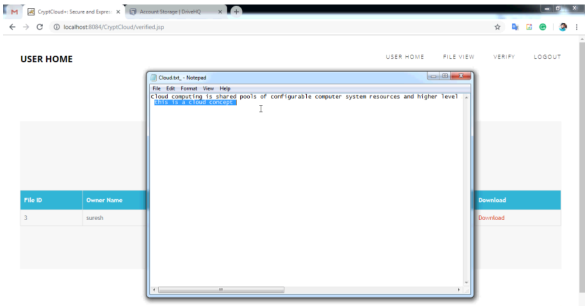
USER HOME

Cloud.txt_ - Notepad

```
Cloud computing is shared pools of configurable computer system resources and higher level
```

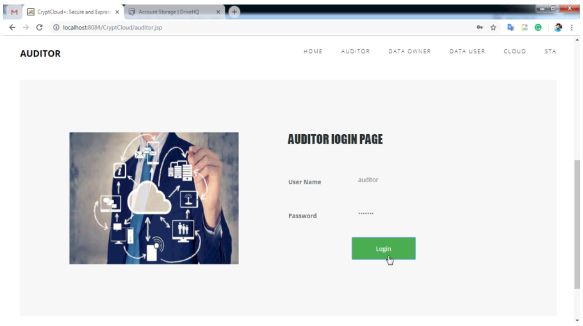
File ID	Owner Name	Download
3	suresh	Download

Opening Cloud.txt_.txt...


CryptCloud+: Secure and Expres:
Account Storage | DriveHQ
localhost:8084/CryptCloud/verified.jsp
USER HOME
USER HOME
FILE VIEW
VERIFY
LOGOUT
Cloud.txt_ - Notepad
File
Edit
Format
View
Help

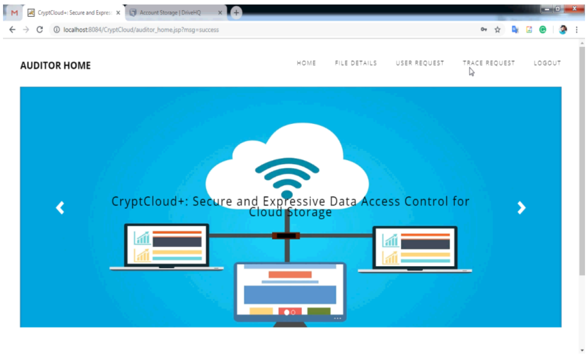
```
Cloud computing is shared pools of configurable computer system resources and higher level
 this is a cloud concept
```

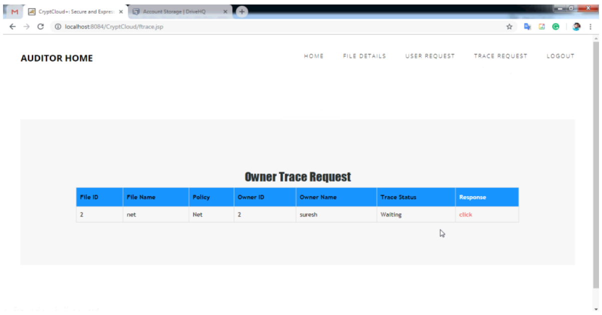
File ID	Owner Name	Download
3	suresh	Download


CryptCloud+: Secure and Expres:
Account Storage | DriveHQ
localhost:8084/CryptCloud/auditor.jsp
AUDITOR
HOME
AUDITOR
DATA OWNER
DATA USER
CLOUD
STA
AUDITOR IOGIN PAGE
Login

User Name auditor

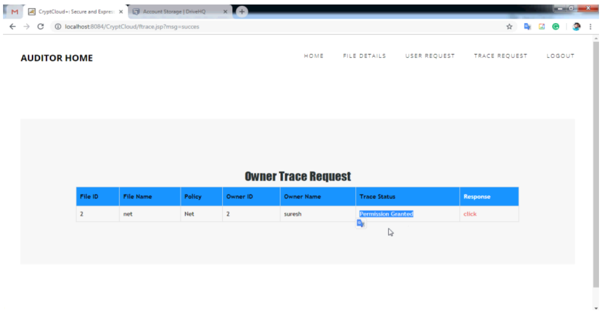
Password •••••••


CryptCloud+: Secure and Expres:
Account Storage | DriveHQ
localhost:8084/CryptCloud/auditor_home.jsp?msg=success
AUDITOR HOME
HOME
FILE DETAILS
USER REQUEST
TRACE REQUEST
LOGOUT
CryptCloud+: Secure and Expressive Data Access Control for Cloud Storage


CryptCloud+: Secure and Expres:
Account Storage | DriveHQ
localhost:8084/CryptCloud/ftrace.jsp
AUDITOR HOME
HOME
FILE DETAILS
USER REQUEST
TRACE REQUEST
LOGOUT

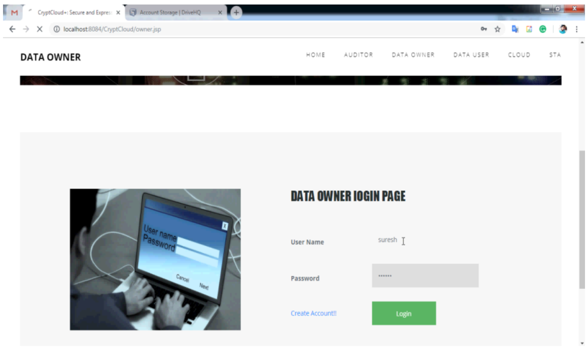
Owner Trace Request

File ID	File Name	Policy	Owner ID	Owner Name	Trace Status	Response
2	net	Net	2	suresh	Waiting	click


CryptCloud+: Secure and Expres:
Account Storage | DriveHQ
localhost:8084/CryptCloud/ftrace.jsp?msg=succes
AUDITOR HOME
HOME
FILE DETAILS
USER REQUEST
TRACE REQUEST
LOGOUT

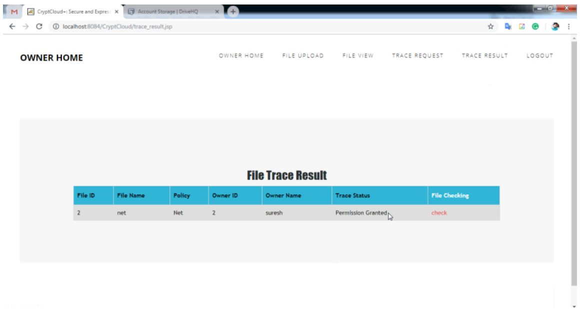
Owner Trace Request

File ID	File Name	Policy	Owner ID	Owner Name	Trace Status	Response
2	net	Net	2	suresh	Permission Granted	click



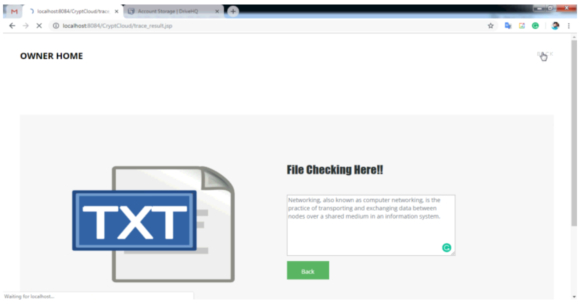
User Name suresh

Password ••••••

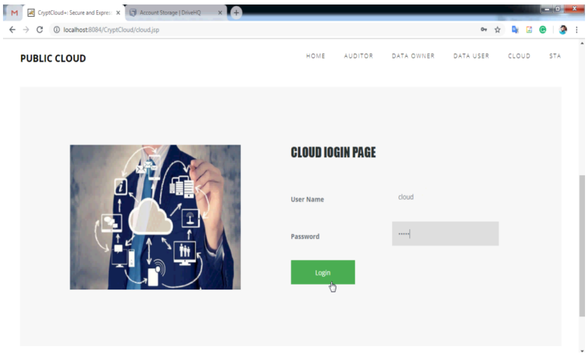

CryptCloud+: Secure and Expres:
Account Storage | DriveHQ
localhost:8084/CryptCloud/trace_result.jsp
OWNER HOME
OWNER HOME
FILE UPLOAD
FILE VIEW
TRACE REQUEST
TRACE RESULT
LOGOUT

File Trace Result

File ID	File Name	Policy	Owner ID	Owner Name	Trace Status	File Checking
2	net	Net	2	suresh	Permission Granted	check

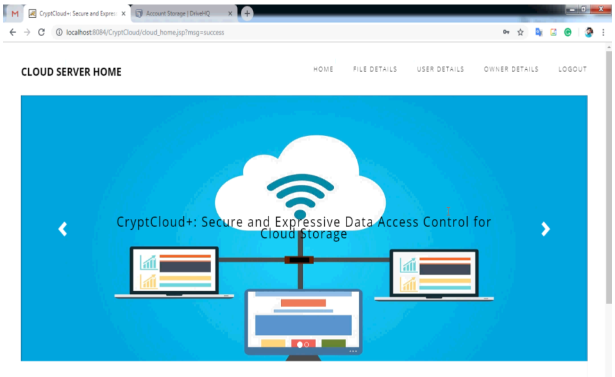

localhost:8084/CryptCloud/trace
Account Storage | DriveHQ
localhost:8084/CryptCloud/trace_result.jsp
OWNER HOME
TXT
File Checking Here!!
Back
Waiting for localhost...

Networking, also known as computer networking, is the practice of transporting and exchanging data between nodes over a shared medium in an information system.


CryptCloud+: Secure and Expres:
Account Storage | DriveHQ
localhost:8084/CryptCloud/cloud.jsp
PUBLIC CLOUD
HOME
AUDITOR
DATA OWNER
DATA USER
CLOUD
STA
CLOUD IOGIN PAGE
Login

User Name cloud

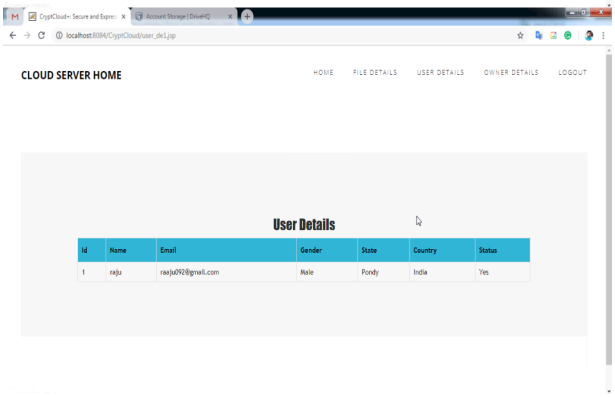
Password •••••



localhost:8084/CryptCloud/cloud_home.jsp?msg=success

CLOUD SERVER HOME

CryptCloud+: Secure and Expressive Data Access Control for Cloud Storage



localhost:8084/CryptCloud/user_de1.jsp

CLOUD SERVER HOME

User Details

Id	Name	Email	Gender	State	Country	Status
1	raju	raaju092@gmail.com	Male	Pondy	India	Yes

Conclusion:

In this work, we have tended to the test of credential leakage in CP-ABE based cloud storage framework by designing an responsible position and revocable Crypt Cloud which supports white-box discernibility and examining (alluded to asCryptCloud+). This is the main CP-ABE based cloud storage system that all the while underpins white-box traceability, accountable power, evaluating and viable revocation. Specifically, CryptCloud+ permits us to follow and revoke malicious cloud clients (spilling qualifications). Our approachcan be likewise utilized for the situation where the clients' accreditations areredistributed by the semi-confided in power.

We note that we may require discovery delectability, which is a more grounded thought (contrasted with white-box traceability),in Crypt Cloud. One of our future works is to consider theblack-box discernibility and auditing.Furthermore, AU is thought to be completely confided in inCryptCloud+. Notwithstanding, practically speaking, it may not be the case.Is there any approach to lessen trust from AU? Intuitively,one strategy is to utilize different AUs. This is similarto the procedure utilized in edge plans. Be that as it may, it willrequire extra correspondence and organization cost andmeanwhile, the issue of agreement among AUs remains.Another potential methodology is to utilize secure multi-partycomputation within the sight of noxious enemies. However,the productivity is likewise a bottleneck. Planning efficientmulti-party calculation and decentralizing trust amongAUs (while keeping up a similar degree of security andefficiency) is additionally a piece of our future work.We use Paillier-like encryption to fill in as an extractable commitment to accomplish white-box recognizability. From anabstract see point, any extractable responsibility may be employed to accomplish white-confine recognizability hypothesis. To improvethe effectiveness of following, we may utilize a morelight-weight (matching reasonable) extractable responsibility.

Likewise, the follow calculation in Crypt Cloud+ needs to takethe ace mystery key as contribution to accomplish white-box traceability of noxious cloud clients. Naturally, the proposed Crypt Cloud+ is private traceable5. Private detestability only allows the following calculation to be controlled by the framework administrator itself, while halfway/full open recognizability enables the head, approved clients and even anyonewithout the mystery data of the framework to satisfy thetrace. Our future work will incorporate expanding CryptCloud+to give "halfway" and completely open discernibility withoutcompromising on execution..

REFERENCES

REFERENCES

[1] Mazhar Ali, RevathiDhamotharan, Eraj Khan, Samee U. Khan,Athanasios V. Vasilakos, Keqin Li, and Albert Y.

Zomaya. Sedasc:Secure data sharing in clouds. IEEE Systems Journal, 11(2):395–404,2017.

[2] Mazhar Ali, Samee U. Khan, and Athanasios V. Vasilakos. Securityin cloud computing: Opportunities and challenges. Inf. Sci.,305:357–383, 2015.

[3] Michael Armbrust, Armando Fox, Rean Griffith, Anthony DJoseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson,Ariel Rabkin, Ion Stoica, et al. A view of cloud computing.Communications of the ACM, 53(4):50–58, 2010.

[4] NuttapongAttrapadung and Hideki Imai.Attribute-based encryptionsupporting direct/indirect revocation modes. In Cryptographyand Coding, pages 278–300. Springer, 2009.

[5] Amos Beimel. Secure schemes for secret sharing and key distribution.PhD thesis, PhD thesis, Israel Institute of Technology, Technion,Haifa, Israel, 1996.

[6] MihirBellare and OdedGoldreich.On defining proofs of knowledge.In Advances in Cryptology-CRYPTO’92, pages 390–420.Springer, 1993.

[7] Dan Boneh and Xavier Boyen.Short signatures without randomoracles. In EUROCRYPT - 2004, pages 56–73, 2004.

[8] HongmingCai, BoyiXu, Lihong Jiang, and Athanasios V. Vasilakos.Iot-based big data storage systems in cloud computing:Perspectives and challenges. IEEE Internet of Things Journal,4(1):75–87, 2017.

[9] Jie Chen, Romain Gay, and Hoeteck Wee.Improved dual systemABE in prime-order groups via predicate encodings. In Advancesin Cryptology - EUROCRYPT 2015, pages 595–624, 2015.

[10] Angelo De Caro and Vincenzo Iovino.jpbc: Java pairing basedcryptography. In ISCC 2011, pages 850–855. IEEE, 2011.

[11] Hua Deng, Qianhong Wu, Bo Qin, Jian Mao, Xiao Liu, Lei Zhang,and Wenchang Shi. Who is touching my cloud. In ComputerSecurity-ESORICS 2014, pages 362–379. Springer, 2014.

[12] Zhangjie Fu, Fengxiao Huang, Xingming Sun, AthanasiosVasilakos,and Ching-Nung Yang. Enabling semantic search basedon conceptual graphs over encrypted outsourced data. IEEETransactions on Services Computing, 2016.

[13] VipulGoyal. Reducing trust in the PKG in identity based cryptosystems.In Advances in Cryptology-CRYPTO 2007, pages 430–447.Springer, 2007.

[14] VipulGoyal, Steve Lu, AmitSahai, and Brent Waters. Black-boxaccountable authority identity-based encryption. In Proceedings ofthe 15th ACM conference on Computer and communications security,pages 427–436. ACM, 2008.

[15] VipulGoyal, OmkantPandey, AmitSahai, and Brent Waters.Attribute-based encryption for fine-grained access control of encrypteddata. In Proceedings of the 13th ACM conference on Computerand communications security, pages 89–98. ACM, 2006.

[16] Qi Jing, Athanasios V. Vasilakos, Jiafu Wan, Jingwei Lu, andDechaoQiu. Security of the internet of things: perspectives andchallenges. Wireless Networks, 20(8):2481–2501, 2014.

[17] Allison Lewko. Tools for simulating features of composite orderbilinear groups in the prime order setting. In Advances inCryptology–EUROCRYPT 2012, pages 318–335. Springer, 2012.

[18] Allison Lewko, Tatsuaki Okamoto, AmitSahai, KatsuyukiTakashima, and Brent Waters. Fully secure functional encryption:Attribute-based encryption

and (hierarchical) inner productencryption. In Advances in Cryptology–EUROCRYPT 2010, pages62–91. Springer, 2010.

[19] Allison Lewko and Brent Waters. New proof methods forattribute-based encryption: Achieving full security through selectivetechniques. In Advances in Cryptology–CRYPTO 2012, pages180–198. Springer, 2012.

[20] Jiguo Li, Xiaonan Lin, Yichen Zhang, and Jinguang Han. KSFOABE:outsourced attribute-based encryption with keywordsearch function for cloud storage. IEEE Trans. Services Computing,10(5):715–725, 2017.

[21] JiguoLi,Wei Yao, Yichen Zhang, HuilingQian, and Jinguang Han.Flexible and fine-grained attribute-based data storage in cloudcomputing. IEEE Trans. Services Computing, 10(5):785–796, 2017.

[22] Jin Li, Qiong Huang, Xiaofeng Chen, Sherman SM Chow, DuncanS Wong, and DongqingXie. Multi-authority ciphertext-policyattribute-based encryption with accountability. In Proceedings of the6th ACM Symposium on Information, Computer and CommunicationsSecurity, ASIACCS 2011, pages 386–390. ACM, 2011.

[23] Jin Li, KuiRen, and Kwangjo Kim. A2be: Accountableattributebasedencryption for abuse free access control. IACR CryptologyePrint Archive, 2009:118, 2009.

[24] Jiaqiang Liu, Yong Li, Huandong Wang, Depeng Jin, Li Su,LieguangZeng, and ThanosVasilakos. Leveraging softwaredefinednetworking for security policy enforcement. Inf. Sci.,327:288–299, 2016.

[25] Qiang Liu, Hao Zhang, JiafuWan, and Xin Chen. An access controlmodel for resource sharing based on the role-based access controlintended for multi-domain manufacturing internet of things. IEEEAccess, 5:7001–7011, 2017.

[26] Zhen Liu, Zhenfu Cao, and Duncan S Wong.Blackbox traceablecp-abe: how to catch people leaking their keys by selling decryptiondevices on ebay. In Proceedings of the 2013 ACM SIGSACconference on Computer & communications security, pages 475–486.ACM, 2013.

[27] Zhen Liu, Zhenfu Cao, and Duncan S Wong.White-box traceableciphertext-policy attribute-based encryption supporting anymonotone access structures. IEEE Transactions on InformationForensics and Security, 8(1):76–88, 2013.

[28] Ben Lynn et al. The pairing-based cryptography library. Internet:crypto. stanford. edu/pbc/[Mar. 27, 2013], 2006.

[29] Dalit Naor, MoniNaor, and Jeff Lotspiech.Revocation andtracing schemes for stateless receivers. In Advances in Cryptology -CRYPTO 2001, pages 41–62. Springer, 2001.

[30] JiantingNing, Zhenfu Cao, Xiaolei Dong, Junqing Gong, and JieChen. Traceable cp-abe with short ciphertexts: How to catchpeople selling decryption devices on ebay efficiently. In ComputerSecurity-ESORICS 2016, pages 551–569. Springer, 2016.

[31] JiantingNing, Zhenfu Cao, Xiaolei Dong, Kaitai Liang, Hui Ma,and LifeiWei. Auditable -time outsourced attribute-based encryptionfor access control in cloud computing. IEEE Transactions onInformation Forensics and Security, 13(1):94–105, 2018.

[32] JiantingNing, Zhenfu Cao, Xiaolei Dong, and Lifei Wei.Traceableand revocable CP-ABE with shorter ciphertexts. SCIENCE

CHINAInformation Sciences, 59(11):119102:1–119102:3, 2016.

[33] JiantingNing, Zhenfu Cao, Xiaolei Dong, and LifeiWei. White-boxtraceable cp-abe for cloud storage service: How to catch peopleleaking their access credentials effectively. IEEE Transactions onDependable and Secure Computing, 2016.

[34] JiantingNing, Zhenfu Cao, Xiaolei Dong, Lifei Wei, and XiaodongLin. Large universe ciphertext-policy attribute-based encryptionwith white-box traceability. In Computer Security-ESORICS 2014,pages 55–72. Springer, 2014.

[35] JiantingNing, Xiaolei Dong, Zhenfu Cao, and Lifei Wei.Accountableauthority ciphertext-policy attribute-based encryptionwith white-box traceability and public auditing in the cloud. InComputer Security–ESORICS 2015, pages 270–289. Springer, 2015.

[36] JiantingNing, Xiaolei Dong, Zhenfu Cao, Lifei Wei, and XiaodongLin. White-box traceable ciphertext-policy attribute-based encryptionsupporting flexible attributes. IEEE Transactions on InformationForensics and Security, 10(6):1274–1288, 2015.

[37] RafailOstrovsky, AmitSahai, and Brent Waters.Attribute-basedencryption with non-monotonic access structures. In Proceedingsof the 14th ACM conference on Computer and communications security,pages 195–203. ACM, 2007.

[38] Pascal Paillier. Public-key cryptosystems based on composite degreeresiduosity classes. In Advances in Cryptology – EUROCRYPT'99, pages 223–238, 1999.

[39] YannisRouselakis and Brent Waters.Practical constructions andnew proof methods for large universe attribute-based encryption.In Proceedings of the 2013 ACM SIGSAC conference on Computer &communications security, pages 463–474. ACM, 2013.

[40] AmitSahai, HakanSeyalioglu, and Brent Waters.Dynamic credentialsand ciphertext delegation for attribute-based encryption.In Advances in Cryptology–CRYPTO 2012, pages 199–217. Springer,2012.

[41] AmitSahai and Brent Waters.Fuzzy identity-based encryption.In Advances in Cryptology–EUROCRYPT 2005, pages 457–473.Springer, 2005.

[42] Brent Waters. Ciphertext-policy attribute-based encryption: Anexpressive, efficient, and provably secure realization. In Public KeyCryptography–PKC 2011, pages 53–70. Springer, 2011.

[43] Lifei Wei, Haojin Zhu, Zhenfu Cao, Xiaolei Dong, WeiweiJia,Yunlu Chen, and Athanasios V. Vasilakos. Security and privacyfor storage and computation in cloud computing. Inf. Sci., 258:371–386, 2014.

[44] Hu Xiong, Kim-Kwang Raymond Choo, and Athanasios V Vasilakos.Revocable identity-based access control for big data withverifiable outsourced computing.IEEE Transactions on Big Data,2017.

[45] BoyiXu, LidaXu, HongmingCai, Lihong Jiang, Yang Luo, andYizhiGu. The design of an m-health monitoring system based ona cloud computing platform. Enterprise IS, 11(1), 2017.

[46] FeiXu, Fangming Liu, Hai Jin, and Athanasios V. Vasilakos.Managing performance overhead of virtual machines in cloudcomputing: A survey, state of the art, and future directions.Proceedings of the IEEE, 102(1):11–31, 2014.

[47] Zheng Yan, Xueyun Li, Mingjun Wang, and Athanasios V. Vasilakos.Flexible data access control based on trust and reputationin cloud

computing. IEEE Trans. Cloud Computing, 5(3):485–498,2017.

48] Zheng Yan, Mingjun Wang, Yuxiang Li, and Athanasios V. Vasilakos.Encrypted data management with deduplication in cloudcomputing. IEEE Cloud Computing, 3(2):28–35, 2016.

[49] Kan Yang and XiaohuaJia. Expressive, efficient, and revocabledata access control for multi-authority cloud storage. IEEE transactionson parallel and distributed systems, 25(7):1735–1744, 2014.

[50] Kan Yang, Zhen Liu, XiaohuaJia, and Xuemin Sherman Shen.Time-domain attribute-based access control for cloud-based videocontent sharing: A cryptographic approach. IEEE Transactions onMultimedia, 18(5):940–950, 2016.

[51] Yanjiang Yang, Joseph K Liu, Kaitai Liang, Kim-Kwang RaymondChoo, and Jianying Zhou. Extended proxy-assisted approach:achieving revocable fine-grained encryption of cloud data. InComputer Security-ESORICS 2015, pages 146–166. Springer, Cham,2015.

[52] Shucheng Yu, Cong Wang, KuiRen, and Wenjing Lou. Attributebased data sharing with attribute revocation. In Proceedings of the5th ACM Symposium on Information, Computer and CommunicationsSecurity, pages 261–270. ACM, 2010.

[53] Yong Yu, Liang Xue, Man Ho Au, Willy Susilo, Jianbing Ni,Yafang Zhang, Athanasios V. Vasilakos, and JianShen. Cloud dataintegrity checking with an identity-based auditing mechanismfrom RSA. Future Generation Comp. Syst., 62:85–91, 2016.

[54] Jun Zhou, Zhenfu Cao, Xiaolei Dong, and Athanasios V. Vasilakos.Security and privacy for cloud-based iot: Challenges. IEEE CommunicationsMagazine, 55(1):26–33, 2017.

[55] Jun Zhou, Zhenfu Cao, Xiaolei Dong, NaixueXiong, and AthanasiosV. Vasilakos. 4s: A secure and privacy-preserving key managementscheme for cloud-assisted wireless body area network inm-healthcare social networks. Inf. Sci., 314:255–276, 2015.

[56] Jun Zhou, Xiaolei Dong, Zhenfu Cao, and Athanasios V. Vasilakos.Secure and privacy preserving protocol for cloud-based vehiculardtns. IEEE Trans. Information Forensics and Security, 10(6):1299–1314, 2015.

1.