OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

A SECURE PUBLIC CLOUD ENCRYPTED DATA WITH EFFECTIVE AND EFFICIENT KEYWORD BASED SEARCHING SCHEME

Mohd Abdul Mujeeb Zeeshan[1], Ashlesha K[2]

Research Scholar, Dept. of Computer Science & Engineering, LIET, Hyderabad[1]
Assistant Professor, Dept. of Computer Science & Engineering, LIET, Hyderabad[2]
AcademicStudent@gmail.com[1]
AcademicGuide101@gmail.com[2]

Abstract: **In the present-day cloud computing data service utilization of identical and entrepreneur enormous computational power and scalability over data storage facilities to encourage big data utility applications power domains like insurance, public Health Care, and Research and Development areas needs to focus on Security attributes. An electronic insurance record or sensitive personal health record or client-specific personal information needs to get safeguarded from another id third party uses of the public cloud which could be done by adopting data transformation schemes. In conventional systems, data retrieval of data stored in public clouds could be handled with the same formatted data. The keyword-based searching mechanism couldn't be effectively driven if the data uses don't follow the same formatted data that is been stored in the data store off the cloud. To the present circumstances wherein data needs to get encrypted and preserved in the data store of the database as well data users could be in a situation to search the data with the daily utility formats irrespective of the format stored in the data store. In this project, we recommend proposing a multiple keyword top-k searching mechanism to engage in encrypted data formats effectively and efficiently inter not violating the security policies.This index-based structural multi-keyword search can be effectively performed over encrypted data formats only when searching keywords and data storage format should come to oneness in the runtime without losing the security precautions taken over the data. In the proposed secure multi-keyword search mechanism with the tree-indexing facilitates a significant and effective system in such a way we can emphasize preventing the privacy breaches, data scalability, and time effectiveness in search query keyword processing could be achieved. To enhance the security policies we move ahead by modularizing the whole data into sub-parts and perform encryption then stored so that when data users attempt to retrieve the very same data could be done in a segment-based manner so that reliability and trust on the stored data happens.**

Keywords:- *Cloud computing, multi-keyword top-k search ,privacy preserving, random traversal, data encryption.*

-- ∴ ∴ ∴ --

INTRODUCTION

Cloud computing is having a massive demand to fulfil the present day necessities which is been incorporated with identical benefits like high flexibility and pay as you utilize manner, facilitating data users to invest in procuring computational resources as users services based on situation null Expectations so that the data uses don't worry about out misusing of computational facilities and typical hardware platform architectural facilities [2]. The present situation either identical or Enterprise collectively demands a huge quantity of big data applications through which data outsourcing is done effectively and service deployments could be monitored by cloud Service with effective and efficient data management policies as well as effective query processing is on demand. When we are dealing with user sensitive data we may need to carefully e and has the privacy policies so that the outsourced data is in the hands of reliable circumstances [5]. In general data owner pushes sensitive data like insurance record, personal health record the, commercial transactions into the public cloud servers with an expectation on reliability and trustability over their personal information without having a profound inside look into the proprietor Re security policies. But it is the duty of Cloud Service Provider or cloud servers who administrate the data users has to empower reliability by adopting typical encryption schemes over the sensitive data which is under sharable nature [1]. This sensitive Data Encryption policy should effectively work on the shareable data volumes in such that uses of trustable access only get privileged utilizing the shared data. So the user-sensitive shareable data which is in plain formats should get converted into encrypted formats that are ciphertext may be in table format but can effectively defend the access trails of unauthorized parties[3].

When we try to adopt this kind of typical encryption strategy to bring privacy as a primary e element we may face and overload or computational overhead in the process of multi-keyword search. To deal with this problem we adopt tree indexing over multiple keywords under search using Top-k priority search and effectively filter the appropriate data. When we implement the above-said process effectively and efficiently data owners are widely kept in a trustable platform.[4] To bring this into practice several schemes for methodologies carbon in which situated in such that the whole search process of encrypted data is been effectively driven in such that the user is privileged to utilize it with the multi-keyword boolean search strategy [9]. In the conventional methods, users are facilitated with a single key such process mechanism which is not well suited in practically addressing the present-day ongoing cloud paradigms [7]. In these conventional single key schemes are not providing an efficient search mechanism and lacks in data security factors.

In the present day, big-data data utilities demand flexible effective, and efficient challenges towards the sensitive data stored needs to get the address. That we adopt an attribute index-based multi-keyword searchable encryption scheme with an implicit ranking facility to optimize the time taken to access the desired resource from the cloud servers [6]. In the recommended system we should also think effectively implement random Travels scheme in such that cloud data access control can comfortably travel on the index and reflects a variety of results with the very same multi-keyword query. Show the data owner of the cloud should be facilitated with and has search capabilities not violating or compromising on security and accuracy [8].

By adopting this multi keywords scalable search scheme data on ASA protected with data privacy policies and divide scalability over a huge volume of data sets. In public clouds analysis over data retrievals along with security, parameter pushes data into Cloud Servers in an encrypted format with an encrypted index-based methodology which reduces access time significantly. Securing the sensitive data of the cloud server by converting user compatible formats into secure formats using ciphertext-policy greatly avoids malicious user attack over sensitive data significantly [10].

II LITERATURE SURVEY

Ensuring security and privacy preservation:

When we focus on the present-day emerging demands power facilities of cloud computing whether an independent or corporate utilization of shareable privileged data in Cloud Service suffers from a lack of security standards. Data of data users that is been kept for service into the data service of public cloud must meet high security and reduce risk factors over privacy preservation on how to search for data. To meet the above said expectations advancements and sufficient research is to be done to emphasize privacy protection strategies that deal with the current security threats and facilitates reliable data service capability with a high-level focus. At the bottom line, recommendations are framed on challenges on an open basis and significant research parts in every significant area. These enhancements are being driven from the present-day research that in that is been done on untrusted data access scenarios to facilitate high-level privacy protection over shared data.

Searchable symmetric encryption:

In the present day wide accessibility of share data in public clouds, identical data user could be in a situation to facilitate resources comfortable to another data user party in a more secure manner. Public key encryption model adopted over share data empowers security policies as well shouldn't be a barrier to the search operations over shareable data resources. In this research public key encryption is been adopted over the shared data effectively and facilitates keyword search operations in optimal data access timelines. By following the above-said process we should also focus keenly on decrypting operations and get data more effectively and efficiently.

Public key encryption with a keyword search:

When we emphasize the demanding circumstances of cloud computing especially in that data as a service utility it is required to maintain the data owner resource securely and facilitate flexible data access strategies to meet the data user expectations more effectively and efficiently. More or less when data security e parameter comes in front of us in a cloud computing environment we should adopt a high standard encryption policy at the data owner's end to protect data integrity in cloud platforms. To address the above-said scenario by extracting the facts from recent research works power data security paradigm we ought to move on to public-key encryption of the facilitated data. This scenario that got adopted over share data makes create a barrier in filtering the share data using a keyword search mechanism that could be handled by adopting proper index mapping techniques.

III SYSTEM ANALYSIS

Existing system:

When a data user prepares to outsource sensitive data on public cloud data access it is recommended to encrypt data before uploading into the cloud server to obtain data confidentiality and protect the integrity of data users in cloud environments. Along with that data uses should get privileged with searchable strategies power encrypted shareable cloud data that is searchable encryption to address variety threat models and meet typical search functionalities with single key similarity search. Remote data that got stored in the cloud server contributed by data owner needs to get facilitated with some dynamic ok operations like data inserting and removal activities.

Disadvantages of the existing system:

- Factors involved in data utilization need high operational costs can import phone keyword-based data retrieval process because the plane data contributed by data owner couldn't be stored exactly as it is into the data server and needs to get cipher-text converted to meet requirements of high-security standards.
- In the above-said process, there are some technical non-feasibility issues like huge computational stress to the cloud server that reflects onto the data user when he attempted to access the resource.

Proposed system:

A fully secure keyword-based tree search scheme is being adopted over shareable data of data owner which is been driven with multi-keyword index ranked similarity search over searchable operations of cloud server data. Train text mapping and multi-keyword ranking processes for effective query handling are to be systematically driven by the administrative policies of cloud Service Provider to get public cloud server end. So this index-based structural multi-keyword search is been effectively performed on towards encrypted data format only when searching keywords and data storage format should come to oneness in the runtime without losing the security precautions taken over the data.

Advantages of the proposed system:

- We emphasize preventing privacy breaches, data scalability, and time effectiveness over search query keyword processing is been achieved.

Modularizing the whole data into subsets and performing encryption over the data outsourced by the data owner empowers the reliability and trustability of data services.

IV IMPLEMENTATION

Modules:

In this project, we made four segments based on the operational nature of Domain expectation considering their roles and responsibilities as a deciding factor.

1. Data provider

2. Cloud server

3. Data user

4. Key-word indexing

5. Data encryption

1. Data provider:

The data provider is a module that facilitates shareable data from Cloud owner to cloud server with an appropriate ciphertext conversion policy e to increase security standards. Data provider module service-oriented trustable segment facilitates wide access abilities over the crucial data source permitted by remote data users onto cloud computing remote servers.

2. Cloud server:

The cloud server module is a base platform architectural model that provides infrastructural data storage capabilities enabling data access permissions remotely to a wide number of authorized users. Along with that reliability, other parameters have to be facilitated to the data owner who outsources valuable information into the cloud server.

3. Data user:

The data user module is used to interact with the shareable data the public clouds without disturbing the Data integrity policies framed by the cloud administrator.

An authorized or trustable request that got erased from this data user module will be addressed by a remote server and facilitates appropriate data that meets the data access requirements.

4. Data encryption:

Data that got uploaded by the data owner into the remote server needs to maintain data integrity and high-security standards to obtain reliability.

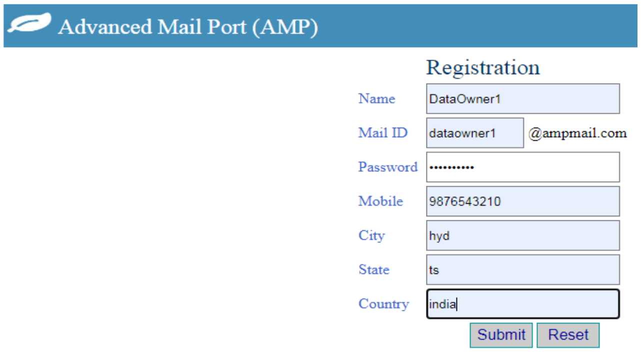
5. Keyword indexing:

A searchable encryption mechanism adopted needs to be maintained with appropriate search criteria with a multi-keyword tag is been mapped to index keyword ranking approach to filter or retrieve appropriate information in an optimal timeline.

V PROJECT EXECUTION AND TESTING

Data Owner Mail account creation page:

User mail account is created using advanced mail port with the user-specific personal information of Data owner and this is been used at the time of Data



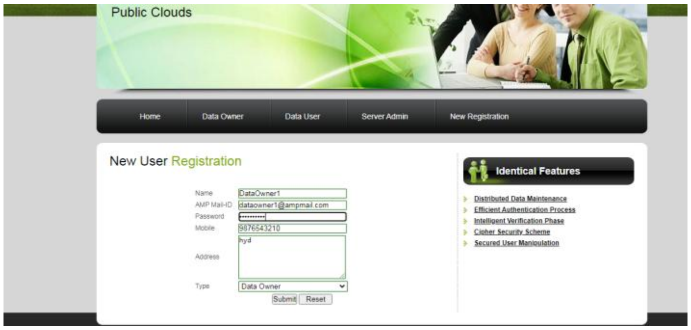
Advanced Mail Port (AMP)

Registration

Name	DataOwner1
Mail ID	dataowner1 @ampmail.com
Password	••••••••••
Mobile	9876543210
City	hyd
State	ts
Country	india

Data owner registration page:

On this page data owner parameters like name, AMP mail ID created the previous step, recommended password, mobile number, address, and type of roll been filled and click on submit button to successfully register a data owner account.



Public Clouds
Home
Data Owner
Data User
Server Admin
New Registration

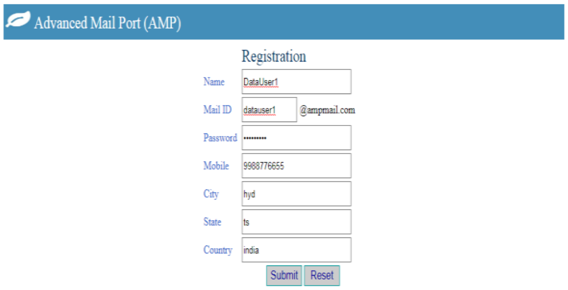
New User Registration

Name	DataOwner1
AMP Mail-ID	dataowner1@ampmail.com
Password	••••••••••
Mobile	9876543210
Address	hyd
Type	Data Owner

Submit
Reset
Identical Features
Distributed Data Maintenance
Efficient Authentication Process
Intelligent Verification Phase
Cipher Security Scheme
Secured User Manipulation

Data user Mail account creation page:

User mail account is created using advanced mail port with the user-specific personal information of Data user and this is been used at the time of Data



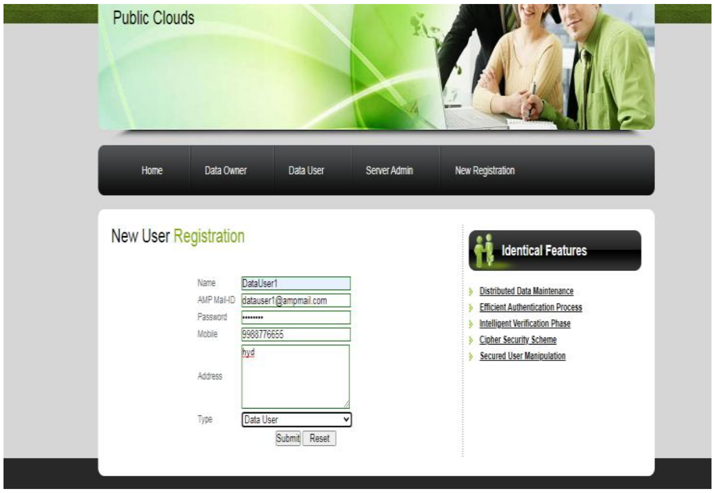
Advanced Mail Port (AMP)

Registration

Name	DataUser1
Mail ID	datauser1 @ampmail.com
Password	••••••••
Mobile	9988776655
City	hyd
State	ts
Country	india

Data user registration page:

On this page, data user parameters like name, AMP mail ID created in the previous step, recommended password, mobile number, address, and the type of role has to be filled and the submit button should be clicked to successfully register a data user account.



Public Clouds
Home
Data Owner
Data User
Server Admin
New Registration

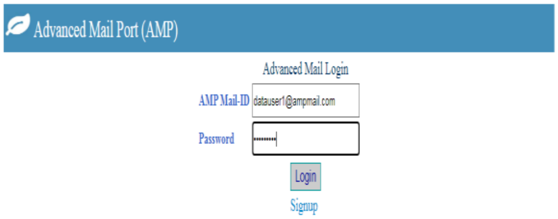
New User Registration

Name	DataUser1
AMP Mail-ID	datauser1@ampmail.com
Password	••••••••
Mobile	9988776655
Address	hyd
Type	Data User

Submit
Reset
Identical Features
Distributed Data Maintenance
Efficient Authentication Process
Intelligent Verification Phase
Cipher Security Scheme
Secured User Manipulation

Mail account login:

On this page mail ID created in the previous operations is used along with the identical password are filled and when we click on login it will redirect to inbox if the credentials are entered correctly photo.



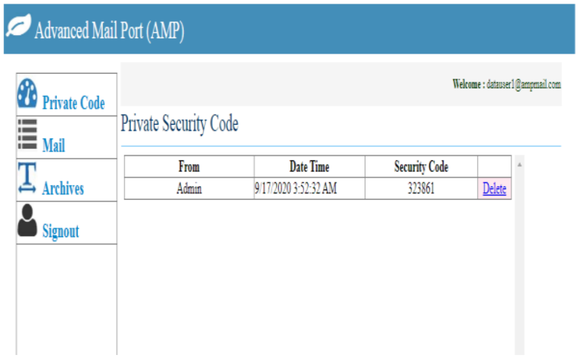
Advanced Mail Port (AMP)

Advanced Mail Login

AMP Mail-ID	datauser1@ampmail.com
Password	••••••••

Mail inbox page:

With the appropriate credentials, we can log in to the mail and check the inbox for the private security codes that got generated if any.



Advanced Mail Port (AMP)

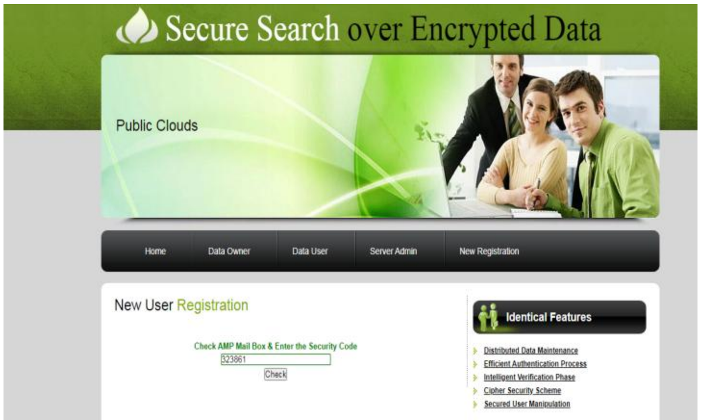
Welcome : datauser1@ampmail.com

Private Security Code

From	Date Time	Security Code	
Admin	9/17/2020 3:52:32 AM	323861	Delete

User registration page:

Remind me to enter the private security code that came to mail inbox to the user personal mail account it is been entered and click on the check button so that we can migrate to the user homepage.


Secure Search over Encrypted Data
Public Clouds
Home
Data Owner
Data User
Server Admin
New Registration
Identical Features
Distributed Data Maintenance
Efficient Authentication Process
Intelligent Verification Phase
Cipher Security Scheme
Secured User Manipulation
Check

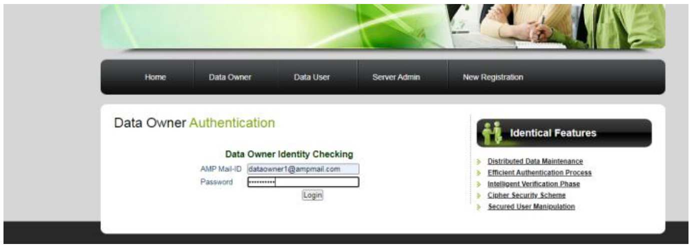
New User Registration

Check AMP Mail Box & Enter the Security Code

323861

Data owner second occasion page:

Here AMP email id and password offer specific data user should be entered and click on login to migrate the control two data owner homepage.


Home
Data Owner
Data User
Server Admin
New Registration
Identical Features
Distributed Data Maintenance
Efficient Authentication Process
Intelligent Verification Phase
Cipher Security Scheme
Secured User Manipulation
Login

Data Owner Authentication

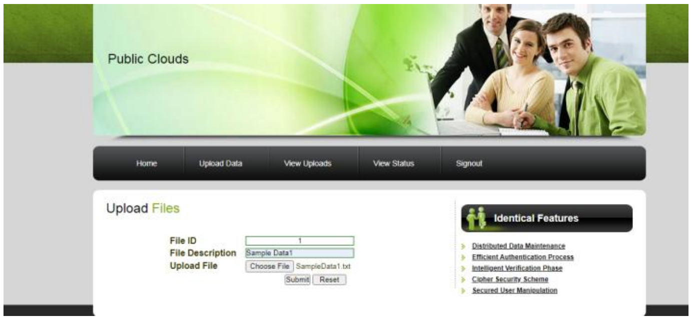
Data Owner Identity Checking

AMP Mail-ID dataowner1@ampmail.com

Password ••••••••••

Upload files page:

On this page, the data that is to be outsourced onto the cloud server should be uploaded, and click on submit to get confirmation.



Upload Files

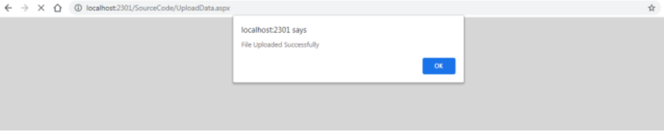
File ID 1

File Description Sample Data1

Upload File SampleData1.txt

Acknowledgment page:

Upon successful uploading of file details in this acknowledgment page will get generated that prompts file uploaded successfully message.

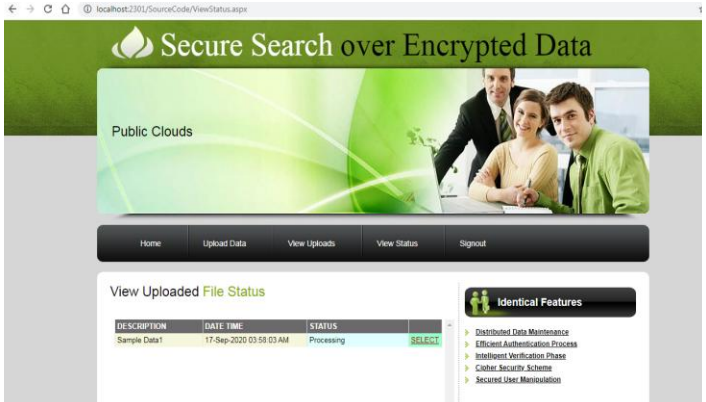


localhost:2301 says

File Uploaded Successfully

File upload status page:

Clear all uploaded files list is been visualized.

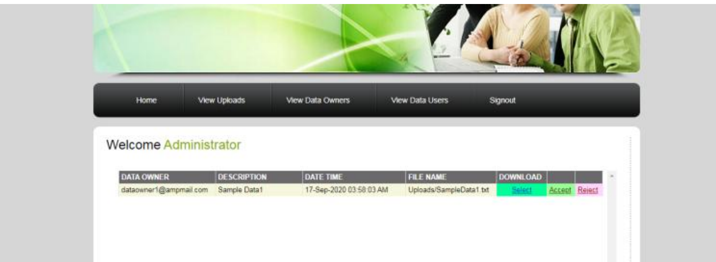

localhost:2301/SourceCode/ViewStatus.aspx
Secure Search over Encrypted Data
Public Clouds
Home
Upload Data
View Uploads
View Status
Signout
Identical Features
Distributed Data Maintenance
Efficient Authentication Process
Intelligent Verification Phase
Cipher Security Scheme
Secured User Manipulation

View Uploaded File Status

DESCRIPTION	DATE TIME	STATUS	
Sample Data1	17-Sep-2020 03:58:03 AM	Processing	SELECT

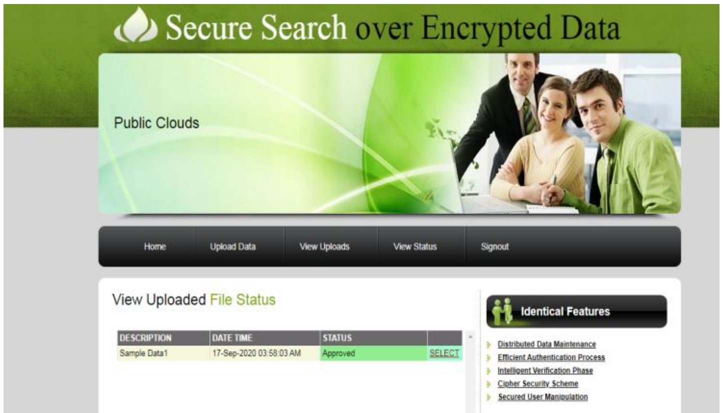
Administrator home page:

On this page operations of an administrator like view uploads, view data owner, view data uses are been facilitated.



Welcome Administrator

DATA OWNER	DESCRIPTION	DATE TIME	FILE NAME	DOWNLOAD		
dataowner1@ampmail.com	Sample Data1	17-Sep-2020 03:58:03 AM	Uploads/SampleData1.txt	Select	Accept	Reject

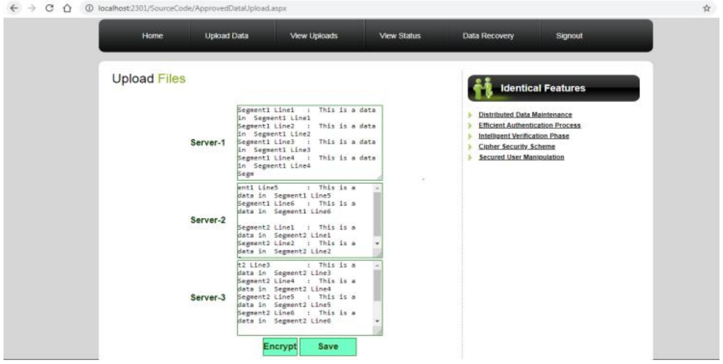

Secure Search over Encrypted Data
Public Clouds
Home
Upload Data
View Uploads
View Status
Signout
Identical Features
Distributed Data Maintenance
Efficient Authentication Process
Intelligent Verification Phase
Cipher Security Scheme
Secured User Manipulation

View Uploaded File Status

DESCRIPTION	DATE TIME	STATUS	
Sample Data1	17-Sep-2020 03:58:03 AM	Approved	SELECT

Data Encryption page:

Segment-wise encryption is been done over the uploaded data to increase privacy standards.


localhost:2301/SourceCode/ApprovedDataUpload.aspx
Home
Upload Data
View Uploads
View Status
Data Recovery
Signout
Identical Features
Distributed Data Maintenance
Efficient Authentication Process
Intelligent Verification Phase
Cipher Security Scheme
Secured User Manipulation
Encrypt
Save

Upload Files

Server-1

```
Segment1 Line1   :  This is a data
in  Segment1 Line1
Segment1 Line2   :  This is a data
in  Segment1 Line2
Segment1 Line3   :  This is a data
in  Segment1 Line3
Segment1 Line4   :  This is a data
in  Segment1 Line4
Segm
```

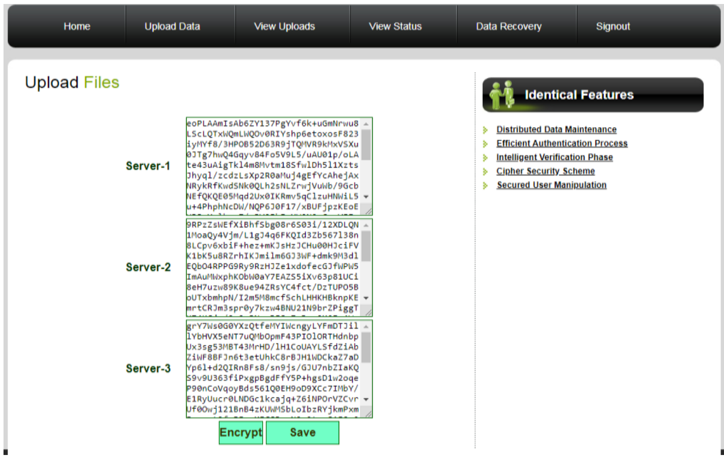
Server-2

```
ent1 Line5       :  This is a
data in  Segment1 Line5
Segment1 Line6   :  This is a
data in  Segment1 Line6

Segment2 Line1   :  This is a
data in  Segment2 Line1
Segment2 Line2   :  This is a
data in  Segment2 Line2
```

Server-3

```
t2 Line3         :  This is a
data in  Segment2 Line3
Segment2 Line4   :  This is a
data in  Segment2 Line4
Segment2 Line5   :  This is a
data in  Segment2 Line5
Segment2 Line6   :  This is a
data in  Segment2 Line6
```


Home
Upload Data
View Uploads
View Status
Data Recovery
Signout
Identical Features
Distributed Data Maintenance
Efficient Authentication Process
Intelligent Verification Phase
Cipher Security Scheme
Secured User Manipulation
Encrypt
Save

Upload Files

Server-1

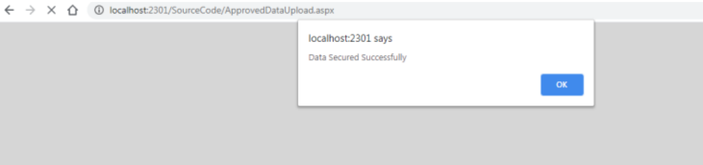
```
eoPLAAmIsAb6ZY137PgYvf6k+uGmNrwu8
LScLQTxWQmLWQOv0RIYshp6etoxosF823
iyMYf8/3HPOB52D63R9jTQMVR9kMxVSXu
0JTg7hwQ4Gqyv84Fo5V9L5/uAU01p/oLA
te43uAigTkl4m8Mvtm18SfwlDh5l1Xzts
Jhyql/zcdzLsXp2R0aMuj4gEfYcAhejAx
NRykRfKwdSNk0QLh2sNLZrwjVuWb/9Gcb
NEfQKQE05Mqd2Ux0IKRmv5qClzuHNWiL5
u+4PhphNcDW/NQP6J0F17/xBUFjpzKEoE
```

Server-2

```
9RPzZsWEfXiBhfSbg08r6S03i/12XDLQN
1MoaQy4Vjm/L1gJ4q6FKQId3Zb567l38n
8LCpv6xbiF+hez+mKJsHzJCHu00HJciFV
K1bK5u8RZrhIKJmilm6GJ3WF+dmk9M3dl
EQbO4RPPG9Ry9RzHJZe1xdofecGJfWPW5
ImAuMWxphKObW0aY7EAZS5iXv63p81UCi
8eH7uzw89K8ue94ZRsYC4fct/DzTUPO5B
oUTxbmhpN/I2m5M8mcfSchLHHKHBknpKE
mrtCRJm3spr0y7kzw4BNU21N9brZPiggT
```

Server-3

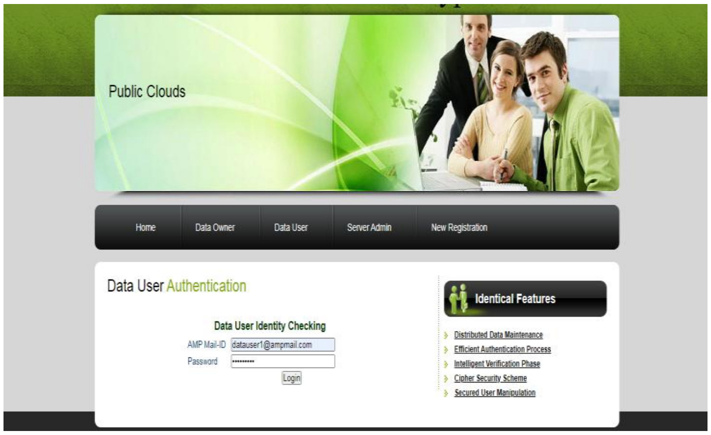
```
grY7Ws0G0YXzQtfeMYIWcngyLYFmDTJil
lYbHVX5eNT7uQMbOpmF43PIOlORTHdnbp
Ux3sg53MBT43MrHD/lH1CoUAYLSfdZiAb
ZiWF8BFJn6t3etUhkC8rBJH1WDCkaZ7aD
Yp6l+d2QIRn8Fs8/sn9js/GJU7nbZIaKQ
S9v9U363fiPxgpBgdFfY5P+hgsD1w2oqe
P90nCoVqoyBds561Q0EH9oD9XCc7IMbY/
E1RyUucr0LNDGc1kcajq+Z6iNPOrVZCvr
Uf0Owj121BnB4zKUWMSbLoIbzRYjkmPxm
```



localhost:2301/SourceCode/ApprovedDataUpload.aspx

localhost:2301 says

Data Secured Successfully


Public Clouds
Home
Data Owner
Data User
Server Admin
New Registration
Identical Features
Distributed Data Maintenance
Efficient Authentication Process
Intelligent Verification Phase
Cipher Security Scheme
Secured User Manipulation
Login

Data User Authentication

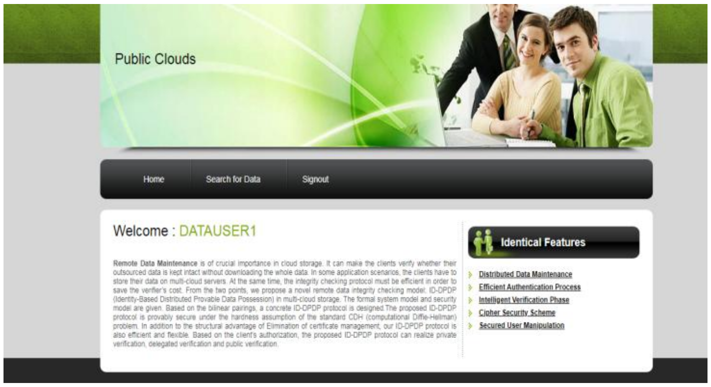
Data User Identity Checking

AMP Mail-ID: datauser1@ampmail.com

Password: ••••••••

Data user home page:

On this page, the primary operation like the search for data has been facilitated to the data user.

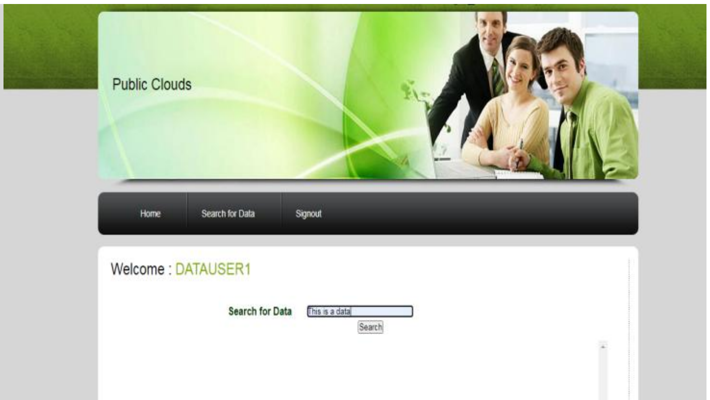

Public Clouds
Home
Search for Data
Signout
Identical Features
Distributed Data Maintenance
Efficient Authentication Process
Intelligent Verification Phase
Cipher Security Scheme
Secured User Manipulation

Welcome : DATAUSER1

Remote Data Maintenance is of crucial importance in cloud storage. It can make the clients verify whether their outsourced data is kept intact without downloading the whole data. In some application scenarios, the clients have to store their data on multi-cloud servers. At the same time, the integrity checking protocol must be efficient in order to save the verifier's cost. From the two points, we propose a novel remote data integrity checking model: ID-DPDP (Identity-Based Distributed Provable Data Possession) in multi-cloud storage. The formal system model and security model are given. Based on the bilinear pairings, a concrete ID-DPDP protocol is designed.The proposed ID-DPDP protocol is provably secure under the hardness assumption of the standard CDH (computational Diffie-Hellman) problem. In addition to the structural advantage of Elimination of certificate management, our ID-DPDP protocol is also efficient and flexible. Based on the client's authorization, the proposed ID-DPDP protocol can realize private verification, delegated verification and public verification.

Search data page:

Here multi-keyword search process is driven after entering an appropriate query string, just click on search to view the relevant results.

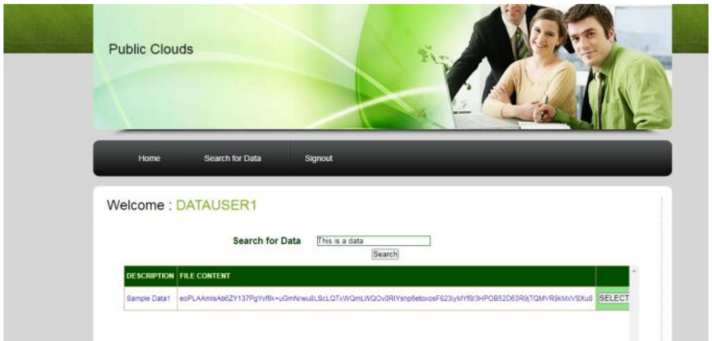


Welcome : DATAUSER1

Search for Data: This is a data

Search results page:

For an appropriate multi-keyword query string an appropriate result is listed and visualized here.



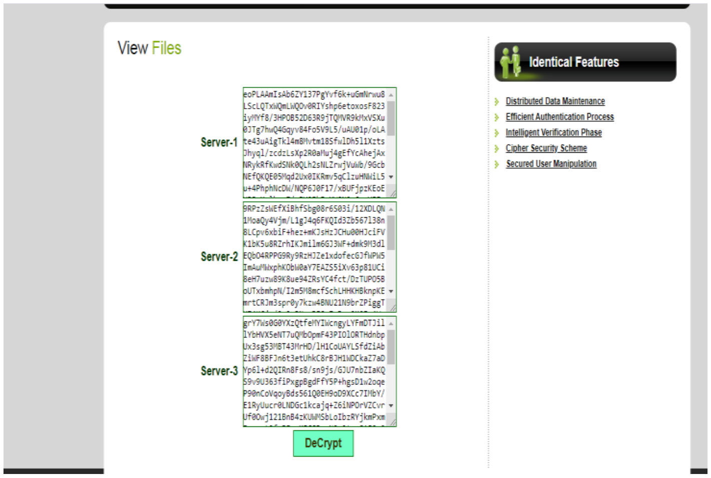
Welcome : DATAUSER1

Search for Data: This is a data

DESCRIPTION	FILE CONTENT	
Sample Data1	eoPLAAmIsAb6ZY137PgYvf6k+uGmNrwu8LScLQTxWQmLWQOv0RIYshp6etoxosF823iyMYf8/3HPOB52D63R9jTQMVR9kMxVSXu0	SELECT

Decryption page:

Data retrieval of encrypted form again back to its plain data formats is been visualized here.


Identical Features
Distributed Data Maintenance
Efficient Authentication Process
Intelligent Verification Phase
Cipher Security Scheme
Secured User Manipulation
DeCrypt

View Files

Server-1

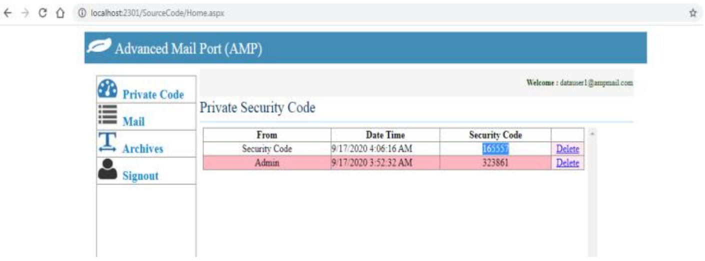
```
eoPLAAmIsAb6ZY137PgYvf6k+uGmNrwu8
LScLQTxWQmLWQOv0RIYshp6etoxosF823
iyMYf8/3HPOB52D63R9jTQMVR9kMxVSXu
0JTg7hwQ4Gqyv84Fo5V9L5/uAU01p/oLA
te43uAigTkl4m8Mvtm18SfwlDh5l1Xzts
Jhyql/zcdzLsXp2R0aMuj4gEfYcAhejAx
NRykRfKwdSNk0QLh2sNLZrwjVuWb/9Gcb
NEfQKQE05Mqd2Ux0IKRmv5qClzuHNWiL5
u+4PhphNcDW/NQP6J0F17/xBUFjpzKEoE
```

Server-2

```
9RPzZsWEfXiBhfSbg08r6S03i/12XDLQN
1MoaQy4Vjm/L1gJ4q6FKQId3Zb567l38n
8LCpv6xbiF+hez+mKJsHzJCHu00HJciFV
K1bK5u8RZrhIKJmilm6GJ3WF+dmk9M3dl
EQbO4RPPG9Ry9RzHJZe1xdofecGJfWPW5
ImAuMWxphKObW0aY7EAZS5iXv63p81UCi
8eH7uzw89K8ue94ZRsYC4fct/DzTUPO5B
oUTxbmhpN/I2m5M8mcfSchLHHKHBknpKE
mrtCRJm3spr0y7kzw4BNU21N9brZPiggT
```

Server-3

```
grY7Ws0G0YXzQtfeMYIWcngyLYFmDTJil
lYbHVX5eNT7uQMbOpmF43PIOlORTHdnbp
Ux3sg53MBT43MrHD/lH1CoUAYLSfdZiAb
ZiWF8BFJn6t3etUhkC8rBJH1WDCkaZ7aD
Yp6l+d2QIRn8Fs8/sn9js/GJU7nbZIaKQ
S9v9U363fiPxgpBgdFfY5P+hgsD1w2oqe
P90nCoVqoyBds561Q0EH9oD9XCc7IMbY/
E1RyUucr0LNDGc1kcajq+Z6iNPOrVZCvr
Uf0Owj121BnB4zKUWMSbLoIbzRYjkmPxm
```

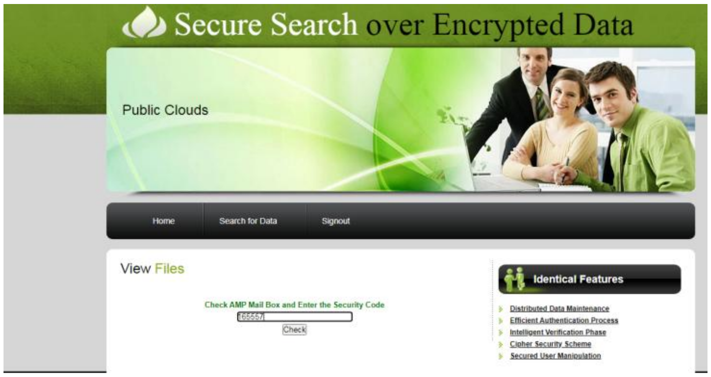


localhost:2301/SourceCode/Home.aspx

Welcome : datauser1@ampmail.com

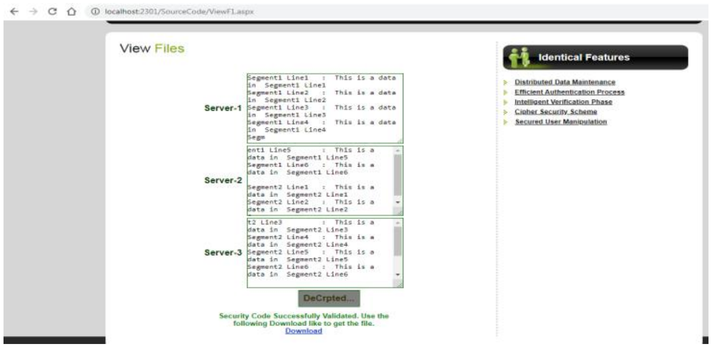
Private Security Code

From	Date Time	Security Code	
Security Code	9/17/2020 4:06:16 AM	165557	Delete
Admin	9/17/2020 3:52:32 AM	323861	Delete


Secure Search over Encrypted Data
Public Clouds
Home
Search for Data
Signout
View Files
Identical Features
Distributed Data Maintenance
Efficient Authentication Process
Intelligent Verification Phase
Cipher Security Scheme
Secured User Manipulation
Check

Check AMP Mail Box and Enter the Security Code

165557


localhost:2301/SourceCode/ViewF1.aspx
View Files
Identical Features
Distributed Data Maintenance
Efficient Authentication Process
Intelligent Verification Phase
Cipher Security Scheme
Secured User Manipulation
DeCrpted...
Download

Server-1

```
Segment1 Line1    :  This is a data
in  Segment1 Line1
Segment1 Line2    :  This is a data
in  Segment1 Line2
Segment1 Line3    :  This is a data
in  Segment1 Line3
Segment1 Line4    :  This is a data
in  Segment1 Line4
Segm
```

Server-2

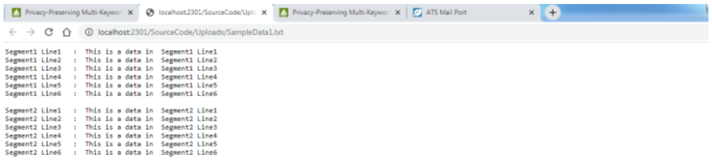
```
ent1 Line5        :  This is a
data in  Segment1 Line5
Segment1 Line6    :  This is a
data in  Segment1 Line6

Segment2 Line1    :  This is a
data in  Segment2 Line1
Segment2 Line2    :  This is a
data in  Segment2 Line2
```

Server-3

```
t2 Line3          :  This is a
data in  Segment2 Line3
Segment2 Line4    :  This is a
data in  Segment2 Line4
Segment2 Line5    :  This is a
data in  Segment2 Line5
Segment2 Line6    :  This is a
data in  Segment2 Line6
```

Security Code Successfully Validated. Use the following Download like to get the file.


Privacy-Preserving Multi-Keywo
localhost:2301/SourceCode/Uplo
Privacy-Preserving Multi-Keywo
ATS Mail Port
localhost:2301/SourceCode/Uploads/SampleData1.txt

```
Segment1 Line1   :  This is a data in  Segment1 Line1
Segment1 Line2   :  This is a data in  Segment1 Line2
Segment1 Line3   :  This is a data in  Segment1 Line3
Segment1 Line4   :  This is a data in  Segment1 Line4
Segment1 Line5   :  This is a data in  Segment1 Line5
Segment1 Line6   :  This is a data in  Segment1 Line6

Segment2 Line1   :  This is a data in  Segment2 Line1
Segment2 Line2   :  This is a data in  Segment2 Line2
Segment2 Line3   :  This is a data in  Segment2 Line3
Segment2 Line4   :  This is a data in  Segment2 Line4
Segment2 Line5   :  This is a data in  Segment2 Line5
Segment2 Line6   :  This is a data in  Segment2 Line6
```

VI CONCLUSION

In this paper, we focus on improving the efficiency and the security over data storage facilities to encourage big data utility applications in such that service utilization of identical and entrepreneur enormous computational power and scalability got improvised greatly. Demerit in conventional systems i.e data retrieval of data stored in public clouds could be handled with the same formatted data. The keyword-based searching mechanism couldn't be e effectively driven if data uses doesn't follow the same formatted data that is been stored in the data store of the cloud got overcome by the below said approach. Data needs to get encrypted and preserved in the data store of the database as well as data users could be in a situation to search the data with the daily utility formats irrespective of the format stored in the data store. In this project, we implemented a multiple keyword top-k searching mechanism to engage in encrypted data formats effectively and efficiently inter not violating the security policies. This index-based structural multi-keyword search can be effectively performed over encrypted data formats only when searching keywords and data storage format should come to oneness in the runtime without losing the security precautions taken over the data is done. In this Project secure multi-keyword search mechanism with tree indexing, facilitate a significant and effective system in such a way we can emphasize preventing privacy breaches, data scalability, and time effectiveness in search query keyword processing got achieved. To enhance the security policies we move ahead by modularizing the whole data into sub-parts and perform encryption then stored so that when data users attempt to to retrieve the very Same data could be done in a segment-based manner so that reliability and trustability of the Stored data got achieved.

REFERENCES

[1] J. Tang, Y. Cui, Q. Li, K. Ren, J. Liu, and R. Buyya, “Ensuring security and privacy preservation for cloud data services,” ACM Computing Surveys, 2016.

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “A view of cloud computing,” Communications of the ACM, vol. 53, no. 4, pp. 50–58, 2010.

[3] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: Improved definitions and efficient constructions,” in Proceedings of the 13th ACM Conference on Computer

and Communications Security. ACM, 2006, pp. 79–88.

[4] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in Advances in CryptologyEurocrypt 2004. Springer, 2004, pp. 506–522.

[5] Z. Ying, H. Li, J. Ma, J. Zhang, and J. Cui, “Adaptively secure ciphertext-policy attribute-based encryption with dynamic policy updating,” Sci China Inf Sci, vol. 59, no. 4, pp. 042 701:1–16, 2016.

[6] D. X. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in Security and Privacy, 2000. SP 2000. Proceedings. 2000 IEEE Symposium on, 2000, pp. 44–55.

[7] E.-J. Goh et al., “Secure indexes.” IACR Cryptology ePrint Archive, vol. 2003, p. 216, 2003.

[8] Y.-C. Chang and M. Mitzenmacher, “Privacy preserving keyword searches on remote encrypted data,” in Applied Cryptography and Network Security. Springer, 2005, pp. 442–455.

[9] Y. H. Hwang and P. J. Lee, “Public key encryption with conjunctive keyword search and its extension to a multi-user system,” in Pairing-Based Cryptography–Pairing. Springer, 2007, pp. 2–22.

[10] P. Golle, J. Staddon, and B. Waters, “Secure conjunctive keyword search over encrypted data,” in Applied Cryptography and Network Security. Springer, 2004, pp. 31–45.