DOI: https://doi.org/10.53555/nncse.v2i3.488 **Publication URL: http://nnpub.org/index.php/CSE/article/view/488**

ENHANCING SECURITY AND CONSISTENCY FOR CLOUD DATABASES

Monisha.M[1]*, Narmathadevi.V[2], Mrs.D. KeranaHanirex[3]
[1,2]Final year-B.tech/CSE Bharath University, [3]Assistant Professor/CSE Bharath University
[1]Monisha.mohan1425@gmail.com,[2]vnarmathadevi93@gmail.com[3]keranarobinson@gmail.com

Corresponding Author: -
Email ID- Monisha.mohan1425@gmail.com

Abstract: -

Cloud computing is one of the most important research areas. The cloud information doesn't seem to be safe and secured, because the third parties will access and acquire the knowledge from cloud at any time and will misuse the data or information of a particular user or organization and thus it is concerned, the information stored in cloud should come with the guarantee of security. The effectiveness of the planned design is evaluated through theoretical analysis and intensive experimental results supported a model implementation subject to the TPC-C (Transaction Processing Control) normal benchmark for various numbers of purchasers and network latencies. Information and table information area unit encrypted through constant encoding key before being saved. This encoding secret is known as a passkey. Only trusted clients that already know the key will rewrite the information and acquire data that is necessary to code and rewrite tenant knowledge. Each information is retrieved by purchasers through associated ID. The ID which is generated by the Message Authentication Code (MAC) function to the name of the object (database or table) described by the corresponding row. Deterministic MACfunction allows clients to retrieve the information of a given table by knowing its plaintext name. The advantage during this design is to boost smart Quality of Service (QoS) and Distributing knowledge among completely different suppliers and taking advantage of secret sharing.

INTRODUCTION

The SecureDBaaS architecture is tailored to cloud platforms and does not introduce any intermediary proxy or broker server between the client and the cloud provider. SecureDBaaS relates more closely to works using encryption to protect data managed by UN trusted databases. In such a case, a main issue to address is that cryptographic techniques cannot be natively applied to standard DBaaS. As expected, the number of transactions per minute executed by SecureDBaaS is lower than those referring to original TPC-C and plain-SecureDBaaS. SecureDBaaS moves away from existing architectures that store just tenant data in the cloud, and the metadata will be stored in the client machine or split metadata between the cloud database and a trust proxy, while considering scenarios where multiple clients can access the same database concurrently.

Even though they using secure DBaaS means Distributing data among different providers and it give more secure but its functions cannot be taking advantage of secret sharing outsourced to an untrusted cloud provider. It Cannot Store them in encrypted format.

The proposed architecture is subject to the TPC-C standard benchmark for different numbers of clients and network latencies shows that the performance of concurrent read and write operations not modifying the SecureDBaaS database structure are comparable to that of unencrypted cloud Database. Even metadata confidentiality is guaranteed through encryption. This table uses one row for the database metadata, and one row for each table metadata. This encryption key is called a master key. The key which is generated are called as the master key. The trusted client who is aware of the master key will rewrite the data and acquire data that is necessary to write in code and rewrite tenant information. Every data is retrieved by clients the through the associated ID.This ID is computed by applying a Message Authentication Code (MAC) function to the name of the object described by the corresponding row. Whatever the data send by the user to cloud server, first our metadata split the data as data type, encrypted type and field confidentiality (size, time, and path) these things are trusted proxy.

Related work

Paper [1] proposesdata encryption. It causes a large overhead in query processing. A distributed architecture is proposed as a solution to this problem where data was stored at multiple sites.

Paper [2]proposes homomorphic encryption scheme. Which unify the first two families of problem. A new fully homomorphic encryption scheme is produced to solve these three problems.

Paper [3] proposes Database as a service. It provides a mechanism to create, store and access their database at the host site. A developed database services on the internet called NetDB2.it is an effective mechanism for organization to purchase data management. Protecting the secrecy of the information has become primary important.Operating on-line querying services securely on open networks is very difficult; therefore many enterprises outsource their data center operations to external application service providers.

Paper [4] proposesto gain access to private data cryptDB because adversaries can exploit software bugs.Which provides practical and provable confidentiality in the face. These attacks backed by SQL databases. The execution is based SQL Queries.

Paper [5] proposes Security of data becomes more important in the cloud technique for achieving security. The implementation of database encryption where, because of high cost, complexity and performance degradation. Data encryption can be done at multiple tiers within the enterprise.

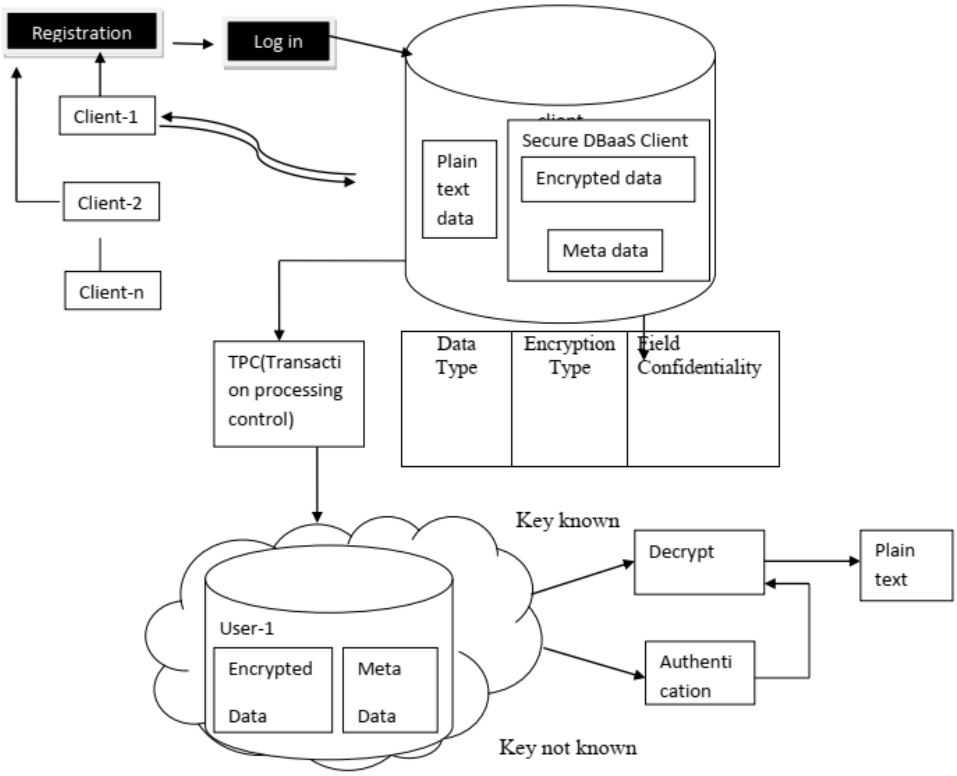
Paper [6] proposesdifferent environmentto perform the experimental network and its emulation, simultaneous and live network Emu lab is an experimentation facility which integrates these approaches. The primary goals are easy to use and control and realism.

Paper [7] proposes random order-preserving function (ROPF). The open problem of characterizing what encryption via a random order-preserving function (ROPF) leaks about basic data.In particular, we show that, for a database of randomly distributed plaintexts and appropriate choice of parameters, ROPF encryption leaks neither the accurate value of any plaintext.

Architecture system

The proposed architecture is subject to the TPC-C standard benchmark for different numbers of clients and network latencies show that the performance of concurrent read and write operations not modifying the SecureDBaaS database structure are comparable to that of unencrypted cloud Database. Even metadata confidentiality is guaranteed through encryption. This table uses one row for the database metadata, and one row for each table metadata. This table uses one row for the database metadata, and one row for each table metadata. This encryption key is called a master key. The key which is generated are called as the master key. The trusted client who is aware of the master key will rewrite the data and acquire data that is necessary to write in code and rewrite tenant information. Every data is retrieved by clients the through the associated ID.This ID is computed by applying a Message Authentication Code (MAC) function to the name of the object described by the corresponding row. whatever user send the data our DB (Data Base) to cloud server in this process first our data base meta data split the data is data type and encrypted type, field confidentiality(size,time,path) these things are trusted proxy. After these data send to cloud server and it is un-trusted DB (data base).

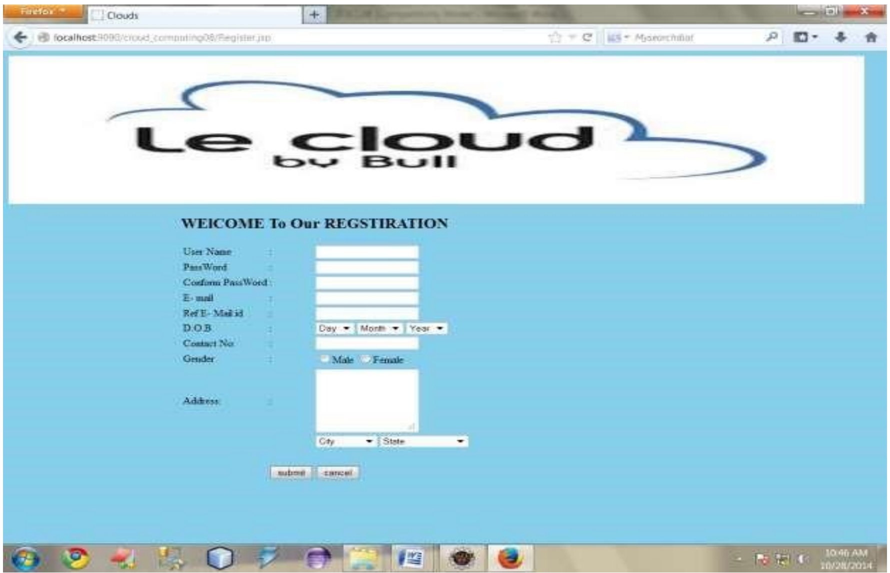
SecureDBaaS includes the data that is managed by the plain text data, encryptedinformation, metadata and encrypted data. The plain text information within the cloud information consists of data during which the tenant needs to store their data. The SecureDBaaS that produces a group of meta information for the clients so as to supply the information an needed to encrypt and decrypt the given data within the cloud information. Solutions supported a sure proxy area unit additional possible, however they introduce a system bottleneck that reduces convenience, elasticity, and measure ability of cloud information services. SecureDBaaS proposes a distinct approach wherever all information and data area unit keep within the cloud information. SecureDBaaS purchasers will retrieve the required data from the untrusted information through SQL statements, in order that multiple instances of the SecureDBaaS consumer will access to the untrusted cloud information severally with the guarantee of constant convenience and measurability properties of typical cloud DBaaS. Encryption ways for tenant information and innovative solutions for data management and storage area are described here as two sections namely data management and metadata management. First user login into user window then if it is a valid user means then it can communicate with the cloud server. The major advantage of the thing is if client requests some data then the request will reach to the server then the data which is requested by the client is there with the cloud server then it will be processed and effectively sending data to the requested client. If the data is not there with the cloud server then it has to search in its related clients and if the resource is there means then it will be shared to the particular requester.



Experimental Results

- The hardware requirements are the processor which is PENTIUM IV 2.6 GHz, Intel Core 2 Duo, Random Access Memory (ARM)512MBDDRAM.
- The software requirements are that the front end here used is java (JSP, Servlet). The backend used here is MySQL 5.5. The operating system used in this secure DBAAS is that Windows XP/07.
- The operation performed in this architecture is Insert, Edit and Delete respectively.

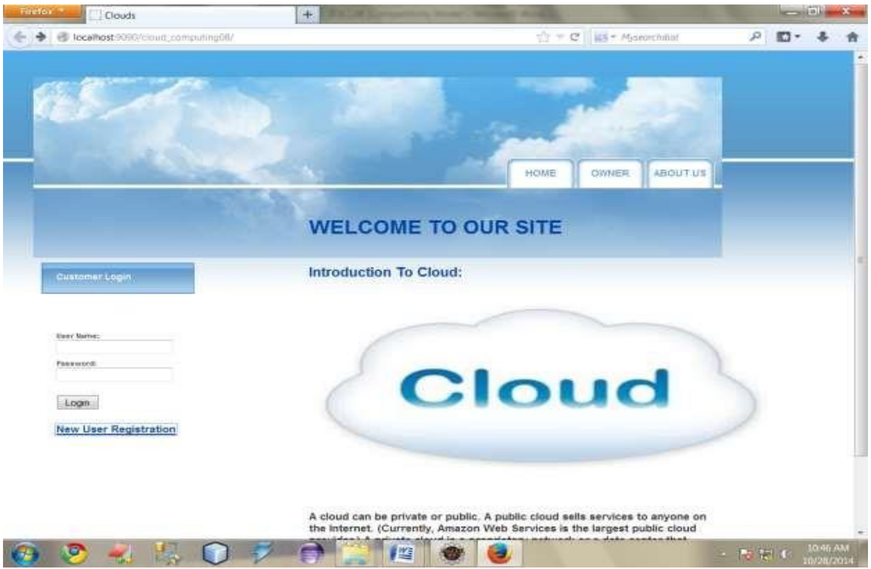
The performances are evaluated by the SQL Operations. The next sets of experiments evaluate the performance and the overheads of our prototype. The Emu-lab test-bed is used here which provides us a restricted environment with several machines. Theexperiment gives the several of scenario in order to consider the terms of workload modules, number of clients and network latencies. A graph which shows the performance of a each clients in the cloud. The Yaxis reports the box plots of the response time expressed in ms. while the X-axis identifies the SQL Operations. The experimental result displays the time response the SQL Operations on database.



WEICOME To Our REGSTIRATION

User Name :
PassWord :
Conform PassWord :
E- mail :
Ref E- Mail id :
D.O.B : Day Month Year
Contact No :
Gender : ○ Male ○ Female
Address :
City State

Fig 1:Registration



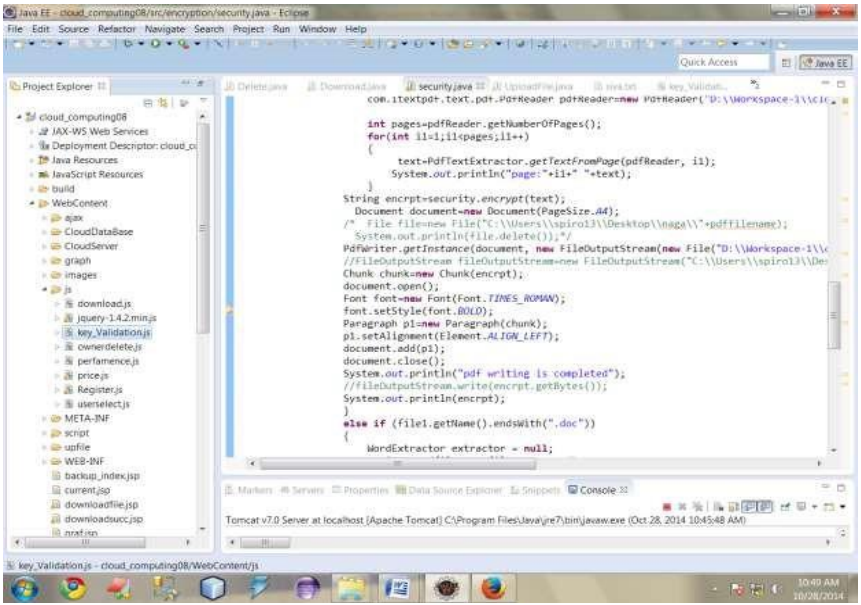
WELCOME TO OUR SITE

User Name:
Password:

Introduction To Cloud:

A cloud can be private or public. A public cloud sells services to anyone on the Internet. (Currently, Amazon Web Services is the largest public cloud

Fig 2:User login

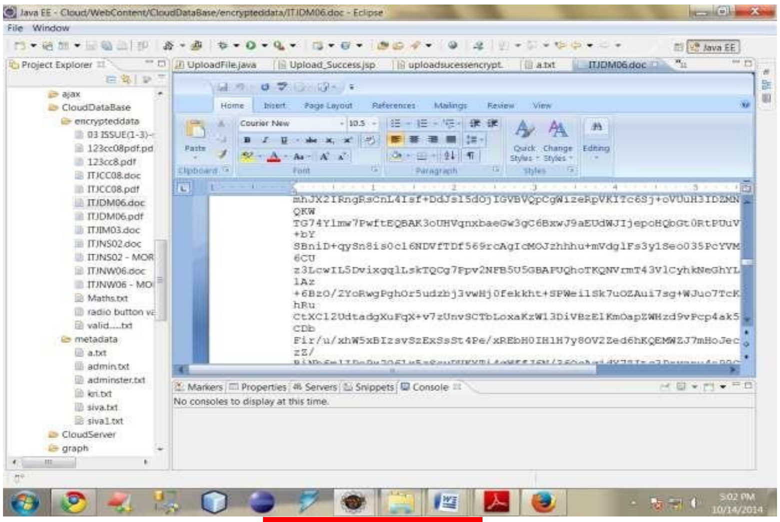


```
        com.itextpdf.text.pdf.PdfReader pdfReader=new PdfReader("D:\\Workspace-1\\clc

        int pages=pdfReader.getNumberOfPages();
        for(int i1=1;i1<pages;i1++)
        {
            text=PdfTextExtractor.getTextFromPage(pdfReader, i1);
          System.out.println("page:"+i1+" "+text);
        }
    String encrpt=security.encrypt(text);
      Document document=new Document(PageSize.A4);
    /*  File file=new File("C:\\Users\\spiro13\\Desktop\\naga\\"+pdffilename);
      System.out.println(file.delete());*/
    PdfWriter.getInstance(document, new FileOutputStream(new File("D:\\Workspace-1\\c
    //FileOutputStream fileOutputStream=new FileOutputStream("C:\\Users\\spiro13\\De
    Chunk chunk=new Chunk(encrpt);
    document.open();
    Font font=new Font(Font.TIMES_ROMAN);
    font.setStyle(font.BOLD);
    Paragraph p1=new Paragraph(chunk);
    p1.setAlignment(Element.ALIGN_LEFT);
    document.add(p1);
    document.close();
    System.out.println("pdf writing is completed");
    //fileOutputStream.write(encrpt.getBytes());
    System.out.println(encrpt);
    }
    else if (file1.getName().endsWith(".doc"))
    {
        WordExtractor extractor = null;
```

```
Tomcat v7.0 Server at localhost [Apache Tomcat] C:\Program Files\Java\jre7\bin\javaw.exe (Oct 28, 2014 10:45:48 AM)
```

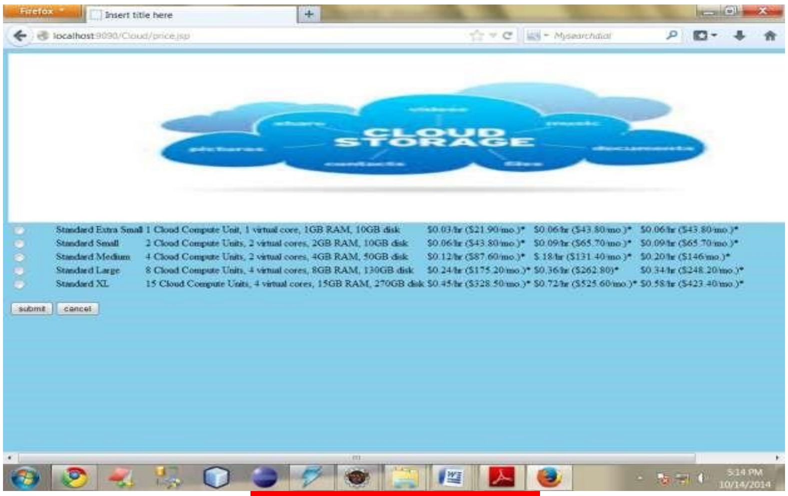
Fig 3:secret coding



```
mhJX2IRngRsCnL4Isf+DdJsl5dOjIGVBVQpCgWizeRpVKITc6Sj+oVUuH3IDZMN
QKW
TG74Ylmw7PwftEQBAK3oUHVqnxbaeGw3gC6BxwJ9aEUdWJIjepoHQbGt0RtPUuV
+bY
SBniD+qySn8is0cl6NDVfTDf569rcAgIcMOJzhhhu+mVdglFs3yl8eo035PcYVM
6CU
z3LcwIL5DvixgqlLskTQCg7Fpv2NFB5U5GBAFUQhoTKQNVrmT43VlCyhkNeGhYL
1Az
+6BzO/ZYoRwgPghOr5udzbj3vwHj0fekkht+SPWeilSk7uOZAui7sg+WJuo7TcK
hRu
CtXCl2UdtadgXuFqX+v7zUnvSCTbLoxaKzW13DiVBzEIKmOapZWHzd9vPcp4ak5
CDb
Fir/u/xhW5xBIzsvSzExSsSt4Pe/xREbH0IH1H7y8OV2Zed6hKQEMWZJ7mHoJec
zZ/
```

No consoles to display at this time.

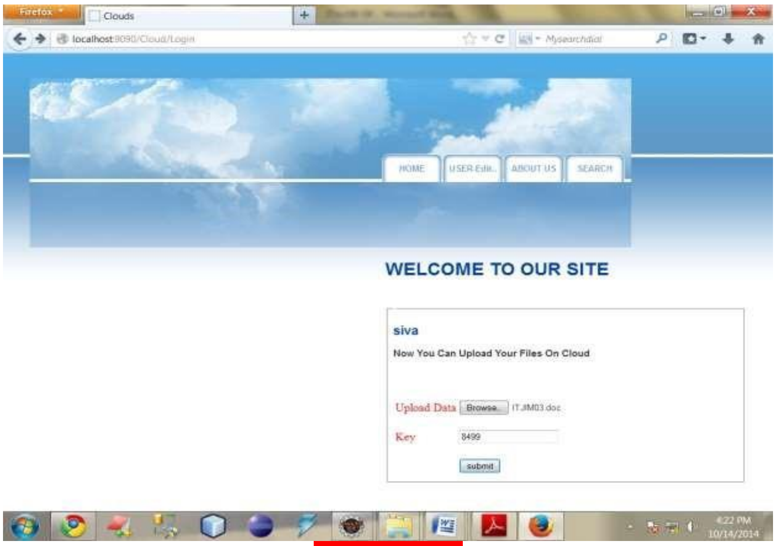
Fig 4:Secret coding



○	Standard Extra Small	1 Cloud Compute Unit, 1 virtual core, 1GB RAM, 10GB disk	$0.03/hr ($21.90/mo.)*	$0.06/hr ($43.80/mo.)*	$0.06/hr ($43.80/mo.)*
○	Standard Small	2 Cloud Compute Units, 2 virtual cores, 2GB RAM, 10GB disk	$0.06/hr ($43.80/mo.)*	$0.09/hr ($65.70/mo.)*	$0.09/hr ($65.70/mo.)*
○	Standard Medium	4 Cloud Compute Units, 2 virtual cores, 4GB RAM, 50GB disk	$0.12/hr ($87.60/mo.)*	$.18/hr ($131.40/mo.)*	$0.20/hr ($146/mo.)*
○	Standard Large	8 Cloud Compute Units, 4 virtual cores, 8GB RAM, 130GB disk	$0.24/hr ($175.20/mo.)*	$0.36/hr ($262.80)*	$0.34/hr ($248.20/mo.)*
○	Standard XL	15 Cloud Compute Units, 4 virtual cores, 15GB RAM, 270GB disk	$0.45/hr ($328.50/mo.)*	$0.72/hr ($525.60/mo.)*	$0.58/hr ($423.40/mo.)*

submit cancel

Fig 6:Resource allocation



WELCOME TO OUR SITE

siva

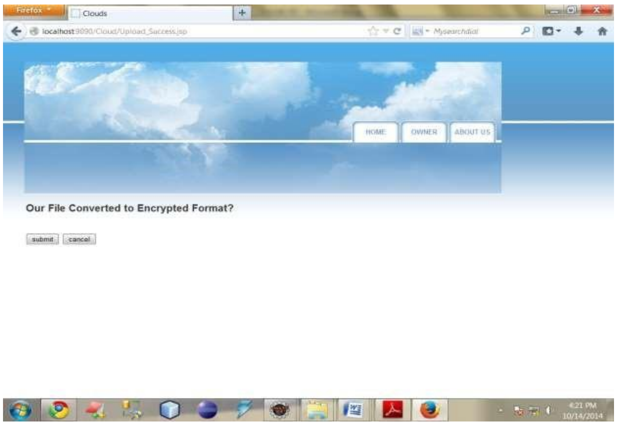
Now You Can Upload Your Files On Cloud

Upload Data Browse... ITJIM03.doc

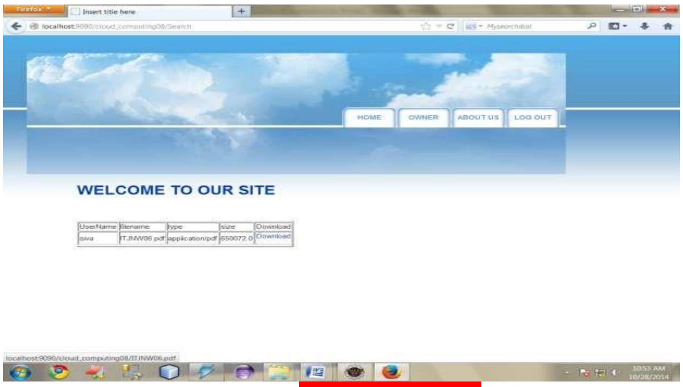
Key 8499

submit

Fig 7:Upload



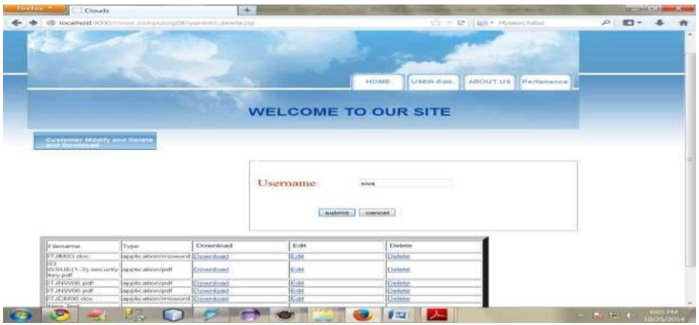
Our File Converted to Encrypted Format?


Insert title here
localhost:9090/cloud_computing08/Search
HOME
OWNER
ABOUT US
LOG OUT
localhost:9090/cloud_computing08/ITJNW06.pdf

WELCOME TO OUR SITE

UserName	filename	type	size	Download
siva	ITJNW06.pdf	application/pdf	550072.0	Download

Fig 8:Download

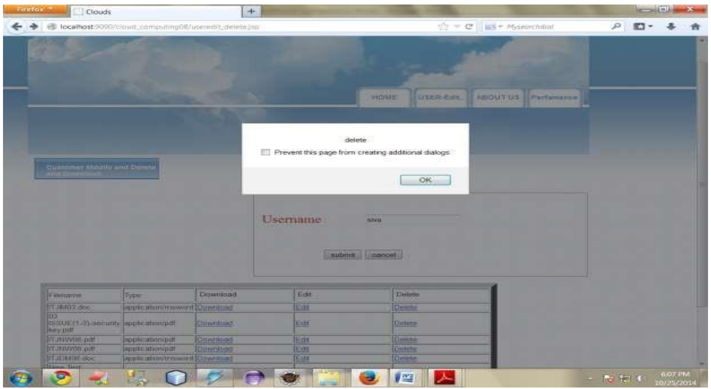

Clouds
localhost:9090/cloud_computing08/useredit_delete.jsp
HOME
USER-Edit
ABOUT US
Perfamence
Customer Modify and Delete and Download
submit
cancel

WELCOME TO OUR SITE

Username siva

Filename	Type	Download	Edit	Delete
ITJIM03.doc	application/msword	Download	Edit	Delete
03 ISSUE(1-3)-security key.pdf	application/pdf	Download	Edit	Delete
ITJNW08.pdf	application/pdf	Download	Edit	Delete
ITJNW06.pdf	application/pdf	Download	Edit	Delete
ITJDM06.doc	application/msword	Download	Edit	Delete
New Text				

Fig 9:User edit


Clouds
localhost:9090/cloud_computing08/useredit_delete.jsp
HOME
USER-Edit
ABOUT US
Perfamence
Customer Modify and Delete and Download
OK
submit
cancel

delete

□ Prevent this page from creating additional dialogs

Username siva

Filename	Type	Download	Edit	Delete
ITJIM03.doc	application/msword	Download	Edit	Delete
03 ISSUE(1-3)-security key.pdf	application/pdf	Download	Edit	Delete
ITJNW08.pdf	application/pdf	Download	Edit	Delete
ITJNW06.pdf	application/pdf	Download	Edit	Delete
ITJDM06.doc	application/msword	Download	Edit	Delete
New Text				

Fig 10: Status

Conclusion

The enhancement of the architecture that guarantees confidentiality of data stored in public cloud databases. The architecture does not require modifications to the cloud database. It is worth observing that experimental results based on the (Transaction Processing control) TPC-C standard benchmark show that the performance impact of data encryption. This also improves the performance of modifying the data using the edit operation. This architecture allows the user to acquire the forgotten key using the find key option only if the user gives the appropriate document name with the user password.Thus the information stored in the cloud is more secured.

References

[1].M. Armbrust et al., “A View of Cloud Computing,” Comm. of theACM, vol. 53, no. 4, pp. 50-58, 2010.

[2].W. Jansen and T. Grance, “Guidelines on Security and Privacy inPublic Cloud Computing,” Technical Report Special Publication800-144, NIST, 2011.

[3].A.J. Feldman, W.P. Zeller, M.J. Freedman, and E.W. Felten,“SPORC: Group Collaboration Using Untrusted Cloud Resources,”Proc. Ninth USENIX Conf. Operating Systems Design andImplementation, Oct. 2010.

[4].J. Li, M. Krohn, D. Mazie`res, and D. Shasha, “Secure UntrustedData Repository (SUNDR),” Proc. Sixth USENIX Conf. OpeartingSystems Design and Implementation, Oct. 2004.

[5].P. Mahajan, S. Setty, S. Lee, A. Clement, L. Alvisi, M. Dahlin, andM. Walfish, “Depot: Cloud Storage with Minimal Trust,” ACMTrans. Computer Systems, vol. 29, no. 4, article 12, 2011.

[6].H. Hacigu¨mu¨ s¸, B. Iyer, and S. Mehrotra, “Providing Database as aService,” Proc. 18th IEEE Int’l Conf. Data Eng., Feb. 2002.

[7].C. Gentry, “Fully Homomorphic Encryption Using Ideal Lattices,”Proc. 41st Ann. ACM Symp. Theory of Computing, May 2009.

[8].R.A. Popa, C.M.S. Redfield, N. Zeldovich, and H. Balakrishnan, “CryptDB: Protecting Confidentiality with Encrypted QueryProcessing,” Proc. 23rd ACM Symp. Operating Systems Principles,Oct. 2011.

[9].H. Hacigu¨mu¨ s¸, B. Iyer, C. Li, and S. Mehrotra, “ExecutingSQL over Encrypted Data in the DatabaseService-ProviderModel,” Proc. ACM SIGMOD Int’l Conf. Management Data, June2002.

[10]. J. Li and E. Omiecinski, “Efficiency and Security Trade-Off inSupporting Range Queries on Encrypted Databases,” Proc. 19thAnn. IFIP WG 11.3 Working Conf. Data and Applications Security,Aug. 2005.

[11]. E. Mykletun and G. Tsudik, “Aggregation Queries in theDatabase-as-a-Service Model,” Proc. 20th Ann. IFIP WG 11.3Working Conf. Data and Applications Security, July/Aug. 2006.

[12]. D. Agrawal, A.E. Abbadi, F. Emekci, and A. Metwally, “DatabaseManagement as a Service: Challenges and Opportunities,” Proc.25th IEEE Int’l Conf. Data Eng., Mar.-Apr. 2009.

[13]. V. Ganapathy, D. Thomas, T. Feder, H. Garcia-Molina, and R.Motwani, “Distributing Data for Secure Database Services,” Proc.Fourth ACM Int’l Workshop Privacy and Anonymity in the Information Soc., Mar. 2011.FERRETTIET AL.: DISTRIBUTED, CONCURRENT, AND INDEPENDENT ACCESS TO ENCRYPTED CLOUD DATABASES 445Fig. 9. TPC-C performance (latency equal to 40 ms). Fig. 10. TPC-C performance (latency equal to 80 ms).

[14]. A. Shamir, “How to Share a Secret,” Comm. of the ACM,vol. 22, no. 11, pp. 612-613, 1979.

[15]. M. Hadavi, E. Damiani, R. Jalili, S. Cimato, and Z. Ganjei, “AS5: ASecure Searchable Secret Sharing Scheme for Privacy PreservingDatabase Outsourcing,” Proc. Fifth Int’l Workshop Autonomous and Spontaneous Security, Sept. 2013.