Proposing DEM Model for Improving the Security of Data in Cloud Environment

Ankita Kaushik
Ph.D. Scholar,
Bhagwant University, Ajmer

Amit Kumar Chaturvedi, PhD
Assistant Prof., MCA Deptt.
Govt. Engineering College, Ajmer

ABSTRACT

Cloud computing, which is the most developing fields of computer science. Apart from many services of cloud computing like software, hardware, infrastructure, desktop as a service and database also available as a service. But along with these, issues regarding security of data or database are of most fear concerns. As cloud users are reluctant to save data on cloud servers, which can be hindrance to this super crucial field of computers. Now the need of the hour is to develop an understanding that storing data on cloud servers is safer and also develop some mechanisms to improve the security of data. New researches are coming up with innovative approaches to provide more safety to data. In this paper, a DEM [Data Encryption Model] Model is introduced with a new approach for data security mechanism. The field base encryption method is used in this model.

General Terms

DEM [Data Encryption Model], DBaaS [database as a Service], Cloud Computing

Keywords

Cloud, Security, Database, Service, DBaaS

1. INTRODUCTION

Cloud Computing is the now growing up field of computer science. Cloud computing deals with dynamically providing IT services (Software, Hardware and Services) from third parties to people. It gives services to users on pay-per-use or subscription based services to users. Cloud computing has many forms such as SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service) and also DBaaS (Database as a Service). Cloud gives enormous advantages to users as expenditure of capital and operational is now much less. Apart from these, availability of resources has increased, applications can be easily accessed and used, administrative costs reduction and lower maintenance. For economic benefit reasons, customers are now interested to outsource data more and more. The upcoming problems of security and trust in outsourcing data in cloud is now a major talk and has become an important concern for customers who are moving data to cloud [1] Cloud has many advantages but any person, who enters the system in order to steal crucial data can be dangerous. It can hamper the privacy of customer's data that have outsourced in cloud. So these situations need to be focused upon [2].

Data is the most important assets in today's scenario. It has provided with the new upcoming model like DaaS (Database as a Service). Through internet Database Service Providers (DSP) give database services to customers.

Many industries like education related and health related are moving towards cloud as just customers have to pay for subscription for the storage space and the processing and its

quite efficient. These all cloud services are being in use irrespective of privacy issues and challenges [3]. The issues of database storage on cloud servers in a secure manner are of major concern [4]. There are many favorable circumstances and also limitations in setting up data handling tasks .There are many database solutions available and all provides some sort of security but still new solutions are required. There is the research gap in storing data in a secure manner on cloud servers and hence need arises for some new solutions in this regard. [5]

2. NEED OF REQUIRED WORK

Among the cloud services, DBaaS or Database as a Service is considered one of the best services .For the storage purpose, most commonly used services are cloud databases. There are many upcoming techniques in the area of cloud databases and many applications are used for testing of applications [6]. As maximum resources are outsourced to cloud, so it becomes difficult to provide a check as for data maintenance. Cloud DBaaS are difficult to regulate as for security conditions are applied because they are spread across different places and many people access them [7]. Price and flexibility, improved availability is important factors while adopting of cloud databases. [8]. But issues are coming related to data theft and many a times data loss, because of that measures have to be taken so as to prevent any unwanted happening. For the purpose of cloud service processing and storage of crucial data, virtualization is required and far apart cloud service provider (CSP) can also create issues regarding privacy and security [9]. Because of database, problem of legal concerns, issues related to privacy matters and sharing of data arises. Sometimes it may happen that issues related to "owning of data" also come up [10].

3. RELATED WORK

Cloud Computing provides on demand network pool of resources. This paper deals with database services which are provided to customers known as Database as a Service (DBaaS). Nowadays people have more and more interest in outsourcing database and also economically it can be beneficial. Storing data locally is facing problems. Among many services, DBaaS is still an emerging field [11]. Here proposed architecture is SCALEDB which is cloud database architecture compatible with mysql. It discusses regarding cloud computing issues like multitenancy, speed and privacy and security [12]. Cloud Database Management System (CDBMS) deals with distribution of cloud database services to multiple customers through internet. E.g. Software as a Service (SaaS) [13]. Characteristics of cloud are given and it describes about different cloud structures. Also it discusses regarding CDBMS and providing and making up applications so as to enhance cloud services [14].

Cloud is a service provider and data can be stored. Database can be processed & computed also. This paper provides cloud

database architecture [15]. There are many upcoming new trends upcoming related to cloud database management which this paper highlights along with there are many positive and negative features of DBMS and also discusses structure proposed.[16] Nowadays demand arising of more availability, elasticity and pay according to usage and providing server, power, storage and bandwidth to users.[17] . Unstructured data is very difficult to manage in cloud database management system and here this paper discusses this issue that for managing cloud database object algebra concept is used [18]. Database in form of service has been now popularly being used now days just as in cloud computing .Various advantages and disadvantages have been talked upon. Much useful information about database in form of service has been discussed [19]. Multi-tenancy, privacy regarding database, and awareness in relation to distribution of load is being presented here. Scalability along with Relational Cloud features are described here [20].

4. PROPOSED MODEL

User gives the query to client. Client machine processes the query. Client includes framework for the query processor and a layer of encryption and decryption. As the form has been provided to operator (the person) to enter sql query according to user specifications .The form has been further explained to enter query. A simple query processor is here suggested which includes query parser, as studied it is the first stage of sql processing. The parser scans the query and checks for keywords and expressions etc. With the help of encryption engine or encryption/decryption layer, Query Rewriter again writes the query to encrypted format. Server can't access to encryption engine. Round Communication Handler present at client works with server for processing .Metadata Handler manages metadata or data about data at client. Arithmetic Engine manages over encrypted data. From Query Rewriter transforms to Query Manager at server and with the help of database engine it processes the query. Data is stored at server in encrypted form and is being processed in encrypted form. Result goes to client layer where encryption / decryption layer decrypts data and result is being given back to user.

5. EXPERIMENTAL RESULTS

Here as dot net framework is taken where forms have been provided to computer operator or user to enter data. Backend server is sql server. Here the first form is shown in figure 2

Encryption and Save Data Form. As we know to add new rows of data to table, we use Insert Query. Here we have provided Input Values section where placeholders for the column values of all the fields of Emp table like Empid, Empname, Deptname, Empsal and Empholiday are given. User or computer operator will enter all details and after entering these values user need to save them. But values to database as provided by computer operator /user are not directly entered, first we are encrypting all values. These values are shown in next figure in changed values column. On clicking on Save the values will go to database, the encrypted values will go to database .We have shown entered values which are encrypted in database in Figure 4 Encryption database .This is database of sql server. In Figure 3, the encrypted values which are saved to database are retrieved back to original form

6. ALGORITHM AND INTERFACES USED FOR IMPLEMENTATION OF THE DEM MODEL

Algorithm 1

ENCR (String Str)

Initialize A to " ";

FOR i=0 to String Length

Initialize n to 0

Initialize x to 0

Set n = Str[i]

If (n % 2==0)

 SET x= n*12;

    Else

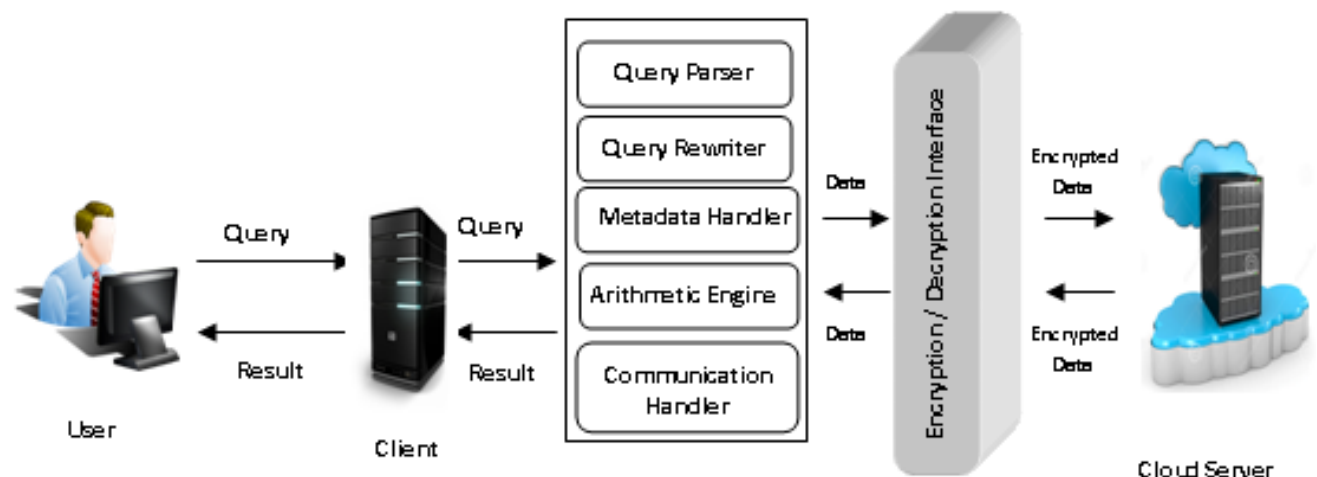   SET x = n *13;

        SET A= A+ x;

    Return A

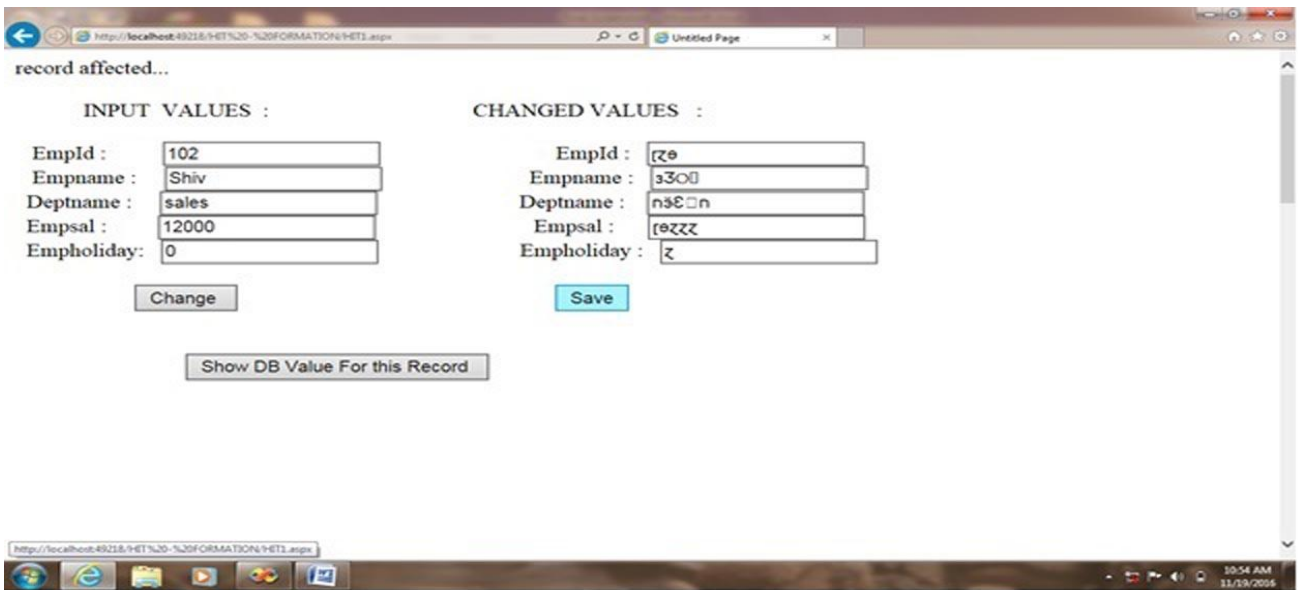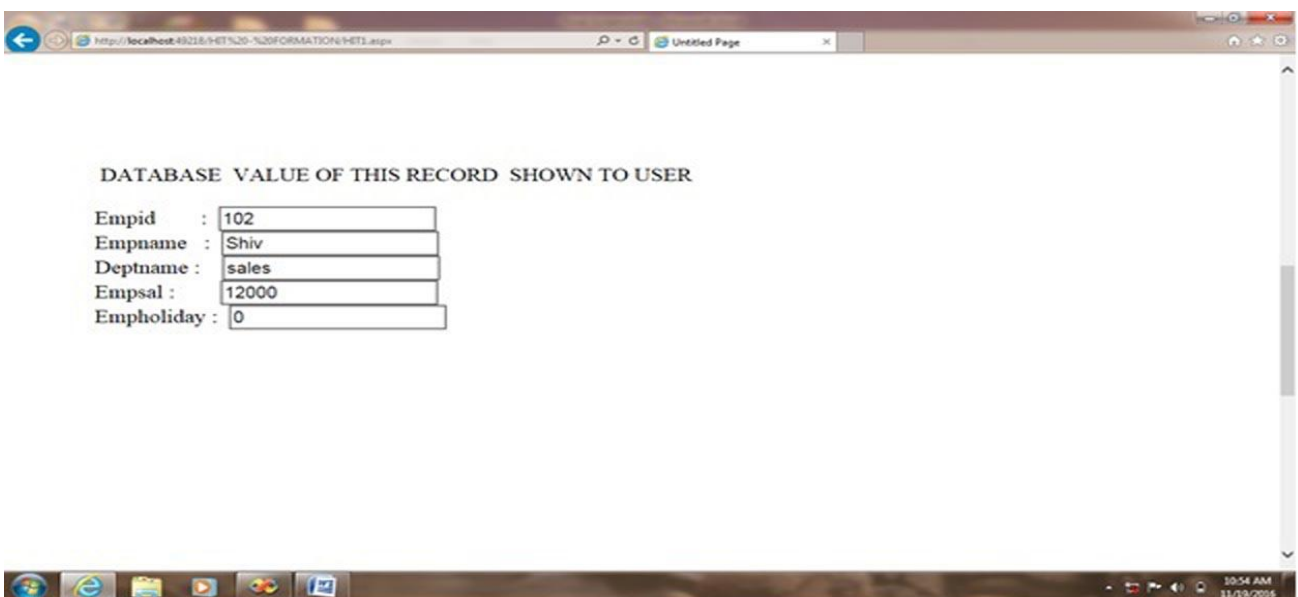
Fig 1: Data Encryption Model [DEM]

Fig. 2. Encryption & Save data form

Algorithm 2
DECR (String Str)

> Initialize A to " ";
>
> FOR i=0 to String Length
>
> > Initialize n to 0
> >
> > Initialize x to 0
> >
> > Set n ← Str[i]
> >
> > If (n % 2==0)
> >
> > > SET x← n/12
> >
> > Else
> >
> > > SET x← n /13
> > >
> > > SET A← A+ x
> >
> > Return A

Fig. 3. Database values decrypted
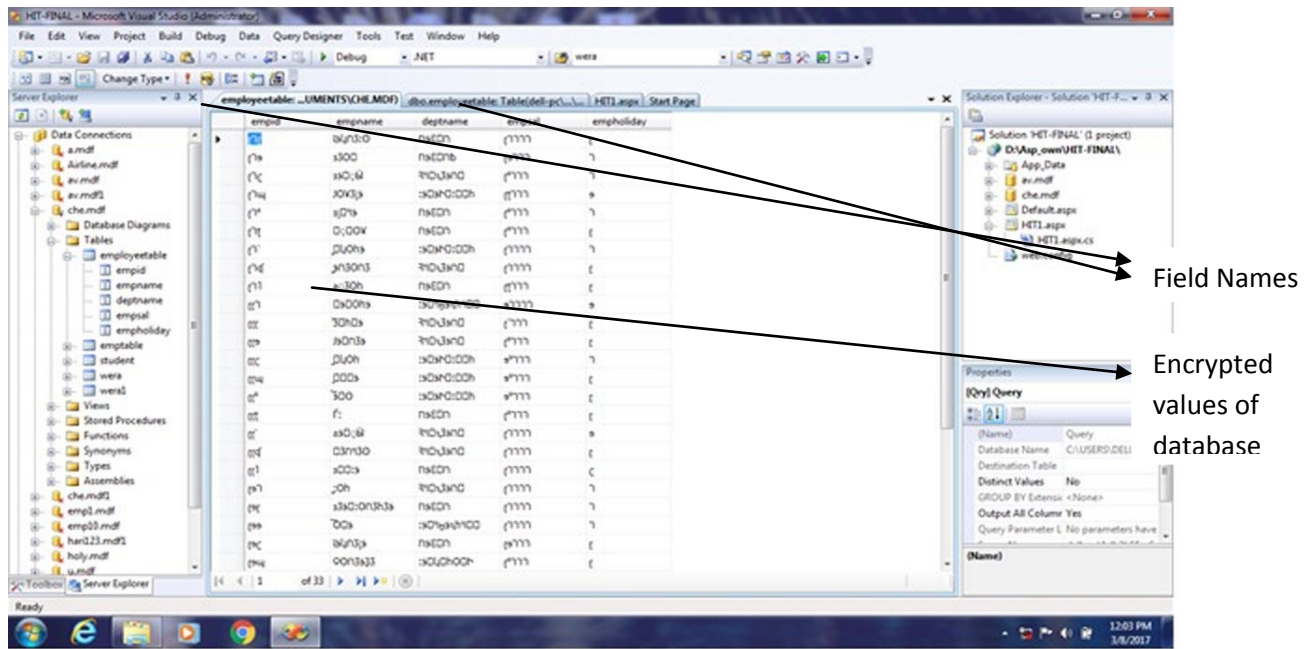
Fig. 4. Encryption database
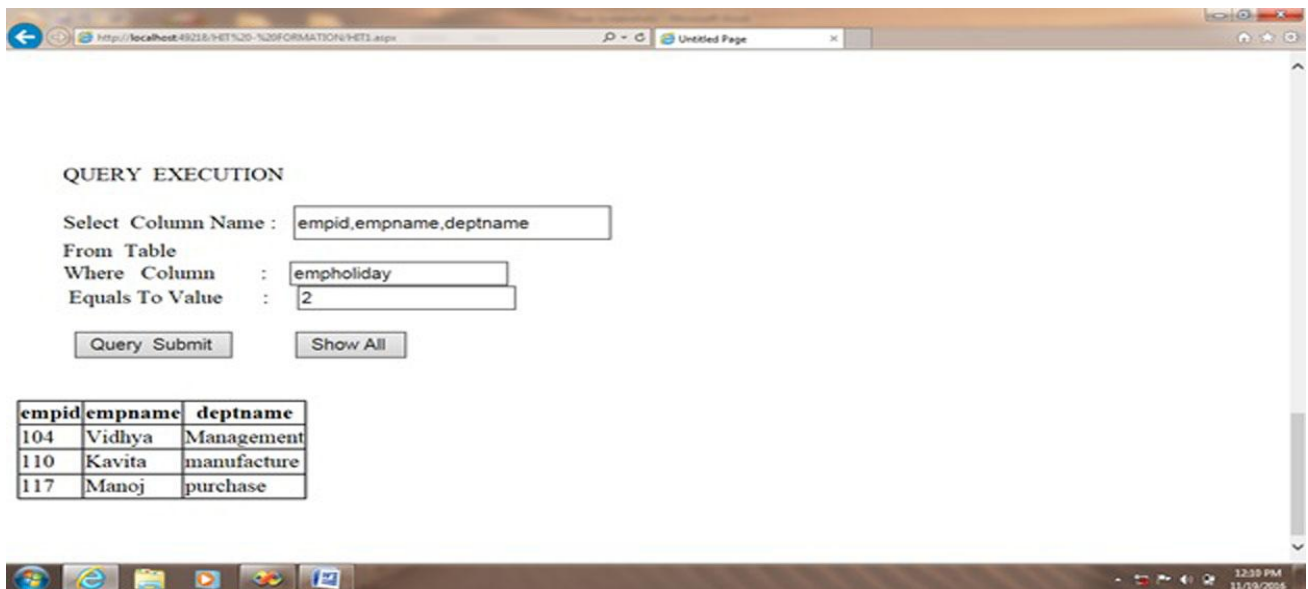

Fig. 5.1. Result

```
SHIFT_ON_SERVER ( )

{

        Declare txta1, txtb1,txtc1,txtd1,txte1;

        String ss;

        Set ss   <= "Insert into relation values
(txta1,txtb1,txtc1,txtd1,txte1)";

        Execute Query;

}

ShowData()

{

Relation dt;

        For i=0 to Rows_Count
```

```
For j=0 to Columns_Count

                dt.Rows[i][j]  <= decrypt(dt.Rows[i][j]);

}

QShow()

{

ss <= "select * from emptable";

showdata();

}
```

DEM Model uses encryption to make secure the data stored at server. Server is not assumed to be trustable so encryption decryption engine is placed at client. As user defined select query concept is introduced. This is executed at run time or dynamically. In figure query execution is shown as follows.
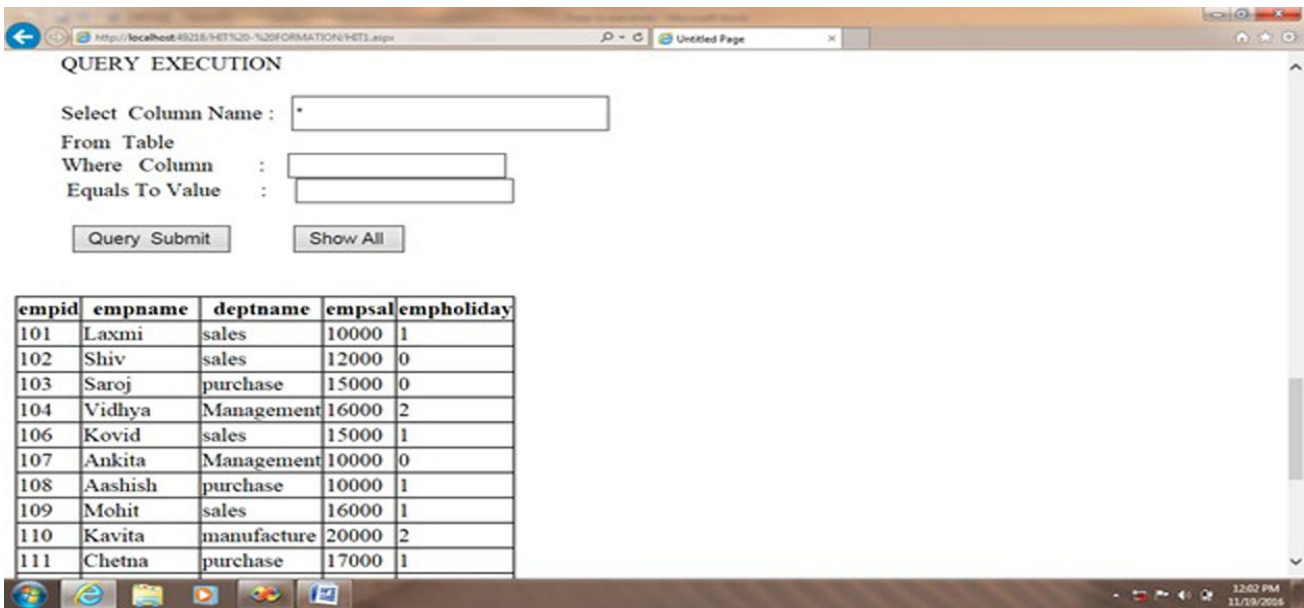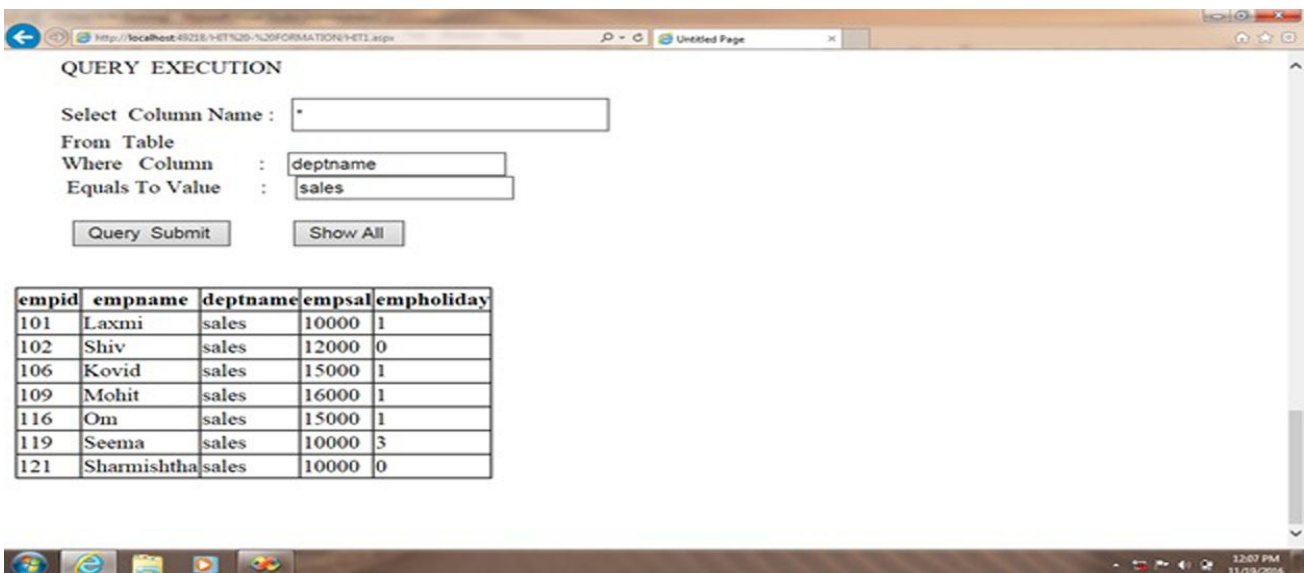
Fig. 5.2. Result

Fig. 5.3. Result

In figure 5.1, here query given is to display empid, empname and deptname of those employees whose holidays is 2 and the result is displayed, the table records can be seen. In figure 5.2 all records of table have been displayed. In figure 5.3, query given is to display all records whose department name is sales whose output is shown in figure.

In figure 5.1, here query given is to display empid, empname and deptname of those employees whose holidays is 2 and the result is displayed, the table records can be seen. In figure 5.2 all records of table are displayed. In figure 5.3, query given is to display all records whose department name is sales whose output is shown in figure.

7. CONCLUSION AND FUTURE SCOPE

Cloud computing offers many advantages over traditional computing. Data stored is accessible, available, and handled by cloud service providers once outsourced. Cloud services are many as SaaS, PaaS, DaaS, IaaS, and DbaaS on which many customers are relying for daily work. Positive aspects of cloud are there, but issues regarding security, control and privacy are coming up because users fear in setting up all data in cloud, so the most important is data to be secured. Here DBaaS have been discussed and a DEM model [Data Encryption Model] has been presented with some algorithms and have implemented it for testing as given above in the paper.

According to the DEM model, data on server has been saved on and retrieved from server successfully, according to customer's choice or as per requirements.

In future, researchers may work more on attribute based or record based encryption on database. Now work related to insertion, sorting, and retrieval has been done. Insert query and select query was in use. More database related tasks like updation and modification can be added up .As security tasks are already implemented with the help of encrypted database but in future more security related works can be added as per requirements. Secure Reports generation is also important an important task for future.
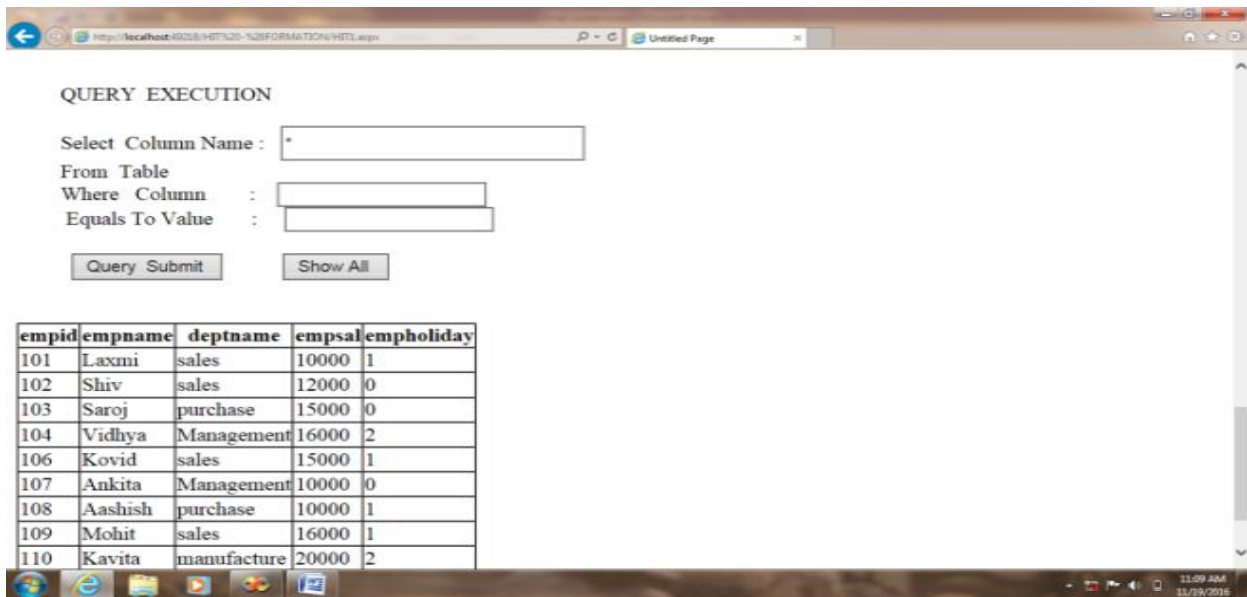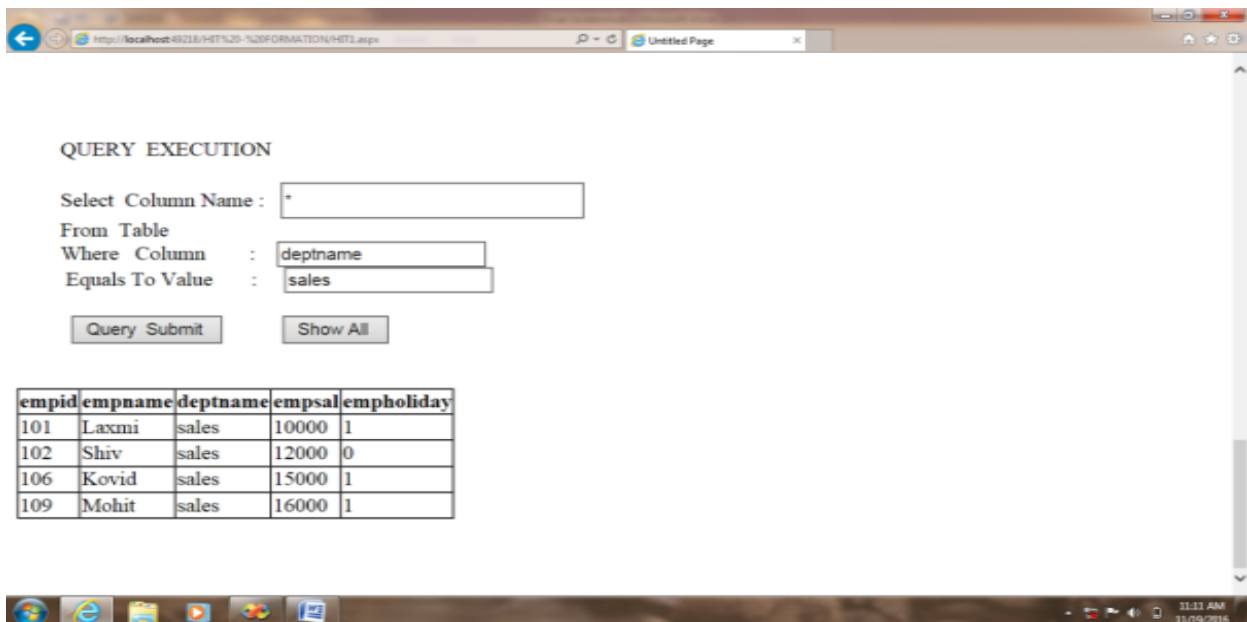
Fig. 5.2. Result

Fig. 5.3. Result

8. ACKNOWLEDGMENTS
We are thankful for all people who gave their suggestions to improve the contents of this paper.

9. REFERENCES
[1]. Jianfeng Yang, Zhibin Chen, Cloud Computing Research and Security Issues, IEEE 2010, 978-1-4244-5392-4/10 ,(2010)

[2]. Prince Jain, Security Issues and their Solution in Cloud Computing, Proceedings of 'I-Society 2012' at GKU, Talwandi Sabo Bathinda (Punjab),International Journal of Computing & Business Research, ISSN (Online): 2229-6166, 2012

[3]. Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy, Cloud Computing : Security Issues and Research Challenges, ISSN: 2249-9555, IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011

[4]. Indu Arora1 ,Dr. Anu Gupta, Cloud Databases: A Paradigm Shift in Databases, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 3, July 2012, ISSN (Online): 1694-0814, www.IJCSI.org

[5]. Daniel J. Abadi, Data Management in the Cloud: Limitations and Opportunities, Bulletin of the IEEE Computer Society Technical Committee on Data Engineering, 2009 IEEE.

[6]. Monica Kadam, Shubhangi Tambe, Pooja Jidge, Ekta Tayade, Cloud Service Based On Database Management System, Pooja Jidge et al Int. Journal of Engineering Research and Applications, ISSN : 2248-9622, Vol. 4, Issue 1(Version 3), January 2014, pp.303-306, www.ijera.com

[7]. Rahul Bhoyar, Prof. Nitin Chopde, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 3, March 2013, ISSN: 2277 128X

[8]. T. Alford, G. Morton, The Economics of cloud computing, Booz Allen Hamilton,2009

[9]. N.G. Carr, The end of corporate computing, MIT Sloan Management Review 46 (3) (2005) 67–73

[10]. Yatharth Bhatnagar, Sarwesh Sethiya, Siddharth Jain, DBMS as a Cloud Service, Department of Computer Science Engineering,Yatharth Bhatnagar et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014,3052-3054,ISSN:0975-9646

[11]. Ylber Januzaj, Jaumin Ajdari, Besnik Selimi, DBMS as a Cloud service: Advantages and Disadvantages, Ylber Januzaj et al. / Procedia - Social and Behavioral Sciences 195 (2015) 1851 – 1859, World Conference on Technology, Innovation and Entrepreneurship, doi 10.1016/j.sbspro.2015.06.412, www.sciencedirect.com

[12]. Yvette E. Gelogo, Sunguk Lee, Database Management System as a Cloud Service, International Journal of Future Generation Communication and Networking Vol. 5, No. 2, June, 2012

[13]. P. Malliga, Database Services for Cloud Computing – An Overview, International Journal of Computers & Technology, Volume 2 No. 3, June, 2012,ISSN: 2277–3061 (online),w w w . i j c t o n l i n e . c o m

[14]. Monica Kadam, Pooja Jidge, Shubhangi Tambe, Ekta Tayade, Vrunda Bhusari, Cloud Database Management System (CDBMS),International Journal Of Scientific Research And Education, Monica Kadam et al. IJSRE Volume 2 Issue 3 March 2014 ,Volume 2 Issue 3 ,Pages 414-420,2014, ISSN (e): 2321-7545,Website: http://ijsae.in

[15]. Snehal B. Shende, Prajakta P. Chapke, Cloud Database Management System (CDBMS) ,COMPUSOFT, An international journal of advanced computer technology, 4 (1), January-2015 (Volume-IV, Issue-I),ISSN:2320-0790

[16]. R. Arokia Paul Rajan, S. Shanmugapriyaa, Evolution of Cloud Storage as Cloud Computing Infrastructure Service, IOSR Journal of Computer Engineering (IOSRJCE) ISSN : 2278-0661 Volume 1, Issue 1 (May-June 2012), PP 38-45 ,www.iosrjournals.org

[17]. Mansaf Alam, Cloud Algebra For Handling Unstructured

[18]. Data In Cloud Database Management System, International Journal on Cloud Computing: Services and Architecture (IJCCSA),Vol.2, No.6, December 2012

[19]. Waleed Al Shehri, Cloud Database As A Service, International Journal of Database Management Systems (IJDMS) Vol.5, No.2, April 2013, DOI : 10.5121/ijdms.2013.5201, International Journal of Database Management Systems (IJDMS) Vol.5, No.2, April 2013

[20]. Carlo Curino, Evan P. C. Jones, Raluca Ada Popa, Nirmesh Malviya, Eugene Wu, Sam Madden, Hari Balakrishnan, Nickolai Zeldovich, "Relational Cloud: A Database-as-a-Service for the Cloud, Curino, Carlo et al. "Relational Cloud: A Database-as-a-Service for the Cloud", 5th Biennial Conference on Innovative Data Systems Research, CIDR 2011, January 9-12, 2011 Asilomar, California.