International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 12 | Dec -2016 www.irjet.net p-ISSN: 2395-0072

# Data security at hard disk level

**Mrs Poonam Khare**

*M.Tech NIT, Bhopal*

*Associate Professor, Department of Information Technology*

*MLR Institute of Technology, Hyderabad, Telangana, India*

---

**Abstract -** *Data is the most valuable asset in today's world as it is used in day-to-day life from a single individual to large organizations. With high demand of security several methods have been developed which help in achieving security to a certain extent but they are lacking somewhere or the other. Most of the work is done in the field of encryption but encryption lacks in providing security in the case of theft of the Hard disk because in case of encryption both data and key are kept in hard disk and if hard disk is lost or given for repairing ,data can be easily retrieved. Therefore the main aim of this paper is to provide security to database in cases of Hard disk theft and corrupted hard drive.*

***Key Words*: Hard disk, security, data loss etc**

## 1. INTRODUCTION

Security a major concerned area. Lots and lots of work is going on, in this area. There are different cases were we are entitled to have data loss due to loop holes in our security methods for example consider a case when we send our computer for repair when the hard disk is still working—either the drive works intermittently or your hard drive isn't the issue requiring repair. If you are concerned about data security and your hard disk is still functioning, you should back up your important data and use the secure erase functions in Disk Utility (described below) to reformat your drive before sending in your computer for service. Other instance is when our hard disk gets stolen. In both the cases our data can be easily lost and misused by an unauthorized person. And hence, an unauthorized person can gain access and manipulate valuable data.

## 2. Related work

In paper [2] proposed fully functional identity based encryption scheme. In paper [3] author proposed advanced cryptography algorithm for improving data security. In paper [4] proposed honey encryption mechanism. Therefore conclusion is that in the existing system, Encryption can provide strong security for data at rest, but developing a database encryption strategy must take many factors into consideration, For example, where

Should be performed the encryption, in the storage layer, in the database or in the application where the data has been produced?

How much data should be encrypted to provide adequate security?

What should be the encryption algorithm and mode of operation?

Who should have access to the encryption keys?

How to minimize the impact of database encryption on performance?

The problem still persists while the data is being recovered from a stolen hard disk or a corrupted hard drive.

## 3. Problem formulation

In the existing system, database security is being provided using Encryption and Cipher keys. But in a situation of Hard Disk theft or corrupted hard Drive, Encrypted data can be retrieved during the data recovery process as the key and data are at the same place the "hard disk". Therefore there is need for a system where we can secure data even in the cases of theft of hard disk.

## 4. Proposed work

The development of this new system's objective is to provide the solution to the problems of existing system. By using this new system, we can provide complete security to the database in the above stated situations.

### 4.1 Highlight of the paper

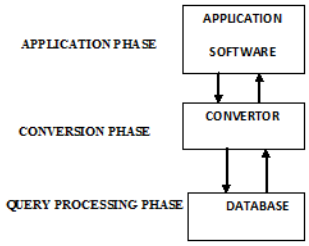
Our solution works at three levels.

1) Module 1/ application phase /image lite which is a front end made in java , this module is actually visible to the user , whatever data they want to retrieve they can easily retrieve through this module while writing queries. It has user authentication and also is password protected.

2) Module 2 is the conversion phase where the text data is converted to binary form or vice-versa.

3) Module 3 is the phase where data is actually stored that is in oracle. Data here is stored in binary form.

### 4.2 PHASES OF THE PROPOSED MODEL




### 4.3 PROPOSED ALGORITHM

1) Design application software in java which acts as a front end to the user for writing queries and fetching results. This software should be password protected i.e. user authentication and password is required to give access to the authorized user. By giving the feature of user authentication and password for valid user we are able to achieve the first level of security.

1a) User first validates that it is a valid user or not by entering his/her username and password. If it is valid then user getting access to this phase.

1b) User then enters his/her query in phase. User is totally unaware of the back process which is going on. He/she gets the results of their queries here only.

1c) now this application phase sends this query to convertor phase.

2) Designing a convertor which converts text data to binary data and binary data to text data. This phase is required because when user fires a query it is in text form but when this query is processed it is in binary form. Refer to the fig 4.4

2a) when convertor phase fetches this query it converts it to binary form and send to database phase.

3) Database phase: Storing of data in ORACLE/ SQL SERVER etc. Processing of data takes place during the third phase, which only reads binary information.

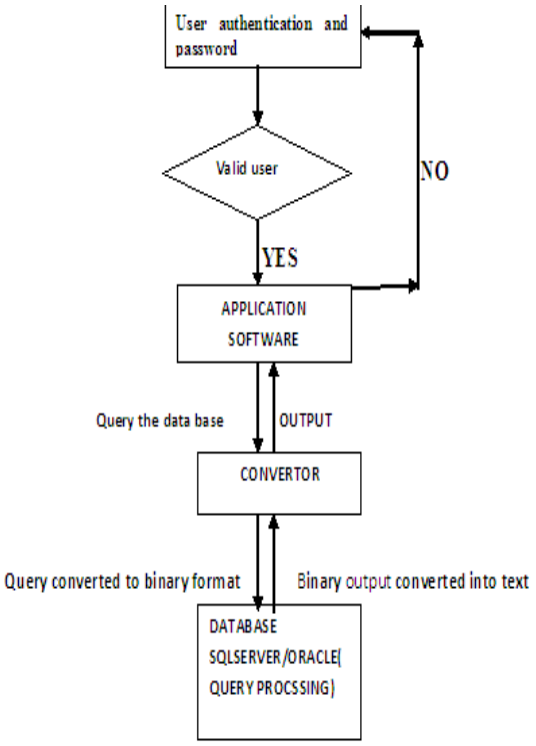
3a) When database gets the query in binary form it processing the query and gives the result in binary form.

3b) Now it send back this binary data back to convertor phase

4) Convertor phase fetches that data ,convertors back to text.

5) Convertor phase now sends back that data to application phase where the user sees the result.

### 4.4 FLOWCHART




## 5. Conclusion

This paper proposes a method in which in case of hard disk theft our data can't be misused by any other unauthorized person because of following reasons: First in the hard disk data is in binary form and to get the data, a person needs both convertor and an application software .Secondly application is kept on server so only authorized user has its

accessibility. Therefore we can conclude that proposed method will be more effect full in case of hard disk theft because in encryption methods both data and key are kept in hard disk so it is easy to retrieve while in this case until and unless a person has application software and authorization he/she won't be able to use the hard disk data.

## 6. References

1)https://support.apple.com/en-s/HT 201857

2)"Identity based encryption from Weil pairing "authors Dan Boneh, Mathew Franklin in 2001. http://crypto.stanford.edu/~dabo/papers/bfibe.pdf

3)"Advanced cryptography algorithm for improving data security" Vishwa gupta,Gajendra Singh,.Ravindra Gupta in IJARCSSE, Volume 2, Issue 1 , Jan-2012

4)Shelly Rohilla, Pradeep Kumar Mittal, "Database Security: Threats and Challenges" International Journal of Advanced Research in Computer Science and Software Engineering,
Volume 3, Issue 5, May 2013 ISSN: 2277 128X

5) Meg Coffin Murray, "Database Security: What Students Need to Know", Journal of Information Technology Education: Innovations in Practice, Volume 9, 2010

6)Mohammed Rafiq, "Database Security Threats and Its Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 2, Feb 2014 ISSN: 2277 128X

7)http://www.crazyengineers.com/

8)http://www.ijarcsse.com/

9) http://www.engpaper.net/

10)http://www.java-tips.org/

11)http://www.stackoverflow.com/

12)http://wikipedia.com/