

# Challenges and Security Vulnerabilities to Impact on Database Systems

Hassan B. Hashim\*

Middle Technical University, IRAQ.

\*Author email: [hassan.bediar@yahoo.com](mailto:hassan.bediar@yahoo.com)

## Article Info

Received  
08/11/2017

Accepted  
07/01/2018

## Abstract

At present, a lot of institutions depend on the systems database operations and their daily activities, thus providing a means for the maintenance of permanent data can refer to it at any time, as well as to search and to modify the data easily. In this paper determine the security challenges in the databases and the requirements necessary to address those challenges in the data value to provide security base, and to determine the security rules and know the weaknesses that can be exploited any information in a manner not allowed, when he must protect the database to make sure of the following purposes: confidentiality, integrity and continuity. One of the solutions used in this research to protect databases, encryption of sensitive data, adjust the system databases, and updates the database systems and we review some of the ways to address these challenges in the security databases.

**Keywords:** Security, databases, weaknesses, challenge.

## الخلاصة

هناك الكثير من المؤسسات التي تعتمد في الوقت الحاضر على عمليات قاعدة بيانات النظم وأنشطتها اليومية، مما يوفر وسيلة للحفاظ على البيانات الدائمة يمكن الرجوع إليها في أي وقت، وكذلك للبحث وتعديل البيانات بسهولة. في هذه الورقة لتحديد التحديات الأمنية في قواعد البيانات والمتطلبات اللازمة لمواجهة تلك التحديات في قيمة البيانات لتوفير قاعدة أمنية وتحديد قواعد الأمن ومعرفة نقاط الضعف التي يمكن استغلالها بأي معلومات بطريقة غير مسموح بها، عندما يجب حماية قاعدة البيانات للتأكد من الأغراض التالية: السرية، النزاهة والاستمرارية. واحدة من الحلول المستخدمة في هذا البحث لحماية قواعد البيانات، هي تشفير البيانات الحساسة، وضبط قواعد بيانات النظام، وتحديث أنظمة قواعد البيانات ونحن نستعرض بعض الطرق لمعالجة هذه التحديات في قواعد بيانات أمنة.

## Introduction

The world is a state of change and development and advancement of clear and widespread in many areas, these areas of databases that hold the largest share databases play an important role in the economic and social due to its control of high conservation and storage aimed at real speed in find the result without any trouble. This is the true essence of who aspires his electronic world, this world-mail shorten us the true concept of databases is a (set of fixtures the same or different, consisting database from one table promised schedules branching these tables even arise fields, and so on). In this way, supports databases private sector or the public in the tasks of their business and setting method and screening for either groups or individuals, this effort is through the engine data that amendment and

deletion, search, and added, and on the whole remain human resources expertise defended to develop databases of everything, and this great development in the databases did not overlook the importance of a high degree of safety and validity of the grant each user cannot bypass. It was noted that most of the databases are known worldwide: MSSQL and Oracle. The assurance and security of databases is a key necessity and applies to every one of the principles connected by the general population in their dealings with that data inside the data framework and oversees them, when you concentrate on the insurance of databases, specifically, the assurance of databases is standout amongst the most imperative improvements in the arrangement of security, the more noteworthy the identification of information on the system which has turned out to be more defenseless

against outside assault, and turn into a wellspring of consistent worry for the expansive number of episodes of loss of data or interruptions are not permitted private data and critical. The security of the database is the framework, procedures, and systems that ensure the databases of the exercises and the operations are not allowed with hazard recognizable proof, assurance purposes, resident insurance, designs essential assurance, and techniques for the counteractive action of hazard can be arranged, action is alluring to: (1) Misuse of data, (2) Malicious assaults on the data, and (3) Errors or unintended operations by approved individual's entrance to databases. The endeavor database framework is liable to a staggering scope of dangers. This "paper" is expected to enable associations to manage the most disparaging of those dangers by giving a rundown of the best ten database vulnerabilities as distinguished by Application Defense Center (ADC), foundation data, general hazard moderation procedures, and secure sphere database security gateway [1].

### Problem Statement

Some of the security vulnerabilities in the databases are caused by software errors, some are structurally weak and any structural system is very important. Configuring system rules improper, configuration and setup of the wrong database system can directly affect system security and external attacks resulting from unsafe authorization privileges.

### Research Objectives

The objectives of this paper are to identify and process three primary sources of vulnerability security in databases:

- The gaps in database management systems often by programming errors and gaps in computer system.
- To improve the structure of weaken system databases by considering any structural system of very important things.
- Evaluate the configuration and the setup of rules of the system.

### Literature Review

In this study, Sandhu, R.S., & Jajodia, S. (2013) shows that the integrity principles can be divided into two groups as follows: on the basis of how well existing DBMS mechanisms can support them [2].

While the study of I. Bacharach, F. Azam, A. Mustafa. (2012) conclude the issues and dangers in the security of the database and database security necessities. Furthermore, they pose a question of how to utilize encryption at various levels to give high security [1].

Murray, M. C. (2010) shows an arrangement of sub-subjects that may be incorporated into a database security segment of such a course. Mapping to the three develops of information security; these subjects incorporate access control, application get to, helplessness, deduction, and evaluating instruments [3].

According to, Franqueira, V. N., van Cleeff, A., van Eck, P., & Wieringa, R. (2010) propose external insiders in which add challenges to the already known insider threat problem because external insiders, unlike outsiders, have granted access and are trusted; and external insiders, unlike traditional insiders, are not subjected to as many internal controls enforced by the organization for which they are external insiders [4].

The study of S. Agrawal, S., Chaudhuri, S., Das, A., & Narasayya, V. (2003) presents an end-to-end solution to the problem of selecting materialized views and indexes. The describe results of extensive experimental evaluation that demonstrate the effectiveness of our techniques. Our solution is implemented as part of a tuning wizard that ships with Microsoft SQL Server 2000 [5].

### Database Security Threats

With the most basic, those dangers are giving a rundown of the main ten database vulnerabilities. Foundation data, general hazard alleviation methodologies, and Secure Gateway assurances are accommodated every danger as shown in Figure 1 [1].

### Excessive Privilege Abuse

All clients or vast gatherings of clients are allowed nonspecific default get to benefits that far surpass particular employment necessities.

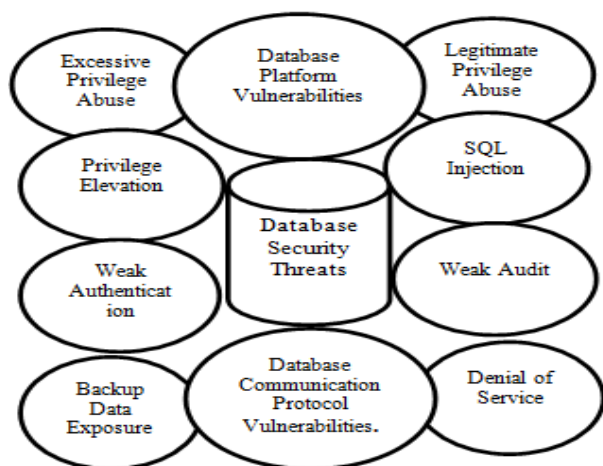


Figure 1: Database Security Threats

## Legitimate Privilege Abuse

Real privilege abuse (RPA) has two dangers to consider: The first is the rebel laborer who is ready for cash. The second (and maybe more typical) is the careless representative that recovers and stores a lot of data to their customer machine for true blue work purposes.

## Privilege Elevation

Assailants may exploit database stage programming vulnerabilities to change over get to benefit from those of a conventional client to those of a head.

## Database Platform Vulnerabilities

The blaster worm, for instance, exploited a Windows 2000 powerlessness to make refusal of administration conditions.

## SQL Injection

These infused proclamations are then passed to the database where they are executed. Utilizing SQL infusion, assailants may increase unhindered access to a whole database.

## Weak Audit

Trail weak database review arrangement speaks to a genuine hierarchical hazard on many levels.

## Denial of Service

Dissent of Service (DOS) is a general assault class in which access to organize applications or information is denied to proposed clients.

## Database Communication Protocol Vulnerabilities.

The developing number of security vulnerabilities are being distinguished in the database correspondence conventions of all database sellers.

## Weak Authentication

Powerless validation plans enable assailants to expect the personality of authentic database clients by taking or generally getting login accreditations.

## Backup Data Exposure

Reinforcement database stockpiling media is regularly and totally unprotected from assault. Few prominent security ruptures have included robbery of database reinforcement tapes and hard circles. This latter is happen by tending to these best ten dangers, associations will meet the consistence and hazard moderation prerequisites of the most managed ventures on the planet.

## Example

There is an alternative framework in Oracle databases called "REMOTE\_OS\_AUTHENT". If it is set to true value, esteem will be considered as unapproved individuals to enter the system, consider Figure 2.

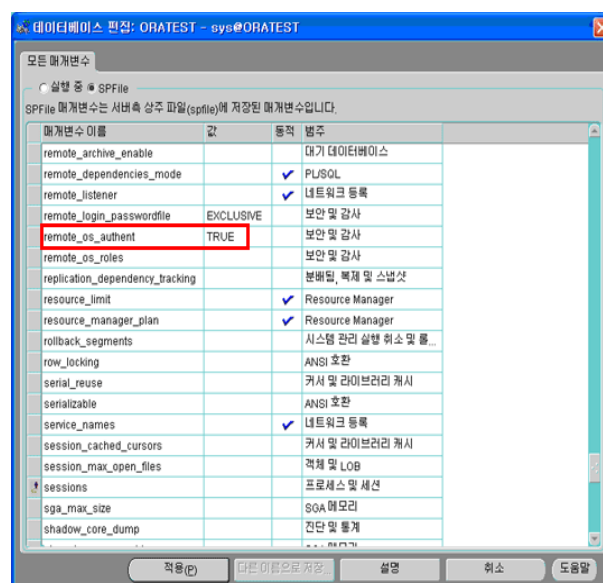


Figure 2: Option Remote\_os\_authent

## Database Technologies

The investigation on all or large database advances. The advances of information and data administration are a vital and dynamic research field. As of late, in many energizing outcomes, security in this day and age is one of the imperative difficulties that individuals are confronting everywhere throughout the world in each part of their lives. The utilization of database is ending up essentially in the present undertaking and databases contain data that is real endeavor resource. The subject of information security and controls are fundamentally with regards to Database Management Systems (DBMS). The accentuation is fundamental standards and instruments, which have been effectively utilized by experts in real items and frameworks. Where proper, the constraints of these systems are likewise noted. In the more point by point contemplations constrain ourselves particularly to social DBMS. The target of information security can be partitioned into three particular, yet interrelated, Areas as takes after, (1) Secrecy is worried about ill-advised revelation of data, and (2) Integrity is worried about shameful adjustment of data or procedures, and (3) Availability is worried about dishonorable disavowal of access to data [6].

Database Migration, a Literature Review, and Case Study provide an overview of various areas of research in database migration between different database security models [7-13].

The general objective of this paper is to give a writing audit of a portion of the key territories in relocation research, and to talk about the importance of that exploration to a 46 particular contextual analysis with information movement on such subjects as movement instruments, and figuring out. Essayist unique gives easier GUI or electronic help. Likewise, there are additionally various contextual analyses that framework approaches that clients have connected in relocating starting with one framework or stage then onto the next. Some contextual analyses include particular seller innovations, while others include hierarchical particular advances that have been produced with the expectation to

help with a specific issue in database movement.

The database security encryption access control in real security issues confronted databases are recognized and some encryption techniques are examined that can lessen the assaults chances and ensure the delicate information. It has been presumed that encryption gives secrecy however give no confirmation of honesty unless we utilize some computerized mark or Hash work. Utilizing solid encryption calculations decreases the execution. The future work could be done make encryption more compelling and productive:

- The best encryption calculation utilized as a part of the blended cryptography database on execution and security viewpoints.
- Second access control strategies used to control access for all equalities utilizing the database.
- Ordering and joining between various databases [6].

The Chinese analysts who are working in the United States have submitted reviews compact and covering the advance, they have in spite of the way that such an exertion would draw in an ever increasing number of scientists, especially in China, to enter inside the database and research to reinforce collaboration and concentrate the methods of principles information, or all the more by and large, information administration strategies and data, is an imperative field of research and dynamic. As of late, has been accounted for a few fascinating outcomes, (1) Automatic Database Tuning and Administration, for instance, building lists and appeared enhance the execution on a given inquiry workload, the cost of equipment has dropped, (2) Integrating Information from Heterogeneous Data Sources: Intensive research has been led on challenges that emerge in information reconciliation. The principal challenge is to help Interoperability of sources, which have diverse information models (social, XML), outline, and questioning interfaces, (3) Mining Changes from Data Streams, For instance the Emerging examples portray he changes from one informational collection to the next, (4) Aggregation Query Processing: The determination inquiry has been

one of the most broadly utilized inquiries in databases, and (5) Clustering Biological Data: when all is said in done, bio-data intends to take care of muddled natural issues, e.g., quality administrative system acceptance theme disclosure, and so on with computation algorithms [8].

### Principles and Requirements Security

- There are many principles and requirements adopted by the information security to protect users' information and institutions, and how to protect this information. The purpose of the protection of any part of the information was in the database or other to make sure of the following purposes [9].
- Secrecy (confidentiality) they ensure that the data is not unveiled nor seen it before by individuals are "not" permitted to do as such.
- Integrative and honesty of substance (trustworthiness) they ensure that the substance of the data has not been appropriately balanced or messed with, and specifically, won't be substance to wreck or change through unlawful impedance.
- The coherence of the accessibility of data or administration (accessibility). They ensure that the client data would not be utilized to deny them or enter them.

### Protection Technology Database

Each system even if he was working behind the effective security systems must be found by the gaps can be used to circumvent the access to the data. As an example, there are methods to circumvent a method known injects the command vehicle (SQL Injection) own databases, which are a method for endeavoring to alter a request sent from the web server to the database.

#### A. Adjust the framework databases

- Make beyond any doubt to scratch off or change all records or client names virtual emerging amid the way toward introducing the framework.

- Not to acknowledge association demands from problematic sources.
- Adjust the quantity of fizzled endeavors to enter the framework, for instance, /after three unsuccessful endeavors to enter the framework won't acknowledge endeavors from following an indistinguishable substance so from to keep the utilization of the strategy for speculating the watchword.

Disable the summon Ping organizing so as not to permit the gadget that contains a database framework to react to the solicitations of this issue, and this prompts an absence of strengthening endeavor to impair the framework by the wrong use for the charge Figure3, The order Ping .

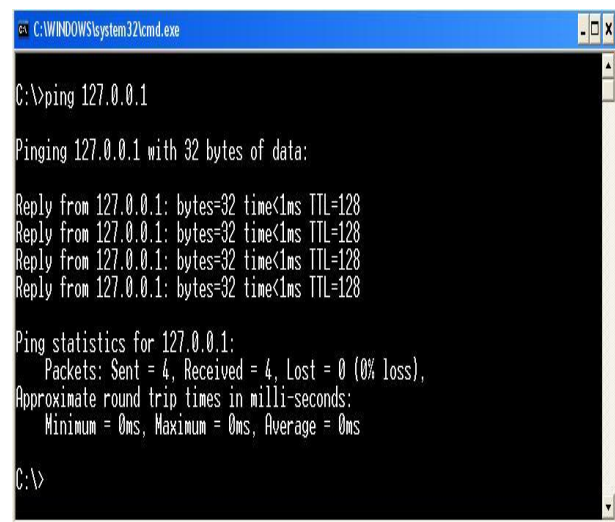


Figure 3: the command Ping

#### B. Update database system

The bugs and escape clauses in the principles of information from sources that debilitate the security of the framework, so it is critical and important to take after the new updates and got by the result of the framework and its establishment, if accessible.

#### C. Use to characterize the benefits and intends to utilize Access Control Methods

Along these lines, we can characterize the forces and extent of the client to get to the information in view of the client's personality. There are two known techniques can be utilized.

- **Mandatory Access Control**  
(Required Access Control) to be specific, that the client cannot allow access to the information to another client, so it is of the most stringent.
- **Access control in view of parts**  
(Part Based Access Control) It is conceded the specialist to tie to particular parts or positions (les as opposed to giving the) expert to tie specifically to the client, so along these lines the client gets every one of the forces in the part attributed to it.

#### D. The utilization of other security arrangements

You can get higher productivity through the utilization and advantage of security arrangements and other understood case of these arrangements: firewalls and discovery frameworks and interruption avoidance.

#### E. Checking the data in the system logs

Database systems contain mechanisms for the registration system Mai PEOPLE him from activities with the recording date and time for these exercises, and review the records of important steps to see if there was a breakthrough or even trying to get through the system [10].

#### F. Encryption of touchy information

The information encryption is one of the viable security answers for ensure data databases, however it can be a wellspring of issues if not utilized appropriately, there are three approaches to encode databases: (1) Encryption at the level of database documents: thusly is scrambled database records are completely at the level of capacity, (2) Encryption at the level of the sections in the database tables, thusly is scrambled fields in spreadsheets in view of the segments to which they have a place, and (3) In along these lines the information is encoded by the product application and not by the database framework, before putting away the information, the program scrambles the information itself. What's more, information encryption process is not an answer is basic to the insurance of databases, yet in a portion of the accompanying cases, (1) Prevent illicit access to the information, (2) Reduce the danger of robbery of records containing this information, and (3) Prevent approved clients from survey information is not permitted to see them, show Table (1) and Table (2).

The Penetrator enter in the password field '%OR username LIKE" Thus, it becomes the sender in the program to inquire about the password SELECT \* FROM username LIKE " WHERE username = " AND password. [9-13].

Table 1: Encryption in Databases

Strategies / Techniques	Algorithm	Where encryption can be performed
Blended Cryptography Technique in light of information grouping strategies	Any symmetric Encryption calculation can be utilized	Encryption is done at Customer side Untrusted database Server
Hash Security Module Encryption Strategy	State – of-the workmanship calculation and method of operation ought to be utilized	Encryption can be at . Capacity Level • Database Level • Applicate on Level
Mix of the ordinary encryption and open key encryption, using the speed of traditional encryption and comfort of open key encryption.	X	X
Straightforward Data Encryption utilized by Master database key	X	Page level
Quick Comparison Encrypt	Symmetric encryption calculation	Information Ware houses



Table 2: Correlation of encryption strategies/methods

Strategies/Techniques	Advantages	Disadvantages
Blended Cryptography Technique in light of information arrangement strategies	Touchy information is shielded from assaults even at numerous levels due to hosting many keys to various gatherings Security server isn't altered	Execution of questions and security investigation is influenced as a result of encryption calculations
Hash Security Module Encryption Strategy	Encryption keys are never uncovered.	Complex
Straightforward Data Encryption utilized by Master database key	Gives insurance to touchy information on plate drives and reinforcement media from unlawful access.	Encryption crosswise over correspondence channels isn't given

## Security Policy

The purpose of a security policy is to elaborate the three generic security objectives of secrecy, integrity and availability and Confidentiality, in the context of a particular system show Figure 4, Properties of Database Security [6-14]

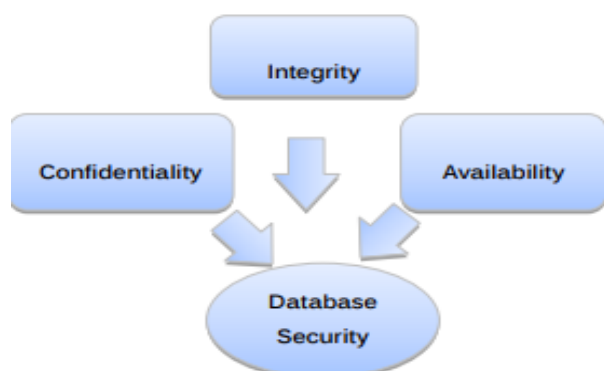


Figure 4: Properties of Database Security

To discover the measure of recurrence of event of an issue the Criticality factor is separated three sections i.e. Medium, High and Very High. The rate extend for criticality is characterized beneath in Table 3:

Table 3: Percentage & Criticality

Percentage	Criticality
81 – 100%	Very High
41– 80 %	High
20 - 40 %	Medium

Analysis of security parameters achieved using Encryption methods Table 4 and Figure 5:

Table 4: parameters Comparison

Security Parameters	Criticality	percentage
Confidentiality	Very High	100 %
Integrity	High	60 %
Availability	Medium	40 %

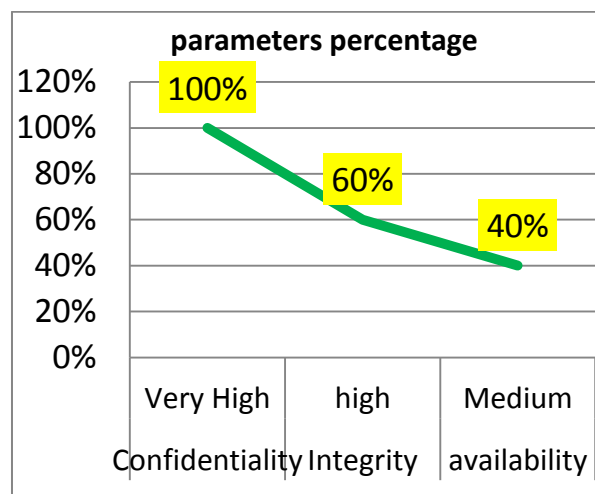


Figure 5: parameters percentage

## Database Security Issues

The security of the database has turned into a subject of expanding significance; fundamental targets of the database security to anticipate unapproved access to information, and to avoid altering or unapproved change of information,

and it stays to guarantee that the information is accessible when required and these streets [4].

- Daily maintenance.
- A variety of ways for security applications.
- Evaluate after the upgrade.
- Split site
- Apply Impersonating
- Management User passwords.

These are only a couple of the database security issues that exist inside associations. The most ideal approach to stay away from a ton of these issues is to utilize qualified. Work force and separate the security obligations from the everyday database upkeep duties. Another approach has been received for securing the databases. It has been examined that to make the databases secure diverse arrangements at association level can be actualized. Information/data is dependably a most critical resource for any association whose security can't be traded off. With the advances in innovation, the hazard to these important resources is increment. So their security is a major test. In various database security layers are characterized three layers are, (1) database executive, (2) framework manager, and (3) security officer, designers and worker. For Each layer some all-around characterized securities Arrangements have been foreseen. These approaches are only a couple of the database security issues that exist inside associations. The most ideal approach to stay away from a ton of these issues is to utilize qualified. Work force and separate the security obligations from the everyday database upkeep duties [11].

Another approach has been received for securing the databases. It has been examined that to make the databases secure diverse arrangements at association level can be actualized.

These approaches guarantee the security highlights, protection, classification and trustworthiness.

### Database Security Challenge

The Defense Information Systems Agency of the US Department of Defense (2004), in its Database Security Technical Implementation

Guide, expresses that database security ought to give controlled, ensured access to the substance of a database and save the respectability, consistency, and general nature of the information. Understudies in the registering disciplines must build up a comprehension of the issues and difficulties identified with Database security and must have the capacity recognize Conceivable arrangements the areas of Database Design, Structured Query Language, Database Transactions, and Database Security. SQL infusions, database induction, Database examining, and security grids: Data quality and completeness, Privacy-preserving databases, Sophisticated Access control models and mechanisms Security for large scale dynamically federated database, Security for GIS and spatial databases, Data security in pervasive computing, Environments, Integration of DB access control systems with trust, Negotiation systems and identity management Schemes, and Security for multimedia database [12].

### Conclusion

Data to any association is the most important property. Security of touchy information is dependably a noteworthy test fort has. In This examination the significant security issues confronting confidential information. Future work should be possible by scrambling information that diminishes the odds of liabilities and to guarantee the security of delicate data all the more viably and effectively, and addressing weaknesses in the security of databases.

### References

- [1] Basharat, Iqra, Farooque Azam, and Abdul Wahab Muzaffar. "Database security and encryption: A survey study." *International Journal of Computer Applications* 47.12 (2012).
- [2] Sandhu, Ravi S., and Sushil Jajodia. "Data and database security and controls." *Handbook of information security management*, Auerbach Publishers (1993): 1-37.



- [3] Murray, Meg C. "Database security: What students need to know." *Journal of Information Technology Education: Innovations in Practice* 9 (2010): IIP-61.
- [4] Imran, Sohail, and Irfan Hyder. "Security issues in databases." *Future Information Technology and Management Engineering*, 2009. FITME'09. Second International Conference on. IEEE, 2009.
- [5] Agrawal, Sanjay, et al. "Automating layout of relational databases." *Data Engineering*, 2003. Proceedings. 19th International Conference on. IEEE, 2003.
- [6] Agrawal, Sanjay, Surajit Chaudhuri, and Vivek R. Narasayya. "Automated selection of materialized views and indexes in SQL databases." *VLDB*. Vol. 2000. 2000.
- [7] Franqueira, Virginia NL, et al. "External insider threat: A real security challenge in enterprise value webs." *Availability, Reliability, and Security*, 2010. ARES'10 International Conference on. IEEE, 2010.
- [8] Agrawal, Sanjay, Surajit Chaudhuri, and Vivek R. Narasayya. "Automated selection of materialized views and indexes in SQL databases." *VLDB*. Vol. 2000. 2000.
- [9] Petković, Milan, and Willem Jonker, eds. *Security, privacy, and trust in modern data management*. Springer Science & Business Media, 2007.
- [10] Bertino, Elisa, and Ravi Sandhu. "Database security-concepts, approaches, and challenges." *IEEE Transactions on Dependable and secure computing* 2.1 (2005): 2-19.
- [11] Whitman, Michael E., and Herbert J. Mattord. "Principles of information security. Cengage Learning." receives US patent for personal identification device.(2005). *Wireless News* (2011): 1-1.
- [12] Seifert, Jeffrey W. "Data mining and the search for security: Challenges for connecting the dots and databases." *Government Information Quarterly* 21.4 (2004): 461-480.
- [13] Bansleben, E. "Database Migration: A Literature Review and Case Study." (2004).
- [14] Crain, Matthew. *The revolution will be commercialized: finance, public policy, and the construction of internet advertising*. University of Illinois at Urbana-Champaign, 2013.