Safeguarding Data Privacy by Placing Multi-level Access Restrictions

Lakshmi Bhaskarla[1]
Asst. Professor,
Department of Computer Applications,
V.R.S.E.C, Vijayawada -7,
Andhra Pradesh, India

Abstract: People always tend to protect assets regardless of what they are. For example, a user may keep a memorable picture of his parents in a safe place. However, the degree of protection he provides is directly based on how much he values the assets. If the user highly value the picture of his great-grandparents, he might take an extra measure of precaution by copying it and placing it in a fireproof safe where it is guarded from most natural disasters and from theft, or he may just put it in a frame because he has many similar pictures or because he can reproduce it. Usage of Database management systems to store information in every aspect of an enterprise is rapidly growing. Every company need to protect all tangible assets like valuable information stored in a DBMS is often vital to the business interests of the organization and is regarded as a corporate asset of the company that must be protected. There is no doubt that a password is the key to opening a user account. The Stronger the password, the longer it takes a hacker to break in. User authentication depends on a password to ensure the user account's identity. Since organizations increase their implementation of database systems as the key data management technology for regular operations and decision making, the security of data managed by these systems is an important task.

Keywords: *Database Security Methodology, Data Confidentiality, Data Integrity, Data Secrecy, Password Policies*

*****

I INTRODUCTION

All organizations, may suffer heavy losses from both financial and human points of view as a consequence of unauthorized data observation. Incorrect modifications of data, either intentional or unintentional, result in an incorrect database state. Any use of incorrect data may result in heavy losses for the organization. When data is unavailable, information crucial for the proper functioning of the organization is not readily available when needed. Database security concerns the use of a broad range of information security controls to protect databases includes the data, the database applications or stored functions, the database systems, the database servers against compromises of their Secrecy, integrity and availability.

II. ASSET TYPES AND THEIR VALUE

Assets are the infrastructure of the company operation. Depending on the type of asset and how much the company values it, the company build security policies and procedures and executes actions to protect these assets. There are 4 main types of assets.

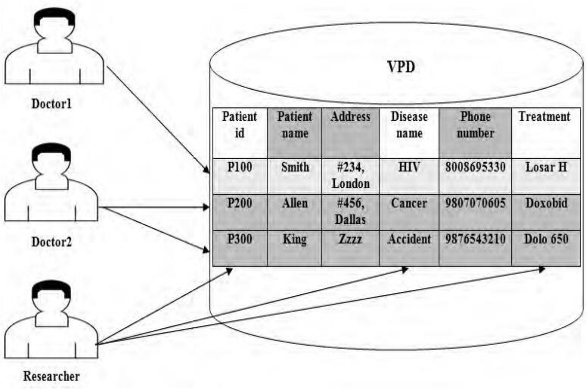
- **Physical Asserts:** Also known as tangible assets, these include buildings, vehicles, hardware, and so on.
- **Logical Assets:** Logical aspects of an information system, such as business applications, in-house programs, purchased software, operating systems, databases, and data.
- **Intangible Assets:** Business reputation, quality, and public confidence.
- **Human Assets:** Human Skills, knowledge, and expertise.

III. AUDITING ACTIVITIES

Auditing activities are performed as a part of an audit, audit process, or audit plan. Some of these activities can be thought of as the auditor's responsibilities or they can be incorporated into an organization's audit policies.

- Evaluate and appraise the effectiveness and adequacy of the audited entity according to the auditing objectives and procedures.
- Ascertain and review the reliability and integrity of the audited entity
- Ensure the organization being audited is in compliance with the policies, procedures, regulations, and standards of the government and the industry.
- Establish plans, policies, and procedures for conducting audits.
- Act a liaison between the company and the external audit team.
- Organize and conduct internal audits

Virtual Private Database (VPD) is also called as Tuple - level Security. It ensures additional security to the database by ***masking*** data so that users only see their private records. Separate sites for data, departments and individuals are stored together in a single database exclusively. The users have no knowledge about it. It works by transparently modifying requests for data to present a partial view of the tables to the users based on a set of defined criteria. Fig: 1 In this, we explain the main endeavor of VPD. These examples shows the database of health clinic system, it provides both Tuple – level and Column – level security for sensitive data of the patients. Each Doctor have access only modify data of his patients and sensitive information it is kept confidential from other sections of hospital.



Patient id	Patient name	Address	Disease name	Phone number	Treatment
P100	Smith	#234, London	HIV	8008695330	Losar H
P200	Allen	#456, Dallas	Cancer	9807070605	Doxobid
P300	King	Zzzz	Accident	9876543210	Dolo 650

Figure 1: Tuple- level Access implementation using VPD.

View is used to create a query in a database. It retrieves the data from the base tables. If a complex query is to be referred multiple times then it can be stored in the a temporary table i.e. nothing but a view. For example, the attribute names may be changed and or various attributes may be displayed as single attribute or single attribute may be split into two or more attributes. Views isolate application from the modifications in the table definition. Thus View are not a good practice for enforcing database security.

IV. PASSWORD POLICY

A Password Policy is a set of guidelines that enhances the robustness of password and reduces the likelihood of its being broken. Most guidelines deal with various aspects of passwords, such as password complexity, frequency of password changes, and password reuse. These guidelines not only enhance password protection, they also establish standards for institutions to increase employee and public confidence in their security measures.

- **Designing Password Policies:** Most companies use a standard set of guidelines for their password policies. These guidelines can comprise one or more of the following:
    1. **Password Complexity-** The purpose of password complexity is to decrease the chances of a hacker guessing or breaking a password. A set of guidelines used when selecting a password. For example, a company could require that a password be eight characters in length and contain at least one digit and a symbol. **Password Aging -** Indication of how long a password can be used before it expires.
    2. **Password Storage -** A method of storing a password in an encrypted manner.
    3. **Password Usage -** Indication of how many times the same password can be used.

V. DATABASE SECURITY METHODOLOGY

It is time to put the pieces of the database security jigsaw puzzle together to compose a process that will assist in building database security. The following list presents the definition of each phase of the data security methodology. The following Fig2 shows the enforcement of database security.

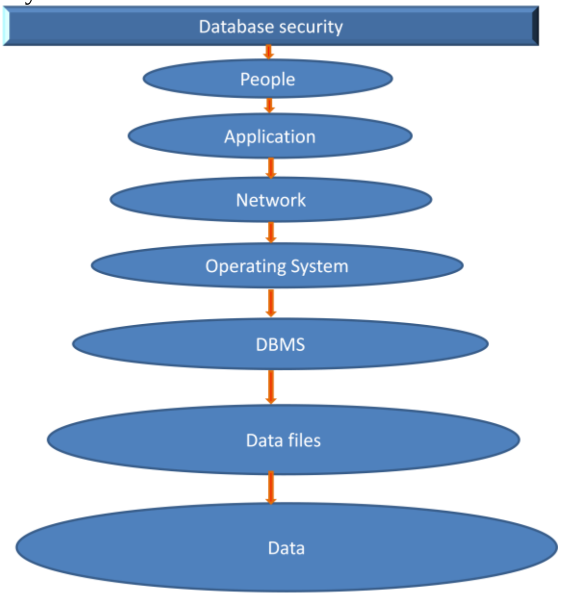


Figure2: Database Security Enforcement

1. **Identification –** This phase entails the identification and investigation of resources required and policies to be adopted.
2. **Assessment -** This phase includes analysis of vulnerabilities, threats, and risks for both aspects of database security: physical and logical.
3. **Design-**This phase results in a blueprint of the adopted security model that is used to enforce security. The blueprint shows how security measures are implemented to enforce data integrity and accessibility.
4. **Implementation –** Code is developed or tools are purchased to implement the blueprint outlined in the previous phase.
5. **Evaluation -** In this phase evaluate the security implementation by testing the system against typical software attacks, hardware failures, natural disasters, and human errors. The result of this phase is a determination of the system's degree of security.
6. **Auditing –** After the system goes into production, security audits should be performed periodically to ensure the security of the system.

- **Screenshots**

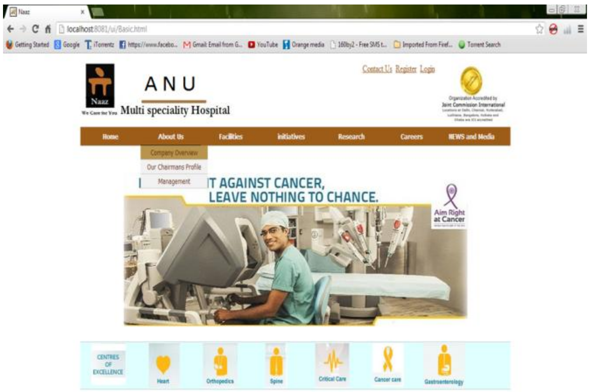
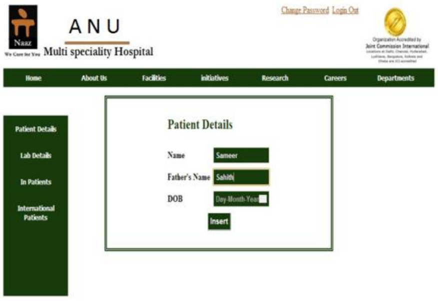


Figure3: Home page



Patient Details

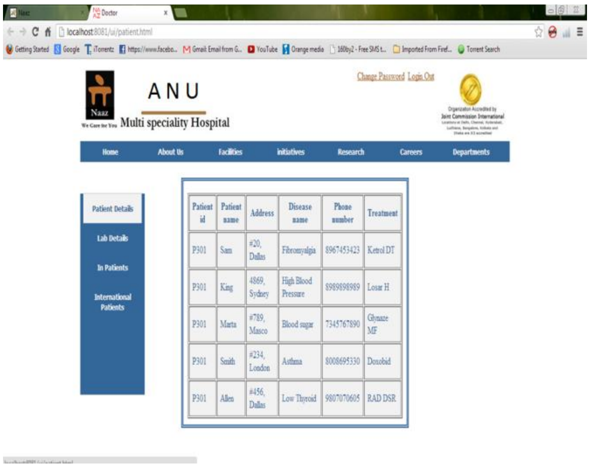
Name: Sameer

Father's Name: Sahith

DOB: Day-Month-Year

Figure 4: Patient Details

Figure 5: Doctor's page



Patient id	Patient name	Address	Disease name	Phone number	Treatment
P301	Sam	#20, Dallas	Fibromyalgia	8967453423	Ketrol DT
P301	King	4869, Sydney	High Blood Pressure	8989898989	Losar H
P301	Marta	#789, Masco	Blood sugar	7345767890	Glynaze MF
P301	Smith	#234, London	Asthma	8008695330	Doxobid
P301	Allen	#456, Dallas	Low Thyroid	9807070605	RAD DSR

Figure 6: Specific patient details for a Doctor

VI. CONCLUSION

It is easy to think of data masking and data encryption as the same things, since they are both data-centric means of protecting sensitive data. However, data encryption is not all time safeguard for the database management systems. Many hacker security violations begin with breaking the password to an account and thereby opening the door to the network, the system, the system, and password-protected files. Many companies spend countless hours training and educating their employees on methods for selecting passwords that are not easily breakable. This paper is aimed at password policies for database users, these password policies can be applied to any account, regardless of the environment or the platform. Virtual Private Database provide solution to ensure data secrecy, integrity and security as is deals with tuple level protection of key data. Data accessing and response to query is relatively high, which increase database performance.

REFERENCES

[1]. B. Lakshmi, "Data Confidentiality and Loss Prevention using Virtual Private Database."

[2]. Elisa Bertino and Ravi Sandhu, "DatabaseSecurity—Concepts, Approaches, and Challenges", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, JANUARY-MARCH 2005.

[3]. Lakshmi B, Ravindra Babu H and Murali Krishna A "Preserving Privacy using Column Masking and Data Encryption Techniques", International Journal of Computer Sciences and Engineering, Volume-4, Issue-6, @2016, pp 136-141.

[4]. R.J. Lauf and B.S. Hoffheins, "Analysis of Liquid Fuels Using a Gas Sensor Array," Fuel, vol. 70, pp. 935-940, 1991.

[5]. https://qz.com/1121547/how-smart-is-the-first-robot-citizen/

[6]. "Securing Database as a Service", COPUBLISHED BY THE IEEE COMPUTER AND RELIABILITY SOCIETIES, NOVEMBER 2011.

[7]. Venkat Krishnan, James D. McCalley, Samir Issad and Sebastien Henry, "Efficient Database Generation for Decision Tree Based Power System Security Assessment", NOVEMBER 2011.

[8]. Vrundan R. Parode, "An analysis on Fine-grained Access Control in Databases", published by International Journal of Computer Applications, April 2012.

[9]. Wangchao Le and Feifei Li, "Query Access Assurance in Outsourced Databases" APRIL-JUNE 2012.

[10]. The virtual private database in oracle9ir2: An oracle technical white paper. http://www.cgisecurity.com/database/oracle/pdf/VPD9ir2twp.pdf

[11]. Kenneth Goldman and Enriquillo Valdez, "Matchbox: Secure Data Sharing", December 2004 IEEE