RSU Journal of Biology and Applied Sciences

ISSN:

RSUJBAS

About us

Rivers State University Journal of Biology and Applied Sciences (RSUJBAS) publication is a quarterly, open access, international journal for all academic research in science discipline. Microbiology, Botany, Zoology, Environmental Biology, Chemistry, Physics, Mathematics, Computer Science, Biochemistry, Medical Laboratory Sciences and other applied science related areas. RSUJBAS is a platform set for elites to influence, contribute and communicate to the global environment through their various academic researches. We synergistically engage our noble efforts to contribute to the knowledge development, discoveries and innovations in all fields of study. In RSUJBAS we publish research papers on current academic issues with standard scientific reviews. RSUJBAS publishes original research articles, review articles, case studies, short communications, survey report, comparative studies and many more.

Aim and scope

Rivers State University Journal of Biology and Applied Sciences aims to publish high quality papers that communicate fundamental and contemporary discoveries both theoretical and practical. Most importantly RSUJBAS seeks to establish a platform for communicating emerging trends in various discipline such as Microbiology, Botany, Zoology, Environmental Biology, Chemistry, Physics, Mathematics, Computer Science, Biochemistry, Medical Laboratory Sciences and other applied science related areas.

Description:

- Area of concentration: All science academic disciplines
- Frequency of publishing: Quarterly
- Mode of publishing: both online and print publication
- Language of publication: English
- Double Blinded Review Process
- Zero Level Plagiarism Tolerance

Why publish with us

Low Article Processing Charge (ACP) to promote the research work
Easy and Rapid review process
Instant publication upon acceptance
Dedicated editorial and review team for fast review process
RSUJBAS provides hard copies of publication every quarterly

Editorial Board

All Correspondence to
Dr. Sam Wenedu (Editor-in-Chief)
Department of Microbiology, Rivers State University
Editor.jbas@yahoo.com

Or

OLUCHI DICKSON
Publication Manager
Dicksonoluchi87@gmail.com

Consulting Editors

Guideline for Manuscripts

Manuscripts should be typewritten on an A4 sheet having B1.5= line spacing throughout the text. The margins should be 2B54cm (1 inch) in all sides and page number should be consecutively on the bottom of the page. The manuscript should be written in Times New Roman using '12' font size.

For original research paper, the manuscript should be arranged in the following order: Title page, Abstract, Keywords, Introduction, Materials and Methods, Results, Discussion, Acknowledgment, References, Tables with legends, figures with legends and supplementary materials

The title page should contain the title, the name(s) of the author(s), the name(s) and address(es) of the institution(s) where the work was carried out, including a valid e-mail address from the corresponding author along with telephone numbers. The title of the manuscript should be specific and concise but sufficiently informative.

The Abstract should not exceed 250 words and it should contain brief summary of the findings including brief introduction, methodology, results, and conclusions,

The keywords should have a minimum of five and maximum of seven words.

The introduction should provide a clear statement of the problem and indicates aim of the study citing relevant literature to support background statements.

The Materials and Methods should include the methods and methodology of the research.

The Results should be presented in the form of tables or figures. It should be presented with clarity and precision. Statements used to present results should be written in the past tense. Detailed interpretation of data should not be included in the results but should be put into the Discussion section.

The Discussion should interpret the results clearly and concisely, and should integrate the research findings of this and past studies on this topic. Highlight the significant/unique findings of the research under conclusion.

The acknowledgments of people, grants or funds should be brief.

Contents

List of Contributors

Kingsley-Opara, Ngozi
Research Scholar, Department of Computer Science, Ignatius Ajuru University of Education, Rivers State, Nigeria.
Advanced Database Management

Prof. Asagba, Prince Oghenekaro.
Visiting Scholar, Department of Computer Science, University of
Port-Harcourt, Rivers State Nigeria.
Email:asagba.prince@uniport.edu.ng

Gabriel B.C., Gabriel M. N, P. O. Asagba
School of Graduate Studies Ignatius Ajuru University Of Education (IAUE),
Rumuolumeni, Port Harcourt, Rivers State, Nigeria.
Department Of Computer Science.
gabrielbariyira@gmail.com, meegabz@gmail.com

WAIDOR, Tamaramiebi Keith[1]& ASAGBA, Prince Oghenekaro[2]
Department of Computer Science,
Faculty of Natural and Applied Sciences
Ignatius Ajuru University of Education, Port Harcourt
zalimaxxx@gmail.com

[2]Department of Computer Sciences,
University of Port Harcourt, Port Harcourt, Nigeria
Prince.asagba@uniport.edu.ng

Fiberesima, Alalibo Ralph
Visiting Scholar, Department of Computer Science,
University of Port-Harcourt, Rivers State Nigeria.
fiberesima.a.r@outlook.com;

Asagba, Prince Oghenekaro
Visiting Scholar, Department of Computer Science,
University of Port-Harcourt, Rivers State Nigeria.
asagba.prince@uniport.edu.ng

Kingsley-Opara, Ngozi
Research Scholar, Department of Computer Science,
Ignatius Ajuru University of Education, Rivers State, Nigeria.
Email: ngozikopara@gmail.com

Prof. Asagba, Prince Oghenekaro.
Visiting Scholar, Department of Computer Science,
University of Port-Harcourt, Rivers State Nigeria.

A Review on Database Security and Authorization

Gabriel B.C., Gabriel M. N, P. O. Asagba
gabrielbariyira@gmail.com, meegabz@gmail.com

School of Graduate Studies Ignatius Ajuru University Of Education (IAUE),
Rumuolumeni, Port Harcourt, Rivers State, Nigeria.
Department Of Computer Science.

Abstract:

Data protection is vital to many secure systems, and majority of users rely on a database management system to manage the protection. This work is all about the security of database management systems and user authorization, as an example of how application security can be designed and implemented for specific task, rights and privileges issued to different categories of users. There is considerable current interest in DBMS Security because databases are newer than the programming and operating systems. Databases are important to many business and government organizations, in order to enable the retrieval and maintenance of data easy and efficient it is stored in a database. Database creation, organization and contents are considered valuable corporate assets that must be securely protected because databases are a favourite target for information thieves and attackers. The primary security requirements of database system are not unlike those of other computing system. The basic problems are database authorization; access control, exclusion of spurious data, authentication of users and reliability. In this work database authorization and the challenges and threats in database security are identified.

Keywords: Attack, Database security, Threat, Integrity**.**

1. Introduction

Protecting data is at the heart of many secure systems, and many users rely on a database management system to manage the protection. Databases are essential to many business and government organizations, holding data that reengineered to make them more effective and more tune with new and revised goals [1].Database security is a difficult operation that any organization should enhance in order to run its activities smoothly. The various threats pose a challenge to the organization in terms of integrity of the data and access. The threats can result from either by an outside illegal program action or by an outside force such as fire or a power failure [1]. Most of the database contains sensitive data for users which can be vulnerable to hacking and misuse [3]. Therefore, firms have greater control and check on their database to maintain the integrity of the information and ensure that their systems are monitored closely to avoid deliberate violations by intruders.

2. Threats of Database Security

Database security issues have been more complex due to widespread use. Database are a firm main resource and therefore, policies and procedure must be put into place to safeguard its security and the integrity of the data it by contains. Besides, access to the database has been become more rampant due to the internet and intranets therefore, increasing the risks of unauthorized access.

The objective of database security is to protect database from accident or intentional los. These threats pose a risk on the integrity of the data and its reliability. Database security allows or refuses users from performing actions on the database.

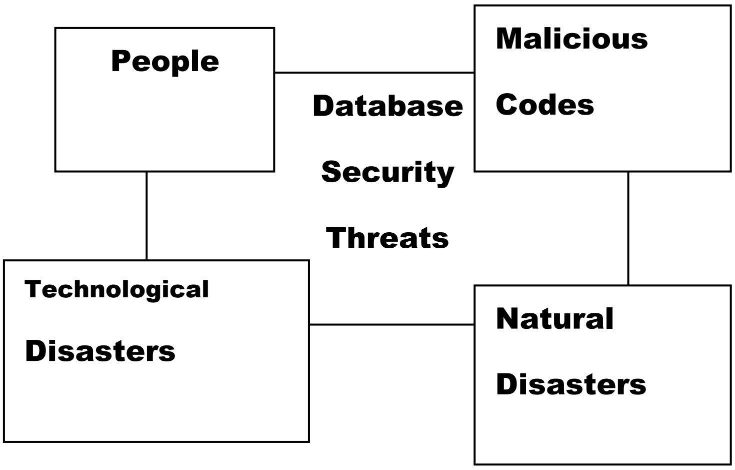

Figure 1: Threats of database security

There are different threats to the database systems. Such as Excessive Privilege Abuse When users are granted database access privileges that exceed the requirements of their job function, these privileges may be abused for malicious purpose [3]. Another threat is a weak audit trial. This is due to weakness in organizational internal system. This is due to weak deterrence mechanism. Denial of service is another problem in database security. Weak database audit policy represents a serious organizational risk on many levels. Another threat to the problem of database insecurity is weak system and procedures for performing authentication. Weak authentication schemes allow attackers to assume the identity of legitimate database users by stealing or otherwise obtaining login credentials. Strong authentication is therefore required to address these challenges [4].

3. Database Security Requirements

The basic security requirements of database systems are not unlike those of other computing systems. The basic problems access control, exclusion of spurious data, authentication of users, and reliability.

a) **Physical database integrity:** The data of a database are immune to physical problems, such as power failures, and someone can reconstruct the database if it is destroyed through a catastrophe.

b) **Logical database integrity:** The structure of the database is preserved. With logical integrity of a database, a modification to the value of one field does not affect other fields.

c) **Audit ability:** It is possible to track who or what has accessed the elements in the database.

d) **Access control:** A user is allowed to access only authorized data, and different users can be restricted to different modes of access.

e) **User authentication:** Every user is positively identified, both for the audit trail and for permission to access certain data.

f) **Availability:** Users can access the database in general and all the data for which they are authorized.

4. Database Security Guidelines

a) Operating System: No matter how secure the database system is, weakness in operating system security may serve as a means of unauthorized access to the database.

b. Network**:** Since almost all database systems allow remote access through terminals or networks, software-level security within the network software is as important as physical security, both on the Internet and in networks private to an enterprise.

c) Database System**:** Some database-system users may be authorized to access only a limited portion of the database. Other users may be allowed to issue queries, but may be forbidden to modify the data [2].

Security at all these levels must be maintained if database security is to be ensured.

If a database is to serve as a central repository of data, users must be able to trust the accuracy of the data values. This condition implies that the database administrator must be assured that updates are performed only by authorized individuals. The DBMS can require rigorous user authentication. For example, a DBMS might insist that a user pass both specific password and time-of-day checks. This authentication supplements the authentication performed by the operating system [1].

Databases are often separated logically by user access privileges. For example, all users can be granted access to general data, but only the personnel department can obtain salary data and only the marketing department can obtain sales data. Databases are very useful because they centralize the storage and maintenance of data. Database integrity concern that the database as a whole is protected against damage, as from the failure of a disk drive or the corruption of the master database index. These concerns are addressed by operating system integrity controls and recovery procedures [2]. If sensitive data are encrypted, a user who accidentally receives them cannot interpret the data. Thus, each level of sensitive data can be stored in a table encrypted under a key unique to the level of sensitivity.

5. Database Security levels

To protect the database, we must take security measures at several levels:

a) People**:** Users must be authorized carefully to reduce the chance of any such user giving access to an intruder in exchange for a bribe or other favours.

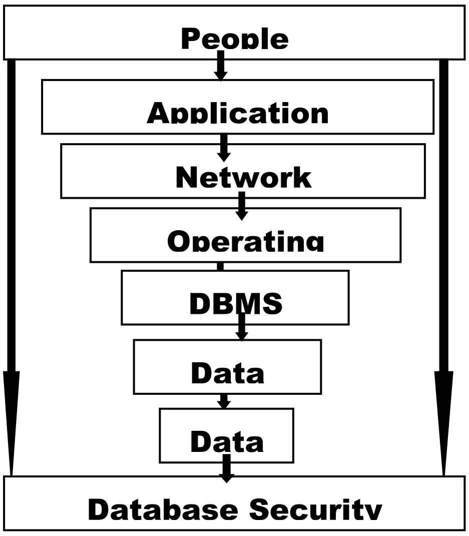

Figure 2: Database Security levels

6. Techniques for Database Security

One of the most basic concepts in database security is authentication, which is quite simply the process by which it system verifies a user's identity, A user can respond to a request to authenticate by providing a proof of identity, or an authentication token. An authenticated user goes through the second layer of security, authorization. Authorization is the process through which system obtains information about the authenticated user, including which database operations that user may perform and which data objects that user may access. A secure system ensures the confidentiality of data. This means that it allows individuals to see only the data they are supposed to see.

Confidentiality has several aspects like privacy of communications, secure storage of sensitive data, authenticated users and authorization of users. Another technique that can be used to secure database is the use of access control [1]. This is the where the access to the system is only given after verifying the credentials of the user and only after such verification is done, the access is given. Audit trial is another method that can help in the database security. Audit trial need to be carried to found the history of operations on the database [4]. One of the techniques for achieving security is by using a DBMS for multiple users of different interests is the ability to create a different view for each user.

7. Database Management System Advantages

The user interacts with the database through a program called a database manager or a database management system (DBMS), informally known as a front end. A database administrator is a person who defines the rules that organize the data and also controls who should have access to what parts of the data [1]. A database offers many advantages over a simple file system. It improves data sharing in a way that enables the end users have better access to data that is correctly managed. There is improved data security in that the security is guaranteed and the data privacy is maintained [4].

Database management has an effect of ensuring that there is promotion of data integration in a whole organization and one can see a bigger picture of all activities [2]. It is also

probable that data access is facilitated and could be used to provide quick answers to queries giving out. There is better decision making is achieved due to accuracy, timelessness and validity of the information generated.

8. Principles of integrity and reliability in database security

Databases amalgamate data from many sources, and users expect a DBMS to provide access to the data in a reliable way. When software engineers say that software has reliability, they mean that the software runs for very long periods of time without failing. Users certainly expect a DBMS to be reliable, since the data usually are key to business or organizational needs. Moreover, users entrust their data to a DBMS and rightly expect it to protect the data from loss or damage.

Data integrity refers to reliability and accuracy of the data that is stored and used in business. Data should assist a firm to make the right decision and avoid inconsistencies. Element integrity concern that the value of a specific data element is written or changed only by authorized users. Proper access controls protect a database from corruption by unauthorized users [5]. Users trust the DBMS to maintain their data correctly, so integrity issues are very important to database security.

9. Database Authentication

This is the process of confirming that a user logs in only in accordance with the rights to perform the activities he is authorized to perform. User authentication can be performed at operating system level or database level itself.

By using authentication tools for biometrics such as retina and figure prints are in use to keep the database from hackers or malicious users.

The database security can be managed from outside the db2 database system. Here are some types of security authentication process:

1. Based on Operating System authentications
2. Lightweight Directory Access Protocol (LDAP)

For DB2, the security service is a part of operating system as a separate product. For Authentication, it requires two different credentials; those are userid or username, and password.

You can access the DB2 Database and its functionality within the DB2 database system, which is managed by the DB2 Database manager. Authorization is a process managed by the DB2 Database manager.

The manager obtains information about the current authenticated user, that indicates which database operation the user can perform or access.

Here are different ways of permissions available for authorization:

a) Primary permission: Grants the authorization ID directly.
b) Secondary permission: Grants to the groups and roles if the user is a member
c) Public permission: Grants to all users publicly.
d) Context-sensitive permission: Grants to the trusted context role.

Authorization can be given to users based on the categories below:

a) System-level authorization
b) System administrator [SYSADM]
c) System Control [SYSCTRL]
d) System maintenance [SYSMAINT]
e) System monitor [SYSMON]
f) Authorities provides control over instance-level functionality.

Authority provide to group privileges, to control maintenance and authority operations. For instance, database and database objects. Authorities provide controls within the database. Other authorities for database include with LDAD and CONNECT.

OBJECT-LEVEL AUTHORIZATION: Object-Level authorization involves verifying privileges when an operation is performed on an object.

CONTENT-BASED AUTHORIZATION: User can have read and write access to individual rows and columns on a particular table using Label-based access Control [LBAC].

DB2 tables and configuration files are used to record the permissions associated with authorization names. When a user tries to access the data, the recorded permissions verify the following permissions:

a) Authorization name of the user
b) Which group belongs to the user
c) Which roles are granted directly to the user or indirectly to a group
d) Permissions acquired through a trusted context.

While working with the SQL statements, the DB2 authorization model considers the combination of the following permissions:

a) Permissions granted to the primary authorization ID associated with the SQL statements.
b) Secondary authorization IDs associated with the SQL statements.

System control authority (SYSCTRL)

It is the highest level in System control authority. It provides to perform maintenance and utility operations against the database manager instance and its databases. These operations can affect system resources, but they do not allow direct access to data in the database.

1. Users with SYSCTRL authority can perform the following actions:

System maintenance authority (SYSMAINT)

It is a second level of system control authority. It provides to perform maintenance and utility operations against the database manager instance and its databases.

These operations affect the system resources without allowing direct access to data in the database. This authority is designed for users to maintain databases within a database manager instance that contains sensitive data.

Only Users with SYSMAINT or higher level system authorities can perform the following tasks:

a) Taking backup
b) Restoring the backup
c) Roll forward recovery
d) Starting or stopping instance
e) Restoring table spaces
f) Executing db2trc command

Conclusion

Security is an important issue in database management because information stored in a database is very valuable and many time, very sensitive commodity. So the data in a database management system need to be protected from abuse and should be protected from unauthorized access and updates. Database Security paper has attempted to explore the issue of threats that may be poised to database system. These include loss of confidentiality plus loss of integrity. The paper has also discussed areas concerning techniques to encounter any issue of threat using views and authentication. Another method is through back-up methods which ensure that the information is stored elsewhere and recovered in case of failure and attacks. This work has also discussed the various requirements necessary for the database security and the various levels of security.

References

Ashdown, Lance; Kyte, Tom (September 2011). "Oracle Database Concepts, 11g Release 2 (11.2)". Oracle Corporation. Archived from the original on 2013-07-15. Retrieved 2013-07-17. Distributed SQL synchronously accesses and updates data distributed among multiple.

Bertino et al Database security-Concepts, Approaches and challenges IEEE Transactions on dependable and secure computing, 2005.

Emil Burtescu, "DATABASE SECURITY - ATTACKS AND CONTROL METHODS", Journal of Applied Quantitative Methods, Vol. 4, no. 4, Winter 2009.

http://www.imperva.com/downloads/Top Ten Database Security Threats.pdf

O'Brien, J. & Marakas, G.M.(2008) Management Information Systems (pp. 185-189). New York, NY: McGraw-Hill Irwin

R. Tejashri "A Review on Database Security", International Journal of Science and Research, Volume 3 Issue 4, April 2014"

"Security in Computing" 4th edition Mr. Charles P. Pfleeger-Pfleeger Consulting Group, Shari Lawrence Pfleeger.

S. Singh, Database System: Concepts, Design and applications New Delhi: Pearson Education India, 2009.

S. Sumanthi, Fundamentals of relational database management systems Berlin: Springer, 2007.
http://www.appsecinc.com/downloads/Risksto Database Security in 2012.pdf.

"TechNet Glossary". Microsoft. Retrieved 2013-07-16. distributed query[:] Any SELECT, INSERT, UPDATE, or DELETE statement that references tables and row sets from one or more external OLE DB data sources.