The American Journal of Social Science and Education Innovations
(ISSN – 2689-100x)
Published: November 30, 2020 | **Pages:** 443-447
Doi: https://doi.org/10.37547/tajssei/Volume02Issue11-74

IMPACT FACTOR
2020: 5. 525
OCLC - 1121105668

Journal Website: http://usajournalshub.com/index,php/tajssei

Copyright: Original content from this work may be used under the terms of the creative commons attributes 4.0 licence.

New Scheme For Security Of DBMS

Kurbonov Feruz Yaxshimurodovich
Tashkent University Of Information Technologies Named After Muhammad Al-Khwarizmi, Uzbekistan

Baxromova Yulduz Sheren Kizi
Tashkent University Of Information Technologies Named After Muhammad Al-Khwarizmi, Uzbekistan

ABSTRACT

In this paper is presented security matrix sub-module, analyzing of vulnerabilities, threats and security methods. At the end of the work is proposed new scheme of Security of DBMS.

KEYWORDS

Matrix, security, DBMS, threats, vulnerability, scheme.

INTRODUCTION

Database security refers to the various measures organizations take to ensure their databases are protected from internal and external threats. Database security includes protecting the database itself, the data it contains, its database management system, and the various applications that access it. Organizations must secure databases from deliberate attacks such as cyber security threats, as well as the misuse of data and databases from those who can access them.

In the last several years, the number of data breaches has risen considerably. In addition to the considerable damage these threats pose to a company's reputation and customer base, there are an increasing number of regulations and penalties for data breaches that organizations must deal with, such as those in the General Data Protection Regulation (GDPR)—some of which are extremely costly. Effective database security is key for remaining compliant, protecting organizations' reputations, and keeping their customers.

The American Journal of Social Science and Education Innovations
(ISSN – 2689-100x)
Published: November 30, 2020 | **Pages:** 443-447
Doi: https://doi.org/10.37547/tajssei/Volume02Issue11-74

IMPACT FACTOR
2020: 5. 525
OCLC - 1121105668

MAIN PART

A Security Matrix sub-module is presented in Figure 1. A customer-order scenario is depicted. Seven tables are listed across the top. Seven forms are listed down the left-hand side [1]. Scanning the matrix left to right shows that the Order Form requires access to five tables including modification rights to three of them. Specifically the Order Form needs only read access to the Customers and Employees tables, requires read, insert, update, and delete rights to the Order_Details and Orders table, and requires read and update rights to the Products table. Scanning top to bottom shows that three applications, Customer Labels, Customer Information, and Order Form, access the Customers table. The Customer Labels and Orders Form require read access to the Customers table while the Customer Information form requires read, insert, update, and delete rights. The Security Matrix sub-module includes an accompanying set of interactive questions that ask users to identify relationships between the tables and the application programs.

Figure 1. Security Matrix Sub-module: Example Security Matrix

Also there are security level and solutions:

- Database Level: Masking, Tokenization, Encryption.
- Access Level: Access Control Lists, Permissions.
- Perimeter Level: Firewalls, Virtual Private Networks.

In table 1 have identified the vulnerabilities, threats and security methods of database management system with the help survey conducted on researches of data-base security [2].

Table 1. Vulnerabilities, Threats and Security methods

Vulnerabilities	Threats	Security methods
Vendor Bug: Buffer Overflow, Programming errors	May damage or violate the database	Unauthorized access control policy

The American Journal of Social Science and Education Innovations
(ISSN – 2689-100x)
Published: November 30, 2020 | **Pages:** 443-447
Doi: https://doi.org/10.37547/tajssei/Volume02Issue11-74

IMPACT FACTOR
2020: 5. 525
OCLC - 1121105668

Poor Architecture: Weak form of encryption	May damage database environment components (networks, applications, operating systems, DBMS and data)	Security Models
Misconfiguration: Not properly locking database	Loss of integrity of the database	Physical database integrity protection, Logical data integrity protection, Data element integrity protection
Incorrect usage: SQL injection	Misuse of availability of database	Intrusion Detection System: 1. A Misuse Detection System for Database System 2.SQL Injection and Insider Misuse Detection System 3. Detecting Intrusion in Databases through Fingerprinting Transactions 4. Semantic inference model
Irresponsible DBA: Deactivation of necessary security mechanism	Easy access of data	Two principles should be followed: 1. The access control models for databases should be expressed in terms of the logical data model; thus authorizations for a relational database should be expressed in terms of

The American Journal of Social Science and Education Innovations
(ISSN – 2689-100x)
Published: November 30, 2020 | **Pages:** 443-447
Doi: https://doi.org/10.37547/tajssei/Volume02Issue11-74

IMPACT FACTOR
2020: 5. 525
OCLC - 1121105668

		relations, relation attributes, and tuples. 2. For databases, in addition to name-based access control, where the protected objects are specified by giving their names, content- based access control has to be supported.
Hidden Flaws in DB: Undetected defects	Allow hackers to connect to the database server by exploring those defects.	Intrusion Detection System
Unauthorized Users: Unauthorized users "still" the credentials of authorized users	Easy access of da-tabase servers	Intrusion Detection System
Misused Privileges: Authorized users take ad-vantage of their privileges.	Maliciously access or destroy data	Database Administrator should provide securi-ty on the basis of above mentioned principles.

In figure 2 is presented security scheme and mechanisms of protection of the DBMS. Here, main threats are added and protection tools are installed. Also, we can add fallowing configurations [3]:

- Mandatory auditing

The American Journal of Social Science and Education Innovations
(ISSN – 2689-100x)
Published: November 30, 2020 | **Pages:** 443-447
Doi: https://doi.org/10.37547/tajssei/Volume02Issue11-74

IMPACT FACTOR
2020: 5. 525
OCLC - 1121105668

- Standard database auditing
- Fine-grained auditing (FGA)
- Value-based auditing
- Administrator auditing

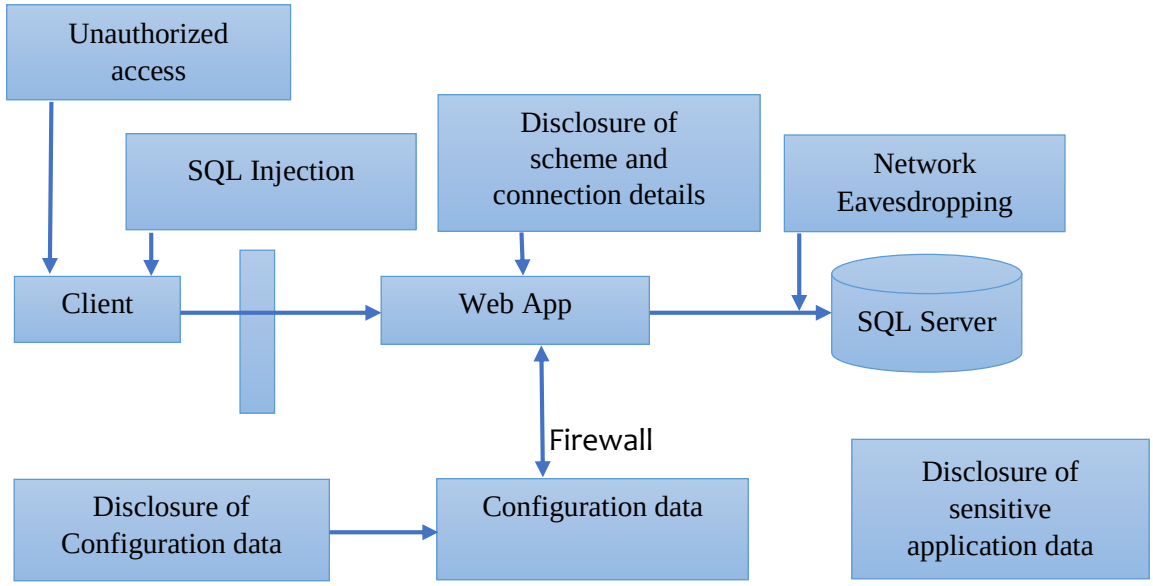

Figure 2. New scheme of Security of DBMS

CONLUSION

The result of the survey we have described in the paper and summarized in tabular form. As a result

we can conclude that though remarkable work has been done in this field, with the invention of internet

Technology, the risk to database has increased.

REFERENCES

1. Murray M. C. Database security: What students need to know //Journal of information technology education: Innovations in practice. – 2010. – T. 9. – C. IIP-61.
2. Muntjir M. et al. Security Issues and Their Techniques in DBMS-A Novel Survey //International Journal of Computer
Applications. – 2014. – T. 85. – №. 13.
3. Basharat I., Azam F., Muzaffar A. W. Database security and encryption: A survey study //International Journal of Computer Applications. – 2012. – T. 47. – №. 12.