*Jurnal Mantik, 5 (4) (2022) 2535-2541*

Published by:Institute of Computer Science (IOCS)

Jurnal Mantik

Journal homepage: www.iocscience.org/ejournal/index.php/mantik/index

# Database Audit System Design and Implementation

**Parmonangan R. Togatorop, Hetty Ana Thasya Sitorus, Ramos M. Sirait, Tessalonika Manurung**

[1,2,3,4]Sistem Informasi, Fakultas Informatika dan Teknik Elektro, Institut Teknologi Del
Jln. Sisingamangaraja, Sitoluama, Laguboti, Toba Samosir, 22381, Sumatera Utara, Indonesia

Email: mona.togatorop@del.ac.id, hettyana.ts@gmail.com, ramossirait57@gmail.com, tessamaretta17@gmail.com

**ARTICLEINFO**

***Article history:***

Received: Jan 10, 2022
Revised: Jan 29, 2022
Accepted: Feb 17, 2022

***Keywords:***

Audit,
Database Audit,
Log,
Trigger,
CAAT

**ABSTRACT**

Database auditing has become a very important aspect of security as organizations today use database management systems (DBMS) as the main asset that stores, maintains and monitors sensitive information. Using the Computer-Assisted Audit Technique (CAAT) technique can make it easier for auditors to complete the audit. This study aims to build an automatic tool for conducting database audits in the category of log on / off audit, database usage audit, database usage outside operating hour audit, and security attribute audit (privileges, user / login, and password changes. The resulting audit in this study begins with creating an audit environment, logging and then producing an audit report. Creating triggers and logs are the steps in obtaining data for the audit process. The resulting reports include suspicious access, inactive users, access outside of operational hours, and Inactive users are accompanied by recommendations that can be used by the auditor when conducting the audit.



## 1. Introduction

Data and information are important assets for an organization that will experience increasing numbers continuously rapidly. The increasing number of users and heavy dependence on digital information is one of the barometers for the importance of maintaining and ensuring the security of data or information [1]. Therefore to ensure data security and maintain integrity, an audit is necessary. The audit is a formal examination and verification to check whether standards or guidelines have been implemented or efficiency and effectiveness have been met [2]. Information Technology (IT) has become widespread in the global business environment in the last two decades, especially its rapid changes in customer requirements and the desire to overcome competitors in providing better and quality services promptly and at lower costs [3]. Therefore, an IT audit is carried out to evaluate all components of an organization's information technology such as business processes, services, systems, infrastructure, or other technology components [4], as a control to protect information technology as a whole and produce effective solutions to overcome problems so that not only serves to report problems but also provides considerations for solutions that can be applied.

Audits can be done in 2 ways, by manual and computerized. To make it easier for auditors to carry out IT audits, audit techniques can be carried out with computers. This technique is known as the Computer-Assisted Audit Technique (CAAT). With CAAT, auditors will be able to produce more analytical audit evaluation and reporting and work efficiently and productively [5] [6]. CAAT can be defined as any use of technology to assist the completion of an audit [5]. Based on that, there are various types of CAAT, ranging from word processors or electronic spreadsheets up to expert systems [7] [8] [9].

Database audit is one of the main issues of information security [10] [11]. There is information that needs to be maintained its integrity, so database audits are needed to detect system failures or human errors and detect attacks on databases to prevent major losses for the organization and other related parties [12]. Auditing the database have a lot of advantages. Database auditing entails keeping track of the actions in order to detect, prevent, and mitigate the effects of illegal access to your database management system. Company can improve security by concentrating on specific parts of the databases. For instance, improving



**Accredited "Rank 4"(Sinta 4),** DIKTI, No. 36/E/KPT/2019, December 13th 2019.

user access can help reduce human error, while prioritizing data cleanup can help maintain system structured and simple to use. Database auditing tools make it a lot easier with function that fit business demands is the best method to protect their database. Based on the audit category [13], it is possible to choose what audit category and how to implement it to assist in meeting the standards.

For this reason, in this study, the author will analyze, design, and implement a database audit automation tool to assist auditors in collecting data for the audit process, process analysis, and generate audit reports.

## 2. Method

The first step is to analyze the database audit architecture to obtain the right steps and techniques in conducting database audits. Information about the database audit process was obtained from the literature study conducted. After that, a design was carried out to produce a database audit framework design based on the analysis carried out on the database audit process. The resulting framework will be used in the application to perform audits on the database. After that, application development is carried out based on the design or design according to the needs specified in the analysis process.

In this study, a database system is needed as a database storage medium and as an audit object. The database used in this research is Ms. SQL Server RDBMS and MySQL. The databases used in this study are the Northwind sample database which runs on MySQL and the BikeStores sample database on Microsoft SQL Server 2014. The categories included in the Access Database audit are Database log out/in audit, database usage source audit, and Audit of database usage outside normal operating hours.

For database logout/login information, database user sources, and failed logins, can be obtained using the logs provided by the database. Each log will be saved into several files which are limited in number. The log that is being written or used is called current. When the current log has been written and will be saved then the last log will be deleted. MySQL has several logs that can help users know what activity is going on. Log in and out, user data sources and database users can be obtained from the general log. Each SQL Server database has a transaction log that records all transactions and database modifications made by each transaction. The attributes that will be audited include a user name, time, TCP/IP address, and the name of the program that performs access.

The information to be used can also be obtained by using SQL commands. One of the important pieces of information that can be obtained from the table is the date of the last modification of user information. However, this information cannot be used to determine the date of the last password change, because that date also changes when there is a change in user information other than the password. Other information that will be seen is the list of database users, the roles each user has, and the programs that access the database.

This research uses triggers to obtain login information by creating a logon audit trigger on SQL Server. A trigger is used as an audit trail implementation. Triggers are also used to select which attributes are important to audit.

## 3. Result and Discussion

### 3.1 Audit Architecture

In this research, the audit categories used are database logout/login audits, database usage sources audits, and database usage audits. The audit architecture design in this research can be seen in Figure 2.

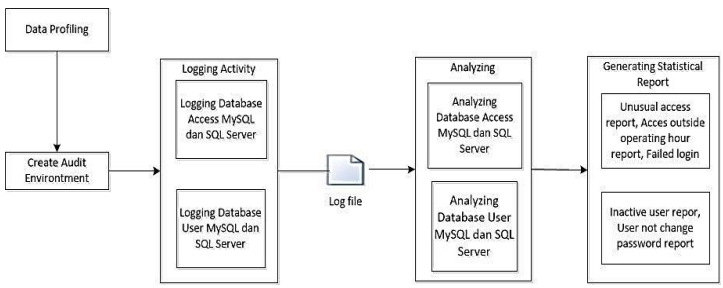


**Figure 2.** Database Audit Architecture Planning



**Accredited "Rank 4"(Sinta 4),** DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Data profiling is an important step that needs to be done first before conducting an audit. This stage is carried out to determine the database to be audited and to study every data contained in the database. The things that were learned were the tables in the database, the structure of the tables, and the dependency relationships between the tables. In this study, one of the databases used is the Northwind database using MySQL and the BikeStores database using SQL Server. The next stage is to Create an Audit Environment. This stage is carried out to produce an audit environment as a storage medium for the information generated by the audit. Where at this stage the process of creating an audit database is carried out on the database. In the Audit Environment, a table creation process will also be carried out, where these tables will be the source of data for analysis funds for reporting audit results. The audit environment will be used as a database along with SQL commands that are used to obtain information and store audit information into the database that has been created. Information that will be stored in the Audit Database includes information on access to the database. The information will be obtained from the metadata provided by Microsoft SQL Server and MySQL. In addition to metadata, some information is also obtained from SQL Server Logs, MySQL Logs, and triggers.

Logging Activity is an important first step in starting a database audit. The logging process aims to record access information and user activities in the database. Logging in the database keeps transactions/logs containing "who", "when", "where", "why" and "how" the database is accessed. The logging function aims to record every database information and activity that takes place in the database. In the implementation of logging on the database in SQL Server, triggers are used which function to log when activity occurs. One type of activity that is logged in the database access logging process by a trigger is successful access to the database. Creating a trigger with the name access_logon_trigger serves to record information from each user's successful access to the database. This trigger is created at the server level so that every access can be logged. Each information is temporarily stored in a variable which is then written to the success_access_log log table.

After the log is stored in the table, the analysis will be carried out on the data stored in the log. The analysis is carried out to obtain information that can be used in the audit. The analysis is used by creating views in the database or by creating functions in the application code. After that, a Generating Statistical Report was carried out. At this stage, the system will automatically generate and display the audit report. The resulting audit report will use the results of the analysis process as in the framework that has been designed. This report will be the final result of an automated audit process. Based on the report that has been generated, the auditor will be able to determine the next steps or provide recommendations to overcome the problems found and improve the security of the database.

### 3.2 Audit Environment

The implementation of the audit environment is carried out to produce an environment as a place to store data generated and used in the database audit process. The data is stored in a log including successful and failed access to the database, database usage, and errors that occur in the database. The steps taken are creating a log table to store logs from the audited target database and creating a System Accounts table. The log table is intended to store logs and other information needed for the audit process. The tables will be filled automatically by the logging function when the database is used. The first table is a log table with the name success_access_log. This table is used to store successful access information into the database. The log table has attributes named access_log_id, spid, login_name, program_name, ip_address, and access_time. An index is created in the username and program name fields. The second table is named audit_period. This table serves to store information about the audit period carried out. The table has the attributes period_id, period_name, status, period_start, and period_end. An index for the current audit period date column is also created in the table.

### 3.3 Logging Implementation

After making the audit database, the next stage is the logging function will be implemented by recording logs into the log table that was created previously where logging is carried out on the access database and user database. The sources of information used are database metadata, triggers, and SQL Server Logs. Database metadata is used to get information about database objects. A trigger is used to get information on successful access, while SQL Server Log is used to get information about errors that occurred in the database.



**Accredited "Rank 4"(Sinta 4),** DIKTI, No. 36/E/KPT/2019, December 13th 2019.

In its implementation, triggers that are used as a source of information on successful access can cause overhead in the database if done in real-time. To overcome this problem, SQL Server Agent is implemented, with job creation to update all data in the database automatically and periodically. In the system that has been implemented, the update time can be adjusted according to needs. As for the implementation of database access, the type of access used is direct access to the database. For database types that apply role-based access control, or use a collection of database connections, you can also use an automated database audit system, because even if you apply role-based access control, the distribution of access rights will still be done so that there will be at least 2 connections to the database. However, the information obtained is not as complete as using the type of access directly to the database, so this can cause the audit process to be carried out not very efficiently.

### 3.4 Audit Tools Implementation

On the start page of the database audit application, the system will provide a Login feature for users who already have an account or register for a new user for the first time. After login, the system will provide a feature to select the RDBMS to be used and a feature to select the creation of a new database or the use of a database.

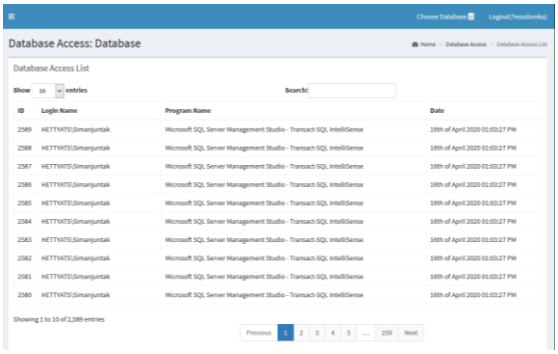


**Figure 3.** System View for Database Access List

Several reports can be used in the application, namely displaying a list of user access in the database as shown in Figure 3, account usage information can be seen in Figure 4, and a list of failed logins in Figure 5. Information on the account usage submenu in database access is shown to view users. that performs access outside normal operating hours.


**Figure 4.** System View for Account Usage

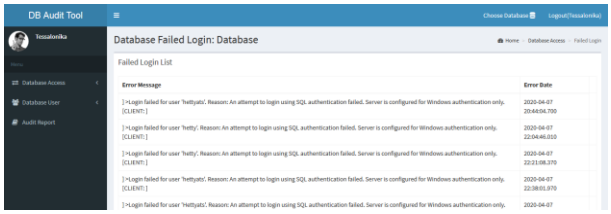


**Figure 5.** System View for Login Failed List



**Accredited "Rank 4"(Sinta 4),** DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Information regarding the list of database users, password changes, access rights by database users, and the roles owned by database users (user list) can be seen in Figure 6. The user list submenu on the database user is displayed to view the users in the database and the last time the user was in the database. it accesses the database. Through the user list submenu, as shown in Figure 6, users who are still active can be identified and analyzed who have not accessed the database for a certain period.


**Figure 6.** System View for Database User List

The display for database privileges information can be seen in Figure 7. The information displayed on the database privileges submenu is in the form of users and types of activities carried out by users in the database, as well as the status of access rights owned by users. Through this information, it can be known if there are users who do not access according to their access rights.

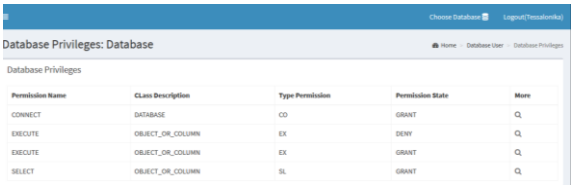


**Figure 7.** System View for Database Privilege

The display for the role list information can be seen in Figure 8. The role list submenu in the user database is displayed to show the roles owned by each user in the database.

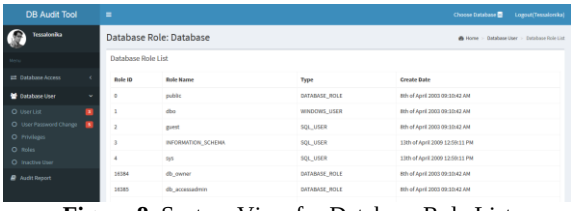


**Figure 8.** System View for Database Role List

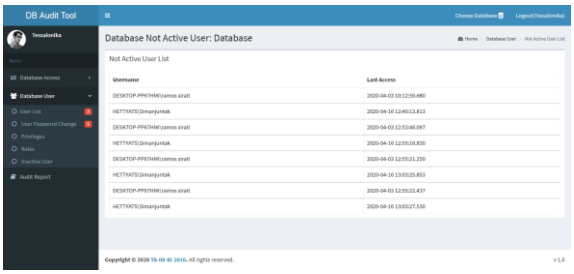


**Figure 9.** System View for Inactive User

### 3.5 Audit Report

The resulting audit report in Figure 10 is a summary of the information in the audit category which includes database access, database user. The audit report will be automatically generated by the system, where the audit report also contains recommendations for evidence found to be not under the established standards.



**Accredited "Rank 4"(Sinta 4),** DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Suspicious access report to display suspicious database access list generated from the analysis phase. The database access list consists of access date, user name, program name, and the number of accesses. This needs to be included in the audit report because any suspicious access found could be in the form of an attack on the database.

Inactive users report showing a list of users who have not accessed the database in a certain period. This needs to be included in the audit report because knowing the list of inactive users will help the auditor to provide recommendations such as changing the status of active users to inactive users. So that users can no longer access the database.

An out-of-hours access report is necessary because activities performed during off-hours are often suspect and may be the result of unauthorized users trying to access or modify data. Auditing access information outside of operating hours helps reduce the size of the audit trail that may need to be checked, as only activities that will be recorded outside of operating hours will be logged.

Reports of users who did not change their passwords within a certain period contain a list of users who did not change their passwords within a certain period. This needs to be included in the audit report because, in many sites and applications/systems that have user accounts, data verification is required to ensure that those who access a site or application are real users. One part of the data verification is to enter a password.

Therefore, changing the password within a certain period will help users maintain the privacy of existing data.

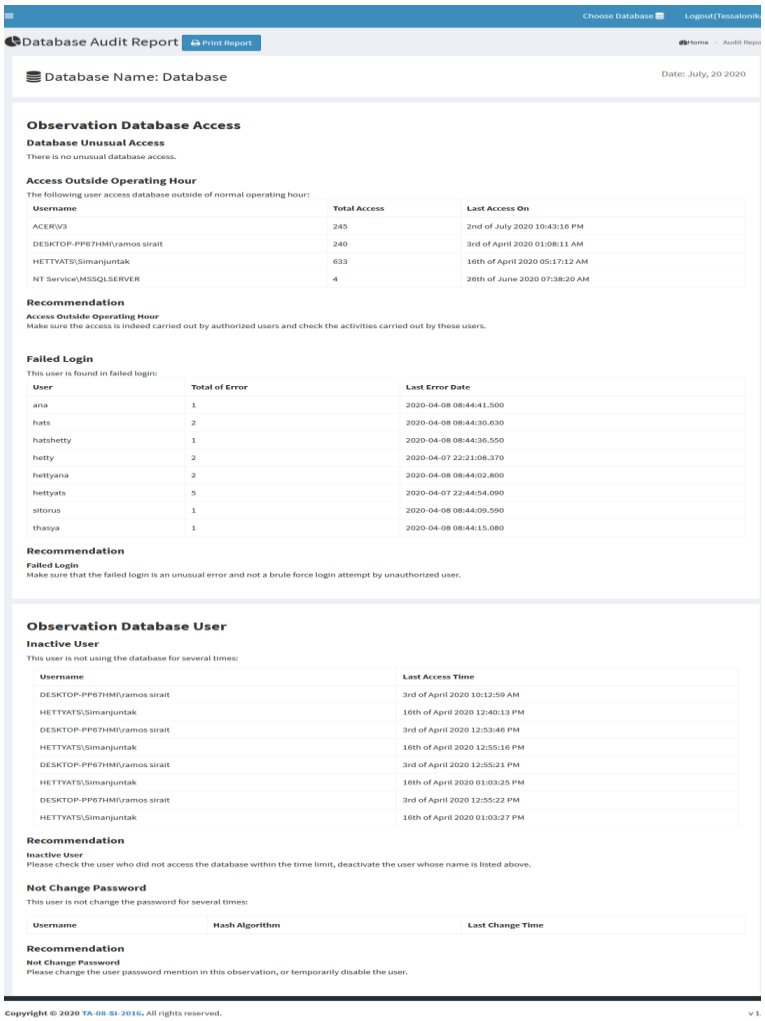


**Figure 10.** System View for Audit Report



**Accredited "Rank 4"(Sinta 4),** DIKTI, No. 36/E/KPT/2019, December 13th 2019.

## 4. Conclusion

The database audit architecture that has been designed can be used to assist auditors in collecting audit data, analyzing processes, and generating audit reports automatically. This research was successfully carried out by determining the aspects needed to conduct database audits, namely database audit architecture, database audit standards, and rules and database audit categories. The database audit automation design is then implemented in software in the form of a database audit automation system which is used as an evaluation tool for the success of the framework.

## 5. References

[1] M. Sendiang, A. Polii, and J. Mappadang, "Minimization of SQL injection in scheduling application development," 2017. doi: 10.1109/KCIC.2016.7883619.
[2] "ISACA GLOSSARY," www.isaca.org/pages/glossary.aspx?tid=1095&char=A .
[3] H. Abou-El-Sood, A. Kotb, and A. Allam, "Exploring Auditors' Perceptions of the Usage and Importance of Audit Information Technology," International Journal of Auditing, vol. 19, no. 3, pp. 252–266, 2015, doi: 10.1111/ijau.12039.
[4] S. D. Gantz, The Basics of IT Audit: Purposes, Processes, and Practical Information. 2013. doi: 10.1016/C2013-0-06954-X.
[5] S. A. Sayana, "Using CAATs to support IS audit," Information Systems Control Journal, vol. 1, pp. 21–23, 2003.
[6] I. Maciejewska, "Computer-assisted audit tools in relation with international standard on quality control 1 (ISQ1): (Based on experiences from polish small audit practices)," in 2015 10th Iberian Conference on Information Systems and Technologies, CISTI 2015, 2015, pp. 15–16. doi: 10.1109/CISTI.2015.7170617.
[7] N. A. Ismail and A. Z. Abidin, "Perception towards the importance and knowledge of information technology among auditors in Malaysia," Journal of Accounting and Taxation, vol. 1, no. 4, pp. 61–69, 2009.
[8] N. Mahzan and A. Lymer, "Examining the adoption of computer-assisted audit tools and techniques: Cases of generalized audit software use by internal auditors," Managerial Auditing Journal, vol. 29, no. 4, pp. 327–349, 2014, doi: 10.1108/MAJ-05-2013-0877.
[9] I. Pedrosa and C. Costa, "Computer assisted Audit Tools in real world: Idea applications and approache's in real context," in Proc. of the IADIS Int. Conf. Intelligent Systems and Agents 2010, Proc. of the IADIS European Conference on Data Mining 2010, Part of the MCCSIS 2010, 2010, pp. 151–155.
[10] Narongit Waraporn, "Database Auditing Design on Historical Data," Proceedings of the Second International Symposium on Networking and Network Security (ISNNS '10), vol. 1, pp. 275–281, 2010.
[11] O. O. Matthew and C. Dudley, "Critical Assessment of Auditing Contributions to Effective and Efficient Security in Database Systems," 2015, pp. 1–11. doi: 10.5121/csit.2015.50801.
[12] J. Woo, S. Lee, and C. Zoltowski, Database Auditing. 2006.
[13] Implementing Database Security and Auditing. Burlington: Elsevier Inc, 2009. doi: 10.1016/b978-1-55558-334-7.x5000-2.
[14] M. Bishop, Computer Security Art and Science. 2003.