A

Dissertation

On

Decision Table Based Model & its Implementation for Automatic Prevention of Unauthorized Database Transactions by Trusted Database Users

for the submission of partial fulfilment of degree of

Master of Technology

In

Computer Science and Engineering

2014

Submitted by:

Rohit Jain

2K11/CSE/24

Under the supervision of:

Dr. Kapil Sharma

Associate Professor, DTU.

Department of Computer Engineering

Delhi Technological University

Shahbad Daulatpur, Bawana Road, New Delhi

2013-2014

A

Dissertation

On

Decision Table Based Model & its Implementation for Automatic Prevention of Unauthorized Database Transactions by Trusted Database Users

for the submission of partial fulfilment of degree of

Master of Technology

In

Computer Science and Engineering

2014

Submitted by:

Rohit Jain

2K11/CSE/24

Under the supervision of:

Dr. Kapil Sharma

Associate Professor, DTU.

Department of Computer Engineering

Delhi Technological University

Shahbad Daulatpur, Bawana Road, New Delhi

2013-2014

Abstract

Database security is one of the most important issues for any organization, especially for financial institutions such as banks, stock exchanges, insurance firms, etc. Database security has always been an important subject of research for researchers. Existing security policies are inadequate to prevent the attacks from insiders (trusted users) and require human intervention in some form or other to detect unauthorized transactions.eg Oracle Vault. This thesis addresses this issue and proposes an automated detection and prevention mechanism with minimal/nil human interaction. Each database user is authorized to do particular transactions by performing a sequence of queries. These queries perform operations (select, insert, update, delete) on various attributes of different tables in RDBMS. However the sequence of queries, attributes & tables authorized to User1 are not authorized to User2. User2 may be authorized to perform a different sequence and types of queries. If in a Database, User2 is able to deviate from its normal course of transaction queries and perform such a query for which it is not authorized then it is a serious breach in database security. This thesis proposes a Decision Table based methodology and a working model to protect databases from such security breaches and prevent trusted database users from doing unauthorized Transactions. Our approach recommends creation of Decision tables with the help of TQLC (Transaction Queries Log Crawler), Authorized Query Indicator Arrays (AQIA), Transaction Query Sequence Analyzer Arrays(TQSAA), Query Weight Analysis and Quad Phase Verification Techniques. These decision tables automatically identify any malicious intent during Transaction initiated from a User thereby, suggesting and activating a particular action as specified in Decision Table. We have implemented this system model in Oracle-J2EE based environment. Our model is also equipped with the feature of "Customization in Implementation".. For experimental purposes, we are generating arbitrary dummy transaction loads to measure the overall performance of our mechanism through graphical Dashboard.

Keywords: Transaction Authorization, Decision Table, Transaction Queries Log Crawler (TQLC), Authorized Query Indicator Arrays (AQIA), Transaction Query Sequence Analyzer Arrays (TQSAA), Query Weight Analysis, Quad Phase Verifier.

Acknowledgement

I would like to express my deepest gratitude to my supervisor **Dr. Kapil Sharma** for his invaluable guidance and support. His creativity and innovative skills have always been a constant source of motivation for me. He is a great person and one of the best mentors. I will always be thankful to him. I would also like to thank **Mr. G.K. Maishi (GGM/CRIS)** for devoting his precious time in discussing ideas with me, guidance on relevant topics and giving his invaluable feedback. I also wish to convey my sincere gratitude to **Prof. O.P Verma, Head of Department** for the enormous support provided by him. I would like to extend the thanks to all the faculty members for their motivation and moral support. I would like to thank all my fellow students for their cooperation and support. I would like to dedicate this thesis to my supportive parents and caring wife who have always been with me to make it a complete success.

Rohit Jain
2K11/CSE/24,
Master of Technology,
Computer Science & Engineering,
Delhi Technological University

Certificate

This is to certify that the work submitted in this thesis entitled **"Decision Table based Model & its implementation for Automatic prevention of Unauthorized Database Transactions by Trusted Database Users"** submitted in partial fulfilment for the award of degree of **Master of Technology in Computer Science & Engineering** at **Department of Computer Engineering, Delhi Technological University** by **Rohit Jain, Roll No. 2K11/CSE/24** is carried out by him under my supervision and guidance. The matter embodied in this thesis has not been submitted earlier for the award of any degree or diploma in any institution to the best of my knowledge and belief. He has completed his work with utmost diligence and sincerity.

Place:
Date:

Dr. Kapil Sharma
Associate Professor
Department of Computer Engineering
Delhi Technological University

Declaration

I hereby declare that the thesis entitled **"Decision Table based Model & its implementation for Automatic prevention of Unauthorized Database Transactions by Trusted Database Users"** which is being submitted to the **Delhi Technological University**, in partial fulfilment of the requirements for the award of degree of **Master of Technology in Computer Science & Engineering** is an authentic work carried out by me. The material contained in this thesis has not been submitted to any university or institution for the award of any degree.

Rohit Jain
Master of Technology
(Computer Science & Engineering)
Roll No. 2K11/CSE/24
Department of Computer Engineering
Delhi Technological University

Table of Contents

Abstract **(ii)**

Acknowledgement **(iii)**

Certificate **(iv)**

Declaration **(v)**

List of Figures **(vi)**

List of Tables **(vi)**

1. Chapter 1 : Introduction.....1
1.1. Introduction.....1
1.2. Organization of the Thesis.....2

2. Chapter 2 : Literature Survey.....3

3. Chapter 3 : Proposed Methodology.....4
3.1. AQIA- Authorized Query Indicator Arrays.....7
3.2. TQSAA- Transaction Query Sequence Analyzer Array.....9
3.3. QWA- Query Weight Analysis Algorithm.....10

4. Chapter 4 : Quad Phase Verifier.....13
4.1. Phase I- Operator Verifier.....14
4.2. Phase II- Relations/Attributes Verifier.....15
4.3. Phase III- Sequence Verifier.....16
4.4. Phase III- Weight Algorithm Verifier.....17
4.4.1. Query Weight Analysis Algorithm.....17

5. Chapter 5 : Decision Table.....20
5.1. Background.....20
5.2. Decision Table based Model.....20

6. Chapter 6 : Oracle-J2EE Implementation.....25
6.1. Enabling Database Audit Setup.....25
6.2. TQLC Implementation.....26
6.3. AQIA Implementation.....27

7. Chapter 7 : Experimental Evaluation.....29
7.1. Decision Table Reference Time.....29
7.2. False Negatives.....30
7.2.1. False Negatives Percentage vs Single Phase selection.....30

7.2.2. False Negatives Percentage vs Double Phases selection.....30
7.2.3. False Negatives Percentage vs Triple Phases selection.....31
7.2.4. False Negatives Percentage vs Quad Phases selection.....31
7.3. Coverage.....32

8. Chapter 8 : Conclusion and Future Work.....33
8.1. Conclusion.....33
8.2. Scope for Future Work.....33

References.....34

Publications from the work.....35

Appendix-I Source Code.....36

Appendix-II Screen Shots of Application.....66

List of Figures

1. Quad Phase Verifier.....6
2. Decision Table 1.....23
3. Decision Table 2.....23
4. Decision Table Reference Time Vs No. of Phases.....29
5. False Negatives Percentage Vs Single Phases selection.....30
6. False Negatives Percentage Vs Double Phases selection.....30
7. False Negatives Percentage Vs Triple Phases selection.....31
8. False Negatives Percentage Vs Quad Phases selection.....31
9. Coverage Vs Quad Phases phase selection.....32

List of Tables

1. Data from Audit Tables.....5
2. AT Store Entries.....5
3. AQIA.....8
4. Query Weights Table.....9