Degree Project in Computer Engineering
First cycle, 15 credits

Mapping out the Key Security Components in Relational Databases (MK-SCoRe)
Enhancing the Security of Relational Database Technology

MURTADHA ALOBAIDI
ABDULLAH TRABULSIAH
Mapping out the Key Security Components in Relational Databases (MK-SCoRe)

Enhancing the Security of Relational Database Technology

MURTADHA ALOBAIDI
ABDULLAH TRABULSIAH

Degree Programme in Computer Engineering
Date: January 29, 2024

Supervisor: Mira Kajko-Mattson
Examiner: Ki Won Sung

School of Electrical Engineering and Computer Science
Swedish title: Kartläggning av Nyckelkomponenter för Säkerhet i Relationsdatabaser (MK-SCoRe)
Swedish subtitle: Förbättring av Säkerheten i Relationsdatabasteknik
Abstract

Relational database security has become an increasingly important issue for organizations worldwide in the current era of data-driven operations. The urgent need for an extensive knowledge of relational database security components in relational databases is addressed in this thesis. Database security is constantly improving, but there is still a lack of research that analyzes these important factors. Because of this gap, databases are not sufficiently secured from new cyber threats, which endangers its accessibility, confidentiality, and integrity.

The problem that the thesis addresses is the lack of comprehensive research covering all key security components in relational databases which, presents a challenge for organizations seeking to comprehensively secure their database systems. The purpose of this thesis is to systematically map the key security components essential to relational databases. The goal is to assist organizations and Database professionals to secure their relational databases against diverse cyber threats. Using a qualitative and exploratory methodology, the research analyzes a wide range of literature on database security. The research offers a balanced and comprehensive perspective on the current security landscape in relational databases by integrating theoretical study with structured interviews. This method guarantees that all essential security components is fully investigated.

The results of this thesis involve a detailed mapping of the key security components within relational databases, which are uniquely informed by a combination of academic research and empirical findings from structured interviews with Database security experts. This thesis analyzes these security components based on how well they address current security threats, how well they secure databases, and how well they can adapt to different organizational needs.

Keywords

Sammanfattning

Säkerhet i relationsdatabaser har blivit en allt viktigare fråga för organisationer världen över i den nuvarande eran av datadriven verksamhet. I den här avhandlingen behandlas det akuta behovet av en omfattande kunskap om säkerhetskompomenter för relationsdatabaser i relationsdatabaser. Databassäkerheten förbättras ständigt, men det finns fortfarande en brist på forskning som analyserar dessa viktiga faktorer. På grund av denna brist är databaser inte tillräckligt skyddade mot nya cyberhot, vilket äventyrar deras tillgänglighet, konfidentialitet och integritet.


Resultatet av denna avhandling innebär en detaljerad kartläggning av de viktigaste säkerhetskompomenterna inom relationsdatabaser, som är unikt informerade av en kombination av akademisk forskning och empiriska resultat från strukturerade intervjuer med databassäkerhetsexperter. Denna avhandling analyserar dessa säkerhetskompomenter utifrån hur väl de hanterar aktuella säkerhetshot, hur väl de säkrar databaser och hur väl de kan anpassas till olika organisatoriska behov.

Nyckelord

Säkerhet i Relationsdatabaser, Databassäkerhet, Cyberhot, Datasäkerhet, Åtkomstkontroll, Sårbarheter i Databaser, Kryptering, Nätverkssäkerhet.
Acknowledgments

We are very thankful to Mira Kajko-Mattsson for all the help and advice she gave us while we were working on our thesis. We also want to thank Ki Won Sung for being our Examiner during this very important academic time.

We extend our sincere gratitude to our families for their unwavering support and dedication. Their encouragement has been invaluable throughout this journey. Additionally, we would like to express our profound appreciation to Hesham Abbas for his generous contribution of time and expertise, which significantly assisted us in our endeavors.

Stockholm, January 2024
MURTADHA ALOBAIDI  ABDULLAH TRABULSIAH
# Contents

1 Introduction ................................. 1
   1.1 Background ................................. 1
   1.2 Problem .................................. 2
   1.3 Research Question ......................... 2
   1.4 Purpose .................................. 3
   1.5 Goals .................................... 3
   1.6 Research Methodology ..................... 3
   1.7 Target Audience ............................ 4
   1.8 Scope and Limitations ...................... 4
   1.9 Benefits, Ethics and Sustainability ........ 6
   1.10 Thesis outline ............................ 6

2 Relational Databases ......................... 9
   2.1 History of the database ...................... 10
   2.2 Fundamentals of Relational Database Systems .... 11
      2.2.1 Defining Relational Databases Structure .......... 11
      2.2.2 SQL Language ........................... 12
      2.2.3 Benefits of relational databases ............... 13
   2.3 Database Security .......................... 14
   2.4 Related work ................................ 15
      2.4.1 Importance of Relational Database Security .... 16
      2.4.2 Overview of Database Security and Technology ... 16
      2.4.3 Data Protection in Remote Information Systems ... 17

3 Research Methodology ......................... 19
   3.1 Research Strategy .......................... 19
   3.2 Research Methods .......................... 20
   3.3 Research Phases ........................... 21
      3.3.1 Pre-study ............................... 22
3.3.2 Literature Study ........................................... 24
3.3.3 Data Synthesis .............................................. 26
3.3.4 Critical Analysis and Evaluation ......................... 28
3.3.5 Final Improvements ...................................... 30
3.4 Research instruments ..................................... 32
3.5 Respondents .................................................. 33
3.6 Validity Threats .............................................. 34

4 Evaluation Model ............................................. 35
  4.1 Expert Evaluation Criteria .................................. 35
  4.2 Interviewee Credibility .................................... 36
  4.3 Semantic Correctness ..................................... 37
  4.4 Syntactic Correctness ..................................... 37
  4.5 Usefulness .................................................. 38
  4.6 Open-ended Questions .................................... 39

5 Preliminary Results .......................................... 41
  5.1 Overview .................................................... 41
  5.2 Access Controls .......................................... 42
    5.2.1 Authentication ....................................... 42
    5.2.2 Authorization ........................................ 44
  5.3 Data Protection ........................................... 46
    5.3.1 Encryption ........................................... 46
    5.3.2 Backup Strategies ................................... 48
  5.4 Monitoring and Auditing .................................. 50
    5.4.1 Dynamic Auditing and Logging ...................... 50
    5.4.2 Database Activity Monitoring (DAM) ............... 51
  5.5 Network Security .......................................... 53
    5.5.1 Network Security Protocols ......................... 53
    5.5.2 Database Firewall .................................... 54
  5.6 Vulnerability Prevention .................................. 56
    5.6.1 Parameterized Queries and SQL Injection Prevention ........................................... 56
    5.6.2 Patch Management .................................... 57
  5.7 Awareness and Education .................................. 58
    5.7.1 Security Training ..................................... 59

6 Expert Assessment and Component Evaluation ............ 61
  6.1 Expert Assessment ......................................... 61
  6.2 Interviewee Credibility .................................... 62
  6.3 Semantic Correctness ..................................... 63
6.4 Syntactic Correctness ........................................... 63
6.5 Usefulness ......................................................... 63
6.6 Open-ended questions ........................................... 64
   6.6.1 Interviewee 1 .............................................. 64
   6.6.2 Interviewee 2 .............................................. 64

7 Improved Results .................................................... 67
   7.1 Refinement of Access Control Strategies ....................... 67
   7.2 Enhanced Monitoring and Auditing ............................ 69
   7.3 Proactive Vulnerability Management .......................... 70
   7.4 Summary ........................................................ 70

8 Analysis and Discussion ............................................ 73
   8.1 Analysis of Key Security Components .......................... 73
      8.1.1 Access Controls ......................................... 73
      8.1.2 Data Protection .......................................... 74
      8.1.3 Monitoring and Auditing ................................ 76
      8.1.4 Network Security ........................................ 77
      8.1.5 Vulnerability Prevention .................................. 78
      8.1.6 Awareness and Education ................................ 79
   8.2 Evaluating the Validity ...................................... 80

9 Conclusions and Future Work ..................................... 82
   9.1 Conclusions .................................................... 82
   9.2 Limitations ..................................................... 83
   9.3 Future Work .................................................... 83
   9.4 Reflections ...................................................... 84

References ............................................................. 85

A Supporting materials ............................................... 93
   A.1 Interview answers ............................................ 93
List of Figures

2.1 Various type of databases (adapted from [10]) .......................... 10
2.2 Relational databases Schema .............................................. 12
2.3 Create a new database SQL query ......................................... 13
2.4 Create table with SQL Language ............................................ 13
2.5 Insert SQL query ................................................................. 13

3.1 Research Strategy .................................................................. 20
3.2 Overview of The Research Phases ........................................... 22
3.3 Overview of Pre-study Phase ................................................. 24
3.4 Overview of Literature Study Phase ........................................ 26
3.5 Overview of Data Synthesis Phase ......................................... 28
3.6 Overview of Critical Analysis and Evaluation Phase ............... 30
3.7 Overview of Final Improvements Phase .................................. 31

5.1 Key Security Components Overview ..................................... 42
5.2 Two-factor authentication flowchart[29] ................................. 43
5.3 A system architecture for an adaptable authorization mechanism[33] 45
5.4 TDE Encryption Overview[35] .............................................. 47
5.5 AES algorithm working ...................................................... 48
5.6 Overview of the Backup Strategies ........................................ 49
5.7 Overview of Database Activity Monitoring (DAM) .................. 52
5.8 Intrusion Detection and Prevention Systems (IDPS) (IDS & IPS) 54
5.9 Database Firewalls overview .................................................. 55
List of Tables

2.1 Relational databases table (Users Table) . . . . . . . . . . . . . . . . . . . . 11
4.1 Open-ended Questions . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 40
7.1 Enhancements in Relational Database Security Components from Preliminary to Improved Results . . . . . . . . . . . . . . . . . . . . . . . . 72
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABAC</td>
<td>Attribute-Based Access Control</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>AI</td>
<td>Artificial Intelligence</td>
</tr>
<tr>
<td>AOL</td>
<td>America Online</td>
</tr>
<tr>
<td>DAG</td>
<td>Directed Acyclic Graph</td>
</tr>
<tr>
<td>DAM</td>
<td>Database Activity Monitoring</td>
</tr>
<tr>
<td>DBaaS</td>
<td>Database as a Service</td>
</tr>
<tr>
<td>DBMS</td>
<td>Database Management Systems</td>
</tr>
<tr>
<td>HIDS</td>
<td>Host-based Intrusion Detection System</td>
</tr>
<tr>
<td>IDPS</td>
<td>Intrusion Detection and Prevention System</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>IPS</td>
<td>Intrusion Prevention System</td>
</tr>
<tr>
<td>KTH</td>
<td>KTH Royal Institute of Technology</td>
</tr>
<tr>
<td>MFA</td>
<td>Multi-Factor Authentication</td>
</tr>
<tr>
<td>ML</td>
<td>Machine Learning</td>
</tr>
<tr>
<td>NIDS</td>
<td>Network-based Intrusion Detection System</td>
</tr>
<tr>
<td>NoSQL</td>
<td>Non-relational</td>
</tr>
<tr>
<td>OTP</td>
<td>One-Time Password</td>
</tr>
<tr>
<td>RAAC</td>
<td>Risk-Adaptive Access Control</td>
</tr>
<tr>
<td>RBAC</td>
<td>Role-Based Access Control</td>
</tr>
<tr>
<td>RDBMS</td>
<td>Relational Database Management Systems</td>
</tr>
<tr>
<td>SIEM</td>
<td>Security Information and Event Management</td>
</tr>
<tr>
<td>SQL</td>
<td>Structured Query Language</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>TDE</td>
<td>Transparent Data Encryption</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction

The need to store and process massive volumes of data has grown since the beginning of the digital age. Big tech companies like Google and Meta are collecting and storing vast amounts of personal data in their databases, making them leaders in the data revolution. The increasingly growing challenge of securing this data from possible cyber threats is a direct result of its collection.

Recently, there has been a significant rise in the importance of ensuring the security of databases, especially those containing information on sensitive or critical systems. The security of databases is a major concern for data centers, particularly those linked to organizations in the government sector. Ensuring the security, integrity, and authenticity of the information stored within them requires this safeguard.

1.1 Background

In the field of information security, and particularly within relational databases, the primary focus has always been on the security of data. The implementation of a variety of security measures by database management systems in the digital context is a reflection of the traditional necessity of securing valuable data. Critical at various points: when data is processed within applications, while it is transmitted across network channels, and when it is stored in data stores for future use. The complex nature of database security are further complicated by the wide variety of database management systems. Showing how complicated and varied data security is, each system may use its unique mechanisms and procedures to keep data secure.

Database security faces new challenges as the landscape of cyber threats
changes constantly. With the help of more complex methods, cybercriminals are breaching data warehouses and exploiting vulnerabilities to steal sensitive company information. The complicated relationship between cybersecurity and database administration is underlined by the association between these methods of attack and database operations [1].

With an evolving environment of stored data and the sophistication of cyber attack methods, database security is a dynamic topic that requires ongoing adaptation and evolution. Developing strong security frameworks and establishing efficient defenses in place are crucial for maintaining the reliability and security of relational databases.

1.2 Problem

There is still a major problem that has not been solved in both theoretical and practical database security research, even though there has been considerable progress and heightened awareness about database security in general and relational databases in particular. The lack of thorough and organized research that identifies and maps out the critical security components essential to relational databases is the root cause of this problem.

In the current state of database security research and practice, isolated security incidents or particular defensive measures are frequently the focus. Despite its usefulness in dealing with current vulnerabilities and threats, this approach does not take the big picture into consideration. It fails to investigate or comprehend the interconnections of relational databases numerous security components. Due to a lack of comprehensive research and understanding, security measures are implemented in stages, potentially leaving important aspects unexplored or unsecured. This research gap has serious and broad impacts. With the growing reliance on relational databases for sensitive data storage, processing, and management, organizations find themselves dealing with a variety of complex and constantly evolving cyber threats. Attacks may target neglected or under-researched areas because there is not an comprehensive research that outlines all important security components within relational databases.

1.3 Research Question

This thesis addresses the critical issue of the lack of comprehensive and systematic research on identifying and mapping out key security components
in relational databases with the following research question:

What are the key security components in relational databases, how can they be comprehensively identified and mapped out, and what are the most prevalent methods and approaches associated with these components to enhance the security and integrity of these databases?

This thesis’ foundational research question guides the research process. It explores into database security, particularly in relational databases, and produces an outline that identifies security components, understands their interconnectivity, and supports relational databases secure. The question encourages an overall approach to database security, moving beyond isolated incidents and defensive methods to secure relational databases systematically.

1.4 Purpose

The purpose of this thesis is to map out the relational database security key components. The focus of this research is to systematically identify and defines all critical security components found in relational databases as well as the most prevalent methods and approaches associated with these components to enhance the security and integrity of these databases.

1.5 Goals

The goal is to assist organizations and database professionals with securing their relational databases intensively against modern cyber threats by providing them with comprehensive mapping of the security components of relational databases. By encouraging for a more advanced and comprehensive perspective on relational database security measures and their execution.

1.6 Research Methodology

A systematic mapping of the critical security components of relational databases is the central emphasis of this thesis. A thorough familiarity with database security mechanisms as well as new threats was necessary for this. An extensive literature review and structured expert interviews were the main components of the qualitative methodology that was used. The relational database literature review aimed to compile data on the various
security measures, flaws, and safeguards in relational databases. Critical security components were categorized and possible gaps were identified by synthesizing the results of the publications. Critical security components are categorized and possible gaps are identified by synthesizing the results of the publications. In order to strengthen and supplement theoretical findings with practical perspectives from the industry, expert interviews are conducted. Phases of scope definition, data collection, data synthesis, critical analysis, and refinements make up the research design’s iterative process. Belief in the robustness and generalizability of the conclusions is ensured by rigorous validity criteria centered on reliability, credibility, transferability, and objectivity [3] [4].

In summary, structured expert interviews and a thorough literature review serve as the foundation for a qualitative methodology. Establishing a systematic road map of the critical components that resolve integrity and security issues in relational database implementations is the objective. Further details of the research method are presented in Chapter 3.

1.7 Target Audience

This thesis addresses industry professionals and researchers. The findings can assist information security engineers, database administrators, and technical leaders secure relational databases by industry. Detailed mapping of critical database security components helps improve and tailor defense mechanisms. Also, the research methodology and results add to database security academic literature. The thesis identifies current knowledge gaps that need further study. It categorizes and evaluates security controls. Academics can use this research to study database vulnerabilities, new attack vectors, and innovative safeguards.

In summary, this thesis aims to help technology practitioners harden production databases and promote rigorous research into database security and cryptographic controls. Both audiences benefit from the synthesis of practical and theoretical perspectives.

1.8 Scope and Limitations

This thesis mainly aims to map out the essential security components of relational database systems and analyze their efficacy. The management of vulnerabilities, such as Structured Query Language (SQL) injection attacks,
and other security measures, including authentication procedures, encryption methods, and access control mechanisms, are all thoroughly examined. To better understand the present security practices and issues in relational databases, our study incorporates insights from structured interviews with academic and industry professionals and conducts a comprehensive literature review. A comprehensive understanding of how these security components function in real-world scenarios is achieved by focusing on both theoretical concepts and practical applications.

Having said that, it is important to note that the thesis does have some limitations:

- **Scope of Research:** While the thesis covers a wide range of security components, due to the vastness of the field, it does not delve into every aspect of database security. The study focuses primarily on the most critical and widely used security measures in relational databases.

- **Diversity of Databases:** The research focuses primarily on relational databases. As a result, the findings and conclusions may not apply directly to other types of database systems, such as Non-relational (NoSQL) databases.

- **Rapidly Evolving Field:** The field of cybersecurity, particularly database security, is rapidly evolving. As a result, some of the findings may become outdated as new technologies and security threats emerge.

- **Subjectivity in Interviews:** Despite the structured approach to interviews, there is some subjectivity in the responses and interpretations, which may influence the study’s findings.

- **Generalizability:** Given the study’s focus on relational databases and the specific security components chosen, the findings may not be fully generalizable to all database environments or security scenarios.
1.9 Benefits, Ethics and Sustainability

The section emphasizes the research’s commitment to ethical standards and its contribution to sustainable practices in database security, while also highlighting the research’s multifaceted advantages. With its detailed outline of critical security components in relational databases, this study is an advantage to academics and businesses alike, paving the way for better security measures and more well-informed decisions. It stresses the importance of doing research and evaluations with the highest standards of honesty and confidentiality, as well as the ethical obligation to protect the privacy of individuals. The research is also in line with sustainable practices since it supports security models that can change with the times and new threats. This strategy guarantees database security’s long-term viability and resilience, aiding in the long-term growth of secure digital infrastructures. A more secure and safe digital environment that strikes a balance between technological progress, ethical concerns, and sustainable practices is the objective of the study’s meticulous research.

1.10 Thesis outline

This thesis is organized into seven chapters:

- **Chapter 2**: Detailed history of databases, focusing on security developments and challenges.
- **Chapter 3**: Outlines research strategy, methods used, and phases of research process.
- **Chapter 4**: Structured evaluation of database security components through professional knowledge.
- **Chapter 5**: The preliminary results obtained from the extensive study focused on mapping out the key security components in relational databases.
- **Chapter 6**: Evaluating the efficacy and relevance of key security components identified in relational databases.
- **Chapter 7**: Presents enhanced methods for access control and vulnerability reduction.
• Chapter 8: It goes into analysis, providing insightful reviews that support the research’s main points and database security measures.

• Chapter 9: Summarizes the research’s findings, suggests recommendations, and points out potential avenues for future research.
8 | Introduction
Chapter 2

Relational Databases

Relational Database are pivotal in data management across various industries. These systems store and organize vast amounts of data in related tables, accessible and modifiable via SQL. The relational structure facilitates intricate queries and transactions, vital for diverse business and application needs.

The central role of Relational Database in organizational operations renders them susceptible to cyber-attacks. Breaches or unauthorized access could lead to substantial losses in terms of finance, reputation, or functionality. These incidents highlight vulnerabilities in the key areas of database security: confidentiality, availability, and integrity. Both academia and industry are focused on bolstering Relational Database security. Notable security breaches, like the America Online (AOL) data leak and Adobe's loss of user credentials and source code, underscore the dire consequences of security lapses. The widespread use of Relational Database necessitates a nuanced approach to security, encompassing best practices and compliance with standards like ISO 27001. Yet, security implementations vary across different Relational Database platforms, leading to disparities in security controls [5][6][7][8][9].

The urgent need for a comprehensive, coherent strategy tailored to Relational Database security is clear. This necessitates identifying and integrating best practices, regulatory standards, and advanced security measures into a cohesive framework. The aim is to fill gaps in traditional security approaches and adapt to the ever-changing cyber threat landscape, bolstering the security posture of relational databases with a resilient, forward-thinking protection strategy.

In this chapter, the groundwork is laid for understanding the evolution, security concerns, and academic contributions in the realm of relational database. Section 2.1 outlines the evolution of Relational Databases,
emphasizing key developments and milestones. Section 2.2 explores the structure and significance of relational databases, particularly focusing on SQL's role. Section 2.3 examines the security challenges and consequences of breaches in relational databases. Lastly, Section 2.4 presents a synthesis of influential research and studies in the field of database security.

## 2.1 History of the database

In the 1960s, organizations increasingly adopted computer technology, which led to the development of early models such as the hierarchical CODASYL and the networked IMS. E.F. Codd introduction of the relational model in the 1970s, which organized data in tables independent of physical storage, marked a significant transition. This era also witnessed the development of SQL and theoretical advancements such as Peter Chen’s Entity-Relationship model.

In the 1980s, relational database systems from Oracle, IBM, and Microsoft became mainstream, solidifying their dominance. This decade also saw the introduction of novel development tools and the client-server model. The 1990s witnessed the development of open source databases such as MySQL and PostgreSQL, as well as the transition of databases into consumer interactions, such as ATMs. The era of "Big Data" was ushered in by the internet and e-commerce in the 2000s. Today, databases serve as the foundation for a variety of digital platforms, including websites and applications [10].

As database technologies continue to advance, so does the need to identify and correct inherent security vulnerabilities. It is essential to ensure the safety of users who interact with these technologies. Whatever of the type, databases that are commonly used integrate a variety of security mechanisms, each with its own strengths and weaknesses [11].

![Figure 2.1: Various type of databases (adapted from [10])](image)
2.2 Fundamentals of Relational Database Systems

In order to have a thorough comprehension of the thesis, it is important to systematically present facts related to the two particular database technologies. The relevant details can be located in the following subsections. In the subsections 2.2.1 exploration the relational database definition and fundamental principles. Subsections 2.2.2 exploration the pivotal role of Structured Query Language (SQL). Subsections 2.2.3 The discussion aims to elucidate the structured design of relational database and how this design facilitates efficient data management across various industries.

2.2.1 Defining Relational Databases Structure

A relational database is a specific form of database that is designed to contain and facilitate access to linked data points. Relational databases are based on the relational model, which is a logical and natural approach for organizing and expressing data in tabular form. Within the context of a relational database, it is crucial to note that every individual row included within a table represents a distinct record, which is assigned a unique identifier referred to as the key. The attributes of the data are stored in the columns of the table, with each record typically containing a value for each property. This facilitates the establishment of associations between data points [12]. The tables in a relational database has defined relationships for easy access and consist of columns and rows, each column is a property that describes the relation and each row presents a unique record. The relationships created between the tables with help of a key see table 2.1. These structures make it simple for database administrators to edit the physical data storage [13].

<table>
<thead>
<tr>
<th>UserID</th>
<th>Username</th>
<th>FirstName</th>
<th>LastName</th>
<th>Email</th>
<th>RegistrationDate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>user1</td>
<td>John</td>
<td>Doe</td>
<td><a href="mailto:john.doe@email.se">john.doe@email.se</a></td>
<td>2022-01-15</td>
</tr>
<tr>
<td>2</td>
<td>user2</td>
<td>Jane</td>
<td>Smith</td>
<td><a href="mailto:jane.smith@email.se">jane.smith@email.se</a></td>
<td>2022-02-20</td>
</tr>
<tr>
<td>3</td>
<td>user3</td>
<td>Alice</td>
<td>Johnson</td>
<td><a href="mailto:alice.johnson@email.se">alice.johnson@email.se</a></td>
<td>2022-03-10</td>
</tr>
</tbody>
</table>

Table 2.1: Relational databases table (Users Table)

For example, in a small library, users can borrow books, and each user has a unique key called UserID which is used to establish the relationship between the Users table and the BorrowedBooks table see Figure 2.2.
Structured Query Language, or SQL, was developed at IBM by Don Chamberlin and Ray Boyce. It is now the industry-standard programming language for communicating with relational databases. SQL makes it simple for database administrators to insert, edit, or delete rows of data. It was originally referred to as SEQUEL, but because of a trademark dispute, it was shortened to SQL. Using SQL queries, users are able to retrieve data from databases while just having to write a few lines of code. Due to the close relationship between the two, it is not hard to see why relational databases are sometimes referred to as "SQL databases." [14].

For instance, if we need to make a User Table, we would do the same thing as in this image (see figure 2.1). Creating a database is the first thing that has to be done. In this scenario, we created a new database by using MySQL; for an example, see the figure referenced here (2.3). Then, in order to create the table, we make use of the SQL Query Language (see figure 2.4). We use this SQL query to insert data into this table, which is referred to as the Users Table (see Figure 2.5).
2.2.3 Benefits of relational databases

Relational database have been an indispensable component of the data management industry. They offer a variety of advantages:

- Ease of Use: Relational databases have been around for a very long time, which has allowed for the development of a strong community that revolves around them. Their user-friendliness is helped along by the big community that supports them [14].
• Efficient Data Retrieval: Users of relational databases have the ability to easily access data from many tables and execute modifications such as filtering and aggregation thanks to the support provided by structured query language (SQL). In addition, the use of indices in relational databases ensures that data may be located quickly, doing away with the need to search through each row in a table. This is made possible by the fact that indices are implemented [14].

• Flexibility: The opinion that relational databases are less flexible and more strict than other storage solutions has changed, despite the fact that this opinion has been held for a long time. These databases are becoming more flexible as a result of developments in technology, as well as the proliferation of Database as a Service (DBaaS) offerings; this is particularly true when they move to cloud-based operating environments [14].

• Reduced Redundancy: Relational databases are built to reduce the amount of duplicate data as much as possible, so guaranteeing that data is stored in an effective and consistent manner [14].

2.3 Database Security

Since the beginning of digital data storage, the practice of database security has significantly evolved. Initially, the focus was on physical security measures and basic access control. Nevertheless, as databases became crucial to organizational operations, the need for more advanced security measures emerged.

Database management software originally centered on building strong perimeter defenses. The underlying assumption of this strategy was that external threats were more common and more serious than internal ones. Among the perimeter defense mechanisms were measures to stop outsiders from getting into the network. Network authentication systems and firewalls are two examples of such mechanisms. The strategy’s underlying assumption was that internal security controls could be reduced once users were inside the perimeter, allowing for greater trust. The complexity of security requirements and our growing awareness of internal threats have caused a change in this viewpoint, though. To defend against both internal and external database threats, modern security measures must be more complex and multi-layered.

Over time, this view shifted dramatically with increased recognition of
internal dangers, such as malicious insiders and compromised accounts [15]. Consequently, database security has advanced substantially with the advent of digital data storage. At first, efforts were concentrated on setting up basic access regulations and other forms of physical security. However, it became apparent that additional, more sophisticated security measures were required as database management became more integral to the operations of the organization [16]. Assuming that threats from within were uncommon, the first database management systems implemented perimeter defense mechanisms. This perspective, however, significantly changed as an increasing number of people learned about the risks posed by malicious insiders and compromised accounts [15].

Databases in the modern digital landscape are more than just data warehouses; they are living, breathing entities that communicate with other programs and their users. Because of this interaction, databases are vulnerable to a wide variety of threats, such as outsider access, data breaches, SQL injection, and even attacks from within the organization. Databases are frequently the primary target of cyberattacks because they store sensitive and crucial information. The sophistication of these attacks has increased over time, necessitating a more comprehensive approach to database security [17].

In the realm of relational databases, maintaining robust security is a critical endeavor. The complexity and sensitivity of data managed within these systems necessitate vigilant protection against a spectrum of cyber threats. As technology evolves, so do the challenges in securing relational databases, highlighting the need for advanced and adaptable security measures. These measures not only defend against current threats but also prepare systems to withstand future vulnerabilities. The history of database security reveals a trajectory from rudimentary access controls to multifaceted security techniques. This evolution underscores the necessity of comprehensive security strategies tailored to the complexities of modern database systems. Focusing on key security components, this section delves into the various measures and methodologies employed to fortify relational databases, thereby safeguarding the integrity, confidentiality, and availability of critical data [18].

2.4 Related work

Focused on relational databases, this section critically reviews key research initiatives and studies addressing security issues across various database technologies. The methodologies and approaches in this thesis are developed based on these studies, aiming to address gaps and challenges identified in our
research. Subsection 2.4.1 examines the critical need for securing relational databases. Subsection 2.4.2 provides an overview of database security and evolving technologies. Finally, Subsection 2.4.3 discusses the unique security challenges in remote information systems.

### 2.4.1 Importance of Relational Database Security

The work of Zeb [19] provides an important historical perspective that is particularly relevant to our thesis in the context of relational database security. Zeb’s study, which covers more than three decades, emphasizes the vital role relational databases have played in the development of organizational strategies. Understanding the increasing complexity and sophistication of security challenges that databases face today requires an understanding of this historical evolution.

Zeb’s research focuses on securing Relational Database Management Systems (RDBMS) from unauthorized access, which is consistent with our thesis. This is an aspect that aligns well with our analysis of relational database access control and data privacy. An in-depth examination of the issues and solutions in database security is given by Zeb’s extensive study of numerous threats as well as the development of preventative measures and security techniques. The comprehensive examination not only enhances the "Related Work" section of our thesis but also makes an important contribution to our comprehension of the significance of relational database security. It establishes a basis for our following discussions and analysis, assisting us in developing a thoughtful and nuanced strategy to handle the intricate security requirements faced by modern relational databases. The knowledge gained from Zeb’s work has greatly influenced our research approach, directed our investigation of important security elements, and highlighted the importance of strong security protocols in protecting relational databases from evolving threats.

### 2.4.2 Overview of Database Security and Technology

Paul and Aithal’s study [20] provides a thorough summary of databases’ function within the larger field of information science, emphasizing how important it is for them to act as data repositories. This work carefully demonstrates the importance of different technological elements, emphasizing database technology in particular, highlighting their combined contribution to societal advancement.
This investigation provides an essential context for our thesis, understanding the complex relationship between database systems and their technological foundations is made easier with the help of Paul and Aithal’s insights. Our thesis is directly informed by their discussion of the difficulties encountered in database security and the solutions available to address these problems, particularly when assessing the current approaches and trends in relational database security. Furthermore, we were able to frame our own investigation of security strategies thanks to their comprehensive review of database security challenges. It has given us a useful point of comparison, allowing us to make connections between our research and accepted ideas in the field.

2.4.3 Data Protection in Remote Information Systems

In the context of remote information systems, the study by Mousa, Karabatak, and Mustafa [21] explores how data protection is changing, especially in light of the growth of Internet-based services. Their research highlights a critical issue that strongly aligns with the goals of our thesis: the growing susceptibility of databases to diverse threats as online services grow.

This work highlights the need for complete and reliable security measures by critically examining the frequently neglected aspect of database security in many organizations. The findings have been crucial in helping us focus our thesis on finding and strengthening possible weak points in relational database security systems. This study has given us an overview of the diverse and complicated threat nature by examining the various threats and their effects on sensitive data.

The examination of dynamic and contextual security measures in our thesis is enhanced by Bertino and Sandhu’s work [22] on the necessity of sophisticated data protection strategies in distributed information systems. Their focus on the application of access control policies—which take into account subject qualifications, data content, and contextual elements like time—aligns well with our research on context-aware and adaptive security mechanisms. Our thesis’s emphasis on multi-layered and nuanced security approaches is directly informed by the discussion about integrating semantic considerations for efficient access control policies and tailored data integrity techniques for database systems. This source has been crucial in helping us develop our understanding of advanced database security techniques and the modern problems they face. As a result, it has influenced the way our suggested solutions have been developed and deepened the scope of our research.
Chapter 3

Research Methodology

This chapter details our research methodology, starting with Section 3.1 which outlines the foundational strategy. Section 3.2 details the specific methods and protocols used, while Section 3.3 describes the research’s phased progression. Section 3.4 reviews data collection and analysis tools. Section 3.5 focuses on the selection of experienced relational database security professionals and their contributions to our research. Lastly, Section 3.6 discusses steps taken to ensure the robustness of our methodology.

3.1 Research Strategy

The research strategy that is being utilized for this thesis is centered on the process of methodically mapping out the key security components that have been incorporated in relational databases. For the purpose of ensuring the integrity and security of relational databases, this strategy has been meticulously designed to incorporate a wide range of security measure that are essential. So, in order to meet the requirements of this extensive and investigative work, the research method that was chosen was adapted. In Figure 3.1, a diagram is presented that illustrates the research strategy that we plan on carrying out.

Research Methods, Research Phases, Research Instruments, and Validity Threats are the four fundamental elements that comprise the tactical approach of this research. Combining these elements, we lay the foundation for our research methodology. This methodology guides the organization, development, and execution of our research, which focuses on comprehensively mapping security components in relational databases.
3.2 Research Methods

Exploring security components in relational databases involves complex issues that require a detailed and advanced analytical approach. In order to address the intricacies of database security, we decided to go to qualitative research methodologies. These methodologies excel at capturing the details and variety of experiences, which are crucial for a thorough comprehension of database security. Qualitative research, as mentioned in [3][4], provides an in-depth exploration of the intricate dynamics of database security that goes beyond conventional data gathering methods.

The qualitative methodology employed in this thesis goes beyond simple data collection. It involves an interpretive process that seeks to comprehend the complex connections and patterns that form the foundation of security measures in relational databases. The flexibility of this strategy is essential, considering the volatile nature of the cybersecurity environment. An in-depth investigation is essential for understanding the intricate dynamics of relational database security.

Our research includes a comprehensive examination of various scholarly
works, conference papers, and industry-specific publications. This review is crucial for identifying the essential security components and the ongoing development of security mechanisms in relational databases. Additionally, it aids in identifying current deficiencies in research. Our objective is to combine all of this information in order to establish a thorough comprehension of relational database security, which is essential for enhancing security procedures and directing future research in this domain.

3.3 Research Phases

This project follows a structured methodology that is divided into four crucial phases that are aimed to methodically discover and analyze the key security components in relational databases. Figure 3.2 illustrates the progression through these phases, offering a clear visual representation of the research process. Section 3.3.1 addresses the Pre-study phase, in which the project begins with a domain investigation and a clear statement of the research objectives. This phase entails laying the foundation for the research by identifying the important areas of attention in relational database security. Section 3.3.2 digs into the Literature Study phase, which involves conducting a comprehensive investigation and critical review of publications in order to acquire relevant research findings. This phase is critical for establishing a solid grasp of the existing state of security components in relational databases. Section 3.3.3 goes over the Data Synthesis phase, explaining how to combine and understand the information acquired from the literature review. This phase focuses on finding knowledge gaps in relational database security components. Finally, Section 3.3.4 discusses the Critical Analysis and Evaluation phase, in which the synthesized data is carefully examined. This phase entails analyzing the findings, reviewing the interviews, drawing conclusions, and summarizing the study’s significance in the context of relational database security. Section 3.3.5 describes the phase of final improvements which is critical in building a comprehensive map of the key security components in relational databases.
3.3.1 Pre-study

Starting with a thorough examination of the components of relational database security, the Pre-study phase lays the groundwork for the rest of our research. Learning the basics of the domain sheds light on the complex components and ongoing discussions around database security, which is the initial and most important step. Having a solid grasp of the subject at hand is crucial because it establishes the foundation for further research and provides a structure for interpreting results. The study moves on to preliminary research after the domain orientation. An examination of the foundational studies, important publications, and existing literature that have influenced our knowledge of database security is part of this process. Through this initial analysis, we are able to gather relevant data in a robust manner and pinpoint areas that warrant additional investigation.

After we have a good understanding of the domain and the results of the first research, we can go on to building the project scope. This important first step is to define the scope of the research, outlining what will be included and what will not, so that the subject matter can be examined thoroughly and effectively. In conjunction with defining the scope, we formulate a problem statement that encapsulates the core of the research topic. Every aspect of the investigation is grounded in this statement, which clarifies the primary...
concerns that the research aims to tackle.

Once the Pre-study phase is complete, the next step is to establish research objectives. These objectives show the way forward for the study and are the precise aims that the research is trying to accomplish. With these clear, measurable, and feasible objectives in place, the research may move on with confidence. A crucial aspect of the pre-study phase is the feasibility assessment, which is represented in the Figure 3.3 by the question ”Is it Do-able?” In this review, we look at the research goals and determine if they are achievable given the time, resources, and scope limitations. When the possibility of success is doubted, a procedure for evaluation and correction is begun. To make sure the research stays feasible and focused on producing informative conclusions, iteratively adjusting the research strategy, changing objectives, or redefining the scope is done as needed.

In order to establish the search objectives, the project’s feasibility must be verified before proceeding with the Pre-study phase. With these clear goals in mind, the literature search can be guided to provide the most pertinent and important results. The Pre-study phase concludes with the development of keywords. To find the right information in the massive amount of literature and achieve the research goals, choosing the right keywords is essential. Once these processes are finished, the Pre-study phase ends, and the Literature Study phase can begin, as shown in the Figure 3.2.
The research is solidly established in a comprehensive domain understanding, has clear scope, and is equipped with well-defined objectives and strategies thanks to this sequential and systematic approach. It sets a solid foundation for the in-depth exploration of security components within relational databases.

### 3.3.2 Literature Study

The Literature Study phase is an essential, iterative phase in our research methodology, specifically intended to carefully find and study academic
articles, technical reports, and other relevant publications focused on relational database security. We intend to collect a complete set of data that informs the core of our thesis through an in-depth examination of varied academic resources such as Google Scholar [23], the KTH library catalog [24], ScienceDirect [25], IEEE Xplore [26], and ResearchGate [27].

Our literature search is both thorough and specialized, guided by a dynamic list of keywords such as Database Security, Relational Databases, Encryption, Vulnerabilities, Access Control, SQL Injection, Cyber Attacks, Hacking, and Data Storage, Data leak, Data security issue. These keywords were picked not only for their initial significance, but also for their ability to change in sync with the research findings, as we iteratively adjust our search parameters to align with evolving trends and essential components observed in the field of database security.

Each recognized publication was carefully evaluated to determine its relevance and usefulness to our unique research objectives. To ensure that our Result Collection is of the greatest standard, we place a high value on the methodological reliability, practical validity, and recentness of research. This collection is more than just a data repository; it is a carefully curated selection of insights that shed light on the complex problem of database security. Publications that do not satisfy our tough criteria are discarded, allowing us to modify our search approach and improve the quality of the Result Collection.

The review of literature is a iterative journey of discovery and evaluation. We delve further into the issue with every iteration, uncovering gaps in the literature and potential for important contributions. This methodical approach guarantees that our Result Collection becomes a repository of information, containing a thorough and up-to-date understanding of the security problems and best practices associated with relational databases.

As the literature review progresses, we gain a comprehensive understanding of the multi-dimensional security landscape characterizing relational databases. The procedure is repeated until a saturation point is achieved, at which point more research has no substantial impact on the trajectory of our understanding. The Literature Study phase naturally flows into the Data Synthesis and Analysis phase at this point, where the synthesized knowledge serves as the foundation for a deep assessment of the major security components. This analysis is both introspective and forward-thinking, assessing the implications of our findings for database security. Figure 3.4 visually summarizes the entire Literature Study phase, with its careful balance of breadth and depth, giving a template for the shift from comprehensive research to insightful analysis and debate.
3.3.3 Data Synthesis

A crucial part of our thesis, data synthesis connects the previous phase, Literature Study, to the next one, critical analysis and reflection. The critical security components of relational database, which were individually found throughout our thorough literature review, are assembled, examined, and explained during this phase.

Beginning with the data collected in the Literature Study phase, we now go on to collecting and organizing it. A thorough investigation and categorization of these security components is now required. In this section, we dissect how each component works, how it helps prevent security breaches, and how it fits into the bigger picture of database security. While evaluating the efficacy of each component in warding off different security risks, this task is analytical rather than descriptive. Each security
mechanism’s strengths, limitations, and overall efficacy are studied in depth in this thoroughly process. After the components have been categorized and analyzed, we move on to outlining their features. This requires study of the interplay between security components and various relational databases, as well as their resistance to various security risks. In order to build a comprehensive understanding of the security components, we use a narrative synthesis approach throughout this phase. Giving a balanced picture that includes both the theory and practice of database security is the aim.

Through the end of this phase, a comprehensive, multi-faceted picture of relational database security components has been produced. In addition to summarizing our findings, this knowledge base serves as a foundation for the Critical Analysis and Reflection that will follow this current phase. Reflecting on the complexities and difficulties of the relational database environment, we will critically analyze the feasibility of incorporating these security components. This synthesis of knowledge, which not only consolidates our understanding of database security but also sets the stage for the next phase of our research, is visually summarized in Figure 3.5.
3.3.4 Critical Analysis and Evaluation

When we get to this phase of our thesis, we begin an in-depth investigation of the findings that were obtained from the Data Synthesis phase. The purpose of this phase was to examine the material that has been synthesized in order to discover the complexities and potential gaps in our understanding of relational database security. The approach that we use comprises doing a thorough examination of the security components that have been identified. During this
process, we not only evaluate the suitability of these components in relation to
database security, but we also identify areas that need to be improved upon. A
critical evaluation of the synthesis data is the primary objective of this phase.
We are establishing the groundwork for the future “Final Improvement” phase
by highlighting the areas that require improvement through the use of this
study. Furthermore, during this phase, an evaluation of the validity threats
that our study faces, such as credibility, transferability, dependability, and
objectivity, is carried out.

This phase ensures that our conclusions are robust and reliable. In
order to bring the practical perspectives into alignment with our theoretical
conclusions, we also look into the insights that were gathered via interviews.
The purpose of this alignment is to validate our conclusions and to create
a context that is relevant to the real world for our research. A reflection on
the results of our study serves as the culmination of the “Critical Analysis
and Evaluation” phase. This reflection prepares the way for the subsequent
phase of final improvements, in which we address the holes that have been
identified and polish our research findings. Due to the fact that it offers a
comprehensive analysis of our research and establishes the groundwork for
our ultimate conclusions and recommendations for further research in the
subject of relational database security, this phase is of critical importance
in the process of forming the concluding sections of our thesis. Figure 3.6
visually summarizes the entire Critical Analysis and Evaluation phase.
3.3.5 Final Improvements

In this phase of our thesis, which follows the "Critical Analysis and Evaluation" phase, we began the critical task of refining our research findings. This phase is critical in improving the overall quality and comprehensiveness of our thesis, particularly in the context of relational database security.

The phase begins with the integration of the previous phase’s insights and observations. Our primary focus here is on addressing the gaps and potential areas for improvement in the security components of relational databases that were identified during the section 3.3.4. This process entails revisiting each identified security component, evaluating feedback and suggestions for improvement, and incorporating necessary changes. This iterative process ensures that the research remains dynamic and adaptable to evolving security challenges and trends in relational database technology.

Concurrently, we conduct a thorough reconsideration of the validity
threats identified earlier. This reconsideration is critical for strengthening the dependability and credibility of our results. We carefully examine each aspect of our research methodology, considering alternative perspectives and approaches that could strengthen the robustness of our conclusions. The goal is to ensure that our research is not only thorough, but also resistant to potential misconceptions and limitations.

We thoroughly document the changes and improvements made once the enhancements are completed. This documentation serves as a transparent record of our research evolution, demonstrating our commitment to rigorous academic standards. It also provides valuable insights for future researchers, emphasizing the iterative nature of academic research and the importance of continuous improvement in education. Figure 3.7 visually summarizes the entire Final Improvements phase.

Figure 3.7: Overview of Final Improvements Phase
3.4 Research instruments

Our methodology is built on a comprehensive literature review, which involves the careful collection of articles and studies from a wide variety of academic databases and digital libraries. A comprehensive literature review, which involves the careful gathering and evaluation of scholarly articles from various online libraries and databases, serves as the foundation of our methodology. Google Scholar, ResearchGate, ScienceDirect, IEEE Xplore, and the KTH library catalog are some of the main sources. We acknowledge the role of useful tools, such as Grammarly for checking grammatical accuracy and Zotero for streamlining reference management, in enhancing the quality and efficiency of the literature review process. For this review, we initially extracted 65 articles using a set of dynamic keywords specifically tailored to our research focus on relational database security. These keywords encompassed terms such as Database Security, Relational Databases, Encryption, Vulnerabilities, Access Control, SQL Injection, Cyber Attacks, Hacking, Data Storage, Data Leak, and Data Security Issues.

Each publication was rigorously evaluated for its relevance and methodological soundness in relation to relational database security. Of the initial collection, 52 articles were carefully selected for in-depth analysis, rejecting 13 articles that were proven to be less relevant to our needs. This selection process ensured that our literature review focused on publications that specifically address the challenges and strategies in securing relational databases, thereby providing a robust foundation for our research.

For the purpose of refining our preliminary findings, our research methodology incorporates structured interviews as an important instrument. In order to evaluate and improve our initial results, these interviews are methodically conducted with industry professionals and academic professionals. The insights that these individuals provide are extremely valuable. The objective of these interviews is to provide us with a deeper knowledge of the challenges that are faced in the real world and the applications of security components within relational databases. This will be accomplished by bridging the gap between theoretical analysis and practical application. By means of these conversations, we intend to validate, challenge, and elaborate upon the preliminary conclusions that we have drawn from the review of the relevant literature. We are able to gain access to current, on-the-ground perspectives that may not be fully captured in published literature if we engage with professionals who are actively working in the field. With the help of this interaction, we are able to critically evaluate the validity and
applicability of our initial findings, which ultimately leads to outcomes that are more refined and practical. Because of this, the incorporation of structured interviews is an essential component of our research. In conclusion, this methodological approach significantly strengthens the overall contribution that our thesis makes to the field of relational database security.

3.5 Respondents

Using structured interviews with a subset of respondents, we mapped out critical security components in relational databases. A combination of convenience sampling and purposeful sampling is used to recruit interviewees in order to increase the likelihood of participation. For further details on the interview methodologies and participant selection process in Chapter 4. Careful definition of the selection criteria for our respondents guarantees that the information they supply is rich and relevant. All of the following must be met:

- Expertise in Database Security: Each respondent must have extensive knowledge of relational database security in order to provide insightful and pertinent responses.

- Professional Experience: The ideal respondent will have worked in the industry for at least ten years, and we give preference to those with more experience. This criterion guarantees that the participants will contribute extensive knowledge and historical context to the discussion, which is crucial for comprehending the development and present status of database security.

- Diverse Backgrounds: Our selection consists of seasoned database administrators and industry veterans with backgrounds in database security. This variety guarantees that the topic in question will be examined from every perspective.

We have made sure to include a diverse and nuanced view on the security components of relational databases in this study by selecting two respondents who fulfill these criteria. Our research questions will be addressed from various perspectives by the valuable insights that each respondent is expected to provide, thanks to their unique background and expertise. Our knowledge of database security mechanisms, both in theory and practice, is expected to be greatly enhanced by their contributions.
These interviews are crucial to our research because they are based on a deliberate and strategic selection process. They offer a multifaceted perspective on the complexities involved in securing relational databases by allowing us to validate, challenge, and enhance the findings from our comprehensive literature review. We can guarantee that our thesis will be relevant and useful in both academic and practical domains of database security thanks to the synthesis of insights from these interviews.

### 3.6 Validity Threats

This thesis is validated based on rigorous criteria, including credibility, transferability, dependability, and objectivity. Adherence to these criteria is crucial to ensure that the resultant conclusions are not only robust but also lay a foundational premise for future research endeavors and pragmatic implementations, particularly for software engineers dedicated to enhancing database security. These criterion are discussed further in section 8.2.

- **Credibility:** The text establishes credibility by stating the research is based on a comprehensive investigation of reliable academic resources on database security. The in-depth examination of these sources provides a full appreciation of the complexities [28].

- **Transferability:** The text argues the findings are generalizable to systems with similar architectures by examining a diverse range of academic literature and security scenarios. However, it notes complexity may vary by environment [28].

- **Dependability:** The text claims the technique is reliable through meticulous procedures and solid evaluation criteria. This enables replication of studies on database security [28].

- **Objectivity:** The text cites the use of technical writings rather than subjective narratives, and careful documentation of any shifts, to lend authority and objectivity to the research [28].
Chapter 4

Evaluation Model

This chapter outlines the evaluation model consisting of five distinct criteria essential for assessing the security components of relational databases. These criteria are pivotal in addressing the research question detailed in Section 1.3. The model’s criteria, apart from interviewee credibility which was introduced to increase validity, are as follows: (1) interviewee credibility, (2) semantic correctness, (3) syntactic correctness, (4) usefulness, and (5) Open-ended Questions.

In Section 4.1, we focus on assessing experts’ credibility to ensure informed insights in database security evaluation. In Section 4.2, we assess interviewee expertise in database security. Component clarity and relevance are evaluated in Section 4.3. Section 4.4 focuses on analyzing the logical structuring of security components. The practicality of the components is examined in Section 4.5. Finally, open-ended questions for deeper insights are presented in Section 4.6.

4.1 Expert Evaluation Criteria

A critical component of our evaluation model is the process used to select and evaluate the experts whose insights inform our research. To ensure the validity and relevance of their contributions, we employed a structured approach for expert evaluation, focusing on the following aspects:

1.1 Professional Expertise and Background: We assessed the experts’ qualifications, including their educational background, certifications, and areas of specialization in database security. This helped ensure that they possessed a deep understanding of the subject matter.
1.2 Relevance of Current Role: The current roles of the experts were evaluated to determine their direct involvement in database security. This involved looking at their job responsibilities, the scope of their work, and their impact on the field.

1.3 Experience and Track Record: We considered the duration and breadth of their experience in database security, including previous roles and projects. This helped in understanding their long-term engagement and evolution in the field.

1.4 Contributions to the Field: The experts’ contributions to the field of database security, such as research publications, speaking engagements, and participation in significant projects, were reviewed.

This evaluation process ensured that the selected experts were not only knowledgeable but also actively contributing and recognized in the field of database security. Their insights, therefore, come from a place of both experience and current relevance.

4.2 Interviewee Credibility

In the exploration of relational database security, the credibility and depth of knowledge of the interviewees are of paramount importance. Given the specialized and evolving nature of database security, it is crucial to select experts with comprehensive experience in this field. The following questions aim to establish the expertise and relevance of the interviewees’ background:

2.1: Can you detail your professional background in database security?

2.2: Describe your current role and its relevance to relational database security.

2.3: For how long have you been engaged in your current role?

2.4: Could you provide an overview of your past roles that are pertinent to database security?

2.5: What is the duration of your experience in each of these roles?

2.6: Have you participated in projects focused on securing or analyzing relational database systems?
These questions are designed not only to validate the interviewees’ expertise but also to understand the depth and breadth of their experience in the field.

4.3 Semantic Correctness

For the purpose of ensuring that the identified security components used in this thesis are beneficial and relevant, it is essential that they have semantic correctness. It is essential for professionals working in the field of relational database security to accurately comprehend and employ the components, and this aspect places an emphasis on the components’ clarity and understandability. The questions that are listed below were proposed in order to evaluate the correctness of the semantics.

3.1: Relevance in Contemporary Context: In the context of modern relational data database threats, how do you see the relevance of the identified security components?

By ensuring that the components are both theoretically valid and practically applicable, this question seeks to determine whether they are relevant to current and emerging security challenges.

3.2: Clarity and Comprehension: Examine the clarity and comprehension of the security component descriptions. Can they be employed and grasped easily?

The purpose of this question is to make sure that the descriptions of the security components are precise enough to be understood and implemented without any confusion. Simplifying and making these components easily applicable to real-world security measures is of the highest priority.

Validation of the security component’s semantic integrity relies heavily on the answers to these questions. The development of effective security strategies for relational databases begins with making sure they are applicable to the current threat landscape and easy for users to understand.

4.4 Syntactic Correctness

The evaluation model places great importance on syntactic correctness, which pertains to the logical organization and coherence of the identified security
components within the map. The map must include all relevant components and arrange them in a way that accurately represents their interconnections and alignment with operational workflows in relational database security. This guarantees that the map is not only accurate but also pragmatic and accessible for professionals in the industry. In order to evaluate the syntactic accuracy, we took into account the following key questions:

4.1: **Relevance and Pertinence**:  
- Are there any component parts within the identified security components that you consider unnecessary or irrelevant?  
- The purpose of this question is to determine if there are any unnecessary or unrelated components, in order to make sure that the map is efficient and concentrates on the crucial aspects of database security.

4.2: **Comprehensiveness of Components**:  
- Can you identify any essential components that are absent and necessary for comprehensive security in a relational database?  
- The purpose of this question is to determine if the map encompasses all essential components of a comprehensive security strategy, thereby ensuring that no crucial aspect is neglected.

4.3: **Logical Sequence and Workflow Alignment**:  
- Analyze the sequence of the identified components. Does their arrangement demonstrate logicality and reflect practical security workflows?  
- This question evaluates the coherence and congruence between the map’s structure and real-world operational processes, thereby improving its practicality and usability.

The information gained from these types of questions is crucial in enhancing the grammatical arrangement of the security elements, guaranteeing that the model is both proficient in its composition and successful in its real-world application.

4.5 **Usefulness**

Understanding the usefulness and practical applicability of the identified security components in relational database security is the focus of this section of the evaluation model. Ensuring these components are not only reliable in theory but also practically valuable and capable of improving database security
in real-world scenarios is the aim of this endeavor. The following important questions were set to assess their usefulness:

5.1: Evaluating Practical Utility: Reflect on the practical utility of the identified security components in improving database security.

Expert opinions on how well the security components can be used in practical settings are sought in this question. With respect to their functionality, ease of use, and effect on overall security posture, it seeks to determine whether these components can actually improve database security practices.

5.2: Future Integration and Strategy Thoughts: Would you consider incorporating these components into your upcoming security strategies for relational databases?

The purpose of this question is to evaluate the security components’ adaptability and long-term viability. By considering their potential to stay applicable and efficient as security threats change, it evaluates whether experts see these components as essential components of future security strategies.

The practical value of the security components must be determined based on the answers to these questions. They aid in determining whether these components are not only conceptually strong but also flexible and adaptable enough to be incorporated into various security frameworks and strategies in the field of relational database security.

4.6 Open-ended Questions

To gain a deeper understanding and broader insights into relational database security, a set of open-ended questions is proposed. These questions are intended to stimulate detailed discussions, enabling a richer collection of data and perspectives, that presented in 4.1:
<table>
<thead>
<tr>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1: How effective have the access control measures been in enhancing the security and integrity of the database?</td>
</tr>
<tr>
<td>6.2: In your opinion, how have the implemented authentication systems contributed to the overall security posture of the database?</td>
</tr>
<tr>
<td>6.3: Can you evaluate the success of the data protection strategies, like encryption and backup, in safeguarding sensitive data?</td>
</tr>
<tr>
<td>6.4: How would you assess the role and effectiveness of monitoring and auditing in identifying and mitigating security risks?</td>
</tr>
<tr>
<td>6.5: From your perspective, how significantly have the network security measures, including firewalls and encryption protocols, impacted database security?</td>
</tr>
<tr>
<td>6.6: How successful have the vulnerability prevention methods been in maintaining the database’s security against emerging threats?</td>
</tr>
<tr>
<td>6.7: How do you evaluate the impact of security training and awareness programs on enhancing the database’s overall security?</td>
</tr>
<tr>
<td>6.8: Based on your experience, what areas of database security do you think require further improvement or attention?</td>
</tr>
</tbody>
</table>

Table 4.1: Open-ended Questions
Chapter 5

Preliminary Results

Section 5.1 synthesizes crucial findings, providing a cohesive overview of our research insights. Section 5.2 delves into the access control mechanisms, such as authentication and authorization, crucial for regulating database access. In Section 5.3, we shift our focus to data protection strategies, including encryption and backup strategies. Section 5.4 then examines the pivotal role of monitoring and auditing in maintaining oversight of database activities. Network security aspects, including firewall and management, are discussed in Section 5.5. We explore proactive measures for vulnerability prevention, including parameterized queries and regular patching, in Section 5.6. Finally, Section 5.7 highlights the significance of human elements in security, emphasizing the importance of education and training in enhancing overall database security.

5.1 Overview

This section delves into the preliminary results of our extensive study focused on mapping the key security components in relational databases. In section 3.3, we discuss and describe in detail how systematic our literature study has been. The study’s structure systematically covers various critical areas, each contributing uniquely to our comprehensive understanding of database security strategies (see Figure 5.1).
5.2 Access Controls

Among the many components of relational database security, access controls stand out as absolutely necessary for protecting the confidentiality, authenticity, and integrity of data. Their job is to make sure that only authorized users can access and change the database. Ensuring that sensitive information is accessible only to authorized personnel involves a range of mechanisms, such as user authentication and authorization protocols [2].

5.2.1 Authentication

The most important security measure for a database is authentication, which checks the credentials of any devices or users trying to access the database before granting them access to private information. At their core, authentication techniques rely on verifying “factors,” which can be anything a user knows, like a password, has, like a cryptographic key, or is, like
intrinsic biometric traits. The difficulty of impersonation attempts is increased by the requirement of multiple factors. An access control list that maps individual credentials to clearance levels is used to validate user IDs in core authentication processes [29].

Access to database resources necessitates the use of two or more verification factors, highlighting the importance of multi-factor authentication (MFA) in relational databases. MFA is effective due to its multi-layered approach, reducing the risk associated with single points of failure like stolen passwords. Implementing MFA is crucial in ensuring that even if one authentication factor is compromised, other protective barriers remain to safeguard sensitive data. Figure 5.2 illustrates a flowchart of the multi-factor authentication process, beginning with the user’s interaction with the login page.

User credentials are initially verified against a user database. Post verification of the user’s password, a second form of authentication, such as a one-time password (OTP), is requested. Manual entry and verification of the OTP against the OTP keys database significantly lower the likelihood of unauthorized access.

![Figure 5.2: Two-factor authentication flowchart](image)
This study advocates the adoption of advanced authentication methods for enhanced database security. Biometric authentication methods like fingerprint scanners, facial recognition systems, and voice recognition technologies are recommended due to their intrinsic link to a person’s physical traits, which are inherently more difficult to duplicate or falsify. Behavioral biometrics, analyzing patterns in user behavior to detect anomalies indicative of unauthorized access, are also supported. These methods offer a continuous authentication layer, vigilant for signs of intrusion such as changes in keystroke dynamics, mouse movement, and navigation patterns throughout a user’s session.

The study underlines the necessity for regular updates to authentication protocols in response to evolving cyber threats, emphasizing the commitment to robust authentication in relational database security. Conducting frequent security audits and assessments is critical in identifying and rectifying vulnerabilities in authentication systems. Our focus on mapping key security components in relational databases aims to build a comprehensive defense against cyber threats, maintaining stringent control over database access. The proactive approach to safeguarding a critical aspect of database security is reflected in the emphasis on strengthening authentication methods.

5.2.2 Authorization

Authorization in relational databases ensures data security and integrity. Based on their authorized identities, it involves granting or denying users certain permissions. In the database, this key security component controls what users can read, write, and modify. Effective authorization mechanisms prevent unauthorized access and manipulation of sensitive data, maintaining database security. In relational databases, authorization protects against security breaches by strictly controlling user privileges.

Implementing flexible authorization mechanisms is essential in mapping out key security components in relational databases. These mechanisms, designed to be adaptable and dynamic, are critical in addressing the varied and ever-evolving security needs of relational databases. Our study emphasizes the importance of flexibility in authorization procedures, tailoring them to the specific security policies and operational protocols of each database system.

A sophisticated Role-Based Access Control (RBAC) model forms the basis for authorizing users in relational databases. This model, as highlighted in our research, is adaptable, allowing precise role specification and on-
the-fly adaptation to changing business processes and security requirements [32]. Figure 5.3 in our study illustrates the flexible nature of the RBAC model, demonstrating its ability to quickly respond to shifting threats in the cybersecurity landscape.

![Figure 5.3: A system architecture for an adaptable authorization mechanism[33]](image)

Our research explores the integration of Attribute-Based Access Control (ABAC) alongside RBAC. ABAC grants permissions based on a range of attributes related to users, resources, and the context of access requests [34]. Its policy evaluation process is more specific, resulting in an authorization approach that better handles complex security needs. Our research also introduces the concept of metadata segregation, enhancing adaptable authorization. Data is categorized by sensitivity levels, and referential integrity constraints are applied dynamically [2], allowing the database to adapt to changing structures and operational needs with greater flexibility.

Incorporating Transparent Data Encryption (TDE), similar to Oracle 11g, exemplifies the practical application of these flexible authorization mechanisms. Our study discusses how TDE illustrates the customization of
encryption policies based on each database’s unique characteristics and the importance of the information it stores [35].

Our research advocates for the introduction of innovative approaches to authorization, ensuring the study’s relevance in the face of evolving cybersecurity threats. In conclusion, our exploration of flexible authorization mechanisms in relational databases underscores a commitment to delivering effective, adaptable, and forward-thinking security measures, making databases resilient to both current and future threats.

5.3 Data Protection

Relational database security is built around data protection. This study examines the multifaceted approach to protecting sensitive data in these databases. It includes encryption, backup. This section discusses data protection methods and their importance in preventing data breaches and maintaining database system integrity. These trends are shaping the future of secure data storage in relational databases [36].

5.3.1 Encryption

One of the most important ways to protect sensitive information in relational database security is by using encryption. It entails encoding data such that it can only be read by those who have the right decryption key. In the event that data is intercepted or accessed without authorization, this process guarantees that it will remain unreadable and secure. For the purpose of securing data at rest and data in transit, encryption techniques such as symmetric and asymmetric encryption are utilized. A key line of defense against unauthorized database access and data breaches, this security measure is essential for maintaining the privacy and integrity of data within relational databases.

Strategic encryption deployment is a pivotal aspect of mapping out key security components in relational databases. This segment of our study focuses on advanced encryption strategies to ensure robust security for data both at rest and in transit, addressing the diverse security demands of relational database systems. Central to our exploration is Transparent Data Encryption (TDE), such as Oracle 11g TDE (see Figure 5.4). TDE’s efficient storage-level encryption is crucial for protecting data from unauthorized access, even if storage infrastructures are compromised [35]. Our study seeks a balance between strong encryption and practical application.
A key part of our exploration is the Advanced Encryption Standard (AES) (see Figure 5.5), renowned for its strong encryption capabilities and processing efficiency. AES's flexibility, with its predetermined block size and variable key lengths, makes it ideal for securing sensitive data in relational databases. This aligns with insights from "Database Encryption - How to Balance" [37] and "A Framework for Efficient Storage Security in RDBMS" [38]. Additionally, we emphasize the necessity of end-to-end encryption for all data transfers, as advocated in "A Practical Encrypted Relational DBMS" [39], to protect data during transmission and reduce interception risks.

Our examination extends to efficient encryption key management, endorsing protocols for regular key changes, secure storage, and restricted access, which are essential for maintaining data integrity and availability. By integrating these strategies, including the use of AES, our study presents state-of-the-art encryption capabilities as vital components of relational database security, safeguarding private information and aligning with evolving cybersecurity standards.

Figure 5.4: TDE Encryption Overview[35]
5.3.2 Backup Strategies

To ensure data resilience and recovery and to prevent corruption or loss of data, backup strategies are crucial in relational databases. Differential, incremental, and full backups are all methodologies that are encompassed by these strategies. In order to keep information available and undamaged in the event of unexpected disruptions or disasters, it is essential to use these backup techniques to create a robust security system for data. This comprehensive method is critical for relational database systems’ data management and security in perpetuity. In the context of relational database security, backup strategies are paramount for data resilience and recovery. This thesis emphasizes the importance of robust backup and recovery procedures in relational databases, focusing on safeguarding data against corruption, deletion, or loss [40][19].

Through a well-structured backup strategy, databases can be restored with minimal data loss, ensuring operational continuity even in the face of hardware failures, human errors, malicious attacks, or natural disasters. Key aspects of an effective backup strategy include:

- **Types of Backups**: Emphasizing the use of both full and incremental backups, this approach balances comprehensive data snapshots with efficient, change-oriented backups.

- **Backup Frequency**: The thesis advocates for a balanced approach to backup frequency, aligning recovery point objectives with data variability and business needs.

- **Retention Duration**: Recommendations include maintaining backups for a minimum period, guided by business requirements and compliance
regulations, with essential data stored for extended periods.

- **Storage Location**: Suggests diversifying storage locations, including cloud storage, to enhance data safety in disaster scenarios.

- **Encryption**: Highlights the necessity of encrypting backup files both during transit and storage to prevent unauthorized access.

- **Testing**: Stresses the importance of regular testing for backup recoverability, preferably in cloned environments to avoid production downtime.

This thesis acknowledges the dynamic nature of database sizes and business demands, suggesting adaptive strategies like ‘incremental forever backups’ to cater to current and future needs. Thus, it ensures backup strategies evolve, keeping pace with the ever-changing database environment and emerging cybersecurity threats (see Figure 5.6).

![Figure 5.6: Overview of the Backup Strategies](image-url)
5.4 Monitoring and Auditing

Relational database security monitoring and auditing are critical for keeping an eye on things and making sure everyone is held responsible. These procedures entail carefully monitoring and evaluating a wide range of database operations, from user access to complex transaction histories. In order to detect anomalies, maintain security policies, and comply with regulations, their implementation in relational databases is key. The database environment’s overall integrity and dependability are greatly enhanced by early detection of security breaches, which is made possible through monitoring and auditing.

5.4.1 Dynamic Auditing and Logging

Dynamic auditing and logging are essential components in relational database security and transparency. Security teams can quickly detect and address anomalies or policy violations thanks to dynamic auditing. At the same time, logging provides a comprehensive record in chronological order, which is essential for analyzing events after the fact and checking for compliance with regulations. The combination of database logging and dynamic auditing strengthens the database’s defense mechanisms, ensuring heightened security.

In the quest to map out key security components in relational databases, our study identifies dynamic auditing and logging as critical elements. These mechanisms extend beyond conventional record-keeping, responding adeptly to the evolving interactions and security challenges within database systems. Fine-grained auditing, exemplified by Oracle9i’s advanced capabilities, allows for the tailoring of audit processes to specific data access scenarios, significantly bolstering the detection of misuse or unauthorized access. This approach not only chronicles distinct data access events but also plays a vital role in proactive threat detection, enabling the definition of precise audit policies that trigger alerts under specific conditions [35][41].

Our research emphasizes the need for dynamic adaptation in auditing to accommodate new usage patterns or emerging threats, thereby enhancing its effectiveness. We highlight the importance of balancing comprehensive logging with system performance to maintain both high security and operational efficiency. Incorporating recent research, such as methods for detecting tampering in audit logs using cryptographically strong hash functions, is pivotal for ensuring the integrity of logs as forensic evidence. The study also acknowledges the developmental stage of database-specific forensic tools, underlining the importance of sophisticated logging and auditing.
capabilities in relational databases [41][42][43].

We explore network-based monitoring as an alternative to native database logging, which offers protection with zero impact on database performance, albeit facing challenges with encrypted communications [43]. In summary, our research on dynamic auditing and logging in relational databases presents a comprehensive, forward-thinking approach to security. By integrating state-of-the-art features like fine-grained auditing and intelligent logging systems, and keeping abreast of the latest developments in database security and forensics, our study ensures robust protection against diverse security threats, thereby safeguarding the integrity and confidentiality of relational database systems.

5.4.2 Database Activity Monitoring (DAM)

Data integrity and privacy are largely protected by Database Activity Monitoring (DAM), an essential component of relational database security. DAM’s ability to provide comprehensive analysis of all database transactions and real-time monitoring has made it famous. The key to spotting odd behavior, policy violations, and potential security threats is to maintain this constant vigilance. Organizations can quickly respond to security incidents and adhere to regulatory norms with DAM’s comprehensive view of database operations. In order to protect and ensure the reliability of relational database systems, DAM must be incorporated into robust database security strategies.

In the study of relational database security, Database Activity Monitoring (DAM) emerges as a vital component, ensuring vigilant oversight and protection. DAM tools, operating independently from the DBMS (as depicted in figure 5.7), offer real-time or near-real-time surveillance, crucial for maintaining database integrity and confidentiality.
These systems capture and record all database actions, including those of database administrators, across various platforms. Stored securely away from the actual database, this data is pivotal for detecting and alerting about potential security threats or policy violations [44]. In our research, DAM is integral for comprehensive auditing of database activities, encompassing transactions, administrative actions, and access attempts. It logs extensive details such as SQL queries, user context, timestamps, tables accessed, and more, laying a solid foundation for expert analysis in the event of a security breach.

- Enhanced Security and Compliance: Continuous monitoring by DAM aids in adhering to security policies and regulatory standards.

- Anomaly Detection: DAM’s ability to flag unusual behaviors assists in identifying potential security breaches.

- Forensic Analysis: In the aftermath of a security incident, DAM’s detailed logs are invaluable for understanding the scope and nature of the breach.

- Alert Generation: DAM systems can generate instant alerts to prompt rapid response to suspicious activities or policy infractions.
DAM thus plays a crucial role in our study on relational database security, offering a comprehensive approach to safeguard databases against various threats.

5.5 Network Security

The management and control of data transfers across relational connections is the primary focus of network security, which is essential to protecting relational databases. It emphasizes the value of implementing robust network security measures like intrusion detection systems, firewalls, and encrypted communication protocols. By limiting database access to authorized and legitimate traffic, these components dramatically reduce the likelihood of data breaches and unauthorized access. The integrity and confidentiality of sensitive information stored in relational databases must be protected from external threats by effective network security strategies.

5.5.1 Network Security Protocols

The emphasis on network security within the realm of relational database security is a pivotal aspect of safeguarding these systems against network-based threats and unauthorized access. A comprehensive approach to network security protocols is essential to maintain the integrity and confidentiality of data within relational databases.

A key component of this security strategy involves the implementation of SSL/TLS encryption. This encryption method ensures the privacy and integrity of information transmitted between the database server and clients or other servers. Secure Sockets Layer (SSL)/Transport Layer Security (TLS) effectively creates an encrypted tunnel over potentially unsecured networks, thereby protecting data from eavesdropping, tampering, and message forgery. Regular network security audits and penetration testing play a significant role in identifying and addressing vulnerabilities. These measures provide a thorough analysis of the network infrastructure, seeking potential security flaws that could be exploited by malicious actors. Penetration testing, often carried out by ethical hackers, evaluates the strength of a system’s defenses by simulating real-world attack scenarios [45].

The incorporation of advanced Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) is also suggested. Figure 5.8 illustrates the deployment of these systems. IDS and IPS work collaboratively to monitor network traffic, identifying and responding to any signs of malicious activity.
or known attack patterns. While IDS primarily focuses on threat detection and alerting administrators, IPS takes a proactive approach by actively blocking and preventing attacks before they compromise the database systems [45].

![Diagram of Intrusion Detection and Prevention Systems (IDPS) (IDS & IPS)]

Figure 5.8: Intrusion Detection and Prevention Systems (IDPS) (IDS & IPS)

Intrusion Detection and Prevention System (IDPS) tools are integral for continuous traffic monitoring, providing automatic alerts and countermeasures in real-time upon threat detection. The IDPS tools can be categorized into Network-based IDS (NIDS) and Host-based IDS (HIDS), each catering to specific monitoring needs. The proactive defense provided by IDPS is further enhanced by regular updates and maintenance, ensuring efficacy against emerging threats, including zero-day exploits. Integration of IDPS with Security Information and Event Management (SIEM) systems offers an additional layer of security. SIEM systems are primarily used for real-time analysis of security alerts generated by network components [45].

This integration is crucial for enhancing incident response and coordinating security strategies effectively. The multi-layered approach to network security, combining advanced encryption, routine assessments, continuous monitoring, up-to-date software, and stringent access controls, forms a robust defense system for relational database security.

### 5.5.2 Database Firewall

The role of a database firewall is crucial in relational database security, as it acts as a gatekeeper to prevent unauthorized access. It checks all database traffic, both incoming and outgoing, for malicious and helpful operations. It is the job of the database firewall to prevent SQL injections and other forms of malicious query execution by establishing precise policies and rules. For the database to remain intact, secure from cyber threats, and prevent sensitive data from being accessed or altered by unauthorized parties, this preventative security measure is crucial.
In the realm of relational database security, implementing a database firewall is an essential strategy to safeguard against SQL injection attacks and other forms of malicious access \[46\]. This specialized firewall, unlike conventional network firewalls, is adept at parsing and analyzing SQL data streams, providing enhanced security through syntax control and detailed auditing before data interactions reach the database’s core \[47\]. The design of these database firewalls integrates both proactive and reactive components. The proactive component employs advanced techniques such as pattern mining and Bayesian networks for preemptive threat detection and mitigation (see figure 5.9).

![Database Firewall Diagram](image)

Figure 5.9: Database Firewalls overview

The reactive aspect of the firewall’s architecture comes into play post-attack, where it undertakes a thorough analysis of the database to update and refine its pattern recognition based on the most recent attack signatures. This involves collating new attack data with historical records in the Attack Histories database. In real-time scenarios, when an attack is detected, the firewall rapidly constructs a Bayesian network tailored to the specific attack type. This network is pivotal in assessing the integrity of affected data objects and making informed decisions based on the likelihood of various threat scenarios.

Bayesian network-based analysis is particularly advantageous in ambiguous situations where instant and accurate data integrity information is not feasible. It relies on probabilistic reasoning, drawing from past incidents and current data to deduce the integrity state of data objects during an ongoing attack. The Bayesian network’s structure, defined by directed acyclic graphs (DAGs), aids in breaking down complex distribution functions into manageable segments. These DAGs effectively capture causal or temporal relationships among data objects, thereby forming a joint probability distribution that can predict the integrity of data objects in the face of observed anomalies or attack patterns.
In essence, the database firewall’s Bayesian network, equipped with the capability to infer the status of data objects based on one-hop damage spreading patterns, significantly enhances the database’s defense mechanism against advanced cyber threats [45]. This approach aligns with the overarching goal of mapping out key security components in relational databases, providing a robust and intelligent line of defense tailored to the unique security landscape of these systems.

5.6 Vulnerability Prevention

Securing relational databases requires a proactive approach to finding and fixing security flaws, which is known as vulnerability prevention. Strategies like applying software patches on a regular basis, using parameterized queries to prevent SQL injection attacks, and following the principle of least privilege are all included. These measures are essential for preventing unauthorized access to sensitive database data, guarding against possible security breaches, and keeping the database system robust as a whole [36].

5.6.1 Parameterized Queries and SQL Injection Prevention

To protect relational databases from SQL injection attacks, one of the most serious security threats, parameterized queries are crucial. By clearly delineating code from user-supplied data, they improve database security and successfully block the execution of malicious code. By protecting the database and its data from SQL injection, this method guarantees the database’s security and the dependability of its data.

Secure programming practices are integral to our study on key security components in relational databases, specifically addressing SQL injection prevention. The use of parameterized queries and prepared statements is highlighted as a crucial method for constructing SQL queries influenced by user input. For example, a database query searching for a specific term might be:

```sql
select * from notes nt where nt.subject = 'search_word';
```

Traditional SQL Injection tactics like substituting ‘ or 1 = 1; -- , for a genuine search term are thwarted by parameterized queries. This technique ensures that user input is treated exclusively as data and not as executable SQL
code. Prepared statements reinforce parameterized queries by first creating a SQL statement template and then incorporating necessary user inputs. This separation prevents injection, as the database processes the values before executing the query. Our research underscores the implementation of parameterized queries and prepared statements in all dynamic SQL generation influenced by user inputs, advocating for treating user data as bind variables or arguments to maintain the intended SQL logic [48][49][50].

Stored procedures on the database end further encapsulate the concept of parameterized queries. Although parameterized queries are central in our study’s approach to preventing SQL injection, the addition of input validation and escaping techniques significantly fortifies defenses against these vulnerabilities. Input validation involves scrutinizing and sanitizing user inputs prior to their SQL query usage, ensuring only correctly formatted data interacts with the database. This includes verifying data range, format, length, and type, effectively countering many injection attempts where malicious code is disguised as normal input [48][49][50].

Escaping techniques, which modify user inputs to prevent potentially dangerous characters from being interpreted as executable code, are particularly effective with characters like single quotes and semicolons. By rendering these characters harmless in SQL commands, the risk of SQL injection attacks is significantly reduced. Combining these methodologies with parameterized queries establishes a comprehensive defense mechanism, markedly diminishing SQL injection vulnerabilities [48][49][50]. Relational databases are better protected against a wider range of injection threats thanks to the integration of secure coding practices, which strengthens the overall security mechanism.

### 5.6.2 Patch Management

The security and integrity of relational databases must be maintained through Patch Management. Maintaining software security includes updating software and applying patches on a regular basis to fix vulnerabilities and prevent known threats. In order to maintain database security and operational health, this preventative practice is key to protecting databases from both existing and future risks. Consequently, no relational database security strategy is complete without patch management and its function in maintaining database integrity and resilience.

Key Security Components in Relational Databases include patch management as a key component. Maintaining the security and dependability of
relational databases requires effective patch database management strategies. In the dynamic field of cyber security, vulnerabilities in database systems are a serious concern. In order to improve system performance and stability, patch security vulnerabilities, and identify and install updates for database software, patch management is necessary. You must be proactive and methodical when dealing with patches; this includes keeping an eye out for new patches that database vendors release and carefully determining how urgent it is to apply these patches to real database systems [51].

The thesis advocates for a structured patch management protocol that includes:

- **Regular Assessment**: Conducting audits of database systems to identify security flaws and the availability of relevant patches.
- **Risk Evaluation**: Evaluating the impact of vulnerabilities and determining the urgency of applying patches.
- **Testing Before Deployment**: Rigorous testing of patches in a controlled environment before application to production systems to ensure compatibility and prevent disruptions.
- **Scheduled Updates**: Applying patches during scheduled maintenance windows to minimize impact on database availability and performance.
- **Continuous Monitoring and Reporting**: Maintaining records of applied patches, tracking patching history, and documenting issues encountered during patching. This documentation supports compliance, audit trails, and future patch management activities.
- **Collaboration with Vendors**: Engaging with vendor support and the cybersecurity community for timely alerts about critical patches and staying ahead of new threats.

As part of the Key Security Components in Relational Databases, patch management is a crucial procedure that helps secure database systems from both existing and future cyber threats. This strategy is both thorough and flexible.

### 5.7 Awareness and Education

Effective relational database security depends on comprehensive awareness and education initiatives. Users and administrators can identify and counteract
security threats with the help of training programs. Businesses can make themselves more resistant to cyberattacks by fostering a culture that values best practices. The objective is for everyone who comes into contact with sensitive systems to actively follow secure data handling protocols. In the event that an incident does occur, swift identification and response are made possible by establishing organizational proficiency around database vulnerabilities [51].

5.7.1 Security Training

Strengthening relational databases to withstand cyber threats requires security training. It teaches database administrators and users the fundamentals of data management and security. In order to increase awareness of security vulnerabilities and to inculcate best practices, structured training programs are significant. Database staff who have received this training will be better equipped to detect, avoid, and respond to security threats, strengthening the security of relational databases as a whole.

Security training is a vital component in the realm of relational database security, focusing on equipping database users and administrators with essential skills and knowledge for data management and protection. This section of the thesis delves into the significance of structured training programs in enhancing awareness about security vulnerabilities and implementing best security practices [51].

- **Basic Security Education:** All employees with database access are required to undergo introductory training in security. This training establishes a foundational understanding of the risks, regulations, and standards that are crucial for database interaction.

- **Role-Specific Training:** Training is customized according to the roles of the employees. Database administrators might receive training in specific areas like configuration hardening and auditing, while developers might focus on secure coding practices.

- **Practical Application:** The training connects theoretical concepts to their practical applications, utilizing real-world examples of security breaches to underscore the importance of robust security practices.

- **Training Verification and Tracking:** The completion of training is tracked to ensure all users have undergone the necessary education. Access to databases is conditional upon the completion of this training.
• **Ongoing Education:** Regular refresher courses are provided to keep the staff updated on evolving threats and changing security practices.

• **Building a Security-Conscious Culture:** The training aims to cultivate a culture of security awareness within the organization, making users a proactive first line of defense in database security.

This structured approach to security training is fundamental in preparing database personnel to anticipate and respond to various cyber threats, thereby fortifying the security and integrity of relational database systems.
Chapter 6

Expert Assessment and Component Evaluation

This chapter assesses the effectiveness and applicability of the security components identified in the research, aligning with the evaluation model established in Chapter 4. The evaluation is based on structured interviews with database security experts, focusing on the credibility of these experts and their assessment of the security components in terms of semantic and syntactic correctness and usefulness.

In Section 6.1, we utilize a comprehensive approach for expert selection and evaluation. Section 6.2 highlights the interviewees’ expertise and relevance in database security. Semantic correctness of the security components, as evaluated through expert interviews, is discussed in Section 6.3. Section 6.4 assesses the logical structuring of these components based on expert feedback. The practical utility of the identified security components, as reflected upon by the experts, is explored in Section 6.5. Finally, Section 6.6 presents deep insights from experts on relational database security enhancements, gathered from open-ended questions.

6.1 Expert Assessment

Two distinguished experts in the field of database security share their insights in this thesis. To ensure the validity and reliability of their insights, the selection and evaluation of experts for this research used a comprehensive and methodical approach. As described in Chapter 4 each expert was selected based on their extensive background in database security, including academic qualifications, professional certifications, and specific expertise in relational
databases and cybersecurity. This was done to ensure that they bring a depth of technical knowledge that was essential for assessing the security components.

Expert 1 has extensive relational database cybersecurity experience. They developed security protocols for large-scale data environments. This expert’s insights on relational database security strategy implementation and effectiveness help us answer our research questions. They have 13 years of experience in the field of Database security.

Expert 2 has a deep understanding of database architecture and has played a significant role in designing and securing complex database systems for high-profile organizations. Their expertise goes beyond technical database security to include emerging cyber threats. Their perspectives cover database security’s current and future state. They have 15 years of experience in the field of Database security.

In order to verify their active engagement in the field, their current roles were investigated, which provided insights that were both relevant and up to date. To evaluate their practical understanding of the changing database security landscape, we also took into account the breadth of their experience, including career progression, diversity of roles, and involvement in significant projects. In addition, their contributions to the field, which included things like published research, presentations at conferences, and leadership in innovative projects, were evaluated in order to validate their thought leadership and influence in the field of database security.

### 6.2 Interviewee Credibility

Interviewee 1 emphasized their extensive experience in database security, highlighting their current role in developing secure database architectures and previous security roles focusing on encryption and network security. Their credibility was established by the extensive experience they have in a variety of database security aspects, including their participation in projects that aim to improve database encryption. The second interviewee, who has a background in cybersecurity policy and is currently working in database security consulting, highlighted their long-term involvement in the formulation of security strategies and education programs. This demonstrates their extensive knowledge and the relevance they have to this research.
6.3 Semantic Correctness

Particularly appreciative of the clear articulation of encryption strategies and access controls, Interviewee 1 found the security components to be relevant to modern kinds of threats. It was suggested that the descriptions of the monitoring protocols be provided with some minor clarifications in order to improve comprehension. Interviewee 2 praised the clarity of the component descriptions, particularly in relation to vulnerability prevention methods. They also confirmed the relevance of the component descriptions in addressing evolving database threats, indicating that there have been no significant changes.

6.4 Syntactic Correctness

An interviewee identified an overemphasis on certain traditional security measures, while suggesting the inclusion of emerging AI-based threat detection systems. This was in reference to the correctness of the syntactic structure. In order to more accurately reflect the ever-changing nature of database security, they suggested placing the components in a different order. The second interviewee thought that the order of the components was logical, and they praised the flow from data protection strategies to access control in particular.

6.5 Usefulness

The first interviewee reflected on the usefulness of the identified components, particularly the multi-layered approach to access control, as being highly effective in improving database security. They were ready to incorporate such components into future strategies and were eager to do that. The second interviewee viewed the data protection strategies, in particular the emphasis placed on encryption, as being very practical. They expressed their intention to incorporate these strategies into their consulting practices, pointing out that they are adaptable to accommodating a wide range of client requirements.
6.6 Open-ended questions

6.6.1 Interviewee 1

The preliminary findings make it very clear that the foundation for relational database security in our research is strong, particularly with regard to access controls and data protection strategies. One of the strengths is the implementation of multi-factor authentication, which significantly boosts the level of security. Incorporating authentication systems that are driven by artificial intelligence, on the other hand, could further strengthen this aspect by identifying patterns of user behavior that are not typical. When it comes to the protection of data, it would be advantageous to make strategic use of encryption, which includes techniques such as transparent data encryption when applicable. The initial measures taken to ensure the security of the network are commendable, particularly the implementation of firewalls and straightforward encryption protocols. In addition to this, the implementation of advanced Intrusion Detection and Prevention Systems (IDPS) would provide a defense mechanism that is more comprehensive. The emphasis placed on vulnerability prevention is something that they also appreciate; however, they would recommend enhancing parameterized queries with behavior-based monitoring systems in order to provide a more robust defense against SQL injection attacks. The awareness and education programs are a good place to start; however, in order to cultivate a more security-conscious culture within organizations, they could be more consistent and comprehensive.

6.6.2 Interviewee 2

Several strengths can be found in the initial approach to relational database security that was adopted by our research. These strengths include the well-structured monitoring and auditing systems as well as the proactive vulnerability management techniques. On the other hand, there are some areas in which there is room for improvement. The authorization mechanisms in the field of access controls are solid; however, the incorporation of systems that are more dynamic and aware of the context, such as Risk-Adaptive Access Control (RAAC), could improve the adaptability and responsiveness of the system. Although the existing backup strategies are effective, the addition of advanced encryption standards such as AES would further secure sensitive data. This is because the current backup strategies are effective. Although the dynamic auditing approach is beneficial, the incorporation of automated tools for audit
data collection and analysis would be the most effective way to maximize both efficiency and accuracy. In the context of patch management, although the regular updates and applications that are currently in use are efficient, the implementation of predictive patching through the use of artificial intelligence algorithms could proactively protect the database from any potential exploits. Our research, in general, establishes a strong foundation for relational database security, and the enhancements that we have suggested could strengthen it against various cyber threats that are constantly evolving.
Chapter 7

Improved Results

As we approach the conclusion of our thesis on relational database security, it is critical to consider the significant findings from our in-depth research and expert interviews. Building on the extensive analysis provided earlier in Chapter 6, this chapter seeks to highlight crucial areas in need of improvement. We are committed to refining current strategies and staying abreast of cybersecurity trends to ensure that our approach remains effective and relevant. This chapter presents the advancements and refinements made in our research.

Section 7.1 discusses enhancing database security through advanced access control methodologies and techniques. Section 7.2 focuses on improving database integrity and security through comprehensive monitoring and auditing systems. Section 7.3 addresses potential threats proactively for robust database security and resilience. Section 7.4 consolidates the findings and implications of improved security measures in relational databases.

7.1 Refinement of Access Control Strategies

Securing data integrity and confidentiality in relational databases is largely dependent on the domain of access controls. This section incorporates advanced insights from recent studies to improve upon the previous evaluation of the preliminary results.

As described in [2] recent developments in authentication place a strong emphasis on the integration of AI-driven authentication systems. These systems offer a higher level of security by analyzing user behavior patterns using machine learning algorithms. For example, additional authentication requirements are triggered by anomalies in user behavior, such as odd login
times or patterns of data access. By using this method, the risks related to compromised credentials are greatly reduced.

Context-aware authentication systems are crucial, as [1] clarifies. These systems dynamically modify authentication requirements based on an evaluation of the context of access requests, including location and device security status. These context-sensitive systems are particularly important for preventing attacks originating from credentials that have been stolen and used in unidentified contexts.

Behavioral biometrics is an advanced technology that verifies a person’s identity based on their distinct behavioral patterns, such as their typing, mouse movements, or even their gait. A non-intrusive and extremely secure kind of authentication, behavioral biometrics constantly assesses user interaction with their devices in real-time, in contrast to conventional authentication methods that demand user action upon access. Leveraging machine learning, this technology has been shown to be very accurate, adapting and maintaining high levels of precision as it gains a deeper understanding of the user’s behavior patterns over time. Behavioral biometrics also provide better security against fraud and identity theft since they are far more difficult to copy than physical features [52].

In addition to behavioral patterns, other biometric modalities, including voice and facial recognition, are a part of AI-driven biometric authentication. With the help of AI, these systems are now more precise and efficient, which strengthens their defenses against fraud. Artificial intelligence (AI) and biometrics have already helped stop massive fraud losses. references [53][54].

In the banking industry, for instance, Fico acquired Ezmcom, a behavioral biometrics firm that secures millions of users worldwide, and integrated AI-driven authentication into their platform. With the help of this connection, more advanced identity proofing and authentication capabilities, such as biometric, behavioral, and multifactor authentication, have been made possible, greatly improving customer protection and streamlining the onboarding process [55]. These innovations show how AI-powered biometric solutions may improve security while also making the user experience smooth.

As discussed in [2] the idea of Dynamic Access Control (DAC) presents a flexible authorization mechanism. Based on recent threats and unusual user behavior, DAC modifies user permissions in real-time. In contrast to static Role-Based Access Control (RBAC), this approach enables prompt response to possible security breaches.

Furthermore, recommendations made in [1] support the use of Risk-Adaptive Access Control (RAAC). A user’s action’s risk level is assessed
Improved Results | 69

by RAAC systems based on a number of factors, including user role, data sensitivity, and threat intelligence at the moment. This risk assessment modifies user permissions dynamically, ensuring that high-risk actions are closely examined and may even be denied.

These improvements in authorization and authentication that come from current research greatly strengthen relational database security. Data bases can better defend against changing cyber threats by implementing these advanced mechanisms, ensuring the security and integrity of critical data.

### 7.2 Enhanced Monitoring and Auditing

An innovative approach to dynamic auditing and logging is presented in the study [43]. The focus of this approach is on using sophisticated algorithms to dynamically modify audit parameters in response to real-time database activity analysis. By eliminating pointless logging and concentrating on high-risk activities, this strategy optimizes performance through more effective and focused auditing. Moreover, the significance of incorporating automated tools for audit data collection and analysis is emphasized by [42]. In order to ensure accurate and efficient capture of relevant information during the auditing process, triggers and automated scripts are utilized. By improving the overall level of security, these automated processes also enable quicker responses to possible security incidents.

By integrating knowledge from [42], DAM’s efficiency is increased. In order to identify unusual trends and possible security breaches, this also involves integrating intelligent analytics. DAM tools can now support proactive security measures by offering more insightful and actionable intelligence through the use of data analytics. Furthermore, [43] suggests storing audit logs in a decentralized manner. By decreasing the possibility of tampering and improving accessibility for criminal investigation, this method improves the security of logs. It also advises using cutting-edge encryption techniques to secure these logs and guarantee their confidentiality and integrity.

Based on the most recent research, these improvements to logging, DAM, and dynamic auditing greatly improve relational database monitoring and auditing. By implementing these advanced strategies, you can protect sensitive data from illegal access, enhance your defense against emerging cybersecurity threats, and guarantee regulatory compliance.
7.3 Proactive Vulnerability Management

The integrated approach presented in [49] delves further into parameterized query optimization and proposes a method that combines parameterized queries with behavior-based monitoring systems. With this integration, the system can detect and respond to suspicious query patterns that could be signs of an attack, making databases more resistant to advanced injection techniques and providing a stronger defense against SQL injection.

[50] goes on to recommend adding adaptive learning systems to the parameterized query framework. Over time, these systems accumulate attack data and adapt their query parameters and sanitization methods to counter new injection attacks. High levels of security can be maintained by databases by using such adaptive measures to counter the constantly changing tactics used in SQL injection attacks.

To improve this method, which builds on the idea of predictive patching from [49] AI can be used to predict potential vulnerabilities. Artificial intelligence algorithms can proactively secure databases from potential exploits by analyzing trends in cyber threats and vulnerabilities. This allows for the development of patches before these issues become public knowledge.

Another point made in [50] is how patch management needs to take a comprehensive approach. It recommends setting up a centralized patch management system that takes into account the long-term health of the database infrastructure in addition to addressing the immediate vulnerabilities. To guarantee an all-encompassing and constantly shifting strategy for database security, this system should incorporate automated patch deployment, frequent compliance checks, and a feedback loop for ongoing improvement. Relational databases are able to withstand both existing and future security risks because of these advanced improvements in patch management and parameterized queries. The availability, security, and integrity of sensitive data stored in relational database systems are guaranteed by this proactive and advanced approach.

7.4 Summary

We have comprehensively enhanced our strategies and methodologies to elevate security measures in relational database systems, integrating advanced technologies and innovative approaches across key areas such as authentication, authorization, auditing, monitoring, and vulnerability
Our authentication strategy now includes AI-driven systems for nuanced, context-aware processes, vastly improving security against sophisticated cyber threats. In authorization, we have expanded from primarily using Role-Based Access Control (RBAC) to incorporating dynamic models like Dynamic Access Control (DAC) and Risk-Adaptive Access Control (RAAC), offering real-time responsiveness and adaptable permissions. For dynamic auditing and logging, we have moved beyond conventional techniques to implement dynamic auditing parameter modifications and employ automated data collection and analysis tools, alongside decentralized storage of audit logs with advanced encryption. Database Activity Monitoring (DAM) has been enhanced with intelligent analytics for proactive threat identification and mitigation. In tackling SQL injection, we have optimized parameterized queries with behavior-based monitoring and adaptive learning systems, strengthening defenses against advanced attacks. Finally, our patch management strategy now utilizes AI algorithms for predictive patching and employs a comprehensive, automated system for holistic database infrastructure security. This holistic enhancement approach underscores our commitment to advancing relational database security through forward-thinking strategies.

The table 7.1 provided below summarizes these enhancements, contrasting the status of various security components in the preliminary and improved results. This comparison underscores our commitment to advancing relational database security through innovative and forward-thinking strategies.
## Improved Results

<table>
<thead>
<tr>
<th>Security Component</th>
<th>Status in Preliminary Results</th>
<th>Status in Improved Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>Focus on multi-factor authentication and traditional methods like passwords.</td>
<td>Incorporation of AI-driven systems and context-aware authentication for enhanced security.</td>
</tr>
<tr>
<td>Dynamic Auditing and Logging</td>
<td>Emphasis on traditional auditing and logging techniques for transparency and record-keeping.</td>
<td>Introduction of dynamic modification of audit parameters, automated tools for audit data collection and analysis, and decentralized storage of audit logs with advanced encryption.</td>
</tr>
<tr>
<td>Database Activity Monitoring (DAM)</td>
<td>Real-time monitoring of database transactions and activities for security and compliance.</td>
<td>Enhancement with intelligent analytics for trend identification and proactive security measures, and suggestions for storing audit logs in a decentralized manner.</td>
</tr>
<tr>
<td>Parameterized Queries and SQL Injection Prevention</td>
<td>Emphasis on the use of parameterized queries and prepared statements for SQL injection prevention.</td>
<td>Optimization of parameterized queries combined with behavior-based monitoring and adaptive learning systems to counter advanced injection attacks more effectively.</td>
</tr>
<tr>
<td>Patch Management</td>
<td>Regular software updates and patch applications to address known vulnerabilities.</td>
<td>Implementation of predictive patching using AI algorithms, comprehensive patch management strategies including automated deployment, compliance checks, and feedback loops for continuous improvement.</td>
</tr>
</tbody>
</table>

Table 7.1: Enhancements in Relational Database Security Components from Preliminary to Improved Results
Chapter 8

Analysis and Discussion

We analyze and evaluate the final results in this crucial chapter of the thesis. This chapter synthesizes research findings, contextualizes them within security practices, and discusses their practical implications. In Section 8.1, we analyze the individual security components discovered through our research, assessing how well they each contribute to relational database security and their collective effectiveness. Finally, Section 8.2 involves our analysis of the current security measures in the field, contrasting them with the findings from our research.

8.1 Analysis of Key Security Components

The complicated concepts that underlying relational database security are revealed through an in-depth investigation of the core building blocks. The overall defense machinery that secures sensitive data is comprised of a number of components, each of which is an essential component.

8.1.1 Access Controls

The mechanisms for authentication and authorization form the gateway that regulates access based on credentials and permissions. Incorporating biometrics, multi-factor authentication, contextual controls, and password policies, these mechanisms collectively work to prevent unauthorized access. However, with persistent attackers continually searching for validation loopholes and backdoors, the task of updating identity models to keep pace with increasingly sophisticated threats is ever-present and demanding.

The importance of multi-factor authentication (MFA) in securing against
unauthorized access is emphasized in the research. The mentioned implement-
ination of multi-factor authentication (MFA) integrates various layers of
verification, successfully reducing the risk associated with compromised
passwords and other single-factor authentication weaknesses. By requiring
users to validate their identity through multiple independent credentials, this
layered approach (shown in the Figure 5.2) effectively mitigates the risk of
unauthorized access.

An additional layer of security would be added to authentication with
the proposed use of behavioral and advanced biometrics. These techniques
provide ongoing and tailored security measures because they are harder to
copy or alter. Traditional authentication methods are becoming more and
more insufficient in the constantly evolving cybersecurity landscape, which
is why the research supports these methods. An additional dynamic and
responsive layer to database security is provided by behavioral biometrics,
which continually tracks user interactions throughout their session. Granting
permissions based on authorized identities is a critical process for controlling
access to sensitive data within the database, and the research stresses its
importance. Key to preventing unauthorized data access and manipulation is
this emphasis on efficient authorization mechanisms.

The research emphasizes the importance of implementing authorization
mechanisms that are flexible, like Attribute-Based Access Control (ABAC)
and Role-Based Access Control (RBAC), in order to meet the diverse and
continuously shifting security requirements. ABAC’s accuracy in policy
evaluation and RBAC’s flexibility in handling complex security requirements
in relational databases show that authorization is a broad issue.

On top of that, metadata segregation adds a new dimension to authorization
by enabling the data-sensitive dynamic application of referential integrity
constraints. This adaptability is vital for meeting the evolving demands of
operations and database structures. Oracle 11g’s Integration of Transparent
Data Encryption (TDE) demonstrates how encryption policies can be tailored
to the particulars of each database. Incorporating these practical authorization
mechanisms shows that the research is dedicated to providing innovative and
adaptable security measures.

8.1.2 Data Protection

Data protection methods, such as encryption and backup strategies, are
essential components of relational database security for ensuring the security
of sensitive information. This analysis thoroughly examines the methods’
usefulness and implications, with a particular focus on their function in securing database systems from data breaches and keeping their integrity.

To prevent data breaches and unauthorized access, encryption is an essential security measure for relational databases. Encryption ensures that sensitive information remains secure, even if intercepted, by encoding data to be accessible only with the correct decryption key. The research’s focus on symmetric and asymmetric encryption techniques for protecting data while it is in transit and at rest demonstrates the need for a variety of approaches to meet the various security requirements of relational databases.

The research’s analysis of strategic encryption deployment, with a focus on Transparent Data Encryption (TDE) and the Advanced Encryption Standard (AES), highlights the need for a middle ground between theoretically strong encryption and its actual use in the real world. It is important to have robust and flexible encryption strategies, as demonstrated by TDE’s storage-level encryption and AES’s key length and block size flexibility. The research emphasizes the importance of end-to-end encryption for data transfers, which further demonstrates the all-encompassing strategy required to reduce the likelihood of interception and secure data integrity while in transit. Equally important, though, is effective management of encryption keys. Supporting data integrity and availability requires regular changes, secure storage, and restricted key access. The research presents encryption as a crucial part of relational database security, and its support of such protocols is in line with the changing standards in cybersecurity.

Relational databases have backup strategies in place to protect against data loss, corruption, and deletion. In order to ensure data resilience, the study highlights the importance of robust backup and recovery procedures. Various backup methodologies, including differential, incremental, and full backups, are included in the outlined comprehensive strategy to meet different needs and conditions. A thorough understanding of the operational continuity requirements of databases is reflected in the analysis of backup strategies in the thesis. A comprehensive approach to data protection is reflected in the importance placed on various backup types, frequency, retention duration, storage locations, and the requirement of encryption of backup files. It is important to regularly test backup recoverability to make sure backup systems are reliable in practice as well as in theory.

As a result of our study’s acknowledgment of the ever-changing database sizes and business demands, we propose adaptive strategies such as ‘incremental forever backups’. Implementing these adaptive approaches is crucial for maintaining effective backup strategies in dynamic database
environments and against new cybersecurity threats.

8.1.3 Monitoring and Auditing

For a robust defense against relational database security breaches and to maintain accountability, monitoring and auditing are crucial in the context of relational database security. The research’s results emphasize the importance of relational database auditing, logging, and Database Activity Monitoring (DAM) in securing relational databases.

To ensure transparency and security within relational databases, dynamic auditing and logging are essential. Security administrators can quickly detect anomalies or policy violations thanks to these procedures. When it comes to retrospective evaluation and compliance verification, logging provides that necessary historical record, while dynamic auditing adjusts to changing interactions within database systems. Our research highlights the significance of precise auditing, such as that found in Oracle9i, which customizes audit procedures to particular unauthorized data access scenarios, improving the identification of abuse or unauthorized access. In order to generate alerts quickly under certain conditions, this method is critical for proactive threat detection and accurate audit policy definition.

For auditing to remain effective in the face of changing usage patterns or new threats, it must be able to dynamically adapt. Finding an appropriate balance between detailed logging and system performance is key to keeping security and efficiency at a high level, according to the study. Ensuring the integrity of audit logs as evidence of crime is achieved by integrating methods for detecting tampering using cryptographically strong hash functions. Data privacy and integrity in relational databases are ensured by Database Activity Monitoring (DAM). Key to identifying abnormal conduct, policy violations, and potential security threats is its capacity to provide complete inspection of all database transactions and real-time monitoring. Quickly responding to security incidents and abiding to regulatory norms are both made possible by DAM’s comprehensive view of database operations. DAM tools provide real-time or near-real-time monitoring, which is essential for maintaining the confidentiality and integrity of databases, and they work independently of the DBMS.

Database administration systems (DAMs) record and capture every action performed on databases, including those performed by database administrators, across all platforms. This data is crucial for identifying and notifying about possible security threats or policy violations, and it
is stored securely apart from the actual database. The research confirms DAM’s importance for thorough auditing of database operations, including transactions, administrative tasks, and access attempts. In the case of a security breach, it carefully tracks details such as SQL queries, user context, timestamps, tables accessed, and more, providing a strong basis for expert analysis.

The results of the research support the idea that relational database security is a continuous, dynamic process that requires vigilance and adaptation. For protection against threats, dynamic auditing, logging, and DAM integration into database security strategies is essential. These mechanisms provide a multi-layered security approach, enhancing relational database integrity and confidentiality. Dynamic auditing and logging provide proactive security, while DAM provides a complete database activity overview for quick response to threats. This research investigation takes a proactive approach to database security, preparing databases for current and future cybersecurity threats.

### 8.1.4 Network Security

The research’s focus on network security within relational databases emphasizes the need for robust network security measures like intrusion detection systems, firewalls, and encrypted communication protocols for security against network-based threats. The findings show that restricting database access to authorized traffic through these components significantly reduces the risk of database breaches and unauthorized access, maintaining the confidentiality and integrity of sensitive information.

The study emphasizes the importance of SSL/TLS encryption in securing the privacy and integrity of database server-client data transmission. Eavesdropping, tampering, and message forgery can be avoided by this encryption method. Network security audits and penetration testing, which simulate real-world attacks, are essential for finding vulnerabilities. For monitoring network traffic and responding to malicious activity, advanced Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are essential. These systems provide comprehensive security with the combination of threat detection (IDS) and proactive attack prevention (IPS). Relational databases are more resilient to network-based threats thanks to this research’s focus on dynamic database adaptation in auditing and the integration of these systems with Security Information and Event Management (SIEM) systems.

Securing against SQL injection and unauthorized access is crucial for the database firewall. Database firewalls, as opposed to network firewalls, read
and analyze SQL data streams while providing syntax control and thorough auditing. For proactive threat detection, these firewalls use pattern mining and Bayesian networks. After an attack, the reactive aspect analyzes the database to improve pattern recognition based on recent attack signatures.

Importantly, the research used Bayesian network-based analysis in database firewalls. In a live attack, probabilistic reasoning from past and current data is essential for assessing data object integrity. The Bayesian network’s directed acyclic graphs (DAGs) structure simplifies complex distribution functions to predict data object integrity in the face of anomalies or attack patterns.

8.1.5 **Vulnerability Prevention**

The research conducted shows that vulnerability prevention and patch management are crucial to relational database security. Securing against unauthorized access and security breaches requires vulnerability prevention, including parameterized queries and least privilege. Relational databases’ integrity and operation depend on patch management, a proactive security strategy.

This research shows that parameterized queries are a great defense against SQL injection attacks, which are a major risk to relational database security. Parameterized queries and prepared statements are crucial in preventing the execution of malicious code because they separate code from data that the user has provided. These procedures highlight the significance of secure programming practices in relational database security by guaranteeing the database’s security and the data’s reliability.

It is critical to further strengthen these defenses with input validation and escape techniques. To protect SQL queries from malicious code that masquerades as legitimate input, input validation checks and cleans user inputs. The use of escape sequences in SQL commands reduces the dangers posed by malicious characters. A full defense mechanism against SQL injection vulnerabilities can be formed by integrating these methods with parameterized queries.

One of the most important aspects of relational database security is patch management. This procedure includes a methodical approach to guarantee database security and operational health in addition to applying updates to address vulnerabilities. The thesis supports a structured protocol that includes regular assessments, risk assessments, rigorous testing prior to deployment, scheduled updates, ongoing monitoring, and vendor collaboration. The
importance of anticipating and responding to emerging cybersecurity threats is highlighted by this policy.

### 8.1.6 Awareness and Education

The results of this research highlight the significance of security training. An essential tactic for strengthening relational database security as a whole, structured security training programs serve as both an instructional tool and a resource. Ensuring that users and administrators receive comprehensive and role-specific training programs is crucial for their ability to identify, avoid, and handle security threats appropriately.

All employees with database access have to receive basic security education, according to the research. To ensure safe database interactions, it is essential to have a solid understanding of the risks, regulations, and standards. This foundational training provides that basis. Adding role-specific training enhances this approach even more. Database administrators, for example, learn about auditing and configuration hardening, and developers learn about secure coding practices. The database management system is structured in a way that guarantees each role has the specific knowledge and skills needed to do their job well.

The research’s highlighted training programs go beyond just theoretical concepts and incorporate real-world examples of security breaches to make them more applicable. This approach emphasizes the critical need for a strong security framework and the serious consequences of weak security procedures. Staff should be regularly updated on evolving threats and changing security practices through refresher courses. This should be a crucial part of their training. Staff members’ security knowledge and practices are kept up-to-date and effective against modern cybersecurity threats by means of this approach to continuous learning.

Creating a security-aware company culture is one of the major benefits of this training program, according to the research. Users become an active first line of defense in database security by making security awareness a part of the organizational ethos. According to the research, the probability of security breaches can be greatly reduced if users are both knowledgeable and careful.

Implementing mechanisms to verify and track the completion of training modules is an important aspect of the security training program, according to the research. This guarantees that all database users have an understanding within the security measures in place. Such a structured verification system highlights the significance of security training and ties database access to the
completion of these training modules, therefore promoting accountability and compliance within the organization.

8.2 Evaluating the Validity

The validity of the research on mapping out the key security components in relational databases was discussed as early as Section 3.6 to ensure the transparency and reliability of our research in the context of relational database security.

1. Credibility

The robustness of our methodology and the breadth of expertise of our interviewees are the cornerstones of our research credibility. An approach based on structured interviews with database security experts (all with ten years or more of experience) was laid out in earlier chapters. Not only did this give the findings more credibility, but it also made sure that the insights were representative of actual situations and difficulties with database security. In order to make our conclusions more credible, we carefully compared interview data with recent literature to make sure they were not just based on personal opinions but also supported by larger academic and industry discussions. But interviews still have the potential for lowering credibility due to their subjective nature. In order to prevent this, we made sure that our selection of interviewees was diverse and that we took a critical and balanced approach to data interpretation, ensuring that our findings were relevant to the continuously shifting field of relational database security.

2. Transferability

Being able to apply our findings to different situations is what we mean when we talk about transferability. Despite its breadth, our research is mostly concerned with relational databases in business environments. We might not be able to directly apply our findings to different kinds of databases or smaller-scale contexts because of this specificity. This was addressed by including a variety of backgrounds and experience levels in our selection of interviewees, which allowed us to capture a variety of perspectives and situations. Our methodology, including our selection criteria and interview process, is described in detail so that other researchers can understand the situations where our findings are most
relevant (see chapter 3). Improving the transferability of our findings, future research could go further by investigating similar security aspects in non-relational databases or different organizational scales.

3. Dependability

Consistency and reliability in our methodologies and findings over time are crucial for the dependability of our research. A strict and methodical approach to data collection, analysis, and interpretation is used to ensure this. The analysis of these structured interviews was detailed and systematic, and they were carefully planned to cover a wide range of subjects relevant to relational database security. The dependability of our research has been compromised by the ongoing developments in database security, though. We made sure that our findings are still applicable in the dynamic cybersecurity landscape by including discussions on new technologies and trends. The dependability of our research is strengthened by this methodology and our extensive approach.

4. Objectivity

We faced the challenge of maintaining objectivity in our qualitative research because interviews and analysis are inherently subjective. We addressed this by conducting our research with a systematic and open approach. The selection criteria for interviewees were well-defined and strictly followed, guaranteeing a wealth of relevant information. In addition, we critically analyzed the interviewees’ responses to avoid overly relying on personal opinions and to make sure that our conclusions were supported by an extensive study of the interviews and the literature. The objectivity of our findings is increased by this methodical approach, which reduces subjectivity.
Chapter 9
Conclusions and Future Work

In our comprehensive analysis of relational database security, we delved deep into the intricacies of current security practices, shedding light on their robust foundations while also identifying critical areas that require substantial improvements. We meticulously analyzed how these security measures, though effective in certain contexts, often fall short in addressing specific, continuously evolving cyber threats that plague modern digital infrastructures.

The problem of this thesis is the lack of comprehensive research covering all key security components in relational databases, which presents a significant challenge for organizations seeking to secure their database systems comprehensively. The purpose is to comprehensively map the key components in the security of relational databases, aiming to uncover dynamic and adaptable solutions suited to the contemporary threat landscape. The goal is to help organizations and Database security professionals to secure their relational databases against diverse security threats, through a research of current security practices and the proposal of actionable strategies. The results are a comprehensive map of the key security components in relational databases.

9.1 Conclusions

Our study culminates in a nuanced understanding of relational database security, underscoring the necessity for continuous monitoring, the timely incorporation of new security patches, and the importance of holistic security policies and practices. This includes the integration of technical solutions with employee training, regular audits, and a security-aware organizational culture. Our research emphasizes the importance of comprehensive, flexible,
and advanced methods to secure the security, integrity, and confidentiality of data stored in relational databases. Furthermore, it underscores that existing systems, while robust, require ongoing development to counteract security vulnerabilities and adapt to emerging cyber threats.

Our results show that database security requires a multi-faceted strategy. While developing this strategy, it is important to keep in mind that people are just as important as any technological component when it comes to implementing and maintaining security measures. Since the nature of the threats is constantly evolving, database security is an area that requires constant flexibility and adaptation.

9.2 Limitations

Although we go into great detail about relational databases, our results are not applicable with other types of database management systems, such as non-relational or NoSQL databases. Because these systems typically use different security paradigms and architectures, our findings might not apply fully in these settings. A distinguishing feature of the cybersecurity industry is the quick rate of change. There are always new dangers, and security technologies are always improving. Given the dynamic nature of the world, it is possible that some of our results may become irrelevant or outdated sooner than expected. Since this is the case, further research and updates are required to ensure that the results continue to be useful.

While structured interviews are great for getting to the bottom of issues, they also run the risk of being somewhat subjective. It is possible that our research does not capture the full range of opinions and practices in the field due to the fact that different experts have different experiences and viewpoints.

9.3 Future Work

Looking ahead, this thesis lays the groundwork for future research in a number of different directions. To begin, more research into how artificial intelligence and machine learning can improve database security could lead to better ways to identify and respond to threats. One possible approach would be to create models that can predict potential security breaches and provide preventive measures. Second, studies examining security measures specific to distributed database systems and the cloud will hold more significance in the future. Included in this category are solutions to the specific problems caused by
remote data storage and multi-tenant settings. Additionally, it is becoming increasingly important to investigate how privacy regulations like GDPR interact with database security. Creating compliance frameworks that work in combination with security plans could be the subject of future studies. When it comes down to it, database security isn’t complete without considering the human factor. This includes things like corporate culture and training programs. Critical steps in reducing risks associated with human error and insider threats include developing effective training programs and creating a security-conscious organizational culture. Research in the future can further strengthen relational database security by focusing on these areas, making them more resistant to both present and future cybersecurity threats.

9.4 Reflections

In a world that is becoming more and more data-driven, this thesis emphasizes how crucial database security is. Both the complexity of data security and the need for resilience and adaptation in the face of constantly evolving cyber threats have been brought to light throughout this research journey. It serves as a reminder of the importance of our shared duty to keep our cyber future secure and the ongoing struggle to defend our digital infrastructures.
References


https://dl.acm.org/doi/fullHtml/10.1145/2331042.2331051?casa_token=p3rwT1ftp38AAAAA:7s-qxFNCp-OSflh6z8KQp0IG_HhQTiBXHw91LaLM14Z_j71zJ82n5ZKz9GP67ld8Jz8wBD7cskqn6w#authorinfo [Page 9.]


Appendix A

Supporting materials

A.1 Interview answers

Interviewee 1

2.1 Professional Background in Database Security:
"I have been deeply involved in the development and implementation of secure database architectures and encryption technologies for the past thirteen years, during which time I have worked in this industry. With a specific focus on modern solutions to emerging security challenges, my career has been devoted to developing and perfecting security protocols for large-scale data environments."

2.2 Current Role and Relevance:
"I am currently responsible for designing and implementing comprehensive security solutions for relational databases as part of my overall responsibilities in this role. These solutions have been specifically designed to be resistant to a wide variety of modern threats. My strategy places a high priority on the utilization of sophisticated encryption methods and network security, which guarantees the implementation of robust defense mechanisms against potential vulnerabilities."

2.3 Duration in Current Role:
"I have been in this crucial role for a number of years, and during that time I have consistently modified and improved my strategies in order to effectively address new security threats. The ongoing process of adaptation has been extremely important in ensuring that the databases I work with continue to maintain their integrity in terms of security."

2.4 Past Roles in Database Security:
“Throughout the course of my career, I have held a variety of positions, with a focus on database role and security architecture design. I was able to acquire a wide range of experiences and perspectives thanks to the fact that each role I made a significant contribution to the constantly evolving field of database security.”

2.5 Experience Duration:
“My experience in each of these roles has spanned more than a decade, which has provided me with the opportunity to acquire a comprehensive understanding of the complexities of database security from a variety of perspectives.”

2.6 Participation in Security Projects:
“The enhancement of database security has been the focus of several significant projects in which I have played a pivotal role. Within the context of these projects, my primary focus has been on the development of secure architecture designs and robust encryption methods, with the goal of contributing to the advancement of security standards within the appropriate field.”

3.1 Relevance of Security Components:
“The components of security that we have identified are extremely important, particularly when considering the contemporary and developing dangers that are currently present. Due to the fact that they are both theoretically sound and practically applicable, they are tools that are absolutely necessary in the current security landscape.”

3.2 Clarity and Comprehension of Components:
“In general, the descriptions of these components are understandable and convey the information in an efficient manner. In spite of this, I propose that the monitoring protocols be provided with some minor clarifications in order to improve comprehension and guarantee accurate implementation.”

4.1 Relevance and Pertinence of Components:
“In our security model, the majority of the components are considered to be essential. On the other hand, I have noticed that there is an excessive focus on certain conventional security measures. In order to make our model more effective and relevant to the threats that are occurring today, I suggest incorporating threat detection systems that are based on artificial intelligence.”

4.2 Comprehensiveness and Missing Components:
“Even though the current security model is comprehensive in its current form, the incorporation of authentication systems that are driven by artificial intelligence would significantly increase the effectiveness of the model. This integration would bring a new level of sophistication to our security approach,
particularly in terms of dynamically adapting to new threats as they emerge.”

4.3 Logical Sequence and Workflow Alignment: "The arrangement of the security components is logically sound, which reflects an approach to practical security workflows that has been well thought out. The transition from data protection strategies to access control is particularly well-executed by this sequence, which guarantees a unified and efficient security model.”

5.1 Evaluating Practical Utility: "When applied to situations that occur in the real world, I believe that the multi-layered approach to access control is extremely effective. The database security is significantly improved as a result of the fact that it addresses multiple layers of potential vulnerabilities, which results in a more robust defense against unauthorized access.”

5.2 Future Integration and Strategy Thoughts: "The adaptability and practicability of these security components make them an excellent option for the development of future security strategies. In light of the fact that I am confident in these components’ capacity to improve and strengthen database security, I am very excited about the prospect of incorporating them into subsequent plans.”

6.1-6.8 Open-ended Responses: "One of the most significant changes that has occurred in terms of improving security is the implementation of access control measures, particularly multi-factor authentication. Nevertheless, in order to further strengthen our defenses, I would advocate for the incorporation of advanced Intrusion Detection and Prevention Systems (IDPS) as well as authentication systems that are driven by artificial intelligence. Although the methods that are currently being used to prevent vulnerabilities are commendable, the incorporation of behavior-based monitoring systems could provide a more robust defense against sophisticated SQL injection attacks. In conclusion, although the security training programs have established a strong foundation, there is a requirement for additional efforts that are both comprehensive and consistent in order to establish a culture within organizations that is deeply ingrained with a security-conscious mindset.”

Interviewee 2

2.1 Professional Background in Database Security:
"My expertise encompasses a wide range of domains in database architecture and cybersecurity, gained over the course of a career that has lasted for fifteen years. When it comes to designing and securing complex database systems, my primary focus has been on making sure that these systems are resilient against a wide variety of cyber threats. Because I have such a comprehensive
background, I have a profound comprehension of the technical as well as the strategic aspects of database security.”

2.2 Current Role and Relevance:
"In the present moment, I am working as a consultant in the field of database security. In my role, I am responsible for the formulation of security strategies as well as the development of comprehensive education programs. This role is directly connected to the fundamental aspects of relational database security, which enables me to put my knowledge to use in situations that are based in the real world and to make a contribution to the development of security practices in the industry.”

2.3 Duration in Current Role:
"As someone who has been working in this consulting role for a considerable amount of time, I have been able to observe and adjust to the ever-changing landscape of database security responsibilities. As a result, I am able to maintain my position at the forefront of the field and provide my clients with advice that is both pertinent and up to date.”

2.4 Past Roles in Database Security:
"The roles that I have held in the past have been varied, ranging from the formulation of cybersecurity policies to the implementation of database security. Because of these roles, I have been able to make significant contributions to the field by way of strategic planning and the implementation of educational initiatives, which has resulted in an overall improvement in the understanding of database security as well as its strength.”

2.5 Experience Duration:
“Over the course of my career, I have gained a comprehensive and in-depth understanding of the challenges and solutions that are associated with database security. This has been made possible by my extensive experience in a variety of database security contexts.”

2.6 Participation in Security Projects:
“Over the course of my career, I have been actively involved in a number of groundbreaking projects that aim to improve database security. The scope of these projects has encompassed a wide range of activities, including the creation of novel security approaches and the implementation of policies that modify the way database security is viewed and managed within the industry.”

3.1 Relevance of Security Components:
"When it comes to addressing the threats that are currently present and those that are still developing in database security, the security components that we discovered are extremely relevant. In particular, the clarity and precision of the vulnerability prevention methods are noteworthy, and as a result, they are
well-aligned with the urgent requirements of modern database security.”

3.2 Clarity and Comprehension of Components:
"In order to ensure that these security components can be effectively implemented in real-world scenarios, the descriptions of these components are not only clear but also easy to understand to the average person. In order for practitioners to adequately comprehend and accurately apply these components in their respective environments, it is essential that they have this clarity.”

4.1 Relevance and Pertinence of Components: "The current security components have a structure and content that are logical and well-thought-out, demonstrating a seamless flow from data protection strategies to access control measures. Each of these components is a component of the overall security system. Nevertheless, there is room for improvement, particularly through the incorporation of dynamic, context-aware systems such as Risk-Adaptive Access Control (RAAC), which would significantly improve the adaptability and responsiveness of our security model to shifting threat landscapes.”

4.2 Comprehensiveness and Missing Components: "The current security framework is comprehensive; however, the incorporation of advanced artificial intelligence algorithms for predictive patching would be an extremely beneficial addition. The implementation of this preventative strategy has the potential to significantly strengthen the security of our database against potential exploits and emerging threats.”

4.3 Logical Sequence and Workflow Alignment: "There is a consistent and accurate representation of the operational procedures that are involved in the management of databases in the real world, as evidenced by the manner in which the security components are arranged and the order in which they are presented. The implementation of automated tools for audit data collection and analysis would result in an increase in the effectiveness and precision of our security monitoring and response capabilities, which would ultimately lead to an improvement in our overall capabilities.”

5.1 Evaluating Practical Utility: "The fact that our data protection strategies place such a strong emphasis on the use of robust encryption techniques strikes me as being both highly practical and adaptable to the various requirements of our clients. It has been demonstrated that these strategies are effective in improving the security posture in the current database environments. They provide dependable protection against a wide range of threats.”

5.2 Future Integration and Strategy Thoughts: "It is something that I am seriously contemplating incorporating into my future consulting practices
these various security components. Because of their adaptability and ability to be applied over an extended period of time, they are valuable assets in the process of developing advanced security strategies that are able to withstand evolving cyber threats.”

6.1-6.8 Open-ended Responses: ”Our current security model has a number of strengths, one of which is the proactive approach to vulnerability management. The existing monitoring and auditing systems have a commendable structure, and this is a significant strength. Enhancing the authorization mechanisms with systems that are more dynamic and aware of the context, such as RAAC, could significantly improve the effectiveness of these mechanisms. The security of sensitive data would also be increased by incorporating advanced encryption standards. In general, the findings of our research have laid a solid groundwork for relational database security; however, the enhancements that have been suggested would further strengthen our defenses against the constantly shifting landscape of cyber threats.”
Relational database security has become an increasingly important issue for organizations worldwide in the current era of data-driven operations. The urgent need for an extensive knowledge of relational database security components in relational databases is addressed in this thesis. Database security is constantly improving, but there is still a lack of research that analyses these important factors. Because of this gap, databases are not sufficiently secured from new cyber threats, which endangers its accessibility, confidentiality, and integrity.

The problem that the thesis addresses is the lack of comprehensive research covering all key security components in relational databases which, presents a challenge for organizations seeking to comprehensively secure their database systems. The purpose of this thesis is to systematically map the key security components essential to relational databases. The goal is to assist organizations and database professionals to secure their relational databases against diverse cyber threats. Using a qualitative and exploratory methodology, the research analyzed a wide range of literature on database security. The research offers a balanced and comprehensive perspective on the current security landscape in relational databases by integrating theoretical study with structured interviews. This method guarantees that all essential security components is fully investigated.
The results of this thesis involve a detailed mapping of the key security components within relational databases, which are uniquely informed by a combination of academic research and empirical findings from structured interviews with Database security experts. This thesis analyzes these security components based on how well they address current security threats, how well they secure databases, and how well they can adapt to different organizational needs.

"Keywords[eng ]": €€€€

"Abstract[swen ]": €€€€
Säkerhet i relationsdatabaser har blivit en allt viktigare fråga för organisationer världen över i den nuvarande eran av datadriven verksamhet. I den här avhandlingen behandlas det aktua behovet av en omfattande kunskap om säkerhetskomponenter för relationsdatabaser i relationsdatabaser.

Databassäkerheten förbättras ständigt, men det finns fortfarande en brist på forskning som analyserar dessa viktiga faktorer. På grund av denna brist är databaser inte tillräckligt skyddade mot nya cyberhot, vilket åventyra deras tillgänglighet, konfidentialitet och integritet.


Resultatet av denna avhandling innebär en detaljerad kartläggning av de viktigaste säkerhetskomponenterna inom relationsdatabaser, som är unikt informerade av en kombination av akademisk forskning och empiriska resultat från strukturerade intervjuer med databassäkerhetsexpert. Denna avhandling analyserar dessa säkerhetskomponenter utifrån hur väl de hanterar aktuella säkerhetshot, hur väl de säkrar databaser och hur väl de kan anpassas till olika organisatoriska behov.

"Keywords[svse ]": €€€€
Säkerhet i Relationsdatabaser, Databassäkerhet, Cyberhot, Datasäkerhet, Åtkomstkontroll, Sårbarheter i Databaser, Kryptering, Nätverkssäkerhet, €€€€,
Local Variables:
mode: latex
TeX-master: t

The following command is used with glossaries-extra
\setabbreviationstyle[acronym]{long-short}

The form of the entries in this file is \newacronym{label}{acronym}{phrase}
\setabbreviationstyle[acronym]{long-short}

The form of the entries in this file is \newacronym{longplural}{(Debugging Information Entities)}{(DIE)}{(DIE)}{(Debugging Information Entity)}

The following example also uses options
\newacronym{shortplural}{{OSe}s}{{operating systems}{{OSe}s}}{{operating system}}

\newacronym{KTH}{KTH}{KTH Royal Institute of Technology}
\newacronym{LAN}{LAN}{Local Area Network}
\newacronym{VM}{VM}{virtual machine}
\newacronym{WiFi}{WiFi}{Wireless Fidelity}
\newacronym{WLAN}{WLAN}{Wireless Local Area Network}
\newacronym{UN}{UN}{United Nations}
\newacronym{DBMS}{DBMS}{Database Management Systems}
\newacronym{SQL}{SQL}{Structured Query Language}
\newacronym{RDBMS}{RDBMS}{Relational Database Management System}
\newacronym{NoSQL}{NoSQL}{Non-relational}
\newacronym{DAM}{DAM}{Database Activity Monitoring}
\newacronym{MFA}{MFA}{Multi-factor Authentication}
\newacronym{OTP}{OTP}{One-Time Password}
\newacronym{ABAC}{ABAC}{Attribute-Based Access Control}
\newacronym{TDE}{TDE}{Transparent Data Encryption}
\newacronym{AES}{AES}{Advanced Encryption Standard}
\newacronym{BAG}{BAG}{Directed Acyclic Graph}
\newacronym{SSL}{SSL}{Secure Sockets Layer}
\newacronym{TLS}{TLS}{Transport Layer Security}
\newacronym{IDPS}{IDPS}{Intrusion Detection and Prevention System}
\newacronym{IDS}{IDS}{Intrusion Detection System}
\newacronym{IPS}{IPS}{Intrusion Prevention System}
\newacronym{NIDS}{NIDS}{Network-based Intrusion Detection System}
\newacronym{HIDS}{HIDS}{Host-based Intrusion Detection System}
\newacronym{SIEM}{SIEM}{Security Information and Event Management}
\newacronym{AOL}{AOL}{America Online}
\newacronym{RAAC}{RAAC}{Risk-Adaptive Access Control}
\newacronym{DBaaS}{DBaaS}{Database as a Service}
\newacronym{AI}{AI}{Artificial Intelligence}