Confidentiality Preservation in Big Data Centres

IEEE/Volere Hybrid

Software Requirements Specification Template

Supervisor:
Jason Jaskolka

Team Members:
Aleksandar Savic - 100999110
Hasan Issa - 100921446
Ryan Zheng - 100996797
Calvin Soong - 100999332
Tashfiq Akhand - 101004428

Table of Contents

1 Introduction

1.1 Purpose

The purpose of this document is to present the following application, Confidentiality policy of big data centres (CPBDC). This document will explain the purpose, scope and features of the application. It is relevant to all stakeholders involved in the CPBDC app.

1.2 Scope

This software system to be produced is Confidentiality Policy of Big Data Csentres (CPBDC). CPBDC aims to provide database users with more advanced security features to prevent any sensitive data from being exposed to unauthorized personnel or intruders. The proposed system is a web interface used to provide access control to a database and manage the level of exposure to sensitive data depending on the set security clearance role of an authorized user. The system itself does not make insert or modify any data in the database itself, it is merely an interface for users to query data. The main objective of this system is to prevent unauthorized users from performing inference attacks on the targeted database.

1.3 Definitions, Acronyms, and Abbreviations

API	“Application Programming Interface”. A set of functions and procedures allowing access to the features or data of an operating system, application, or other service.
CPBDC	Confidentiality policy of big data centres
Inference attack	An Inference Attack is a data mining technique performed by analyzing data in order to ~~illegitimately~~ gain knowledge about a subject or database

1.4 References

- IEEE830/Volere Hybrid SRS Template Recommended Practice for Software Requirements Specifications. IEEE Computer Society, 1998.

1.5 Overview

The next few sections of the document gives an overview of the functionality and features of the application. The document covers the unofficial and technical requirements needed for the application but explains it in a technical and non technical manner suitable for both audiences.

2 Overall Description

2.1 Product Perspective

CPBDC is a web application available to users of the database and local users. The application must interact with a DBMS through the use of existing APIs in the backend. The CPBDC app shall be running if and only if the database and web server is active. Only users defined by the administrators will be able to get past the login page and query the database.

2.2 Product Functions

- Administrator creates user accounts through the application's settings page by giving the user a unique ID and password. The administrator then defines the role of the user from the given options; Basic-Security Level, High-Security Level, Admin
- Administrator sets the confidentiality policies of the database through the settings page of the application
- User logs into the application by filling in the userID and password fields available on the login page.
- Users with security roles Basic-Security Level, High-Security Level and Administrator search through the database on the GUI Search bar page after logging in successfully.
- CPBDC app keeps a log of all the queries made by the user and dynamically identifies any sensitive fields that can be linked to the data from the previous queries based on the confidentiality policies set by the admin
- User with Basic-Security Level queries for a field that has been identified by the CPBDC app as sensitive and is returned invalid data by the polyinstantiation algorithm.

2.3 User Characteristics

The users of the CPBDC app would need to have specific levels of expertise, experience, and education in order to utilize the CPBDC app. The users would need to be involved with the CPBDC app and would be considered to have access to the database for administrative use. The level would be minimum base entry level to use the CPBDC app. They would also need to be educated to use the system and know what to do with the information accordingly while maintaining customer confidentiality.

There are certain requirements later specified since there will be different levels of database breaches where requirements would need to be modified or introduced to prevent these attacks. Also, if there are new levels of administrations or security level users introduced, then new requirements would need to be modified such as many non functional requirements, especially any that deals with maintenance, constraints, observability and much more.

2.4 Constraints

The items that will limit the developer's options, which is considered the constraints, are the costs towards developing the project, the time it will take to complete this project on time for the final deliverable, and the complexity of the complete program that will allow full efficiency to block any inference attacks.

2.5 Assumptions and Dependencies

There are many factors that affect the requirements stated in the Software Requirements Specification which are: maintenance, security, costs, accessibility, policies, law changes, speed, reliability functionality, protection, time, sensitivity, new threats, and future technological developments that can increase the amount of algorithms for higher level inference attacks.

The factors that are not constraints but can affect changes to the requirements to the software requirements specifications are many things such as security, appearance, authorization, clientele growth, maintainability, performance, number of information demands in the database, number of types of information, database complexity, speed, and efficiency. These would be the transparent factors that would affect the SRS if changed which aren't design constraints.

2.6 Apportioning of Requirements

The requirements that may be delayed until future versions of the system would be many functional and non-functional requirements. The delayed non-functional requirements would be sign-in and log-in procedures dependable on the successfulness of protection against inference attack. Other requirements would include the look and feel requirement, appearance requirement, style requirement, ease of use requirement, accessibility requirements, speed and latency requirement, reliability and availability requirements, longevity requirement, performance requirement, release requirements, maintainability and support requirement, maintenance requirement, supportability requirements, privacy requirements, adaptability requirement, and capacity requirements. All these requirements would be delayed since these requirements won't be fully developed and finished until the end product is delivered due to many factors that can change these requirements to adapt so that the final product is optimal.

3 Functional Requirements

BE1. The user wants to sign-in through the log-in page.

VP1.1 Administrator

i. The CPBDC app shall allow Administrators to sign in using their username and password and gain Administrator access.

VP1.2 Highest Security Level User

i. The CPBDC app shall allow users of the Highest Security Level to sign in using their unique username and password provided to them by the Administrator and gain High Security Level access.

VP1.3 Basic Security Level User

i. The CPBDC app shall allow users of the Basic Security Level to sign in using their unique username and password provided to them by the Administrator and gain Basic Security Level access.

VP1.4 Unauthorized Security Level User

i. The CPBDC app shall not give access to unauthorized users.

BE2. The user wants to add a new database security policy.

VP1.1 Administrator

I. The CPBDC app shall allow the Administrator to add new database security policies to the existing list of database security policies.

VP1.2 Highest Security Level User

i. N/A

VP1.3 Basic Security Level User

i. N/A

VP1.4 Unauthorized Security Level User

i. N/A

BE3. The user wants to modify an existing database security policy.

VP1.1 Administrator

i. The CPBDC app shall verify the database security policy exists in the list of database security policies.

ii. The CPBDC app shall allow the Administrator to modify an existing database security policy from the list of database security policies.

VP1.2 Highest Security Level User

i. N/A

VP1.3 Basic Security Level User

i. N/A

VP1.4 Unauthorized Security Level User

i. N/A

BE4. The user wants to delete an existing database security policy.

VP1.1 Administrator

i. The CPBDC app shall verify the database security policy exists in the list of database security policies.

ii. The CPBDC app shall allow the Administrator to delete an existing database security policy from the list of database security policies.

VP1.2 Highest Security Level User

i. N/A

VP1.3 Basic Security Level User

i. N/A

VP1.4 Unauthorized Security Level User

i. N/A

BE5. The user wants to use the GUI search bar to perform a query.

VP1.1 Administrator

i. The CPBDC app shall allow the Administrator to query the database from the GUI search bar and return the results.

VP1.2 Highest Security Level User

i. The CPBDC app shall allow the user to query the database from the GUI search bar and return the results.

VP1.3 Basic Security Level User

i. The CPBDC app shall allow the user to query the database from the GUI search bar and return the results appropriate to their basic security level.

ii. The CPBDC app shall keep a log of all the users queries.

iii. The CPBDC app shall block queries that are considered illegal based on existing security policies.

VP1.4 Unauthorized Security Level User

i. The CPBDC app shall not allow the user to query the database from the GUI search bar.

BE6. The user wants to create a new user account.

VP1.1 Administrator

i. The CPBDC app shall allow the Administrator to create an account with a unique username and password for a user with High Security Level.

ii. The CPBDC app shall allow the Administrator to create an account with a unique username and password for a user with Basic Security Level.

VP1.2 Highest Security Level User

i. N/A

VP1.3 Basic Security Level User

i. N/A

VP1.4 Unauthorized Security Level User

i. N/A

4 Non-Functional Requirements

4.1 Look and Feel Requirements

4.1.1 Appearance Requirements

LF1. The CPBDC app shall style the website with color of blue.

4.1.2 Style Requirements

LF2. The CPBDC app shall ensure that 90% of users agree they feel they are comfort and able to trust the product

4.2 Usability and Humanity Requirements

4.2.1 Ease of Use Requirements

UH1. The CPBDC app shall be used by administrator after reading the system manual.

UH2. The CPBDC app shall be used by users with no training.

4.2.2 Personalization and Internationalization Requirements

N/A

4.2.3 Learning Requirements

UH3. The CPBDC app shall be used by administrators with basic knowledge of database structure.

UH4. The CPBDC app shall be used by users with basic technology knowledge.

4.2.4 Understandability and Politeness Requirements

UH5. The CPBDC app shall use symbols and words that are naturally understandable by the user community.

4.2.5 Accessibility Requirements

N/A

4.3 Performance Requirements

4.3.1 Speed and Latency Requirements

PR1. The CPBDC app shall modify the query response within 2 seconds of finding a policy violation.

4.3.2 Safety-Critical Requirements

N/A

4.3.3 Precision or Accuracy Requirements

PR2. The CPBDC app shall not affect the querying operation time by +25% compared to the average operation time of the original system.

4.3.4 Reliability and Availability Requirements

PR3. The CPBDC app shall be running once the database and web server is active.

PR4. The CPBDC app shall achieve 99% uptime when both database and web server is running.

4.3.5 Robustness or Fault-Tolerance Requirements

PR5. The CPBDC app shall not operate when the database is not accessible.

PR6. The CPBDC app shall block the users from performing further query operations when the user exceeds the query operation limit.

4.3.6 Capacity Requirements

PR7. This CPBDC app shall cater for 10 queries within 1 minute per user within the period specified by the project/product administrator.

4.3.7 Scalability or Extensibility Requirements

N/A

4.3.8 Longevity Requirements

PR8. The CPBDC app shall be expected to operate for the lifespan of the database.

4.4 Operational and Environmental Requirements

4.4.1 Expected Physical Environment

OE1. The CPBDC app shall run as a web application on the user's computer.

4.4.2 Requirements for Interfacing with Adjacent Systems

OE2. The CPBDC app shall work on Firefox and Google Chrome.

OE3. The CPBDC app shall use the application programming interface (API) provided by the supporting database program.

4.4.3 Productization Requirements

N/A

4.4.4 Release Requirements

N/A

4.5 Maintainability and Support Requirements

4.5.1 Maintenance Requirements

N/A

4.5.2 Supportability Requirements

N/A

4.5.3 Adaptability Requirements

MS1. The product shall run on Windows 10 and Linux.

4.6 Security Requirements

4.6.1 Access Requirements

SR1. The CPBDC app shall ensure that only administrators can access the database security policies page.

SR2. The CPBDC app shall allow any user to access the login page.

SR3. The CPBDC app shall allow the Highest Security Level User, Basic Security Level User, and Administrator to access the GUI search bar page.

SR4. The CPBDC app shall ensure that only administrators can access the account creation page.

4.6.2 Integrity Requirements

SR5. The CPBDC app shall not modify the stored database data when returning queried data to the user.

SR6. The CPBDC app shall not overwrite existing log files.

4.6.3 Privacy Requirements

SR7. The CPBDC app shall make the user aware of its information practices before collecting data from them.

SR8. The CPBDC app shall not disclose the user account information to anyone.

SR9. The CPBDC app shall not allow any users from accessing the log files.

SR10. The CPBDC app shall not disclose or leak any database information to any unauthorized user.

4.6.4 Audit Requirements

N/A

4.6.5 Immunity Requirements

N/A

4.7 Cultural and Political Requirements

4.7.1 Cultural Requirements

N/A

4.7.2 Political Requirements

N/A

Contributions

Calvin

- Section 4.3.8 to 4.7.2
- Help with functional requirements

Ryan

- Section 4.1 to 4.3.7

Aleksandar

- Introduction and Description

Hasan

- Functional Requirements

Tashfiq

- Introduction and Description

Calvin Soong	Calvin Soong
Ryan Zheng	RyanZheng
Aleksandar Savic	A.Savic
Hasan Issa	
Tashfiq Akhand	Tashfiq