09/24/2023

Design Implementation Proposal for Head in the Cloud IT's Client/Server Project

Jasonrochau\_CS457\_IP4

Jason Rochau

Contents

[Introduction 3](#_Toc146440930)

[Purpose of the System 3](#_Toc146440931)

[General Nature of the System and Software 3](#_Toc146440932)

[Identification of Project Client 4](#_Toc146440933)

[Objectives 5](#_Toc146440934)

[Functional Objectives 5](#_Toc146440935)

[Non-Functional Objectives 5](#_Toc146440936)

[Constraints 7](#_Toc146440937)

[Technical Constraints 7](#_Toc146440938)

[Budgetary Constraints 7](#_Toc146440939)

[Timeline Constraints 8](#_Toc146440940)

[Requirements 9](#_Toc146440941)

[Functional Requirements 9](#_Toc146440942)

[Non-Functional Requirements 9](#_Toc146440943)

[Design Description 11](#_Toc146440944)

[Architecture Overview 11](#_Toc146440945)

[Data Models 12](#_Toc146440946)

[Algorithms and Processes 12](#_Toc146440947)

[Pseudocode: 13](#_Toc146440948)

[Interface Designs 13](#_Toc146440949)

[Diagrams 15](#_Toc146440950)

[Architectural Diagram 15](#_Toc146440951)

[Sequence Diagrams 16](#_Toc146440952)

[Sequence 1: User Authentication 17](#_Toc146440953)

[Sequence 2: Accessing Secure Data 18](#_Toc146440954)

[Sequence 3: Logging User Activity 19](#_Toc146440955)

[Risks and Mitigations 20](#_Toc146440956)

[Maintenance and Use Phase Risks 20](#_Toc146440957)

[Mitigation Strategies 20](#_Toc146440958)

[Conclusion 21](#_Toc146440959)

[Summary of Design Implementation Proposal 21](#_Toc146440960)

[Future Recommendations 21](#_Toc146440961)

[Appendix A 22](#_Toc146440962)

[Appendix B 23](#_Toc146440963)

[Appendix C 24](#_Toc146440964)

[References 25](#_Toc146440965)

# Introduction

## Purpose of the System

The purpose of this new client/server system is to migrate our existing on-premises server infrastructure to a more scalable and efficient cloud-based solution. The aim is to transform the way Head in the Cloud IT manages its resources, handles data, and serves its clientele. The new system will capitalize on cloud computing's advantages, including increased scalability, reliability, and cost-efficiency, to ensure a robust, future-proof IT infrastructure.

## General Nature of the System and Software

We're envisioning a multi-tier architecture, ensuring seamless interaction between client applications and cloud-based server systems (Saraswathi, 2020). The system will offer real-time updates, robust backup mechanisms, and a secure operational environment. The software stack will be versatile and layered, including server-side applications for data processing, database management systems for data storage, and client-side user interfaces for interaction and control. Depending on the specific needs of various departments within Head in the Cloud IT, client software may range from lightweight applications for basic tasks to comprehensive dashboard interfaces for more complex operations. Security features are being designed to weave into the system's architecture, thereby ensuring data integrity and confidentiality at all levels.

By transitioning to this cloud-based system, Head in the Cloud IT aims to redefine its operational paradigms and set new benchmarks in operational excellence and client satisfaction (Microsoft 2023, February 28). The use of modern cloud technologies will provide a solid foundation for this transformation.

## Identification of Project Client

The client for this project is our own organization, Head in the Cloud IT. This migration project aims to serve both our internal operational needs and the demands of our external clientele, thereby enhancing overall business efficiency and client service quality (Data Recovery, 2022).

# Objectives

## Functional Objectives

The focal point of the functional objectives is the migration of existing on-premises data and applications to the cloud without any data loss or downtime. The system will also feature strong security measures, like multi-factor authentication (Microsoft. (2023, June 14) and robust data encryption, to safeguard sensitive information. A high level of interactivity will be maintained between client and server through real-time data syncing and efficient request-response mechanisms.

## Non-Functional Objectives

Transitioning to a cloud-based model sets the stage for unprecedented scalability. As Head in the Cloud IT grows, the system will accommodate an expanding user base without compromising performance. Reliability and uptime are also of the essence, with a disaster recovery plan, failover systems, and data backups to ensure seamless operations even under adverse conditions.

Security, always a paramount concern, will be bolstered through cutting-edge encryption methods and real-time intrusion detection systems. In addition, the cloud-based system will undergo regular audits to ensure compliance with data protection laws like GDPR (Violino, B. (2019, May 22), thus safeguarding both the company and its clients.

Performance optimization will be built into the system's DNA, aiming to reduce latency and accelerate data processing speeds. Usability is another cornerstone; the cloud-based client interface will be designed for ease of use, ensuring a smooth transition for all users.

When it comes to maintainability, the cloud-based architecture offers easier upgrades, better bug tracking, and simplified routine maintenance, thereby reducing long-term operational costs. For interoperability, we’ll ensure that our system communicates effortlessly with various types of client hardware and third-party services.

These objectives are designed to ensure that the new client/server cloud-based system aligns perfectly with the strategic goals and operational requirements of Head in the Cloud IT. The system will not only be scalable, secure, and reliable but also optimized for performance, usability, and cost-efficiency, setting the stage for a sustainable future.

# Constraints

## Technical Constraints

Transitioning to a cloud-based architecture often involves rethinking the existing infrastructure, which may not be fully compatible with the new setup. This could require retrofitting or reengineering the old systems, an effort that must be accurately assessed in advance (Cloud Academy Team, 2023).

Older applications were typically not designed with the cloud in mind, leading to integration challenges. The cost and effort to either update or replace these systems need to be clearly defined.

When dealing with data volumes that range from large databases to individual user settings, ensuring that all data transfers correctly without corruption is a massive task. Specialized tools and expert supervision are required for this. This is consistent with the guidelines on Zero Trust Architecture outlined by the Defense Information Systems Agency and the National Security Agency Zero Trust Engineering Team (DISA & NSA, 2022).

## Budgetary Constraints

Although one of the long-term advantages of cloud computing is cost efficiency, the initial setup can be expensive. Costs might include licensing, training, and the purchase of any additional hardware or software needed for the migration.

Customization needs can arise during the migration process that were not initially accounted for. This could include costs for third-party services to handle specific integration challenges (Cloud Academy Team, 2023).

After migration, the operational expenses might differ from the initial estimates. Subscription fees, storage costs, and other recurrent expenditures must be factored into the long-term budget planning.

## Timeline Constraints

Achieving a seamless migration often involves parallel running of old and new systems and a cutover phase, which can be both time-consuming and complex to manage (Gillis, Lelii, & Hefner, n.d.).

The time needed to train the staff and other stakeholders can be significant. These training periods must be strategically placed so they don't interfere with day-to-day operations.

Whether due to technical glitches, errors in data migration, or slower-than-expected user adoption, several factors could push back the project timeline (DISA & NSA, 2022).

# Requirements

## Functional Requirements

**Seamless Data Migration:** Migrating data from on-premises to the cloud must happen without any loss or corruption. This will require rigorous pre-testing and the employment of migration tools that validate data integrity post-transfer.

**Real-time Data Syncing:** The cloud system must automatically reflect any changes in data across all platforms and devices. This requires implementing robust data syncing algorithms and technologies to ensure immediate updates IBM. (n.d.).

**User Management:** Administrative personnel should have the capability to manage users with a set of role-based controls. This feature should enable quick onboarding and offboarding, as well as the ability to modify user privileges as required.

**Multi-factor Authentication:** A security protocol involving multiple steps for user authentication, such as passwords, OTPs, and biometrics, must be integrated into the system to deter unauthorized access (Microsoft 2023, June 14).

**Integration with Legacy Systems**: Given that some existing systems will continue to be used, the cloud solution must offer integration capabilities that don't compromise on performance or security.

## Non-Functional Requirements

**Scalability:** As the user base or data volume grows, the system should adapt without causing a slowdown in performance. This will likely involve load-balancing solutions and automated resource allocation.

**Reliability:** A guaranteed uptime of at least 99.9% means the system should have robust failover mechanisms. Any downtime should be minimized, and the system should be capable of rapid recovery.

**Security:** Ensuring the safety of data, it's vital to have end-to-end encryption both when data is in transit and when it's at rest. Moreover, conducting periodic security audits, such as vulnerability assessments and penetration tests, can help keep the system secure from potential threats (Defense Information Systems Agency & National Security Agency Zero Trust Engineering Team, 2022).

**Usability:** An intuitive user interface will facilitate quicker adoption among employees. The design should follow best practices in UX/UI, offering a clean, straightforward path to performing common tasks (Microsoft. 2023, February 28).

**Maintainability:** Updates and maintenance should be able to be performed without taking the system offline for extended periods. This may involve staged rollouts and the ability to roll back updates if they cause issues.

**Interoperability:** The system must be designed to integrate smoothly with different types of client hardware and other third-party services, whether it’s for data exchange, authentication, or other functionalities.

# Design Description

## Architecture Overview

Our cloud-based system is designed to seamlessly migrate existing on-premises data and applications to the cloud while maintaining data integrity and minimizing downtime. The architecture follows a microservices pattern to achieve modularity and scalability (Nandaniya, 2023).

Key components of our system include:

* Data Migration Service: Responsible for orchestrating the migration process. It interfaces with on-premises data sources and cloud storage.
* Real-time Sync Service: Ensures that data changes are propagated in real-time across all platforms and devices, enabling immediate updates for users.
* User Management Module: Provides administrators with role-based controls for managing user accounts, including onboarding, offboarding, and privilege modification.
* Security Layer: Incorporates multi-factor authentication and end-to-end data encryption to fortify the system against unauthorized access and data breaches.
* Legacy Integration Gateway: Allows our cloud solution to integrate seamlessly with existing on-premises systems while maintaining performance and security.

Our design choices align with the project's objectives. The microservices architecture enhances scalability, enabling us to accommodate an expanding user base without performance degradation (Nandaniya, 2023). It also supports our reliability and uptime goals by allowing individual services to be independently deployed and maintained.

## Data Models

Our data models consist of several entities, including "User," "DataRecord," and "AuditLog." The User entity stores user information such as username, email, and role. DataRecord represents individual data entries, while AuditLog records system activities (Anderson, Hall, Hartline, & Hobbs, 2010).

## Algorithms and Processes

Data Migration Process:

1. Users select the source of data from on-premises systems or external storage.
2. Data from the selected source is pre-tested for compatibility with the cloud environment. Any issues are flagged for resolution (Anderson, Hall, Hartline, & Hobbs, 2010).
3. The migration service orchestrates the transfer of data from the source to the cloud, using migration tools that validate data integrity post-transfer (Anderson, Hall, Hartline, & Hobbs, 2010).
4. After migration, the system validates the integrity of migrated data to ensure no loss or corruption occurred during the process (Anderson, Hall, Hartline, & Hobbs, 2010)..

### Pseudocode:

A screenshot of a computer program

Description automatically generated

## Interface Designs

Our user interface is designed with an efficient layout, catering to the preferences of our technology-savvy users. It mirrors the familiarity of a terminal or PowerShell environment, prioritizing functionality and ease of use. Please see the Appendices for the screenshots of the mentioned layouts.

**Command Dashboard:** Upon login, users are presented with a command dashboard, reminiscent of a terminal interface. This dashboard provides a concise summary of system activities and data migration progress, displayed in a structured text format.

**Data Migration Wizard:** Our data migration wizard is implemented as a series of command-line prompts. Users are guided through the migration process step by step, with each command providing clear instructions and progress indicators in a terminal-style interface.

By adopting this terminal-like interface, we aim to cater to the technical expertise of our user base while maintaining a user-friendly and efficient user experience.

# Diagrams

## Architectural Diagram

Purpose: The architectural diagram illustrates the high-level structure of our new client/server system. It shows how different components interact to achieve our migration objectives (Nandaniya, 2023). It's a visual representation of the system's architecture.

Components:

User Interface: This is the part of the system that users interact with directly.

Application: The application layer handles the processing of data and logic.

Database: This is where data is stored.

Interactions: The arrows or lines in the diagram represent interactions between these components. For example, user requests flow from the User Interface to the Application, which then interacts with the Database.

+----------------------+

| User Interface |

+---------------------+

|

+---------------------+

| Application |

+---------------------+

|

+--------------------+

| Database |

+--------------------+

## Sequence Diagrams

Sequence diagrams provide a time-ordered view of interactions within the system. It shows the order of messages and how control flows between different objects or components.

**Participants:**

* User: Represents the end-user interacting with the system.
* Application: Represents the software application.
* Database: Represents the database system.

**Interactions: In the sequence diagram:**

1. The User initiates a request (e.g., data retrieval) to the Application.
2. The Application processes the request and queries the Database.
3. The Database responds to the Application.
4. Finally, the Application presents the result to the User.

**Sequence Diagram:**

* User --> Application: Request
* Application --> Database: Query
* Database --> Application: Response
* Application --> User: Display Data

# Sequence 1: User Authentication

A diagram of a process

Description automatically generated

Description of Sequence 1:

* The ‘User’ sends a ‘requestAuthentication’ message to the Authentication Server.
* In response, the Authentication Server sends back a ‘requestCredentials’ message to the User, asking for the required authentication credentials.
* The User then sends the credentials, encapsulated in the ‘submitCredentials’ (username, password) message, to the Authentication Server.
* The Authentication Server internally processes these credentials using the ‘verifyCredentials’ action.
* Based on the verification, the Authentication Server sends an ‘authenticationResult’ (authenticated, token) message back to the User. This message will either confirm successful authentication (and possibly provide an authentication token) or inform the User of a failed authentication attempt.

# Sequence 2: Accessing Secure Data

A diagram of a computer

Description automatically generated

Description of Sequence 2:

* The User sends a ‘requestSecureData’ message with a token to the Data Server.
* The Data Server internally checks the validity of the token with the ‘verifyTokenValidity’ process.
* 2a. If the token is valid, the Data Server sends a ‘tokenValid’ message to the User.
* 2b. If the token is invalid, the Data Server sends a ‘tokenInvalid’ message to the User and proceeds to send a ‘logInvalidTokenEvent’ (with the User's details) to the Log Server.
* The Log Server receives the ‘logInvalidTokenEvent’ and stores the information.
* If the token was deemed valid in step 2a, the User then sends a ‘specifyDataRequest’ (dataID) message to the Data Server.
* The Data Server processes the data request and sends back the data to the User using the ‘provideDataResponse’ (data) message.

# Sequence 3: Logging User Activity

A diagram of a computer

Description automatically generated

Description of Sequence 3:

* User -> Logging Server: ‘initiateLogAction’ (actionType)
* Depending on the context, ‘actionType’ could be authenticationResult or ‘tokenValidation’.
* Logging Server: ‘determineLogCategory’ (actionType)
* This is an internal process to determine where or how to log the event based on the action type.
* Logging Server -> User: ‘requestAdditionalInfo’
* This could be an optional step, where the Logging Server might require more details about the action for thorough logging.
* User -> Logging Server: ‘provideAdditionalInfo’ (details)
* Here, the user provides additional information (like a timestamp, IP address, or other relevant details).
* Logging Server: ‘storeLogDetails’ (actionType, details)
* An internal action where the Logging Server ensures the log details are stored correctly.
* If integrating with the Authentication Server or Data Server:
* Authentication Server/Data Server -> Logging Server: ‘forwardLogDetails’ (details)
* The server sends details of the interaction to be logged. This step captures logging interactions originating from system components rather than direct user actions.
* Logging Server: ‘processForwardedDetails’ (details)

# Risks and Mitigations

## Maintenance and Use Phase Risks

## Mitigation Strategies

# Conclusion

## Summary of Design Implementation Proposal

## Future Recommendations

# Appendix A

A screenshot of a computer

Description automatically generated

# Appendix B

A screenshot of a computer

Description automatically generated

# Appendix C

A screenshot of a computer program

Description automatically generated

# References

Microsoft. (2023, June 14). Passwordless authentication options for Azure Active Directory. Retrieved from <https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless#microsoft-authenticator>

Violino, B. (2019, May 22). How to conduct a proper GDPR audit: 4 key steps. CSO Online. Retrieved from <https://www.csoonline.com/article/573755/how-to-conduct-a-proper-gdpr-audit-4-key-steps.html>

Saraswathi, R. (2020, January 6). Four Architecture Choices for Application Development in the Digital Age. IBM Blog. <https://www.ibm.com/blog/four-architecture-choices-for-application-development/>

Microsoft. (2023, February 28). Cloud center of excellence (CCoE) functions. Learn Microsoft. <https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/organize/cloud-center-of-excellence>

Data Recovery. (2022, June 6). Defining Key Stakeholders in a Data Migration Project. <https://datarecovery.com/rd/defining-key-stakeholders-in-data-migration/>

Cloud Academy Team. (2023, July 21). What is Cloud Migration? Strategy, Processes, Benefits & Risks. Cloud Academy. <https://cloudacademy.com/blog/cloud-migration-benefits-risks/>

Defense Information Systems Agency & National Security Agency Zero Trust Engineering Team. (2022, July). Zero Trust Reference Architecture Version 2.0. Department of Defense. <https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf>

Gillis, A. S., Lelii, S., & Hefner, K. (n.d.). Data migration. TechTarget. <https://www.techtarget.com/searchstorage/definition/data-migration>

IBM. (n.d.). Cloud migration planning with IBM Turbonomic. Retrieved [Insert date you accessed this webpage], from <https://www.ibm.com/products/turbonomic/cloud-migration-planning?utm_content=SRCWW&p1=Search&p4=43700076774885473&p5=p&gclid=Cj0KCQjw0vWnBhC6ARIsAJpJM6fYbBacQEIvPpalgmB_JNTHj__zjRwclyo1bcyJsILtWWXcHxkmgpkaAo1NEALw_wcB&gclsrc=aw.ds>

Nandaniya, H. (2023, August 9). Software Architecture Patterns: Driving Scalability and Performance. Maruti Tech. Retrieved from <https://marutitech.com/software-architecture-patterns/>

Anderson, E., Hall, J., Hartline, J. D., & Hobbs, M. (February 2010). Algorithms for Data Migration. Algorithmica, 57(2), 349-380. DOI: 10.1007/s00453-008-9214-y.