**Design document**

**Overview of the project**

**Goal**

The object of the project is to develop a bank account management system for the largest bank in Japan. It enables operators to check the following information.

* Customers’ names, addresses and phone numbers
* The list of account numbers
* Account activities

**Project Structure**

The project consists of following roles. Table1 describes each role.

|  |  |
| --- | --- |
| **Role & Team** | **Description** |
| Project owner | Contributor of the project and a finance stakeholder. |
| Project manager | Be responsible for the progress and the quality of the project. |
| Operation Team | The team members are the users of the customer management system. |
| Onshore Development Team | Be responsible for development activities. |
| Offshore Development Team | Be responsible for the implementation.  Conduct building and unit testing based on instructions from the onshore development team. |

Table 1 : Roles in the project

**Architecture**

Figure1 shows the architecture of the system.

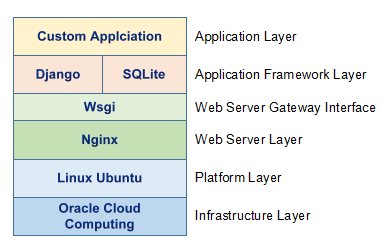


Figure 1 : Technology stack in Bank Account Management System

**Development method**

The following five stages are the standard in the SDLC(Software Development Life Cycle) as described by ISO(International Organisation for Standardization)/IEC(International Electrotechnical Commission)/IEEE(Institute of Electrical and Electronics Engineers) 15288:2015 (Solms & Mamewick, 2018).

**System concept development stage**

In this stage, the business requirement is identified and the architecture and the grand design of a system is considered. In addition, non-functional requirements, such as security or performance, is listed.

**Design and development stage**

The system is designed at a basic and detail level. Developers implement the system with the design specification. After building, testing is conducted at several phase, unit testing, integrated testing and operational testing. Unit testing is called the black box test, which verifies the process of the program. On the other hand, testers confirm if the function follow the requirement in the integrated testing, so-called the white box test. The operational test is conducted in conditions equal to the production environment.

**Production stage**

The system is released and operated in the production environment.

**Development stage in system operations**

The system is modified continuously if there is the need of additional requirement or a defect is detected.

**Retirement stage**

Eventually, the system is abolished due to the EOL, the end of life. It is replaced by an enhanced version of system in some cases.

**SDLC in the project**

This project follows the waterfall model. These five stages described by ISO/IEC/IEEE will be applied to the project, being integrated into 3 phases as below. Also, the way of treating sensitive data at each phase is defined as the security strategy.

Table 2 shows deliverable and sensitive data in each phase.

|  |  |  |
| --- | --- | --- |
| **Phase** | **Deliverable** | **Sensitive Data** |
| Requirement and conceptualization phase | Business requirement list  Functional system requirement list  Non-Functional system requirement list | Information related to business demand and system concept. |
| Implementation phase | Design document  Source code  Infrastructure  Test definition and evidence | System design  Information related to implementation  Test data |
| Operation phase | Production | Personal information of end users |

Table 2 : Deliverable and sensitive data at each phase

**Data sensitivity**

This section describes the data sensitivity by each phase in the system development.

**Requirement and conceptualization phase**

Confidential information related to the core business of system end users is treated between engineers and users to define the requirement at this phase. Also, it is necessary that system concept can be accessed from only project members and stakeholders since it might cause the security risk if the information is leaked out of the organisation.

**Implementation phase**

Personal data such as name or address is treated in the program of the system. Encrypting these kind of data must be taken into consideration for reducing the security risk. Not only data but also other deliverable of this phase should be protected. It can be said that design documents or source codes, even development environments, are confidential information since it describes the specification of the system, which might help malicious attackers penetrate the protection if it can be seen.

**Operation phase**

One of the most sensitive data is treated at this phase. Operators would be able to check personal information that the system holds if no protection is applied. Personal data managed in the system must not be accessed from any members in the project including operators.

**Data model**

Figure 2 illustrates data model in the system. Customer information should be treated as confidential in particular. To protect sensitive data, data encryption strategy, which is described in the next section, is applied to the project.

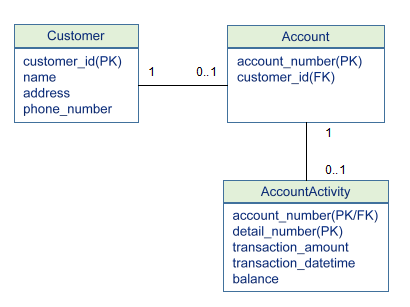


Figure 2 : Entity Relation Diagram on the Bank Account Management System

**Data encryption strategy**

Three ways in encrypting sensitive data will be applied to the project depending on the way of using data or the software development life cycle.

**Encrypting data in a working environment**

In the requirement and conceptualization phase, sensitive information, such as business requirements or the system concept, is communicated between stakeholders and the development team. In addition, the members of the project access various resources during the development. For example, design documents are uploaded in a file server or developers access a testing environment at a test phase. These activities are basically conducted in a remote environment due to the pandemic. It is necessary to encrypt data. VPN is one of the best solutions to protect data privacy on Public Wi-Fi or the internet(Maile & Rob, 2022). Anyone who connect the internet to access the project’s resources must connect VPN.

**Encrypting data in a system flow**

The Bank Account Management system will be implemented as a web-based application and deployed on Oracle cloud service. Users access the web application with a browser via the internet. Data in the transaction is encrypted with SSL/TLS as Figure X shows.

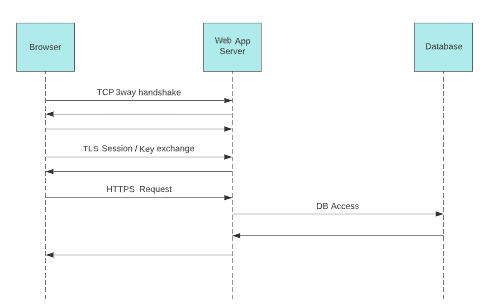


Figure 1 : Sequence diagram between browser and web application

**DB encryption**

Sensitive information such as a user’s name or account number is stored in the database of the Bank Account Management system. These data is encrypted when inserting into the database with Advanced Encryption Standard(AES) algorithm, which is a popular choice for cryptography using a 1280bit cipher(Hans et al, 2004). Any developers or operators cannot refer encrypted data as a result of a SQL transaction. The cryptography which is a Python library using Advanced Encryption Standard(AES) algorithm will be adopted to DB encryption. When registering sensitive data into the database, it is encrypted with a common key. Only allowed operator can check the decrypted data through the management screen on the web application.

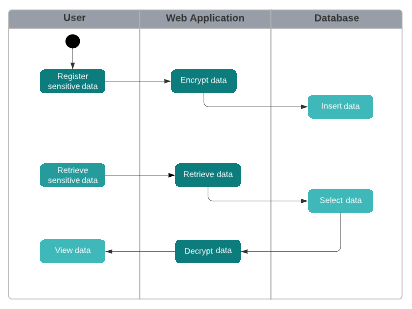
****

Figure 2 : Activity diagram of DB encryption

By combining these three ways of encryption, the security in treating sensitive information will be ensured in every stage of the development.

**References:**

von Solms, S. & Mamewick, A. (2018) ‘Towards Educational Guidelines for the Security Systems Engineer’, in: L. Drevin and M. Theocharidou. (eds) *Information Security Education – Towards a Cybersecure Society.* Switzerland: Springer Nature Switzerland AG. 57-68. Software Engineering. DOI: <https://doi.org/10.1007/978-3-319-99734-6_5>

Maile, M. & Rob, W. (2022) *Forbes What Is A VPN Used For? 9 VPN Uses In 2022*. Available from: <https://www.forbes.com/advisor/business/software/why-use-a-vpn/> [Accessed 25 October 2022].

Hans, D., Lars, K. & Matt, R. (2004) *Advanced Encryption Standard – AES.* Berlin: Springer. Available from : <https://link-springer-com.uniessexlib.idm.oclc.org/content/pdf/10.1007/b137765.pdf> [Accessed 25 October 2022].