



Deusto

Facultad de Ingeniería
Ingeniaritza Fakultatea

DEUSZUM

Curso 2019/2020
Ing. Informática
Programación III
Terres Escudero, Erik B.
Zarate Jayo, Gorka
Zugazaga Alonso, Aritz
Acha Aristegui, Amaia
Gago López, Leire
San Millan Langa, Lander

Contents

1	INTRODUCCIÓN	2
2	FORMA DE TRABAJO	2
2.1	Division del trabajo	2
2.2	Error Handling	3
2.3	Preparacion del temario	3
3	PLANIFICACION	3
3.1	Entrega de la Idea	3
3.2	Fase 1	3
3.3	Fase 2	3
3.4	Informe de Desarrollo	4
3.5	Entrega Final	4
4	Implementacion de Server	4
5	Implementacion de Desktop	4
6	Implementacion de Android	5
7	IA	5
7.1	Analisis de los movimientos	5
7.2	5
8	DATA ANALYSIS	5
9	SEGURIDAD	5
9.1	Encriptacion de los codigos de los sockets	5
9.2	Trackero de los pagos	6
10	DATABASES	6
11	DIVISION DEL TRABAJO	6
12	CONCLUSIÓN	6
13	LIBRERIAS	6
14	LIBROS	6
14.1	Java	6
14.2	Android	6
14.3	Server	6
14.4	IA	6
14.5	Data Analsys	6
14.6	Seguridad	6

1 INTRODUCCIÓN

DeusZum es una aplicación de gestión de dinero online para la gestión de pagos, proyectos o costes grupales. DeusZum ofrece un sistema seguro de transferencias de forma que el cliente no tenga que preocuparse de que este pasando con su dinero en todo momento.

DeusZum estará implementado en un servidor y dará servicio a los usuarios a través de un programa en Windows y una aplicación en Android. Cada una de ellas implementada para conectarse a un servidor central, en el cual se almacenarán los datos, procesarán las peticiones y se garantizará la seguridad de la información.

El servicio que ofrece DeusZum está dividido en diferentes sectores, algunos puramente económicos y otros de análisis de la conducta o de las transacciones. El servidor ejecutara todas las peticiones de los usuarios y devolverá la información que se haya solicitado. Toda la información mientras se enviá se encontrara encriptada para la seguridad del usuario.

2 FORMA DE TRABAJO

2.1 Division del trabajo

Para la realización del proyecto, hemos optado por la división del trabajo en grupos con temáticas separadas. Los dos grupos tendrán que trabajar en una categoría central entre IA y Seguridad, y, trabajar en una parte de la implementación y algoritmia. Las categorías y subcategorías serian las siguientes:

1. Implementacion

- Implementación del Server
- Implementación del cliente Windows
- Implementación del cliente Android

2. IA

- Data Analysis
- Clustering

3. Seguridad

- Databases
- Encriptación
- Conexiones seguras

Cada uno de los grupos tendra un conjunto de tareas las cuales se diviran en *tareas principales* y *tareas secundarias*. Las tareas principales son aquellas a las que se les daran prioridad y buscamos que esten terminadas a la hora de terminar el proyecto. Las tareas secundarias son aquellas que no tienen tanta importancia y que se empezaran una vez se vayan acabando las tareas principales.

A su vez, las tareas estaran numeradas segun importancia, dificultad y tiempo de trabajo con el fin de poder establecer un orden de prioridad para que su progreso haga que el proceso de construccion del proyecto sea relativamente optimo y de forma que su estructura no se vea afectada por software anterior.

Por ultimo, hay un sector no especializado que trata los temas de algoritmia sobre como manejar la forma de minimizar el total de pagos que hay realizar en forma de peticiones. Este algoritmo estara pensado en forma de algoritmo greedy al tener complejidad $O(n)$, pero en caso de que consigamos un algoritmo que no dependa de combinatorial algorithms o complejidades exponenciales para encontrar el minimo numero de pagos, tal vez aniadamos la opcion. Por ahora no sabemos como de rentable resultaria este algoritmo, ni tampoco sabemos ninguna upperbound del numero de movmientos que sea inferior a n aproximadamente. Esto se mostrara en la bibliografia final o en la documentacion sobre el software.

El apartado de algoritmia se dividira segun convenga, aunque se mostrara dentro de la documentacion quien ha hecho que tareas y como ha resuelto los problemas.

2.2 Error Handling

Para evitar errores que afecten al codigo a nivel global, hemos optado por utilizar github y hacer que cada miembro del grupo tenga su propia cuenta. Los errores, comentarios y todo se enviarian a traves de github excepto la informacion mas urgente que se enviaria a traves de un grupo de whatsapp o telegram/discord en si defecto.

2.3 Preparacion del temario

Para la preparacion del temario que queremos trabajar en el trabajo hemos optado por utilizar un conjunto de libros que consideramos basicos para las personas que no tienen mucha experiencia y utiles/importantes para las personas que tengan un cierto control en ciertos aspectos. Esta lista de libros se encontrara en el apendice de este documento categorizada.

3 PLANIFICACION

3.1 Entrega de la Idea

- Reparto de tareas
- Desarrollo de las ideas basicas
- Preparacion de la bibliografia
-
- Crear el Servidor Generico
- Crear la aplicacion Desktop Funcional sin muy grafico
- Crear una aplicacion android funcional sin muy grafico
- planificacion per

3.2 Fase 1

fin noviembre

-

3.3 Fase 2

diciembre

3.4 Informe de Desarrollo

dic

3.5 Entrega Final

enero

4 Implementacion de Server

La implementacion del Server sera una implementacion sencilla de un serversocket con la capacidad de extension de funcionalidades. Incluso tal vez no necesitar modificar el codigo del server per se para la ampliacion de su funcionalidad.

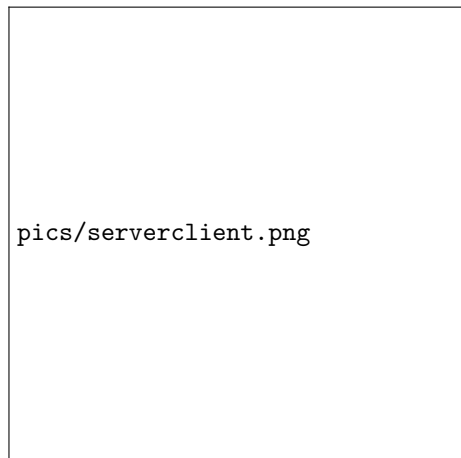
Los sockets del servidor tendrian una estructura tal que:

1. Conseguir acceder a la cuenta de un usuario.
2. Comprobar que el usurio existe y verificar que la contrasenia es correcta.
3. Verificar que no ha habido un abnormal comportation.
4. Devolverle un hash que representa su sesion actual en el servidor.
5. En caso de que quiera guardar la sesion, devolverle otro hash que represente su sesion y guardar en el servidor que esa sera su sesion activa.
6. Este hash debera ser modificado cada x tiempo.

Los sockets de funcionalidad estaran compuestos por un comando, luego el servidor devolvera un codigo hash de sesion activa y a continuacion el cliente enviara toda la informacion con el hash como cabecera.

Estos hash se enviarian a traves de la web mediante un sistema de criptografia implementado por nuestro equipo y, por otro lado, plantearemos un metodo mas seguro para mostrar la capacidad de implementar metodologias mas serias o profesionales.

El ServerHandler no debera ser modificado cada vez que se aniaa un nuevo codigo de funcionalidad en el server. Para manejar esto, hemos pensado en hacer que el serverhandler funcione mediante un arbol Autobalanceado (AVL o Black Red por ejemplo) que se genera al inicio de la sesion del servidor y que despues, en cada peticion, el serverhandler simplemente busque cual de las hojas es y luego ejecute otra funcon que se encuentre en algun otro lado del codigo. Este arbol se generaria mediante una base de datos que contenga el conjunto de funcionalidades y la funcion asociada.



pics/serverclient.png

Figure 1: Modelo del Servicio.

5 Implementacion de Desktop

La aplicacion de escritorio sera puramente una aplicacion que sirva como cliente para el servidor y que sirva para enviar sockets y representar de forma visual todos los comandos que se podran enviar al servidor.

La implementacion del software de Desktop se basará en tres valores principales: comodidad, sencillez y completitud. Buscamos crear una aplicacion que satisfaga todas las necesidades de los usuarios, manteniendo a su vez la sencillez que supone un software minimalista y con el apoyo de IA.

6 Implementacion de Android

7 IA

El apartado de IA de DeusZum se basara puramente en el analisis de la conducta de los usuarios dentro de la aplicacion con el unico fin de garantizar su seguridad.

Las tareas que queremos hacer en el apartado de IA son las siguientes:

- Analisis de los movimientos economicos de los clientes.
- Analisis del tracking de las direcciones de las transacciones de los clientes.
- Analisis conductual del cliente dentro de la aplicacion.
- Prediccion de los clientes dentro de la aplicacion.

7.1 Analisis de los movimientos

7.2

8 DATA ANALYSIS

- Clustering
- Analisis de mercado

9 SEGURIDAD

- Encriptacion de todas las conexiones.
- Capacidad de trackeo del historial de conexiones

9.1 Encriptacion de los codigos de los sockets

A la hora de enviar la informacion al servidor, nos parece importante que no pueda existir un sniffer que robe la informacion de nuestros clientes como puede ser el hash de la sesion o como puede ser el usuario y contrasenia. Para evitar esto, necesitaremos que nuestra informacion se envia encriptada con algun tipo de codigo decriptable asi como con un conjunto de informacion basura para evitar que a base de fuerza bruta en codigos cortos se pueda adivinar lo que ciertos codigos encriptados hagan.

Para solucionar este problema, el grupo de seguridad se encargara de estudiar el funcionamiento de ciertos tipos de encriptacion inyectiva o biyectiva y analizaran algunos metodos para aumentar la seguridad del algoritmo de encriptacion que deberan crear.

Sea A el alfabeto, $f : A^n \rightarrow A^w$ la funcion de encriptacion con $n \in \mathbb{N}$. Las condiciones que establecemos ahora sobre el algoritmo de encriptacion seran las siguientes:

1. f sera inyectiva.

2. $\mathbb{P}(|f(x)| = |x|) \rightarrow 0$ cuando $n \rightarrow \infty$. siendo $x \in A^n$.
3. f no pueda ser roto por analisis de frecuencia.

9.2 Trackero de los pagos

10 DATABASES

Las tareas dentro de este subapartado se dividiran en 2, la de creacion y organizacion inicial de las bases de datos y la segunda, la de optimizacion de las bases de datos y su respectivo ajuste de seguridad con el fin de evitar ciertos tipos de ataque como las SQL Inyection o las code execution.

- Optimizacion de las bases de datos

11 DIVISION DEL TRABAJO

Grupo 1	Grupo 2
Implementacion Desktop	Implementacion Server
Implementacion App	IA
Seguridad	Data Mining
Database 2	Database 1

Grupo 1	Grupo 2
Aritz	Erik
Leire	Lander
Gorka	Amaia

12 CONCLUSIÓN

13 LIBRERIAS

1. **DeepLearning4J**: Usaremos esta libreria para la implementacion de redes neuronales y ejecutarla. A su vez, esta libreria permite el uso de tensores para la representacion de datos, lo cual nos puede ser util.

14 LIBROS

14.1 Java

14.2 Android

14.3 Server

14.4 IA

14.5 Data Analysis

14.6 Seguridad

- 1.

References

- [1] Autor1, Autor2. (2002) *Nombre del articulo*, Lugar de publicación