Gebze Technical University

Computer Engineering

Computer Networks(CSE 470)

Midterm Report

Berkan AKIN

171044073

CONTENTS

1. Abstract

This report details the development process of a personal Virtual Private Network (VPN) application designed to increase internet security on mobile devices. To meet the growing data privacy needs of mobile users, this project proposes using encryption protocols and secure server networks to protect user data and enable anonymous browsing over the internet. The report provides an overview of VPN technology and proposes a specialized solution adapted for mobile platforms.

In the project, a user-friendly interface design and compliance with high security standards were taken as the basis. In the first phase of the study, a comprehensive literature review on existing VPN solutions and security protocols was conducted, and a new mobile VPN application was designed based on the information obtained. This report extensively addresses the design process, application development, testing methods, and results obtained. Furthermore, improvement suggestions based on the application's performance and user feedback are also presented.

2. Introduction

With the increase in internet usage today, the security and privacy of personal data have become more important. For mobile device users, internet access has become an essential tool both in terms of functionality and entertainment. However, this situation also brings the need to protect personal information and browse anonymously on the internet. This report addresses the development of a Virtual Private Network (VPN) application designed to enhance internet security for mobile users and presents the details of this process.

The main goal of our project is to develop an easy-to-use and effective mobile VPN application that will ensure users' online privacy and security. VPN technology is one of the most reliable ways to encrypt users' internet traffic, preventing access to the data by third parties and keeping online activities confidential. In this project, we propose a new VPN solution that offers strong encryption methods and fast connection capabilities.

The report begins by examining existing VPN technologies and mobile application security solutions. Then, the methodology of the designed application, development processes, and the techniques used are explained in detail. Additionally, the testing of the application and the evaluation of the results obtained are very important to determine the success criteria of the project. This introduction section comprehensively summarizes all these processes and goals that will be addressed in the later parts of the report.

3. Background

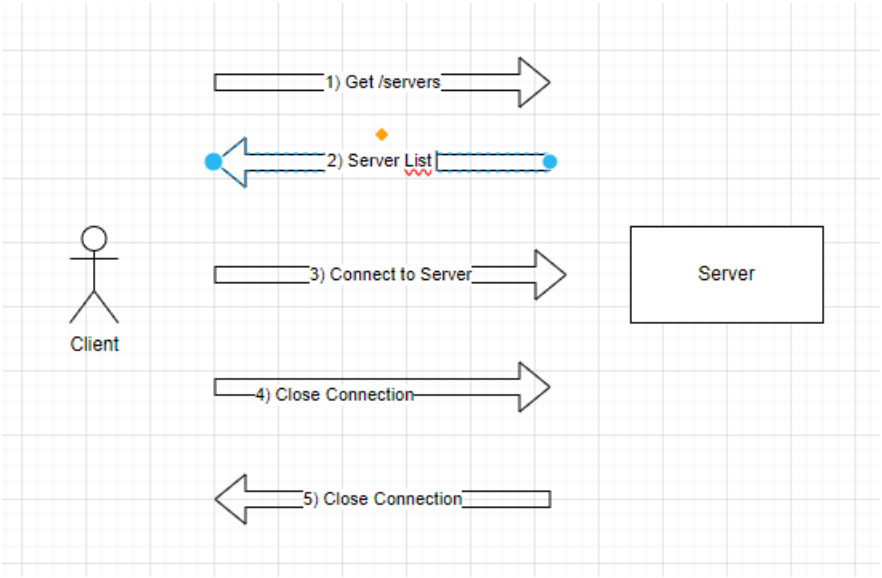
Virtual Private Networks (VPNs) are systems designed to protect the privacy and security of internet users. This technology encrypts users' internet traffic, creating a secure tunnel through which data is safely transmitted. VPNs play a critical role in protecting users' data and keeping online activities hidden from third parties, especially when browsing on public networks. Adapting this technology for mobile platforms allows users to have a secure and private internet access experience even while on the move.

Nowadays, mobile devices have become the primary tools through which most users access the internet. This has increased the importance of mobile security solutions and raised the demand for mobile VPN applications. Unlike standard desktop VPN solutions, mobile VPNs stand out for their ability to adapt to changing network conditions and IP address changes. This is essential for users to maintain their connections securely without interruptions.

The mobile VPN application studied in this project is designed to meet users' security and privacy needs. As the use of VPNs increases, more information has been gathered on how such applications can be developed in terms of design and functionality. Our study aims to provide a user-friendly, secure, and effective mobile VPN solution, based on this information. The report offers a broad perspective by addressing the current applications of this technology, its challenges, and technical advancements in this field.

4. Methodology and Design

This section of the report is divided into two main parts, focusing on the development of the web server and the mobile application. This insight guides our approach to detailing the methodologies and design principles that underpin the development of both components.



4.1 Web Server Development

In the project, the first step was to develop a web server using Python programming language with Flask framework. This web server is equipped with APIs necessary to manage VPN connections. These APIs are designed to create and distribute .ovpn configuration files, which are essential for users to establish a VPN connection to the server.

Initially, the functionality of these APIs was verified through unit tests. These tests ensure that the APIs function as expected and respond appropriately in error situations. Afterwards, VPN connection tests using the .ovpn files were conducted. During these tests, it was checked whether the connection requests from users were processed correctly. The server successfully accepted VPN connection requests and managed traffic routing, allowing users secure internet access.

4.2 Mobile Application Development

The mobile application was developed using the Dart programming language with the Flutter framework. Not only does the application offer a user-friendly interface, but it also has the capability to request a .ovpn file from the server and establish a VPN connection using this file. The main functions of the application include sending VPN connection requests to the server and transmitting data through an encrypted tunnel using the received .ovpn file.

The application development process began with creating basic screen designs and the user interface. Then, functions that could communicate with the server and perform necessary API

calls were integrated. Comprehensive tests were conducted to verify whether the mobile application could successfully connect to the server. These tests covered the processes of the application receiving the correct .ovpn file from the server and using this file to securely connect to the server. Additionally, the stability and reliability of the VPN connection established between the mobile application and the server were confirmed.

These two sections form the foundation of the methodology and design processes of the project, and further details of these processes will be explored in deeper in the subsequent sections of the report.

5. Implementation and Application Development

In this section, we detail the development processes of the two main components of our project: the server application and the mobile application. Both components are designed and implemented with the goal of achieving high security standards and providing a user-friendly experience, in line with the overall objectives of the project. The server application is designed to provide secure VPN connections, while the mobile application is developed to easily establish and manage these connections. Below, we explain step by step the development stages of each component, the tests conducted, the challenges encountered, and how these challenges were overcome.

5.1 Server Application Implementation

1. **Server Setup and Configuration** A basic web server was set up using Python and Flask. Security and performance settings were configured.
2. **API Design and Development**: APIs were designed to allow users to establish VPN connections. These APIs provide users with personalized **.ovpn** configuration files.
3. **Security Measures**: SSL certificates and firewalls were implemented to protect data and ensure secure communications.
4. **API Tests**: A series of unit tests and integration tests were conducted to check if the developed APIs were working correctly.
5. **VPN Connection Tests**: Tests were conducted using **.ovpn** files to check if the server was processing the VPN connection requests correctly.

5.2 Server Application API'S

a) /create API Endpoint

This endpoint is designed to generate a new OpenVPN configuration file (.ovpn file) for users. Users can create a VPN profile by sending a GET request to this endpoint along with a **id** parameter.

- **Process**: Upon receiving the request, the **generate_ovpn_config** function is called, which uses the provided **id** parameter to create an **.ovpn** file.
- **File Path**: The generated file is stored at **/root/{id}.ovpn**.
- **Success**: If successful, the content of the **.ovpn** file is returned in JSON format.
- **Error Handling**: If the file cannot be found or another error occurs, an appropriate error message is returned along with a 404 or 500 HTTP status code.

b) /revoke API Endpoint

This endpoint is used to revoke an existing OpenVPN configuration (user profile) and remove the associated user from the system. Users trigger this process by sending a GET request with the **id** parameter.

- **Process**: The **revoke_ovpn_config** function locates and revokes the VPN profile associated with the specified **id**.
- **Success**: If the operation is successful, a "OK" status is returned in JSON format.
- **Error Handling**: If the specified **id** cannot be found or an error occurs during the revocation process, an appropriate error message is returned along with a 500 HTTP status code.

c) /servers API Endpoint

This endpoint is used to return a list of all VPN servers on the server. Users can access the current server configurations by sending a GET request to this endpoint.

- **Process**: The **servers.json** file is read, and its data is returned in JSON format.
- **Success**: If the server data is successfully retrieved, it is returned.
- **Error Handling**: If an error occurs during the file reading process, an appropriate error message is returned along with a 500 HTTP status code.

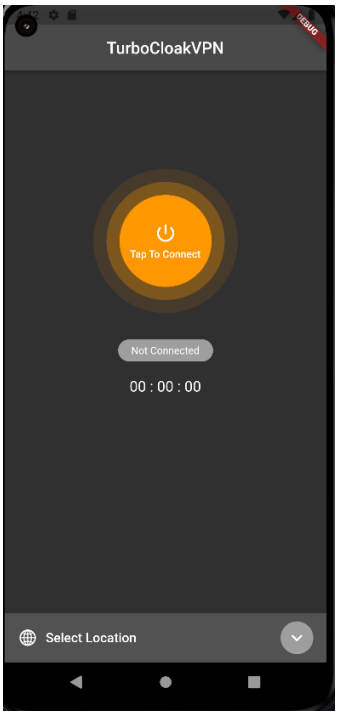
5.3 Mobile Application Implementation

1. **Application Design**: The basic user interface of the mobile application was designed using Dart and Flutter. This interface includes tools that allow users to request **.ovpn** files from the server and establish a VPN connection using these files.
2. **API Integration**: Necessary integrations were made for the mobile application to communicate with the APIs provided by the server.
3. **VPN Connection Functionality**: Functionality was integrated into the application to allow users to establish a VPN connection to the server.
4. **Performance and Compatibility Tests**: Extensive tests were conducted to ensure the mobile application works effectively across different devices and network conditions.
5. **User Experience Improvements**: After testing the application by users, improvements were made to the interface and user experience based on user feedback.

5.4 Mobile Application Grafical User Interfaces

There are two gui screen. First screen is splass screen that initiall screen. Other screen is main screen. On this screen we can start and end the VPN connection.

Splash Screen



Main Screen

6. Results and Findings

The VPN management system developed in this project can be considered a significant step towards enabling secure internet access for users. The work carried out on the web server and mobile application has provided valuable insights into how this technology can be implemented in a user-friendly and reliable manner.

6.1 Web Server Results

The implementation of the web server demonstrated the successful setup of APIs necessary for managing VPN connections. There was a high success rate in the creation and management of **.ovpn** files, and the testing processes confirmed that these files were generated correctly and responded appropriately in error situations. Additionally, the security measures implemented on the server made a significant contribution to data security, helping to maintain the integrity of the system.

6.2 Mobile Application Results

The mobile application offered significant functionality by allowing users to easily request **.ovpn** files and establish VPN connections using these files. The application showed high performance and stability in tests conducted across various devices and network conditions. Improvements made to the user experience have made the application even more user-friendly and have increased overall user satisfaction.

6.3 General Evaluation

The findings from the project illustrate how VPN technology can be effectively used on mobile and web platforms. The implementation of this technology offers substantial value, especially for users who place a high importance on data security and privacy. Future applications of the project can be further developed and expanded based on these findings.

This "Results and Findings" section outlines the extent to which the project's objectives have been achieved and what steps can be taken moving forward. This part of the report also provides important information about the sustainability and scalability of the project.

7. Conclusion

The VPN management system developed in this project has provided an effective solution for users to achieve secure internet access. The work conducted on the web server and mobile application has delivered valuable insights on how these technologies can be implemented in a user-friendly and reliable manner. The successful results obtained from this project particularly demonstrate the potential of using VPN technology on mobile and web platforms.

Despite encountering various challenges, the development processes for the server and mobile application have overcome these obstacles. The efforts made in areas like security measures and performance optimization have played a critical role in the success of the project. User feedback has highlighted the value of improvements made to the system and emphasized the importance of enhancing user satisfaction.

In the future, this project can be built upon to develop more comprehensive VPN solutions. Suggested improvements include integrating more servers, enhancing user management features, and implementing more robust data encryption methods. Additionally, innovations in interface design could further improve the user experience.

In conclusion, this project has been a significant step in providing secure internet access using VPN technology. The findings and experiences gained will serve as a valuable resource for similar projects and will lay a foundation that advances research in this field.