

Rozdział 1

Analiza problemu

1.1 Systemy pisania testów w czasie rzeczywistym

Na rynku istnieją już aplikacje częściowo odpowiadające tematowi pracy inżynierskiej. Ich funkcjonalność spełnia pewne aspekty jakimi są: wybór odpowiedzi, przesyłanie odpowiedzi do serwera oraz pobieranie treści z serwera na aplikację. Najlepszym przykładem jest aplikacja nazywająca się Quizowanie¹. Aplikacja ta pozwala na pobieranie i wyświetlenie pytań z serwera, wyświetlenie możliwych odpowiedzi jako przycisków dla użytkownika oraz wysłanie odpowiedzi do serwera i zweryfikowanie ich. Jej kod źródłowy jest jednak zamknięty co sprawia, że aplikacja ta jest nieprzydatna przy tworzeniu systemu będącego tematem tej pracy.

Inne aplikacje, które można wymienić to English Grammar Test² lub też sameQuizy³. Ich wartość ogranicza się jednak do rozwiązań dotyczących wyglądu interfejsu aplikacji. Nie ma możliwości w legalny sposób uzyskać kodu źródłowego lub opisów rozwiązań w tych aplikacjach z racji ich komercyjnego zastosowania.

1.2 środowisko tworzenia aplikacji na Android

Środowiska, w jakich można tworzyć aplikacje mobilne to Android Studio⁴ oraz Qt⁵. Oba środowiska oferują duże wsparcie ze strony społeczności programistycznej oraz szeroki zestaw narzędzi. Oba pozwalają na tworzenie interfejsu użytkownika w XML oraz udostępniają klasy obiektów przydatne do wizualizowania i przetwarzania danych. Android Studio jest jednak najbardziej popularny oraz posiada najszerszą gamę narzędzi. Pozwala na dołączanie bibliotek z repozytoriów Git lub też bibliotek za pomocą wbudowanego narzędzia Maven⁶, bieżące sprawdzanie kompatybilności użytych bibliotek z wersjami systemu Android, na które aplikacja powstaje oraz tworzenie maszyn wirtualnych do testowania napisanych aplikacji bez użycia telefonu.

1.3 Komunikacja internetowa

1.3.1 Protokoły

Przy tworzeniu systemu gdzie występuje komunikacja serwer-klient przez Internet jest wiele możliwych protokołów, które można użyć. Są to np. TCP, UDP, POP, SMTP, HTTP czy FTP. Wybór protokołu wpływa znacząco na sposób komunikacji pomiędzy klientem a serwerem.

1.3.2 Serwer HTTP

Pierwszym rodzajem serwera do obsługi zapytań aplikacji mobilnych jaki można wykorzystać to serwer HTTP połączony z FastCGI. Najpopularniejsze⁷ aplikacje, które współpracują z FastCGI to między

¹<https://play.google.com/store/apps/details?id=se.feomedia.quizkampen.pl.lite>

²<https://play.google.com/store/apps/details?id=english.grammar.test.app>

³<https://play.google.com/store/apps/details?id=pl.filing.samequizey>

⁴<https://developer.android.com/studio/index.html>

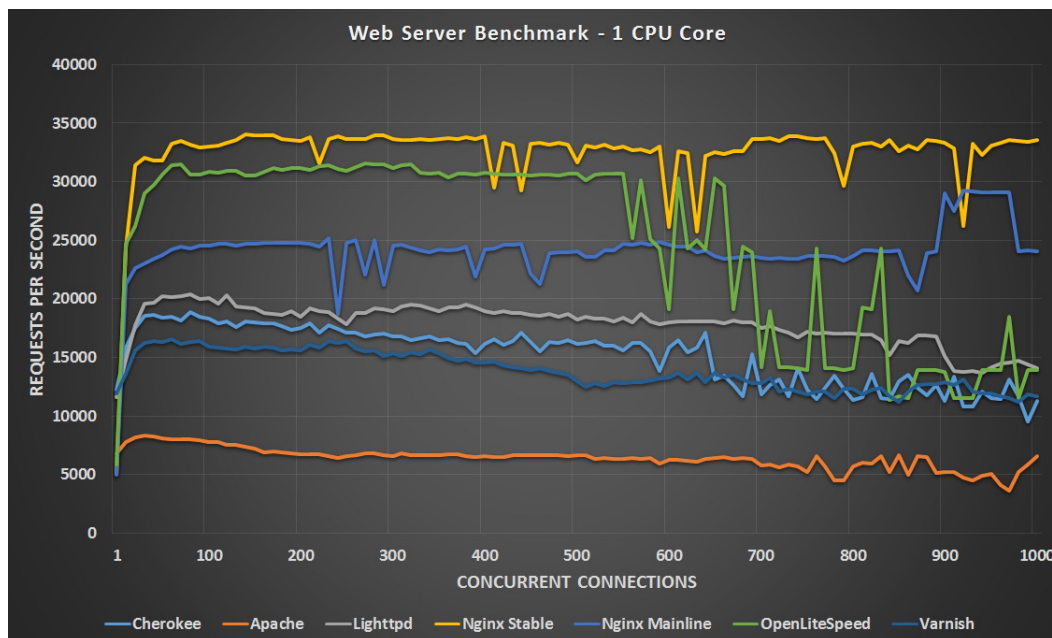
⁵<https://www.qt.io/>

⁶<https://maven.apache.org/>

⁷https://w3techs.com/technologies/overview/web_server/all

innymi: Apache⁸, nginx⁹, Microsoft-IIS¹⁰, OpenLiteSpeed¹¹. Każdy z serwerów obsługuje FastCGI pozwalające na napisanie programu przyjmującego i przetwarzającego przychodzące zapytania. Proces napisany z pomocą FastCGI łączy się z serwerem FastCGI, do którego przekierowywane są zapytania przyjmowane przez serwer HTTP. Ten interfejs jest kompatybilny z wieloma językami programowania, np. C++, Python, Java. W ten sposób można stworzyć mało rozbudowane ale szybkie programy przetwarzające zapytania sieciowe.

Wymienione serwery jednak różnią się między sobą wydajnością obsługi zapytań. Na podstawie Linux Web Server Performance Benchmark¹² z 2016 można stwierdzić, że nginx oferuje największą szybkość obsługi zapytań.



Rysunek 1.1: Ilość obsługiwanych zapytań przy danej ilości otwartych połączeń. Źródło: Linux Web Server Performance Benchmark

1.3.3 Serwer aplikacji

Drugim rodzajem serwera jaki można wykorzystać to serwer aplikacji działający na protokole HTTP. Najpopularniejsze¹³ aplikacje to: Tomcat¹⁴, WildFly¹⁵ (dawny JBoss) oraz Jetty¹⁶. Za ich pomocą można napisać aplikację np. w języku Java lub C++, która później służy do obsługi zapytań. W ten sposób można stworzyć zaawansowane serwery sieciowe odpowiadające potrzebom implementowanego systemu.

Porównanie wyżej wymienionych serwerów aplikacji można znaleźć w artykule Lightweight Java servers and developer view on the App Server¹⁷.

⁸<https://httpd.apache.org/>

⁹<https://www.nginx.com/>

¹⁰<https://www.iis.net/>

¹¹<http://open.litespeedtech.com/mediawiki/>

¹²<https://www.rootusers.com/linux-web-server-performance-benchmark-2016-results/>

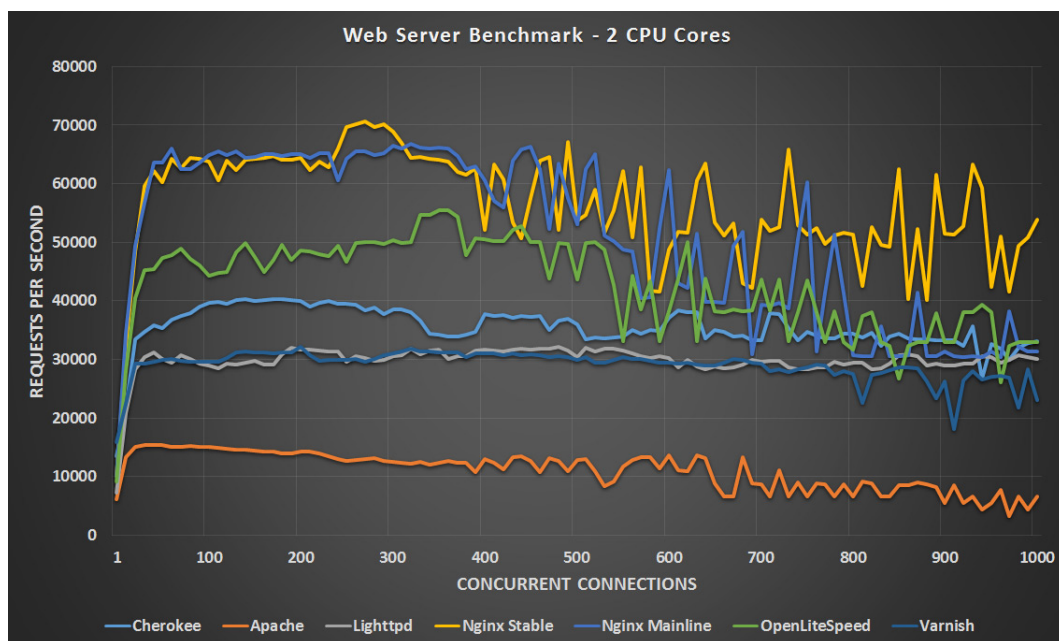
¹³<https://plumbr.eu/uncategorized/most-popular-java-ee-servers-2016-edition>

¹⁴<https://tomcat.apache.org/>

¹⁵<http://wildfly.org/>

¹⁶<https://eclipse.org/jetty/>

¹⁷<https://advantage.ibm.com/2015/09/22/lightweight-java-servers-and-developer-view-on-the-app-server-update/>



Rysunek 1.2: Ilość obsługiwanych zapytań przy danej ilości otwartych połączeń. Źródło: Linux Web Server Performance Benchmark

	IBM WAS Liberty 8.5.5.7	IBM WAS full 8.5.5.6	Tomcat 8.0.26	TomEE+ 1.7.2 ⁴	Jetty 9.3.2	Glass Fish 4.1	Web Logic 12.1.3 ³	WildFly 9.0.1	JBoss EAP 6.4
Server stop+start ⁵	4.9 sec	34.1 sec	5.5 sec	11.2 sec	3.1 sec	9.4 sec		10.2 sec	9.2 sec
App redeploy ⁵	1.2 sec	6.1 sec	2.3 sec	2.5 sec	2.2 sec	2.5 sec		1.2 sec	1.2 sec
RAM ⁵	59 MB	175 MB	125 MB	236 MB	102 MB	376 MB		269 MB	430 MB
Download size ¹	11 to 94 MB	3 GB	10 MB	48 MB	10 MB	103 MB		127 MB	158 MB
Size installed ¹	15-123 MB	2.6 GB	17 MB	52 MB	12 MB	214 MB		159 MB	174 MB
Size per instance	0.5 MB	40 MB	0.4 MB	0.4 MB	0.4 MB	96 MB		1.5 MB	1.2 MB
Dev. Install ⁶	5 sec	30 min	2 sec	3 sec	1 sec	5 sec		5 sec	5 sec
# of config files	1+	100+	8+	12+	20+	14+		16+	16+
Dynamic config ²	99%	80%	20%	20%	20%	20%	80%	60%	60%
IDE	Eclipse, IntelliJ IDEA, NetBeans are supported with some minor differences								
Configuration Editor	Eclipse UI	Browser UI	None	None	None	Browser UI	Browser UI	Browser UI	Browser UI
DevOps	Maven, Jenkins, Ant, Chef and other DevOps tools are supported with some minor differences								
Java EE	Java EE 7	Java EE 6+	JSP/Servlet	Java EE 6 Web Prof.	JSP/Servlet	Java EE 7	Java EE 6	Java EE 7	Java EE 6
Free Dev. License	IBM	IBM	Apache 2.0	Apache 2.0	EPL 1.0	CDDL 1.1	Oracle	LGPL 2.1	LGPL 2.1
Free Dev. Support	IBM ⁷	IBM ⁷	Self	Self	Self	Self	\$	Self	Red Hat ⁸

Rysunek 1.3: Porównanie popularnych serwerów aplikacji. Źródło: Lightweight Java servers and developer view on the App

Rozdział 2

Specyfikacja

2.1 Początkowa specyfikacja

2.1.1 Aplikacja mobilna

Podstawowe wymagania jakie aplikacja ma spełniać są następujące:

- zgodność z systemami Android w wersji 2.2 - 7.0
- komunikacja z serwerem przez HTTP
- szyfrowanie odpowiedzi z testu i przechowywanie ich w pamięci wewnętrznej telefonu
- bezpieczny sposób przechowywania odpowiedzi na telefonie
- ochrona oszukiwaniem poprzez nieuprawnione wyjście i powrót do wykonywanego testu
- logiczny i przyjazny dla użytkownika interfejs

2.1.2 Aplikacja serwerowa

Wymagania aplikacji serwerowej są następujące:

- komunikacja przez HTTP
- duża wydajność przetwarzania zapytań sieciowych
- przetwarzanie i zapisywanie zapytań przychodzących z aplikacji mobilnych
- zachowanie możliwie wysokiej prostoty aplikacji serwerowej

2.1.3 Dodatkowe programy

- deszyfrator plików z odpowiedziami tworzonych przez aplikację mobilną

2.2 Dodatki i zmiany

2.2.1 Aplikacja mobilna

W trakcie implementacji i testowania systemu były wprowadzane zmiany w specyfikacji aplikacji mobilnej. Następujące zmiany to:

- komunikacja z serwerem poprzez HTTPS
- minimalna wersja obsługiwanego systemu Android zmieniona na 4.0
- lista z pytaniami zmieniona ze statycznej na dynamiczną

Dodatki to:

- odrzucanie połączeń przychodzących do użytkownika w trakcie testu

- długotrwałe przechowywanie parametrów konfiguracji takich jak imię, nazwisko, itd., w aplikacji
- wyświetlanie informacji dla użytkownika o procesach zachodzących w aplikacji
- nadanie aplikacji cyfrowego podpisu
- obfuskacja skompilowanego kodu źródłowego aplikacji
- testowanie osiągalności serwera HTTP
- weryfikacja aplikacji za pomocą SafetyNet
- automatyczna konfiguracja parametrów testu na podstawie danych otrzymanych z serwera

2.2.2 Aplikacja serwerowa

Dodatki w specyfikacji aplikacji serwerowej wyglądają następująco:

- walidacja aplikacji mobilnych poprzez SafetyNet
- przesyłanie konfiguracji testu do aplikacji mobilnej

2.2.3 Dodatkowe programy

- konfigurator tworzący pliki konfiguracyjne dla aplikacji mobilnych

Rozdział 3

Implementacja

Biorąc pod uwagę przeprowadzoną analizę problemu zdecydowano, że system do rozwiązywania testów musi być napisany od podstaw. Nie znaleziono przykładów otwartych systemów na tyle użytecznych, żeby można było użyć ich przy tworzeniu systemu. Systemy takie jak Quizowanie mają zamknięty kod i można się nimi sugerować jedynie w kwestii tworzenia interfejsu użytkownika.

3.1 Elementy aplikacji

3.1.1 Widoki aplikacji

Wygląd aplikacji stanowi ważny element aplikacji. W początkowych fazach projektu rozmieszczenie elementów na ekranie telefonu komórkowego jak też ich estetyka wielokrotnie była zmieniana. Potrzebne było wypracowanie przejrzystego oraz przyjaznego dla studenta interfejsu aplikacji. W trakcie tworzenia aplikacji zauważono, że istotnym elementem jest zachowanie kompatybilności z różnymi wersjami systemu Android realizując jednolite i przewidywalne zachowanie się interfejsu. Na przykład nie można było zastosować kolorowania przycisków korzystając z metody `setColorFilter` obecnej we wszystkich wersjach systemu od Android 4.0 do Android 7.0. Efekt wywołania tej metody w systemach Android 4.0 do 4.4 był inny od efektu uzyskiwanego w systemach Android 5.0 i wyższych. Powodowało to brak kompatybilności pomiędzy tymi wersjami.

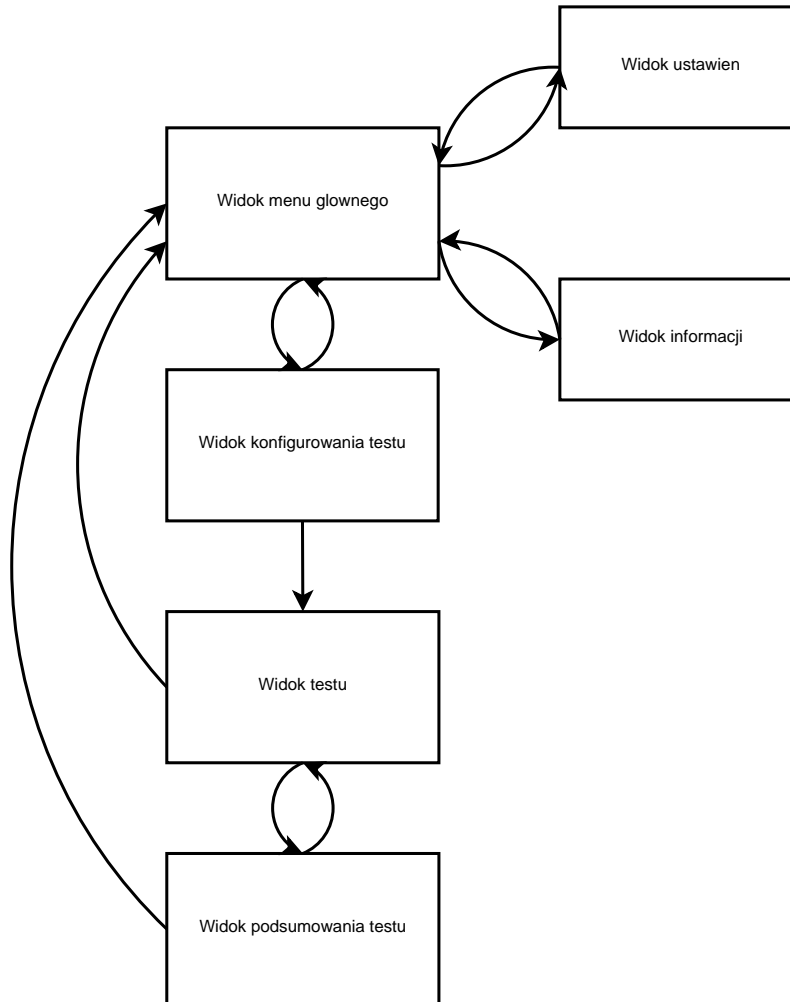
Widoki jakie zostały zaimplementowane w aplikacji to:

- Widok główny
Za jego pomocą użytkownik może wprowadzić swoje miejsce i rząd w jakim się znajduje, wektor wag służący do wyliczenia grupy na teście oraz kod testu. Na tym widoku można uruchomić również skaner kodów QR do automatycznego pobrania wektora wag i kodu testu oraz wyliczenia grupy na teście. Trzy dolne przyciski służą do wyjścia z aplikacji, ręcznego wyliczenia numeru grupy oraz przejścia do testu. Z tego widoku można również otworzyć menu, z którego można dostać się do widoku ustawień i widoku informacji.
- Widok ustawień
Tutaj użytkownik może wprowadzić i zapisać w aplikacji swoje dane takie jak: imię, nazwisko, numer indeksu oraz nazwa przedmiotu. Opcjonalnie może wprowadzić inny adres serwera, na który aplikacja będzie przysyłać odpowiedzi użytkownika.
- Widok informacji
W tym widoku użytkownik może się dowiedzieć z jakiej wersji aplikacji korzysta.
- Widok konfigurowania testu
Tutaj użytkownik jest informowany o przebiegu konfiguracji testu. Aplikacja sprawdza osiągalność serwera, do którego wysyła odpowiedzi oraz pobiera plik konfiguracyjny zawierający takie dane jak: minimalna i maksymalna wersja aplikacji dopuszczona do testu oraz klucz do szyfrowania danych w plikach testu przechowywanych na telefonie użytkownika. Następnie porównuje dopuszczalną wersję aplikacji z aktualną wersją oraz zapisuje klucz szyfrowania.
- Widok testu
W tym miejscu wyświetlany jest zestaw zakładek, po którym użytkownik może się poruszać i

wchodzić w interakcje. UI użytkownika pozwala na przesuwanie ekranu w celu wyświetlenia innych pytań. Początkowo wyświetlana jest tylko jedna zakładka. Na zakładce pytania znajduje się: nr grupy użytkownika, nr pytania, przyciski: tak, nie, nie wiem do wysłania odpowiedzi, przyciski do dodawania pytań oraz do podsumowania testu. Na dole zakładki wyświetlany jest unikalny identyfikator sesji wygenerowany dla aktualnej sesji testowej otwartej na telefonie. Dodanie pytania wymusza przejście do następnego pytania.

- Widok podsumowania

Tutaj wyświetlana jest ilość poprawnie przesłanych odpowiedzi "tak", "nie" oraz "nie wiem" do serwera, oraz ilość odpowiedzi zapisanych w pliku testowym. W razie różnicy w odpowiedziach przesłanych do serwera, a zapisanych w pliku aplikacja wyświetla odpowiednie ostrzeżenie sugerujące użytkownikowi powrót do testu i ponowne przesłanie odpowiedzi. Na ekranie podsumowania wyświetlany jest przycisk pozwalający powrót do testu oraz przycisk kończący test powodujący powrót do menu głównego aplikacji.



Rysunek 3.1: Zależności pomiędzy widokami informujące o tym jak użytkownik może się po nich poruszać

3.1.2 Interaktywne elementy na widokach

Rozwijane listy zostały utworzone w widoku ustawień i widoku głównym. W widoku ustawień po kliknięciu na pole do edycji nazwy testu otwiera się okienko z przesuwalną listą, z której można wybrać nazwę kursu. W widoku głównym taka sama wizualnie lista wyświetla propozycje ID testu wygenerowane na podstawie nazwy kursu.

Zmiennokształtne przyciski służą do sygnalizowania asynchronicznych operacji zachodzących w trakcie konfiguracji i weryfikacji aplikacji. Za podstawę służy Android Circular Progress Button¹, który został umieszczony na widoku ustawień. Przycisk ten w aplikacji zmienia swój kolor oraz wygląd sygnalizując:

- beczyność - niebieski pusty przycisk
- przetwarzanie operacji - wirujące kółko
- powodzenie przetwarzania operacji - zielony przycisk z checkmark
- niepowodzenie przetwarzania operacji - czerwony przycisk

Sygnalizowanie beczyność zostało początkowo użyte dla jednej nieaktywnej funkcji, którą była walidacja aplikacji. Zielony kolor sygnalizuje powodzenie testowego połączenia z serwerem, poprawne pobranie pliku konfiguracyjnego oraz walidację klucza szyfrowania i dopuszczalny zakres wersji aplikacji. Czerwony kolor sygnalizuje niepowodzenie wyżej wymienionych operacji. Wirujące kółko trwa tak długo jak te asynchronicznie wykonywane operacje nie zakończą swojego działania.

tutaj będą obrazki pokazujące jak zmienia się przycisk

Przyciski zmieniające kolor umieszczone są na kartach z odpowiedziami w aplikacji. Sygnalizują swoimi kolorami stan przetwarzania odpowiedzi użytkownika. Biały przycisk informuje o braku wybranej do tej pory odpowiedzi. Szary przycisk sygnalizuje poprawnie zapisaną odpowiedź do pliku testowego. Niebieski przycisk sygnalizuje poprawnie wysłaną odpowiedź na serwer. Jeżeli operacja zapisywania do pliku się nie powiedzie to przycisk pozostaje biały. Jeżeli operacja wysyłania do serwera się nie powiedzie to przycisk pozostaje szary. Użytkownik wtedy wie, że jego aktualna odpowiedź przechowywana jest jedynie lokalnie.

tutaj będą obrazki pokazujące przykładowo wybraną odpowiedź

3.1.3 Powiadomienia

Istotnym elementem aplikacji okazały się być powiadomienia pozwalające na zrozumienie użytkownikowi zdarzeń występujących w aplikacji. Dzięki wypracowaniu zestawu chmurzek oraz monitów użytkownik jest informowany o powodzeniu w edycji ustawień aplikacji, błędach występujących przy konfigurowaniu testu oraz różnych innych zdarzeniach takich jak utrata połączenia z serwerem czy też brak poprawnego testu, na który użytkownik chciał wysłać odpowiedzi.

3.1.4 Komunikacja internetowa

Z powodu tego, że w niezabezpieczonej sieci WiFi Politechniki Wrocławskiej odblokowane są jedynie porty służące do obsługi poczty i protokołu HTTP to do komunikacji internetowej wykorzystano protokół HTTP. Odpowiedzi są wysyłane na zasadzie pobierania nagłówka pliku konfiguracyjnego XML z odpowiedziami umieszczonymi w query string. Kod otrzymany po wykonaniu zapytania jest następnie interpretowany, a jego wartość decyduje o powiadomieniu użytkownika o poprawnym lub niepoprawnym wysłaniu odpowiedzi do serwera.

3.1.5 Szyfrowanie plików

Początkowo pliki były szyfrowane algorytmem DES z kluczem przechowywanym w aplikacji. Było to jednak rozwiązanie niebezpieczne, ponieważ klucz szyfrowania można było uzyskać po zdekompilowaniu aplikacji. Pierwszym ulepszeniem zaimplementowanym w aplikacji było zastosowanie metody "security by obscurity", gdzie klucz szyfrowania zmieniał się w trakcie działania programu. W ten sposób sprawa jego uzyskania została utrudniona. Następnie w aplikacji zaimplementowano pobieranie dokumentu XML z ustawieniami testu. W tym dokumencie znajdował się klucz szyfrowania wykorzystywany później w algorytmie DES. W dalszym etapie wykorzystano szyfrowanie algorytmem RSA, którym zastąpiono algorytm DES, a klucz w dokumencie XML został zamieniony na 4096 bitowy klucz publiczny algorytmu RSA.

¹<https://github.com/flavioarfaria/circular-progress-button>

3.1.6 Skaner QR

W aplikacji wykorzystano również skaner kodów QR. Wykorzystano do tego bibliotekę zxing² (Zebra Crossing). Pozwala ona nie tylko na skanowanie kodów QR ale również kodów kreskowych, kodów Aztec i innych. Skaner skanuje kod QR wyświetlany na ekranie przez rzutnik automatycznie zapisując w aplikacji kodu testu i wektor wag. Po operacji skanowania wymusza wyliczenie nowego numeru grupy. Ułatwia to pracę z aplikacją potencjalnemu użytkownikowi oraz pozwala na zmniejszenie prawdopodobieństwa popełnienia błędu przez użytkownika przy wyliczaniu grupy na teście.

3.1.7 Baza danych

Do długotrwałego przechowywania danych w aplikacji wykorzystano bazę danych MySQL. W tym celu stworzono klasę imitującą bazę danych MySQL oraz klasę imitującą interfejs dostępowy do tej klasy. Interfejs został następnie wykorzystany do zapisywania informacji zawartych w widoku ustawień. Służy dodatkowo jako narzędzie do rozprowadzania informacji po innych widokach aplikacji. Baza danych służy do przechowywania danych użytkownika takich jak: imię, nazwisko, numer indeksu oraz nazwa kursu na którym wykonywany jest test.

3.1.8 Odrzucanie połączeń w trakcie testu

W trakcie testowania aplikacji na grupie studentów pojawiła się potrzeba automatycznego odrzucania przychodzących połączeń telefonicznych. W tym celu stworzono klasę na bazie wbudowanej BroadcastReceiver, która to odrzuca wszystkie przychodzące połączenia jeśli użytkownik jest w trakcie pisania testu. Do odrzucania połączeń wykorzystano kod z portalu Stack Overflow³.

3.2 Programy dodatkowe

3.2.1 Generator konfiguracji

Do tworzenia plików konfiguracyjnych napisany został konfigurator w języku Java. Pozwala na uruchomienie się tylko w linii poleceń. W parametrach wywołania tego programu podaje się kod testu, minimalną wersję aplikacji oraz maksymalną wersję aplikacji dopuszczoną do testu. Program generuje dwa pliki. Pierwszy jest dokumentem XML zawierającym klucz publiczny RSA plus dodatkowe parametry testu przeznaczone dla aplikacji Android. Drugi plik zawiera klucz prywatny RSA służący do rozszyfrowywania odpowiedzi zaszyfrowanych wcześniej kluczem publicznym.

3.2.2 Deszyfrator

Deszyfrator również został napisany w języku Java i umożliwia uruchomienie jedynie w linii poleceń. Początkowa wersja deszyfratora korzystała z algorytmu DES, najpierw ze stałym kluczem zapisanym w aplikacji, potem z kluczem odczytywanym z pliku. Ostatecznie stosuje algorytm RSA, a klucz prywatny pobiera z pliku.

3.2.3 Parser logów

Do przetwarzania logów serwera Apache wykorzystano skrypt napisany w języku AWK. Skanuje on logi serwera Apache w poszukiwaniu zarejestrowanych zapytań przysłanych z aplikacji mobilnych i umożliwia zapisanie ich w formacie użytecznym dla zarządcy systemu. Skrypt został napisany przez dr Witolda Paluszyńskiego.

²<https://github.com/zxing/zxing>

³<https://stackoverflow.com/questions/7347871/how-to-reject-a-call-programmatically-in-android>

Rozdział 4

Testowanie systemu

System został pomyślnie wykorzystany na Wydziale Mechanicznym, Automatyce i Robotyce na kursie Systemy Czasu Rzeczywistego i Sieci Komputerowe. Średnio z aplikacji korzystało około 90 osób na każdym z siedmiu wykonanych testów. Ponadto aplikacja została wykorzystana na testach na Wydziale Elektroniki, Automatyce i Robotyce na kursie SCR Systemy Operacyjne.