

Politechnika Poznańska
Wydział Elektryczny
Instytut Automatyki i Inżynierii Informatycznej



Maciej Marciniak
Damian Filipowicz

Projekt i wykonanie systemu kontroli ruchu i zarządzania
dostępem do pomieszczeń

Praca dyplomowa inżynierska

promotor:
dr inż. Ewa Idzikowska

Poznań, 2018

Karta Pracy Damian Filipowicz



**Temat
pracy dyplomowej inżynierskiej**

Uczelnia:	Politechnika Poznańska	Profil kształcenia:	ogólnoakademicki
Wydział:	Elektryczny	Forma studiów:	stacjonarne
Kierunek:	Informatyka	Poziom studiów:	I stopnia
Specjalność:	Bezpieczeństwo systemów informatycznych		

Zobowiązuję/zobowiązujemy się samodzielnie wykonać pracę w zakresie wyspecyfikowanym niżej. Wszystkie elementy (m.in. rysunki, tabele, cytaty, programy komputerowe, urządzenia itp.), które zostaną wykorzystane w pracy, a nie będą mojego/naszego autorstwa, będą w odpowiedni sposób zaznaczone i będzie podane źródło ich pochodzenia.

	Imię i nazwisko	Nr albumu	Data i podpis
Student:	Maciej MARCINIAK	121996	30.10.2017 <i>Maciniak</i>
Student:	Damian FILIPOWICZ	122002	

Tytuł pracy:	Projekt oraz implementacja systemu kontroli ruchu i zarządzania dostępem do pomieszczeń (projekt zespołowy)
Wersja angielska tytułu:	<i>Design and implementation of movement control and access to spaces management system (team project)</i>
Dane wyjściowe:	1. Jeff Forcier, Paul Bissex, Wesley Chun, Python i Django. Programowanie aplikacji webowych, Helion 2009 2. Adrian Kaehler, Gary Bradski, OpenCV 3. Komputerowe rozpoznawanie obrazu w C++ przy użyciu biblioteki OpenCV, Helion 2017

Zakres pracy:	1. Projekt i implementacja serwera systemu (bazy danych, systemu kontroli uprawnień). 2. Realizacja wewnętrznego PKI służącego do podpisywania cyfrowo kluczy dostępowych dla sterownika zamka fizycznego od strony urzędów certyfikujących systemu. 3. Oprogramowanie sterownika zamka fizycznego. 4. Realizacja oprogramowania do zliczania osób wchodzących i wychodzących z pomieszczenia.
Termin oddania pracy:	31 stycznia 2018
Promotor:	dr inż. Ewa Idzikowska
Jednostka organizacyjna promotora:	Instytut Automatyki, Robotyki i Inżynierii Informatycznej

**Z-ca DYREKTORA INSTYTUTU
Automatyki, Robotyki
i Inżynierii Informatycznej**
Jerzy Bartoszek
dr Jerzy Bartoszek

podpis dyrektora/sterownika jednostki organizacyjnej promotora

**PRODZIEKAN
Wydziału Elektrycznego
Politechniki Poznańskiej**

dr hab. inż. Tomasz Tomczewski
dr hab. inż. Tomczewski

Poznań, 30 października 2017
miejscowość, data

Poznan University of Technology
Faculty of Electrical Engineering
Institute of Control and Information Engineering

Design and implementation of movement
control and access to spaces managment
system

by
Maciej Marciniak
Damian Filipowicz

Abstract

Streszczenie

Spis treści

1	Wstęp	8
1.1	Cel i zakres pracy	8
1.2	Plan pracy	8
1.3	Metodyka pracy grupowej	8
2	Opis dziedziny przedmiotowej pracy	10
2.1	Pojęcia i definicje	10
2.2	Stan wiedzy	10
2.3	Stan pracy wykonany w ramach zajęć przedmiotowych	11
3	Zarys idei systemu <i>Inteligentny zamek</i>	18
3.1	Schemat ideowy systemu <i>Inteligentny zamek</i>	18
3.2	Opis składowych systemu	18
3.3	Podmioty systemu	18
4	Wybór technologii informatycznych	19
4.1	Urządzenie sterujące	19
4.2	Aplikacja serwera	19
4.3	Aplikacja mobilna	19
4.4	Moduł zliczania osób	19
4.5	System kontroli wersji	19
4.6	Prowadzenie dokumentacji	19
5	Projekt systemu <i>Inteligentny zamek</i>	20
5.1	Diagramy UML	20
5.1.1	Diagramy przypadków użycia	20
5.1.2	Diagramy sekwencji systemu	20
5.1.3	Projekt bazy danych	20
5.1.4	Diagramy klas	20
5.2	Uproszczony schemat elektryczny systemu	20
5.3	Komunikacja modułów systemu z aplikacją serwera	20

5.3.1	Komunikaty HTTPRequest pomiędzy aplikacją mobilną, a serwerem	20
5.3.2	Komunikaty HTTPRequest pomiędzy urządzeniem sterującym, a serwerem	20
5.4	Protokoły komunikacji pomiędzy urządzeniem sterującym i aplikacją mobilną	21
5.5	Interfejs graficzny systemu	21
5.5.1	Widoki aplikacji mobilnej	21
5.5.2	Widoki strony internetowej systemu	21
5.5.3	Komunikacja człowiek-interfejs	21
5.5.4	Kolorystyka systemu	21
5.6	Bezpieczeństwo systemu	21
5.6.1	Projekt infrastruktury klucza publicznego (PKI)	21
5.6.2	Poufność	21
5.6.3	Dostępność	21
5.6.4	Integralność	21
6	Implementacja	22
6.1	Aplikacja mobilna	22
6.1.1	Interfejsy programistyczne	22
6.1.2	Przechowywanie danych	22
6.1.3	Graficzna implementacja	22
6.1.4	Walidacja danych wprowadzanych przez użytkownika	22
6.2	Aplikacja serwerowa	22
6.2.1	Strona internetowa	22
6.2.2	Wybrane fragmenty kodu	22
6.3	Urządzenie sterujące - objaśnienie całe kodu programu	22
6.4	Moduł zliczania osób - wybrane fragmenty kodu	22
6.5	Wnioski	22
7	Bezpieczeństwo systemu <i>Inteligentny zamek</i>	23
7.1	Techniki kryptograficzne	23
7.2	Podatności systemu (OWASP Top 10)	23
7.3	Inne zagrożenia występujące w systemie	23

7.4	Możliwości zabezpieczenia systemu	23
7.5	Wnioski	23
8	Wdrożenie i testowanie systemu <i>Inteligentny zamek</i>	24
8.1	Środowisko testowe	24
8.2	Testy jednostkowe	24
8.3	Wizualizacja działania systemu <i>Inteligentny zamek</i>	24
8.4	Wnioski	24
9	Podsumowanie	25
9.1	Dalsze perspektywy rozwoju projektu	25
	Spis rysunków	27
	Spis tabel	27
10	Dodatki	28
10.1	Instalacja systemu <i>Inteligentny zamek</i>	28
10.2	Instrukcja użytkownika systemu <i>Inteligentny zamek</i>	28
11	Załączniki	29

1 Wstęp

1.1 Cel i zakres pracy

Celem pracy jest projekt i implementacja systemu kontroli ruchu oraz zarządzania dostępem do pomieszczeń. System ma na celu zmianę sposobu zarządzania dostępem w budynkach z starszych modeli opartych na fizycznych zamkach z kluczami fizycznymi, bądź systemów opartych na kartach magnetycznych na system posługujący się urządzeniami mobilnymi z system operacyjnym android. Głównym celem jest usprawnienie w uzyskiwaniu dostępu do pomieszczeń dzięki wyeliminowaniu konieczności posiadania przy sobie wielu kluczy fizycznych oraz sytuacji, w których użytkownik zapomniał klucza lub karty magnetycznej i nie mógł uzyskać dostępu poprzez możliwość przenoszenia uprawnień między telefonami. Dodatkowo nasz projekt ma usprawniać takie elementy jak zarządzanie dostępem do wielu pomieszczeń oraz kontrolą osób przebywających w danym pomieszczeniu.

W kwestii bezpieczeństwa systemu naszym zadaniem było spełnienie wymagania dotyczących zabezpieczeń systemu poprzez zastosowanie szeregu funkcji kryptograficznych przy procesie uwierzytelniania jak i przy generowaniu kluczy takich jak np. funkcje skrótu, SSH, algorytmów szyfrowania asymetrycznego oraz zastosowania infrastruktury klucza publicznego.

Zakres pracy w tworzeniu projektu oraz implementacji obejmował takie elementy jak zaprojektowanie oraz stworzenie aplikacji klienckiej, aplikacji serwerowej, oprogramowania do zliczania osób w pomieszczeniu, oprogramowania służącego do przyznawania fizycznego dostępu do pomieszczenia oraz strony internetowej.

1.2 Plan pracy

Plan pracy został podzielony na trzy etapy.

- Pierwszy etap polegał na udoskonaleniu projektu który był wykonywany w ramach przedmiotu projekt zespołowy oraz omówieniu szczegółów kluczowych wykonywanych w dalszej części.
- Drugi etap polegał na implementacji danego projektu w
- Trzecim i ostatnim etapem było przetestowanie działania całego systemu oraz naprawienie wykrytych błędów.

1.3 Metodyka pracy grupowej

Metodyka użyta podczas pracy grupowej była oparta o model kaskadowy składający się z etapów takich jak:

- Planowanie systemu
- Analiza systemu
- Projekt systemu
- Implementacja
- Testowanie
- Wdrożenie i pielęgnacja produktu

Uzasadnieniem wyboru takiej metodyki jest fakt używania takich metodyk podczas dużych projektów inżynierskich oraz brak konieczności pokazywania fragmentów działającego systemu podczas tworzenia pracy inżynierskiej. W początkowej fazie ważniejsze było dla nas określenie specyfiki wymagań systemu oraz sam projekt aniżeli implementacja systemu.

2 Opis dziedziny przedmiotowej pracy

2.1 Pojęcia i definicje

W dokumencie tym posługiwać się będziemy następującymi pojęciami:

Klucz dostępowy - jest to klucz publiczny z pary kluczy prywatny publiczny. Używany jest on do odszyfrowania wiadomości wysłanej z aplikacji mobilnej do urządzenia sterującego.

Klucz szyfrujący jest to klucz prywatny wygenerowany podczas tworzenia pary kluczy publiczny prywatny. Używane jest on do szyfrowania wiadomości wysyłanej z aplikacji mobilnej do urządzenia sterującego

para kluczy szyfrujących- jest to para kluczy (prywatny oraz publiczny) generowanych podczas rejestracji oraz wymiany klucza dostępowego.

Inteligentny zamek - system obsługujący otwieranie elektrozamka bądź serwomechanizmu.

2.2 Stan wiedzy

Przed przystąpieniem do projektu zrobiliśmy porównanie systemów zbliżonych do naszego który na dany moment istniały. I tak doszliśmy do wniosku że wszystkie systemy inteligentnych zamków wykonane przez firmy takie jak Gerda Lock czy DanaLock zostały wykonane typowo dla użytku domowego a nie tak jak nasz projekt inżynierski który jest przeznaczony do zarządzania w budynkach o wielu pomieszczeniach z różnym stopniem dostępu. Opis wraz z porównaniem poszczególnych systemów znajduje się w tabelach poniżej.

Tabela 1 zawiera porównanie firm pod względem otwierania zamka

Tabela 1: Tabela porównania otwierania zamków

	NOKI	August	DanaLock	Gerda Lock
zarządzanie wieloma zamkami z jednej aplikacji	brak	tak	brak	brak
otwieranie zamka przy pomocy strony WWW	brak	brak	tak	brak
inne sposoby otwarcia zamka niż aplikacja	brak informacji	brak informacji	brak	tak
automatyczne zamykanie zamka	brak informacji	tak	tak	tak
tryb otwierania zamka automatycznie	tak	brak	tak	tak

tryb otwierania zamka po zezwoleniu przyciskiem	brak	tak	tak	tak
---	------	-----	-----	-----

Tabela 2 zawiera porównanie firm pod względem zasilania i montażu

Tabela 2: Tabela porównania zasilania i montażu

	NOKI	August	DanaLock	Gerda Lock
zasilanie zewnętrzne (z sieci)	brak	brak	brak	brak
zasilanie bateryjne (podstawowe/ awaryjne)	podstawowe	podstawowe	podstawowe	podstawowe
sposób montażu	nakładka na zamek	nakładka na zamek	nakładka na zamek	nakładka na zamek

Tabela 3 zawiera porównanie firm pod względem dziennika zdarzeń oraz powiadomień

Tabela 3: Tabela porównania zasilania i montażu

	NOKI	August	DanaLock	Gerda Lock
podgląd kto otworzył	brak informacji	brak	brak	tak
powiadomienie o otwarciu drzwi (ogólnie i przez daną osobę)	brak	brak	brak	tak
powiadomienie o nieautoryzowanych próbach otwarcia	tak	brak	brak	tak

2.3 Stan pracy wykonany w ramach zajęć przedmiotowych

W ramach zajęć projektowych oraz laboratoryjnych o nazwie Projekt Zespołowy prowadzonych z mgr. Michałem Apolinarskim oraz dr Ewą Idzikowską zostały wykonane następujące fragmenty systemu: Aplikacja mobilna została wykonana dla wersji androida minimum 4.4 KitKat w stopniu umożliwiającym takie funkcjonalności jak:

- Logowanie
- Rejestracja

- Rejestracja wraz z tworzeniem pary kluczy dostępowych publiczny prywatny
- Generowanie nowego certyfikatu
- Pobieranie certyfikatów z serwera
- Zarządzanie certyfikatami użytkownika
- Zarządzanie prośbami o rejestrację
- Wnioskowanie o certyfikat nowy

Dodatkowo zostało napisane api do obsługi połączenia bluetooth oraz w każdym widoku który korzystał z połączenia z serwerem były napisane fragmenty kodu. Funkcje te oraz kod zostały napisane bez uwzględnienia wzorców architektonicznych (wszystko co dotyczyło danego widoku było w jednej klasie), posiadały szereg błędów powodujących niestabilne działanie systemu oraz posiadały metody z systemu android które były określane przez środowisko android studio jako "deprecated" co mogło przy nowszych wersjach androida powodować wadliwe działanie systemu. Z racji pisania pod wersje systemu android 4.4 wygląd różni się od tego który został zaimplementowany w pracy inżynierskiej. Poniżej przedstawiono wygląd aplikacji w stanie początkowym(???).

Aplikacja serwerowa posiadała następujące rest api

- api służące do pobierania certyfikatu
- api służące do informowania o statusie certyfikatu
- api służące do logowania użytkownika
- api służące do rejestracji użytkownika
- api służące do wylogowania użytkownika
- api służące do pobrania wszystkich certyfikatów użytkowników
- api służące do pobrania listy wszystkich zamków
- api służące do pobrania listy wszystkich użytkowników systemu
- api służące do zmiany hasła
- api służące do pobrania historii użycia zamków
- api służące do pobrania listy oczekujących certyfikatów
- api służące do pobrania listy oczekujących użytkowników na zarejestrowanie
- api służące do generowania nowego certyfikatu

- api służące do określenia decyzji administratora w stosunku do danego oczekującego certyfikatu
- api służące do określenia decyzji administratora w stosunku do danego oczekującego użytkownika na zarejestrowanie

Wszystkie te API zwracały odpowiednio albo odpowiednie dane albo wartość Invalid. Ponadto posiadały szereg niedopatrzeń powodujących wadliwe działanie systemu w szczególnych przypadkach.

Urządzenie sterujące zamkiem ???

Baza danych składała się z 5 tabel o następujących wartościach

- **USERS** — przechowuje dane użytkowników oraz dane niezbędne przy weryfikacji logowania,
- **LOCKS** — zawiera informacje na temat dostępnych w systemie zamków,
- **ACCESS_TO_LOCKS** — archiwizuje próby użycia certyfikatów,
- **LOCKS_KEYS** — zawiera wszystkie klucze dostępowe użytkowników,
- **WAIT_LOCKS_KEYS** — przetrzymuje klucze dostępowe oczekujące na zatwierdzenie przez administratora.

Wiersz tabeli USERS zawierał:

- **ID_USER** — unikalny identyfikator (klucz główny) użytkownika składający się z 10 cyfr,
- **LOGIN** — unikalna nazwa użytkownika niezbędna podczas logowania, zawierająca nie więcej niż 255 znaków,
- **PASSWORD** — hasło zapisane w postaci skrótu, potrzebne do autoryzacji dostępu użytkownikowi,
- **PUBLIC_KEY** — klucz publiczny użytkownika potrzebny do podpisu cyfrowego,
- **NAME** - imię użytkownika,
- **SURNAME** — nazwisko użytkownika,
- **IS_ADMIN** — pole boolowskie wskazujące czy dany użytkownik jest administratorem czy nie,
- **TOKEN** — generowany ciąg pseudolosowy klucz sesji logowania,
- **ISACTIVATED** — pole boolowskie oznaczające, czy dane konto jest zaakceptowane (aktywowane) przez administratora.

Zamek opisywany był poprzez kolumny:

- **ID_LOCK** — unikalny identyfikator (klucz główny) zamka składający się z 10 cyfr,
- **NAME** — unikalna nazwa zamka,
- **MAC_ADDRESS** — adres fizyczny urządzenia sterującego zamkiem,
- **LOCALIZATION** — nieobowiązkowe pole opisujące fizyczne położenie zamka,
- **ADMIN_KEY** — wartość klucza awaryjnego dla administratora.

Klucz dostępowy składał się z:

- **ID_KEY** — unikalny identyfikator (klucz główny) klucza dostępowego składający się z 10 cyfr,
- **ID_LOCK** — klucz obcy do tabeli przechowującej dostępne zamki,
- **ID_USER** — klucz obcy do tabeli przechowującej dane użytkownika, jest to pole służące do określenia kto utworzył klucz dostępu,
- **KEY** — unikalna wartość certyfikatu dostępu,
- **FROM** — data od której obowiązuje klucz,
- **TO** — data do której obowiązuje klucz,
- **ISACTUAL** — data wygaśnięcia klucza, jeśli równa TO, oznacza to że klucz utracił ważność z powodu czasu, jeśli różna oznacza, to że zablokowano z innego powodu ważność,
- **MONDAY** — słowne określenie, w których godzinach zostanie przyznany dostęp w poniedziałki,
- **TUESDAY** — słowne określenie, w których godzinach zostanie przyznany dostęp we wtorki,
- **WEDNESDAY** — słowne określenie, w których godzinach zostanie przyznany dostęp w środy,
- **THURSDAY** — słowne określenie, w których godzinach zostanie przyznany dostęp w czwartki,
- **FRIDAY** — słowne określenie, w których godzinach zostanie przyznany dostęp w piątki,
- **SATURDAY** — słowne określenie, w których godzinach zostanie przyznany dostęp w soboty,
- **SUNDAY** — słowne określenie, w których godzinach zostanie przyznany dostęp w niedziele,
- **IS_PERNAMENT** — zmienna boolowska oznaczająca czy dostęp jest zawsze,
- **NAME** - imię osoby, której dotyczy certyfikat,
- **SURNAME** — nazwisko osoby, której dotyczy certyfikat.

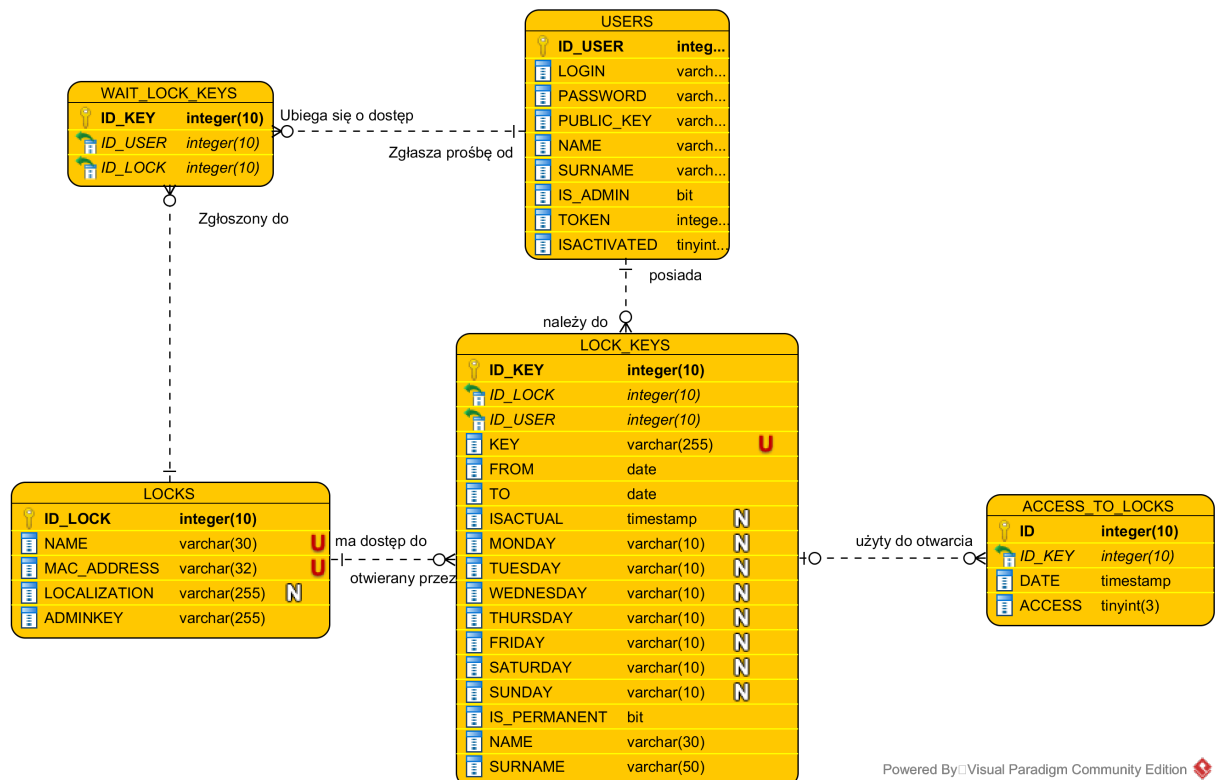
W tabeli archiwizującej akcje na zamku znajdowały się takie dane jak:

- **ID** — unikalny identyfikator (klucz główny) akcji wykonanej na certyfikacie składający się z 10 cyfr,

- **ID_KEY** — klucz obcy do tabeli przechowującej klucze dostępowe, dzięki tej informacji możemy uzyskać dane o zamku, który został otwierany jak również do kogo należał klucz,
- **DATE** — dokładna data z godziną użycia klucza dostępowego,
- **ACCESS** — binarna flaga informująca czy dostęp został przyznany czy odmówiony.

Tabela **WAIT_LOCKS_KEYS** składa się z:

- **ID_KEY** — unikalny identyfikator (klucz główny) oczekującego certyfikatu,
- **ID_LOCK** — klucz obcy do tabeli **LOCKS**, oznacza zamek do którego jest zgłaszana prośba dostępu,
- **ID_USER** — klucz obcy do tabeli **USERS**, oznacza użytkownika który zgłasza prośbę o dostęp do zamka.



Powered By: Visual Paradigm Community Edition

W ramach przedmiotu ochrona danych zostały zaimplementowane w systemie fragmenty PKI takie jak:

- Certyfikat klucza dostępowego
- generowanie nowego Certyfikatu użytkownika
- blokowanie użytkownika systemu

Funkcje te zostały napisane zarówno po stronie aplikacji mobilnej jak i aplikacji serwerowej. Ponadto po stronie androida został opracowany sposób przechowywania klucza prywatnego w formie zaszyfrowanego pliku hasłem użytkownika.

3 Zarys idei systemu *Inteligentny zamek*

3.1 Schemat ideowy systemu *Inteligentny zamek*

3.2 Opis składowych systemu

3.3 Podmioty systemu

4 Wybór technologii informatycznych

4.1 Urządzenie sterujące

4.2 Aplikacja serwera

4.3 Aplikacja mobilna

4.4 Moduł zliczania osób

4.5 System kontroli wersji

4.6 Prowadzenie dokumentacji

5 Projekt systemu *Inteligentny zamek*

5.1 Diagramy UML

5.1.1 Diagramy przypadków użycia

5.1.1.1 Aplikacja mobilna

5.1.1.2 Aplikacja serwera

5.1.1.3 Urządzenie sterujące

5.1.1.4 Moduł zliczania osób

5.1.2 Diagramy sekwencji systemu

5.1.2.1 Aplikacja mobilna

5.1.2.2 Aplikacja serwera

5.1.2.3 Urządzenie sterujące

5.1.2.4 Moduł zliczania osób

5.1.3 Projekt bazy danych

5.1.4 Diagramy klas

5.1.4.1 Aplikacja mobilna

5.1.4.2 Aplikacja serwera

5.1.4.3 Urządzenie sterujące

5.1.4.4 Moduł zliczania osób

5.2 Uproszczony schemat elektryczny systemu

5.3 Komunikacja modułów systemu z aplikacją serwera

5.3.1 Komunikaty HTTPRequest pomiędzy aplikacją mobilną, a serwerem

5.3.2 Komunikaty HTTPRequest pomiędzy urządzeniem sterującym, a serwerem

- 5.4 Protokoły komunikacji pomiędzy urządzeniem sterującym i aplikacją mobilną
- 5.5 Interfejs graficzny systemu
 - 5.5.1 Widoki aplikacji mobilnej
 - 5.5.2 Widoki strony internetowej systemu
 - 5.5.3 Komunikacja człowiek-interfejs
 - 5.5.3.1 Komunikaty tekstowe
 - 5.5.3.2 Symbolika ikon
 - 5.5.3.3 Znaczenie kolorystyki
 - 5.5.4 Kolorystyka systemu
- 5.6 Bezpieczeństwo systemu
 - 5.6.1 Projekt infrastruktury klucza publicznego (PKI)
 - 5.6.1.1 Idea PKI
 - 5.6.1.2 Urzędy certyfikujące
 - 5.6.1.3 Klient systemu
 - 5.6.2 Poufność
 - 5.6.3 Dostępność
 - 5.6.4 Integralność

6 Implementacja

6.1 Aplikacja mobilna

6.1.1 Interfejsy programistyczne

6.1.2 Przechowywanie danych

6.1.3 Graficzna implementacja

6.1.4 Walidacja danych wprowadzanych przez użytkownika

6.2 Aplikacja serwerowa

6.2.1 Strona internetowa

6.2.2 Wybrane fragmenty kodu

6.3 Urządzenie sterujące - objaśnienie całego kodu programu

6.4 Moduł zliczania osób - wybrane fragmenty kodu

6.5 Wnioski

7 Bezpieczeństwo systemu *Inteligentny zamek*

7.1 Techniki kryptograficzne

7.2 Podatności systemu (OWASP Top 10)

7.3 Inne zagrożenia występujące w systemie

7.4 Możliwości zabezpieczenia systemu

7.5 Wnioski

8 Wdrożenie i testowanie systemu *Inteligentny zamek*

8.1 Środowisko testowe

8.2 Testy jednostkowe

8.3 Wizualizacja działania systemu *Inteligentny zamek*

8.4 Wnioski

9 Podsumowanie

9.1 Dalsze perspektywy rozwoju projektu

Literatura

Spis rysunków

Spis tablic

1	Tabela porównania otwierania zamków	10
2	Tabela porównania zasialania i montażu	11
3	Tabela porównania zasialania i montażu	11

10 Dodatki

10.1 Instalacja systemu *Inteligentny zamek*

10.2 Instrukcja użytkownika systemu *Inteligentny zamek*

11 Załączniki

Do pracy dołączono płytę CD-ROM zawierającą:

- treść pracy w pliku PDF,
- treść pracy w formacie LATEX,
- implementację systemu *Inteligentny zamek*,
- kody uruchomieniowe systemu *Inteligentny zamek*.