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 Marciniak
Student:	Damian FILIPOWICZ	122002	

Tytuł pracy:	Projekt oraz implementacja systemu kontroli ruchu i zarządzania dostępem do pomieszczeń (projekt zespołowy)
Wersja angielska tytułu:	*Design and implementation of movement control and access to spaces management system (team project)*
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
dr Jerzy Bartoszek

podpis dyrektora/kierownika jednostki organizacyjnej promotora

PRODZIEKAN
Wydziału Elektrycznego
Politechniki Poznańskiej
dr hab. inż. Andrzej Tomczewski

podpis Dziekana

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 *Inteligentny zamek* **15**

3.1 Schemat ideowy systemu *Inteligentny zamek* 15

3.2 Opis składowych systemu 15

3.3 Podmioty systemu 15

4 Wybór technologii informatycznych **16**

4.1 Urządzenie sterujące 16

4.2 Aplikacja serwera 16

4.3 Aplikacja mobilna 16

4.4 Moduł zliczania osób 16

4.5 System kontroli wersji 16

4.6 Prowadzenie dokumentacji 16

5 Projekt systemu *Inteligentny zamek* **17**

5.1 Diagramy UML 17

5.1.1 Diagramy przypadków użycia 17

5.1.2 Diagramy sekwencji systemu 17

5.1.3 Projekt bazy danych 17

5.1.4 Diagramy klas 17

5.2 Uproszczony schemat elektryczny systemu 17

5.3 Komunikacja modułów systemu z aplikacją serwera 17

5.3.1 Komunikaty HTTPRequest pomiędzy aplikacją mobilną, a serwerem . . . 17
5.3.2 Komunikaty HTTPRequest pomiędzy urządzeniem sterującym, a serwerem . . . 17
5.4 Protokoły komunikacji pomiędzy urządzeniem sterującym i aplikacją mobilną . . . 18
5.5 Interfejs graficzny systemu . . . 18
5.5.1 Widoki aplikacji mobilnej . . . 18
5.5.2 Widoki strony internetowej systemu . . . 18
5.5.3 Komunikacja człowiek-interfejs . . . 18
5.5.4 Kolorystyka systemu . . . 18
5.6 Bezpieczeństwo systemu . . . 18
5.6.1 Projekt infrastruktury klucza publicznego (PKI) . . . 18
5.6.2 Poufność . . . 18
5.6.3 Dostępność . . . 18
5.6.4 Integralność . . . 18

6 Implementacja **19**
6.1 Aplikacja mobilna . . . 19
6.1.1 Interfejsy programistyczne . . . 19
6.1.2 Przechowywanie danych . . . 19
6.1.3 Graficzna implementacja . . . 19
6.1.4 Walidacja danych wprowadzanych przez użytkownika . . . 19
6.2 Aplikacja serwerowa . . . 19
6.2.1 Strona internetowa . . . 19
6.2.2 Wybrane fragmenty kodu . . . 19
6.3 Urządzenie sterujące - objaśnienie całe kodu programu . . . 19
6.4 Moduł zliczania osób - wybrane fragmenty kodu . . . 19
6.5 Wnioski . . . 19

7 Bezpieczeństwo systemu *Inteligentny zamek* **20**
7.1 Techniki kryptograficzne . . . 20
7.2 Podatności systemu (OWASP Top 10) . . . 20
7.3 Inne zagrożenia występujące w systemie . . . 20

7.4 Możliwości zabezpiezpieczenia systemu 20
7.5 Wnioski 20

8 Wdrożenie i testowanie systemu *Inteligentny zamek* 21
8.1 Środowisko testowe 21
8.2 Testy jednostkowe 21
8.3 Wizualizacja działania systemu*Inteligentny zamek* 21
8.4 Wnioski 21

9 Podsumowanie 22
9.1 Dalsze perspektywy rozwoju projektu 22

Spis rysunków 24

Spis tabel 24

10 Dodatki 25
10.1 Instalacja systemu *Inteligentny zamek* 25
10.2 Instrukcja użytkownika systemu *Inteligentny zamek* 25

11 Załączniki 26

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 zamianę 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 orz implementacji obejmował takie elementy jak zaprojektowanie oraz stworzenie aplikacji klienckjiek, aplikacji serwerowej, oprogramowania do zliczania osób w pomieszceniu, oprogramowania służącego do przyznawania fizycznego dostępu do pomiezcenia 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 kaskaodowy składajaćy 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 prywartny publiczny. Używany jest on do odszyfrowania wiadomości wysłanej z aplikacji mobilnej do urządzenia sterujacego.

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 dostepowego.

Inteligentny zamek - system obsługujący otwieranie elektrozamka bądz 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 poszcególnych 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 zasialania i montażu

	NOKI	August	DanaLock	Gerda Lock
zasilanie zewnętrzne (z sieci)	brak	brak	brak	brak
zasilanie bateryjne (podstawowe/ awaryjne)	podstawowe	podstawowe	podstawowe	podstawowbe
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 zasialania 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 nazwe Projekt Zespołowy prowadzonych z mgr. Michałem Apolinarskim oraz dr Ewą Idzikowską zostały wykonane następujace fragmenty systemu: Aplikacja mobilna została wykonana dla wersji andorida minimum 4.4 KitKat w stopniu umożliwiającym takie funkcjonalnośći jak:

- Logowanie
- Rejestracja

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

Dodatkowo zostało napisane api do obsługi połączenia bluetooth oraz w każdym widoku któy korzystał z połaczenia 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 działąnie systemu oraz posiadały metody z systemu android które były określane przez środowisko android stuido jako "deprecatedćo 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. Ponieżej przedstawiono wygląd aplikacji w stanie początkowym(????).

Aplikacja serwerowa posiadałą następujące rest api

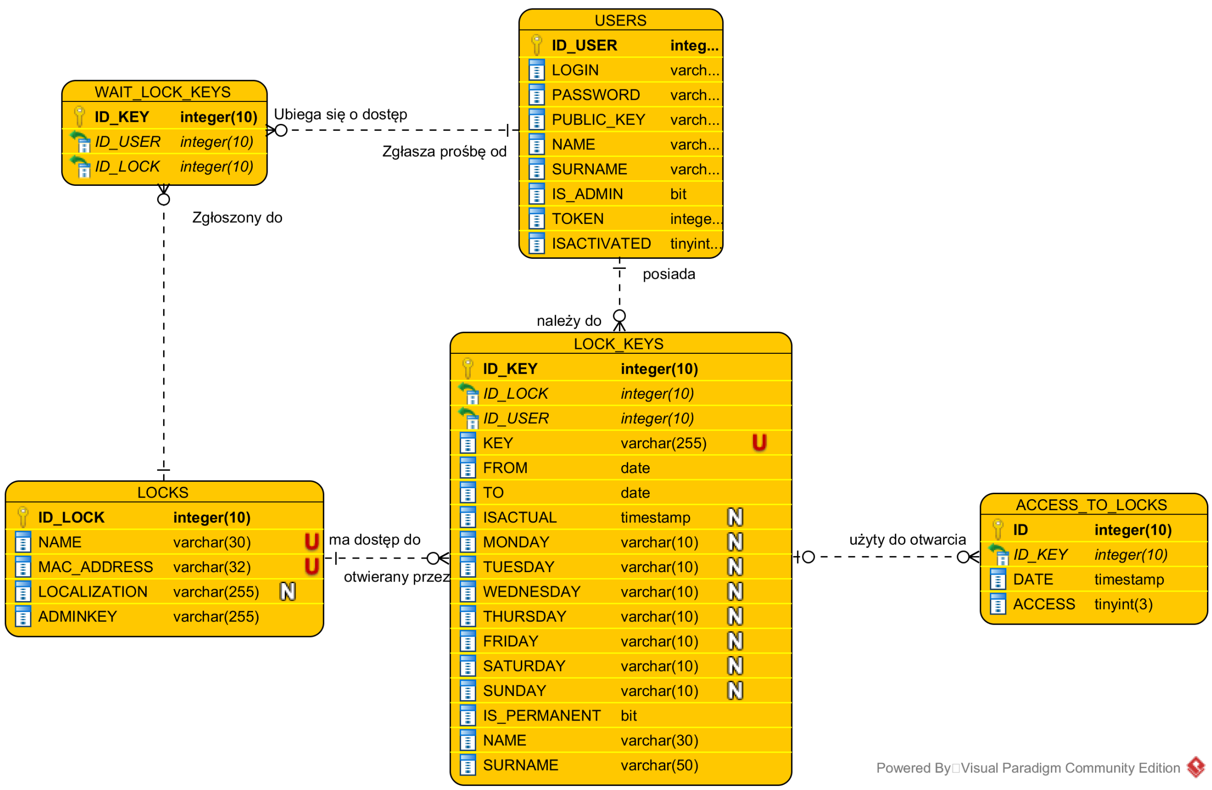
- api służące do pobierania certyfikatu
- api służące do informowania o statusie certyfikatu
- api służące do logowania użytkownika
- api służące do rejstracji uzytkownika
- api służące do wylogowania użytkownika
- api służące do pobrania wszystkich certyfikatów użytkowników
- api służące do pobrania listy wszystkich zamków
- api służące do pobrania listy wszystkich uzytkownikóW systemu
- api służące do zmiany hasła
- api służące do pobrania histori 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 administratorwa w stosunku do danego oczekującego certyfikatu
- api służące do określenia decyzji administratorwa w stosunku do danego oczekującego użytkownika na zarejestrowanie

Wszystkei 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 została wykonana w następujaćy sposób:



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

- Certyfikat klucza dostępowego
- generowanei nowego Certyfikatu uzytkownika
- blokowanie uzytkownika 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 uzytkownika.

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 Urzedy 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 całe 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 zabezpiezpieczenia 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 uruchomieniowne systemu *Inteligentny zamek*.