

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 umieszczona tylko informacyjnie



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:	Damian FILIPOWICZ	122002	30.11.2017r. Da
Student:	Maciej MARCINIAK	121996	

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. Sillars Doug, Wydajne aplikacje dla systemu Android. Programuj szybko i efektywnie, Helion 2016
2. Anders Göransson, Android. Aplikacje wielowątkowe. Techniki przetwarzania, Helion 2015

Zakres pracy:

1. Projekt i implementacja aplikacji mobilnej do zarządzania systemem od strony użytkownika oraz administratora.
2. Projekt i implementacja interfejsu graficznego aplikacji mobilnej.
3. Implementacja wewnętrznego PKI od strony klienta systemu.
4. Projekt i implementacja strony dla administratora z podglądem historii zamków w sieci lokalnej.

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 i kierownika jednostki organizacyjnej promotora

PRODZIEKAN
Wydziału Elektrycznego
Politechniki Poznańskiej

dr hab. inż. Andrzej Tomczewski
podpis Dziekana

Poznań, 30 października 2017
miejscowość, data

karta pracy umieszczona tylko informacyjnie



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>Maciej Marciniak</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
dr Jerzy Bartoszek

podpis dyrektora/sterownika jednostki organizacyjnej promotora

PRODZIEKAN
Wydziału Elektrycznego
Politechniki Poznańskiej
A. G.

dr hab. inż. *Przemysław* 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 management
system

by
Maciej Marciniak
Damian Filipowicz

Abstract

Streszczenie

Spis treści

1	Wstęp	8
1.1	Cel i zakres pracy	8
1.2	Plan pracy	9
1.3	Metodyka pracy grupowej	10
2	Opis dziedziny przedmiotowej pracy	11
2.1	Pojęcia i definicje	11
2.2	Stan wiedzy	12
2.3	Stan pracy wykonany w ramach zajęć przedmiotowych	14
3	Zarys idei systemu <i>Inteligentny zamek</i>	16
3.1	Schemat ideowy systemu <i>Inteligentny zamek</i>	16
3.2	Opis składowych systemu	17
3.3	Podmioty systemu	18
4	Wybór technologii informatycznych	19
4.1	Urządzenie sterujące	19
4.2	Aplikacja serwera	20
4.3	Aplikacja mobilna	21
4.4	Moduł zliczania osób	22
4.5	System kontroli wersji	23
4.6	Prowadzenie dokumentacji	24
5	Projekt systemu <i>Inteligentny zamek</i>	25
5.1	Diagramy UML	25
5.1.1	Diagramy przypadków użycia	25
5.1.2	Diagramy sekwencji systemu	25
5.1.3	Projekt bazy danych	25
5.1.4	Diagramy klas	25
5.2	Uproszczony schemat elektryczny systemu	26
5.3	Komunikacja modułów systemu z aplikacją serwera	27

5.3.1	Komunikaty HTTPRequest pomiędzy aplikacją mobilną, a serwerem	27
5.3.2	Komunikaty HTTPRequest pomiędzy urządzeniem sterującym, a serwerem	27
5.4	Protokoły komunikacji pomiędzy urządzeniem sterującym i aplikacją mobilną	28
5.5	Interfejs graficzny systemu	29
5.5.1	Widoki aplikacji mobilnej	29
5.5.2	Widoki strony internetowej systemu	29
5.5.3	Komunikacja człowiek-interfejs	29
5.5.4	Kolorystyka systemu	29
5.6	Bezpieczeństwo systemu	30
5.6.1	Projekt infrastruktury klucza publicznego (PKI)	30
5.6.2	Poufność	30
5.6.3	Dostępność	30
5.6.4	Integralność	30
6	Implementacja	31
6.1	Aplikacja mobilna	31
6.1.1	Przechowywanie danych	31
6.1.2	Graficzna implementacja	31
6.1.3	Walidacja danych wprowadzanych przez użytkownika	31
6.2	Aplikacja serwerowa	32
6.2.1	Strona internetowa	32
6.3	Urządzenie sterujące	33
6.4	Moduł zliczania osób	34
6.5	Wnioski	35
7	Bezpieczeństwo systemu <i>Inteligentny zamek</i>	36
7.1	Techniki kryptograficzne	36
7.2	Podatności systemu (OWASP Top 10)	37
7.3	Inne zagrożenia występujące w systemie	38
7.4	Możliwości zabezpieczenia systemu	39
7.5	Wnioski	40

8	Wdrożenie i testowanie systemu <i>Inteligentny zamek</i>	41
8.1	Środowisko testowe	41
8.2	Testy jednostkowe	42
8.3	Wizualizacja działania systemu <i>Inteligentny zamek</i>	43
8.4	Wnioski	44
9	Podsumowanie	45
9.1	Dalsze perspektywy rozwoju projektu	45
	Spis rysunków	47
	Spis tabel	47
10	Dodatki	48
10.1	Instalacja systemu <i>Inteligentny zamek</i>	48
10.2	Instrukcja użytkownika systemu <i>Inteligentny zamek</i>	48
11	Załączniki	49

1 Wstęp

Wstęp pracy zawiera krótki opis celu i zakresu planowanego projektu. System nosi potoczną nazwę *Inteligentny zamek*, która związana jest z dodaniem pewnych szczególnych funkcjonalności względnie zwykłym przedmiotom, tak jak dzieje się to w obecnie modnych urządzeniach typu Internet of things. Znaczna część znajdujących się na rynku rozwiązań dedykowana jest użytkownikom indywidualnym, do użytku domowego, opisywany system przeznaczony jest do zastosowań biurowych (dla średnich i dużych przedsiębiorstw).

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 zapomniałby klucza lub karty magnetycznej i nie mógł uzyskać dostępu. Rozwiązaniem tych problemów jest możliwość przenoszenia kluczy (uprawnień) między telefonami. Dodatkowo nasz projekt ma usprawniać takie elementy, jak zarządzanie dostępem do wielu pomieszczeń oraz kontrolę osób przebywających w danym pomieszczeniu poprzez moduł zliczania osób wchodzących i wychodzących.

W kwestii bezpieczeństwa systemu naszym zadaniem było spełnienie wymagań 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 oraz serwerowej, oprogramowania do zliczania osób w pomieszczeniu, oprogramowania służącego do nadzorowania fizycznego dostępu do pomieszczenia, jak również strony internetowej jako panel administracyjny administratora systemu.

1.2 Plan pracy

Praca w pierwszej kolejności przedstawia dziedzinę projektu, którego dotyczy. Zostaną wyjaśnione używane pojęcia oraz nazwy własne umożliwiające poprawną interpretację opisanych działań. Po objaśnieniu terminologii, nasz projekt zostanie porównany z istniejącymi rozwiązaniami podobnego typu oraz zostaną wyciągnięte wnioski na temat niedopracowania lub możliwości poprawy danych rozwiązań jakie zastosowano projektując opisywany w pracy system. Kończąc prezentację dziedziny zostanie opisany stan wykonania pracy w ramach zajęć przedmiotowych w trakcie trwania studiów inżynierskich.

Następny rozdział ma na celu przedstawić ogólny zarys systemu. Opisany zostanie schemat połączeń poszczególnych modułów, interfejsów komunikacyjnych oraz wykaz wszystkich elementów składowych, wraz z możliwymi użytkownikami.

Czwarty rozdział dotyczy przybliżenia użytych technologii raz z uzasadnieniem. Opis wyszczególnia zastosowane narzędzia do implementacji każdego z modułów oraz umożliwiające pracę zespołową.

Główny rozdział pracy dotyczy projektu systemu. W dziale opisane są w pierwszej kolejności diagramy UML (przypadków użycia, sekwencji, bazy danych oraz klas), które są odzwierciedleniem dalszej implementacji. Następnie przybliżony zostaje uproszczony schemat elektryczny urządzenia sterującego zamkiem fizycznym oraz moduł zliczający ludzi. Kolejne punkty opisują szczegółowo komunikacją pomiędzy urządzeniami oraz interfejs graficzny aplikacji mobilnej i strony internetowej. Kończąc tematykę projektu zostaną przybliżone dokładniej zaprojektowane mechanizmy zapewniające bezpieczeństwo ze względu na podstawowe zasady: poufność, dostępność i integralność.

Po omówieniu projektu zostanie opisana implementacja systemu. Dział ten przybliży wybrane, kluczowe fragmenty programów oraz dokładniej określi metodykę powstałego kodu.

Następny dział pracy skupi się na bezpieczeństwie systemu. Omówione zostaną szczegółowo zastosowane metody kryptograficzne oraz zostanie przeprowadzona analiza podatności względem listy najczęstszych podatności OWASP Top 10. Podsumowując dział zostaną zaproponowane możliwości poprawy bezpieczeństwa systemu, których nie uwzględniono w fazie projektu, ani potem implementacji.

Ostatnim rozdziałem przed podsumowaniem jest omówienie przeprowadzanych testów pod względem poprawności działania systemu. Jednocześnie zostanie graficznie przedstawione działanie każdego modułu.

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 zaprojektowanie, aniżeli implementacja systemu.

2 Opis dziedziny przedmiotowej pracy

Rozdział zawierać będzie objaśnienia używanych zwrotów i pojęć umożliwiających poprawne interpretowanie dalszych tekstów. Następnie opisany zostanie stan wiedzy związanej z tematyką pracy, to znaczy omówienie wybranych rozwiązań systemów tak zwanych inteligentnych zamków. W zestawieniu porównane zostaną również zaproponowane w pracy dyplomowej rozwiązania.

2.1 Pojęcia i definicje

W dokumencie tym posługiwać się będziemy następującymi pojęciami:

- Klucz dostępowy — jest to klucz określający dostęp do pomieszczenia dla użytkownika w konkretnych dniach oraz godzinach,
- Klucz szyfrujący — jest to klucz prywatny wygenerowany podczas tworzenia certyfikatu klucza szyfrującego. Używany jest on do szyfrowania wiadomości wysyłanej z aplikacji mobilnej do urządzenia sterującego,
- Klucz deszyfrujący — jest to klucz publiczny wygenerowany podczas tworzenia certyfikatu klucza szyfrującego. Używane jest on do odszyfrowania wiadomości wysyłanej z aplikacji mobilnej do urządzenia sterującego,
- Inteligentny zamek — system obsługujący otwieranie elektrozamka bądź serwomechanizmu,
- Konto — reprezentacja użytkownika w systemie za pomocą takich danych jak login, hasło, imię, nazwisko.
- Administrator — jest to fizyczna osoba posiadająca dla swojego konta uprawnienia administratora co wiąże się z pełnym dostępem do systemu,
- Certyfikat dostępowy — jest to certyfikat przechowujący informacje takie jak dane użytkownika, do jakiego pomieszczenia oraz w jakich dniach i godzinach ma dostęp
- Certyfikat klucza szyfrującego — jest to certyfikat przechowujący dane o użytkowniku, ważności klucza szyfrującego oraz sam klucz deszyfrujący.

2.2 Stan wiedzy

Przed przystąpieniem do projektu wykonaliśmy rozeznanie w około systemów zbliżonych do naszego, który na dany moment były produkowane. I tak doszliśmy do wniosku, że wszystkie systemy inteligentnych zamków wykonane przez uznane 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 większej złożoności, takich jak biurowce, z różnym stopniem dostępu. Opis wraz z porównaniem poszczególnych systemów znajduje się w tabelach poniżej.

Tabela 1 zawiera porównanie firm pod względem otwierania zamka. Już w pierwszym wierszu można zauważyć, indywidualne zastosowanie systemów, ponieważ każdy z prezentowanych systemów, poza firmą August, nie oferuje obsługi wielu urządzeń z poziomu jednej aplikacji. Proponowane przez nas rozwiązanie umożliwia skalowalność systemu oraz wprowadzanie różnorodności w zarządzaniu dostępem. Następne funkcjonalności wprowadzają zagrożenia lub zwiększają podatności systemu na ataki hakerskie. Weźmy pod uwagę otwieranie dowolnego zamka z dowolnego miejsca przez stronę WWW, umożliwia taka funkcjonalność zdalne sterowanie dostępem w całym budynku. Skutkuje to brakiem kontroli, którą nie powoduje znacznych korzyści dla celów biznesowych dla, których nasz system jest dedykowany.

Tabela 1: Tabela porównania otwierania zamków

Funkcja	NOKI	August	DanaLock	Gerda Lock	Nasz system
zarządzanie wieloma zamkami z jednej aplikacji	brak	tak	brak	brak	tak
otwieranie zamka przy pomocy strony WWW	brak	brak	tak	brak	brak
inne sposoby otwarcia zamka niż aplikacja	brak	brak	brak	tak	tak
automatyczne zamykanie zamka	brak	tak	tak	tak	tak
tryb otwierania zamka automatycznie	tak	brak	tak	tak	nie
tryb otwierania zamka po zezwoleniu przyciskiem	brak	tak	tak	tak	tak

Tabela 2 zawiera porównanie firm pod względem zasilania i montażu. Wszystkie systemy zawierały podstawowe wady eksploatacyjne, gdy system w budynku zawierałby wiele urządzeń danego typu, to znaczy problem z zasilaniem. Nasz system oferuje podłączenie zasilania bezpośrednio z sieci, taka konfiguracja pozwala uodpornić system na konieczność wymiany baterii w każdym zamku. Gdyby jednak konieczne było zasilanie awaryjne, w sytuacji zaniku napięcia, możliwe jest zastosowanie UPSów, które podtrzymają urządzenia przez czas awarii.

Tabela 2: Tabela porównania zasilania i montażu

Funkcja	NOKI	August	DanaLock	Gerda Lock	Nasz system
zasilanie zewnętrzne (z sieci)	brak	brak	brak	brak	tak
zasilanie bateryjne (podstawowe/awaryjne)	podst.	podst.	podst.	podst.	możliwe awaryjne
sposób montażu	nakładka na zamek	nakładka na zamek	nakładka na zamek	nakładka na zamek	nakładka na zamek lub elektrozamek

Tabela 3 zawiera porównanie firm pod względem dziennika zdarzeń oraz powiadomień. Funkcjonalność naszego systemu zgodna jest z możliwościami firm NOKI oraz Gerda Lock. Pozostali dystrybutorzy nie udostępniają tak szczegółowych informacji na temat działań urządzeń.

Tabela 3: Tabela porównania dziennika zdarzeń oraz powiadomień

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

2.3 Stan pracy wykonany w ramach zajęć przedmiotowych

W ramach zajęć projektowych oraz laboratoryjnych o nazwę 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 podstawowe funkcjonalności, takie jak:

- Logowanie użytkowników,
- Rejestracja użytkowników,
- Rejestracja wraz z tworzeniem certyfikatu klucza szyfrującego,
- Generowanie nowego certyfikatu,
- Pobieranie certyfikatów z serwera,
- Zarządzanie certyfikatami użytkownika,
- Zarządzanie prośbami o rejestrację,
- Wnioskowanie o certyfikat nowy.

Dodatkowo zostało zaimplementowane gniazdko sieciowe 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 dotyczące danego widoku było zawarte w jednej klasie), posiadały szereg błędów powodujących niestabilne działanie systemu oraz stosowały metody z systemu android, które były określane przez środowisko android studio, jako "deprecated" (niewspierane), co mogło powodować przy nowszych wersjach androida wadliwe działanie systemu. Z racji pisania pod wersję systemu android 4.4 wygląd różni się od tego, który został zaimplementowany w pracy dyplomowej.

Aplikacja serwerowa została wykonana w stopniu umożliwiającym podstawowe funkcje pozwalające na komunikację pomiędzy urządzeniami. Api zapewniało w minimalnym stopniu bezpieczeństwo. Funkcje serwera utworzone w ramach zajęć przedmiotowych:

- Logowanie użytkowników,
- Rejestracja użytkowników,
- Zapisywanie nowego certyfikatu dostępu,
- Udostępnianie certyfikatów dostępowych,
- Pobieranie list certyfikatów, próśb o certyfikaty oraz rejestracji.

Wszystkie te funkcje zwracały odpowiednio pożądane dane, albo wartość "Invalid" co powodowało wyświetlanie komunikatów o błędach użytkownikowi bez rozróżniania powodu, np. awarii serwera (mylnie wysyłany komunikat "Invalid" zamiast komunikatu HTTP typu 500).

Urządzenie sterujące zamkiem zostało napisane w języku Python i pozwalało na odbieranie danych z aplikacji mobilnej oraz posiadało funkcje odpowiedzialną za otwieranie zamka.

W ramach przedmiotu ochrona danych prowadzone przez dr inż. Anne Grocholewską-Czuryło zostały zaimplementowane w systemie fragmenty PKI, takie jak:

- Format certyfikatu klucza szyfrującego,
- Generowanie nowego certyfikatu szyfrującego użytkownika,
- Blokowanie użytkowników oraz certyfikatów szyfrujących systemu.

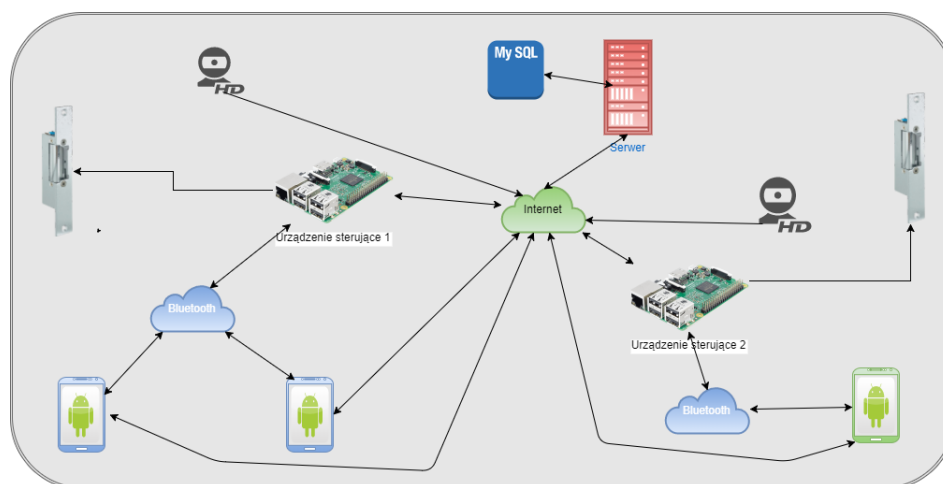
Funkcje te zostały napisane zarówno po stronie aplikacji mobilnej jak i aplikacji serwerowej. Ponadto po stronie androida został opracowany sposób przechowywania klucza prywatnego w formie zaszyfrowanego pliku hasłem użytkownika.

3 Zarys idei systemu *Inteligentny zamek*

W rozdziale zostanie opisana pokrótce idea systemu *Inteligentny zamek*. Projekt składa się z 5 składowych: urządzenia sterującego (zarządzającego otwieraniem /zamykaniem drzwi), modułu zliczającego osoby, aplikacji mobilnej dedykowanej dla systemu Android oraz serwera operującego na bazie danych. Każdy z podsystemów zostanie przedstawiony w jaki sposób ma funkcjonować, aby przybliżyć działanie systemu względem poszczególnych aktorów systemu (użytkowników, urządzeń).

3.1 Schemat ideowy systemu *Inteligentny zamek*

System łączy ze sobą 5 podsystemów różnymi interfejsami komunikacyjnymi. Urządzenia mobilne komunikują się z urządzeniem sterującym poprzez protokół bluetooth, a pozostałe połączenia oparte są na Ethernetie. Schemat połączeń urządzeń znajduje się na Rys. 1.



Rys. 1: Schemat ogólny systemu

Urządzenia sterujące łączą się z elektrozamkiem lub serwomechanizmem poprzez przewody elektryczne, a z kamerą IP oraz serwerem poprzez sieć LAN. Aplikacja serwerowa nawiązuje połączenie z bazą danych przez lokalny interfejs sieciowy.

3.2 Opis składowych systemu

System ma złożoną budowę, ponieważ składa się z 5 podsystemów. Pierwszym z nich jest urządzenie sterujące, w którego skład wchodzi Raspberry Pi 3 oraz serwomechanizm lub zamek elektroniczny. Podstawową funkcją tego modułu jest weryfikacja klucza cyfrowego przesyłanego przez urządzenia mobilne oraz otwieranie zamka przy pozytywnym wyniku weryfikacji. Każde zdarzenie zapisywane jest w pliku z logami. Oprogramowanie mikrokomputera obejmuje system Linux raspbian-jessie oraz skrypt napisany w języku Python 2.7. Programy łączą się do serwera w celu pobrania informacji o poprawności i dacie ważności certyfikatu dostępowego, następnie dane są porównywane z tymi otrzymanymi od użytkownika. Dodatkowo weryfikowany jest podpis cyfrowy, którym sygnowany jest klucz dostępowy. Jeśli dane zostaną zweryfikowane poprawnie, to zostaje wysterowany serwomechanizm (lub wysłany impuls do elektrozamka), który otwiera zamek, w przeciwnym przypadku użytkownik zostanie poinformowany o odmowie dostępu, a nieudana próba dostania się do systemu zarejestrowana zostanie w bazie danych wraz z danymi właściciela klucza dostępowego.

Drugim elementem jest aplikacja mobilna napisana na platformę Android w wersji minimalnej 5.0. Program ma na celu przechowywanie w pamięci smartphona kluczy cyfrowych (dostępowych) użytkownika oraz umożliwić interakcję użytkownika z systemem.

Kolejnym z elementów jest aplikacja serwerowa wraz z stroną internetową. Rolą serwera w tym systemie jest pośredniczenie w operacjach na danych dostępowych w bazie danych MySQL. Dodatkowo serwer obsługuje stronę internetową, która wyświetla na bieżąco historię użycia zamków w systemie.

Przedostatnim elementem składowym systemu jest baza danych, która przechowuje wszystkie kluczowe informacje systemu oraz udostępnia je serwerowi.

Ostatnim z składowych systemu jest oprogramowanie zliczające liczbę osób wchodzących i wychodzących dla danego pomieszczenia lub całego budynku wraz z kamerą, której zadaniem jest obliczanie informacji o aktualnej liczbie osób w danym pomieszczeniu.

3.3 Podmioty systemu

W pracy dyplomowej można wyodrębnić następujące podmioty:

- Użytkownik niezalogowany — jest to użytkownik, który posiada aplikację mobilną na swoim urządzeniu, lecz nie wykonał procesu logowania,
- Użytkownik niezarejestrowany — jest to użytkownik który wysłał prośbę o zarejestrowanie, lecz nie została ona jeszcze zatwierdzona przez administratora,
- Użytkownik zalogowany — jest to użytkownik, który przeszedł poprawnie proces logowania, posiada on ograniczoną funkcjonalność aplikacji,
- Administrator — jest to użytkownik zalogowany, który posiada uprawnienia administratora, co wiąże się z pełnym dostępem do funkcji aplikacji mobilnej (zawiera funkcje użytkownika zalogowanego),
- Aplikacja serwerowa — jest to oprogramowanie zarządzające całym systemem oraz pośredniczące w przekazywaniu informacji z bazy danych,
- Urządzenie sterujące — jest to oprogramowanie zarządzające dostępem fizycznym do pomieszczeń,
- Elektrozamek — urządzenie umieszczone w futrynie drzwi pozwalające sterować stanem otwarcia zamka,
- Serwomechanizm — silnik krokowy, nakładka na zamek fizyczny w drzwiach, sterujący rygłem w futrynie,
- Moduł zliczania osób — jest to oprogramowanie zwracające w czasie rzeczywistym ilość osób przebywających w danym pomieszczeniu,
- Kamera — urządzenie wizyjne udostępniające obraz do celów zliczania osób.

4 Wybór technologii informatycznych

4.1 Urządzenie sterujące

4.2 Aplikacja serwera

Aplikacja serwerowa została stworzona przy pomocy zintegrowanego środowiska programistycznego PyCharm w wersji 2017.1.3. Technologie użyte w aplikacji serwerowej były następujące:

- python w wersji 2.7
- framework Django
- MySQL – wybór tego rodzaju bazy danych został podyktowany dobrym wsparciem dla środowiska linux oraz frameworka Django,
- HTML5 – jest to podstawowa technologia w stronach internetowych, wybór wersji 5 został podyktowany tym że jest to najnowsza wersja,
- Bootstrap – biblioteka ta została wybrana ze względu na łatwość w użyciu
- JSON –format ten został wybrany z względu na jego prostotę użytkowania oraz wsparcie w postaci, bibliotek.

Ponadto oprogramowanie serwera było testowane przy pomocy narzędzia XAMMP w wersji 3.2.2 które emulowało środowisko apache oraz baze danych MySQL.

4.3 Aplikacja mobilna

Aplikacja mobilna została stworzona przy pomocy zintegrowanego środowiska programistycznego Android Studio w wersji 3.0 wraz z zintegrowanym emulatorem Genymotion w darmowej edycji. Wybór Android Studio został podyktowany tym że jest to oficjalne środowisko dla systemu android natomiast Genymotion został wybrany z powodu trudności z oficjalnym emulatorem w środowisku gdzie występują procesory firmy AMD. Ponadto dla wygenerowania diagramów klas zostało wykorzystane środowisko intelliJ idea w wersji trial 2017 Enterprise ze względu na to że udostępniały taką funkcję. Języki użyte w aplikacji były następujące:

- Java – wybór ten był podyktowany wcześniejszą pracą projektową która opierała się o język java,
- Kotlin – powodem wybrania tego języka był wzrost popularności niego pod względem tworzenia aplikacji androidowych, oficjalne wsparcie firmy google dla tego języka oraz chęć lepszego poznania go,
- XML – środowisko android wymusza w swoim projekcie by wygląd aplikacji był napisany w języku xml,
- JSON – format ten został wybrany z względu na jego prostotę użytkowania oraz wsparcie w postaci bibliotek,

Cała aplikacja ponadto została napisana w oparciu o wzorzec architektoniczny Model View Presenter.

4.4 Moduł zliczania osób

4.5 System kontroli wersji

Podczas tworzenia naszej poracy użyliśmy systemu kontroli wersji GIT wraz z oprogramowaniem dekstopowym przeznaczonym do środowiska windows o nazwie GitHub Dekstop. Wybór ten był podyktowany znajomością tego systemu kontroli wersji oraz dużą popularnością jaką cieszy się w środowisku programistycznym.

4.6 Prowadzenie dokumentacji

Dokumentację prowadziliśmy w języku LaTeX przy pomocy oprogramowania TexStudio. Diagramy UML głównie były generowane przy pomocy programu Visual Paradigme wyjątek tutaj stanowią diagramy klas dla aplikacji mobilnej gdzie zostały one wygenerowane automatycznie przy pomocy środowiska IntelliJ IDEA 2017 w wersji enterprise (trial 30 dniowy)

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 Przechowywanie danych

6.1.2 Graficzna implementacja

6.1.3 Walidacja danych wprowadzanych przez użytkownika

6.2 Aplikacja serwerowa

6.2.1 Strona internetowa

6.3 Urządzenie sterujące

6.4 Moduł zliczania osób

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

1	Schemat ogólny systemu	16
---	----------------------------------	----

Spis tablic

1	Tabela porównania otwierania zamków	12
2	Tabela porównania zasilania i montażu	13
3	Tabela porównania dziennika zdarzeń oraz powiadomień	13

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*.