POLITECHNIKA GDAŃSKA
WYDZIAŁ ELEKTRONIKI, TELEKOMUNIKACJI I INFORMATYKI

Imię i nazwisko studenta: Adrianna Piekarska
Nr albumu: 165152
Studia pierwszego stopnia
Forma studiów: stacjonarne
Kierunek studiów: Informatyka
Profil: Architektura systemów komputerowych

Imię i nazwisko studenta: Grzegorz Wąs
Nr albumu: 165464
Studia pierwszego stopnia
Forma studiów: stacjonarne
Kierunek studiów: Informatyka
Profil: Inteligentne systemy interaktywne

PROJEKT DYPLOMOWY INŻYNIERSKI

Tytuł projektu w języku polskim: Bezprzewodowy system dostępu do pomieszczeń

Tytuł projektu w języku angielskim: Wireless access control system

Potwierdzenie przyjęcia projektu	
Opiekun projektu *podpis*	Kierownik Katedry/Zakładu (pozostawić właściwe) *podpis*
dr inż. Tomasz Dziubich	

Data oddania projektu do dziekanatu:

Streszczenie

Systemy wykorzystujące urządzenia elektroniczne od wielu lat stosowane są we wszystkich dziedzinach ludzkiego życia. Rozwój technologii bezprzewodowych oraz postępująca miniaturyzacja urządzeń elektronicznych sprawiają, że stosowane systemy są nowocześniejsze, bezpieczniejsze i wydajniejsze. Jedną z dziedzin, w których szeroko stosowane są tego typu systemu, jest zapewnienie bezpieczeństwa ludziom oraz mieniu. Niniejsza praca opisuje bezprzewodowy system dostępu do pomieszczeń. Omawia architekturę rozwiązania z uwzględnieniem poszczególnych komponentów, przedstawia ciekawe aspekty realizacji projektu oraz jego rezultaty. Ponadto, prezentuje zagadnienia związane z bezpieczeństwem oraz wydajnością energetyczną bezprzewodowych systemów opartych na mikrokontrolerach.

Słowa kluczowe: zamek elektroniczny, mikrokontroler, kontrola dostępu, WiFi, RFID, sieć bezprzewodowa, autoryzacja

Dziedzina nauki i techniki, zgodnie z wymogami OECD:

Abstract

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language.There is no need for special content, but the length of words should match the language.

Keywords:

Spis treści

Spis rysunków

Spis tablic

Wykaz ważniejszych oznaczeń i skrótów

Pojęcie	Wyjaśnienie
Punkt dostępu	Fizyczne zabezpieczenie chroniące przed nieuprawnionym dostępem, przykładowo: zamek, bramka
RFID	Technologia wykorzystująca fale radiowe w celu przesyłania danych (ang. *Radio-frequency identification*)
Karta	Karta zbliżeniowa RFID. Inne określenia: identyfikator, token
Kontroler	Komponent odpowiedzialny za zarządzanie układem zamka

Rozdział 1

Wstep i cel pracy

Zapewnienie bezpieczeństwa przestrzeni użytkowych i osób z nich korzystających stanowi kluczowy aspekt zarządzania obiektami zarówno publicznymi, jak i prywatnymi. Dzięki zastosowaniu odpowiedniej infrstruktury, bezpieczeństwo osób przebywających na terenie obiektu rośnie, a ryzyko kradzieży lub zniszczenia mienia przez niepowołane osoby spada. Podstawową metodą kontroli dostępu do pomieszczeń są metody mechaniczne wykorzystujące jedynie fizyczne zabezpieczenia. Ze względu na postępujący rozwój technologiczny, w obecnych czasach coraz częściej stosowane są systemy oparte na uwierzytelnianiu elektronicznym.

Pod względem celu i ogólnych zasad działania, elektroniczny system kontroli dostępu do pomieszczeń nie rózni się od swojego tradycyjnego odpowiednika. Głównym celem pozostaje autoryzacja prób dostępu użytkowników na podstawie kluczy w taki sposób, aby dostęp został przyznany tylko osobie posiadającej powiązany z danym punktem dostępu klucz.

Przewagę systemów opartych na urządzeniach elektronicznych nad systemami czysto mechanicznymi stanowią cechy takie jak łatwość obsługi czy możliwość zdalnego zarządzania oraz zbierania danych i monitorowania prób dostępu w celu późniejszej analizy.

Celem niniejszej pracy jest projekt oraz implementacja sytemu dostępu do pomieszczeń z wykorzystaniem technologii takich jak WiFi oraz RFID (ang. *Radio-frequency identification*), w którym podmiotem odpowiedzialnym za autoryzację prób dostępu jest serwer, a komunikacja pomiędzy podsystemem sterowania zamkiem a podsystemem autoryzacji jest realizowana bezprzewodowo. Może on znaleźć zastosowanie jako łatwy w instalacji i obsłudze, lekki i wydajny system dla małych i średnich obiektów.

Podstawowe założenia dotyczące opisywanego systemu są następujące:

1. Logika uwierzytelniania powinna być zaimplementowana na serwerze. Urządzenie klienckie (zamek) powinno pełnić jedynie rolę pośrednika w tym procesie.

2. Komunikacja pomiędzy urządzeniami klienckimi (zamkami) a serwerem powinna odbywać się bezprzewodowo.

3. System powinien być wydajny energetycznie i umożliwiać operację zamków na zasilaniu

bateryjnym.

4. System powinien implementować niezbędne mechanizmy bezpieczeństwa.

Dzięki wykorzystaniu zdalnego serwera do przeprowadzenia procesu uwierzytelniania system zapewnia większą elastyczność i łatwość zarządzania niż alternatywne systemy wykorzystujące zamki pracujące w sposób autonomiczny. Informacje o uprawnieniach przechowywane są w centralnej bazy danych, znajdującej się na serwerze, którą można w prosty sposób zarządzać z poziomu aplikacji internetowej.

Rozwiązanie cechuje się wygodą montażu, ponieważ nie wymaga przewodów zasilających i komunikacyjnych prowadzonych w ścianach budynków. Przy wdrażaniu rozwiązania nie jest konieczna modyfikacja istniejącej infrastruktury budynku, z wyjątkiem wymiany samych zamków. System nie wymaga żadnych dodatkowych komponentów sprzętowych poza zamkami i serwerem. Do poprawnego działania systemu potrzebna jest sieć WiFi. Założono, że wykorzystana sieć nie musi być bezpieczna.

Wydajność energetyczna podsystemu sterowania zamkiem została osiągnięta przez zarządzanie zasilaniem jego peryferiów oraz kontrolę stanu zasilania mikrokontrolera w celu minimalizacji poboru mocy i maksymalizacji czasu pracy na zasilaniu bateryjnym.

Bezpieczeństwo systemu na wielu poziomach zapewnia wykorzystanie mechanizmów takich jak TLS (ang. *Transport Layer Security*) w warstwie komunikacji pomiędzy zamkiem a serwerem czy szyfrowanie pamięci Flash w warstwie operacji na danych w mikroprocesorze w układzie zamka.

1.1 Zakres pracy

Pracę nad systemem prowadziły dwie osoby. W ramach tej pracy powstały:

- Protoyp układu zamka,
- Implementacja logiki uwierzytelniania,
- Implementacja prostej aplikacji do zarządzania. **???????**

Praca nie obejmuje zdefiniowania zachowania systemu w przypadkach awarii. Zachowanie to można zdefiniować w dowolny sposób i rozszerzyć prototyp o mechanizmy niezbędne do jego wsparcia.

tutaj cos o podziale pracy

1.2 Struktura pracy

Rozdział 2 pokrótce przedstawia dziedzinę problemu, przywołuje najważniejsze definicje związane z tematem oraz ogólny opis działania systemów kontroli dostępu. Dokonuje także przedstawienia oraz porównania kilku istniejących na rynku rozwiązań.

Rozdział 3 prezentuje projekt rozwiązania.

Rozdział 4 przedstawia proces implementacji systemu wraz z prezentacją najciekawszych problemów implementacyjnych oraz wykorzystanych technologii. W ramach pracy zaimplementowany został prototyp rozwiązania. Rozdział prezentuje również możliwe modyfikacje i rozszerzenia tego prototypu.

Rozdział 2

Dziedzina problemu

Systemy kontroli dostępu stanowią kluczowy aspekt infrastruktury bezpieczeństwa. Wprowadzane są z różnych powodów oraz w różnych celach. Niniejszy rozdział krótko opisuje dziedzinę problemu w oderwaniu od szczegółów technicznych przygotowanego w ramach pracy rozwiązania. Przedstawia również porównanie niektórych z obecnie dostępnych na rynku systemów kontroli dostępu.

2.1 Kontrola dostępu

Kontrola dostępu to środki mające na celu zapewnienie, że do zasobów systemu przetwarzania danych mogą mieć dostęp tylko uprawnione jednostki w uprawniony sposób [1]

British Security Industry Association wyodrębnia kilka komponentów składających się na system kontroli dostępu [2]. Poniżej przedstawiono wybrane komponenty, które mają zastosowanie lub są powiązane z opisywanem systemem.

Poświadczenie tożsamości (ang. *credentials*) to fizyczny lub materialny obiekt, element wiedzy lub cecha biometryczna umożliwiająca uzyskanie dostępu do kontrolowanej strefy. Najczęściej jako poświadczenie tożsamości stosuje się kody, np. PIN (ang. *Personal Identification Number*, osobisty numer identyfikacyjny), tokeny (karty, urządzenia mobilne itp.) oraz dane biometryczne. [2]

British Security Industry Association terminem czytniki(ang. *readers*) nazywa urządzenia odpowiedzialne za kontrolę dostępu. Dla uproszczenia nomenklatura ta została zachowana w niniejszej sekcji. W innych częściach niniejszej pracy termin czytnikużywany jest w znaczeniu urządzenia odpowiedzialnego za odczyt danych z nośnika. **czy tak moze byc?**

Czytniki mogą pracować samodzielnie. Wyposażone są wówczas w urządzenia wejścia/wyjścia niezbędne do zarządzania zamkiem oraz pamięć i moc obliczeniową niezbędne do autonomicznego podejmowania decyzji. Zazwyczaj wyposażone są w uniwersalny kod umożliwiający uzyskanie dostępu każdemu kto wejdzie w jego posiadanie. [2]

Czytniki mogą też pracować pod kontrolą innego urządzenia. Odczytane z nośnika dane po-

świadczające tożsamość przekazują do nadrzędnego urządzenia zwanego kontrolerem. [2]

Istnieją również czytniki łączące funkcjonalność zarówno czytnika jak i kontrolera w jednym urządzeniu. Posiadają one lokalną kopię bazy danych, na podstawie której podejmowana jest decyzja o przyznaniu lub odmowie dostępu. [2]

Tzw. czytniki offline (ang. *offline readers*) różnią się od zwykłych czytników łączących funkcjonalności czytnika i kontrolera tym, iż nie przechwoują kopii bazy danych. W tym przypadku to nośnik danych(karta) zawiera informacje o tym, które zamki może otworzyć. Czytnik offline analizuje te dane i na ich podstawie podejmuje stosowną decyzję o podjęciu lub odmowie dostępu. [2]

Czytniki online (ang. *online readers*) także nie przechowują kopii bazy danych. Decyzja o przyznaniu lub odmowie dostępu jest w ich przypadku podejmowana przez podłączony komputer, który przesyła odpowiednią komendę po udanej autentykacji. [2]

W rozwiązaniach sieciowych czytniki mogą być podłączone do kontrolera, który przechowuje informacje niezbędne do podjęcia decyzji o przyznaniu bądź odmowie dostępu. [2]

Urządzenia wyjściowe (ang. *egress devices*) umożliwiają użytkownikowi opusczenie strefy chronionej od wewnątrz. Jako urządzenia wyjściowe najczęściej używa się przełączników, czujników ruchu lub czytników. Według British Security Industry Association urządzenia wyjściowe można podzielić je na zwykłe oraz awaryjne (ang. *emergency egress*), przy czym, ze względu na krytyczne znaczenie w wypadku awarii, działanie tych drugich nie powinno zależeć od komponentów systemu (kontrolera systemu, oprogramowania itp.). Jako urządzenie awaryjne często stosuje się tzw. *break glass device*, którego uaktywnienie powoduje odcięcie zasilania w zamku, a tym samym wstrzymanie kontroli dostępu w danym punkcie. Dostęp uzyskany za pomocą tego urządzenia powinien wygenerować stosowne powiadomienie bądź alarm. [2]

W zależności od potrzeb, oprogramowanie w systemie może być samodzielnym programem zainstalowanym na komputerze osobistym bądź złożone i bezpieczne oprogramowanie zainstalowane na serwerze. Często opiera się na rozwiązaniach webowych lub mobilnych, umożliwiając dostęp z dowolnego urządzenia. [2]

British Security Industry Association w następujący sposób przedstawia sposób działania systemów kontroli dostępu:

W systemie on-line, w momencie gdy poświadczenie tożsamości zostaje przedstawione czytnikowi, informacja przesyłana jest do kontrolera. Kontroler porównuje otrzymane dane z listą autoryzowanych użytkowników w bazie danych. Jeżeli przedstawione dane znajdują się w bazie, kontroler wysyła sygnał otworzenia zamka. Sygnał wysyłany jest do czytnika w celu wizualnego lub dźwiękowego powiadomienia użytkownika o podjętej decyzji. [2]

W systemie off-line, w momencie gdy poświadczenie tożsamości zostaje przedstawione czytnikowi, czytnik dokonuje sprawdzenia, czy dostęp powinien zostać przyznany. Jeżeli tak, czytnik zezwala na dostęp i aktualizuje przedstawiony nośnik danych poświadczających tożsamość. W momencie zaprezentowania tego samego nośnika w czytniku wyposażonym w kontroler dane na temat dostępów zostaną zanotowane w systemie, a sam nośnik może zostać zaktualizowany o zmiany w prawach dostępu, jeśli takie nastąpiły. [2]

W większości przypadków tylko wejście podlega kontroli. Aby możliwa była również kontrola wyjścia z chronionego terenu, potrzebny jest drugi czytnik umieszczony po drugiej stronie drzwi. Jeżeli obustronna kontrola nie jest wymagana, stosuje się zazwyczaj przycisk umożliwiający otworzenie zamka od środka. [2]

W przypadku, gdy system kontroli dostępu nie funkcjonuje odpowiednio (np. z powodu braku zasilania), stosuje się tzw. *break glass device*. [2]

2.2 Przegląd dostępnych rozwiązań

Obecnie stosowane rozwiązania różnią się od siebie pod wieloma względami. W mniej wymagających systemach często stosuje się rozwiązania oparte są na architekturze rozproszonej. W rozwiązaniach tego typu urządzenia kontrolujące zamki pracują w sposób autonomiczny. Oznacza to, iż cały proces uwierzytelniania dokonywany jest przez oprogramowanie mikroprocesora obsługującego zamek.

Na rynku dostępne są także rozwiązania sieciowe, bądź też takie, które umożliwiają konfigurację urządzeń w tryb zarówno autonomiczny, jak i sieciowy. Rozwiązania sieciowe charakteryzują się znacznym stopniem skomplikowania, zarówno pod względem architektonicznym (ilość i rodzaj potrzebnych komponentów sprzętowych) [3], jak i konfiguracyjnym (trudność instalacji, konieczność modyfikacji istniejącej infrastruktury). Mogą oferować oddzielenie funkcjonalności czytnika dostępu od kontrolera, umożliwiając obsługę do kilkunastu czytników za pomocą jednego urządzenia kontrolującego [3]. Mimo możliwości dołączenia do kontrolera zamków bezprzewodowych, działanie całego systemu wciąż pozostaje uzależnione od komunikacji przewodowej.

Ze względu na ilość komponentów sprzętowych, istniejące rozwiązania bywają drogie.

Rozdział 3

Projekt rozwiązania

Niniejszy rozdział opisuje koncept rozwiązania, który powstał w ramach pracy. Ogólny zarys konceptu działania systemu przedstawiony jest na rysnku 3.1.

3.1 Architektura systemu

W ramach systemu można wyodrębnić następujące podsystemy:

1. Podsystem sterowania zamkiem,
2. Podsystem autoryzacji,
3. Podsystem zarządzania.

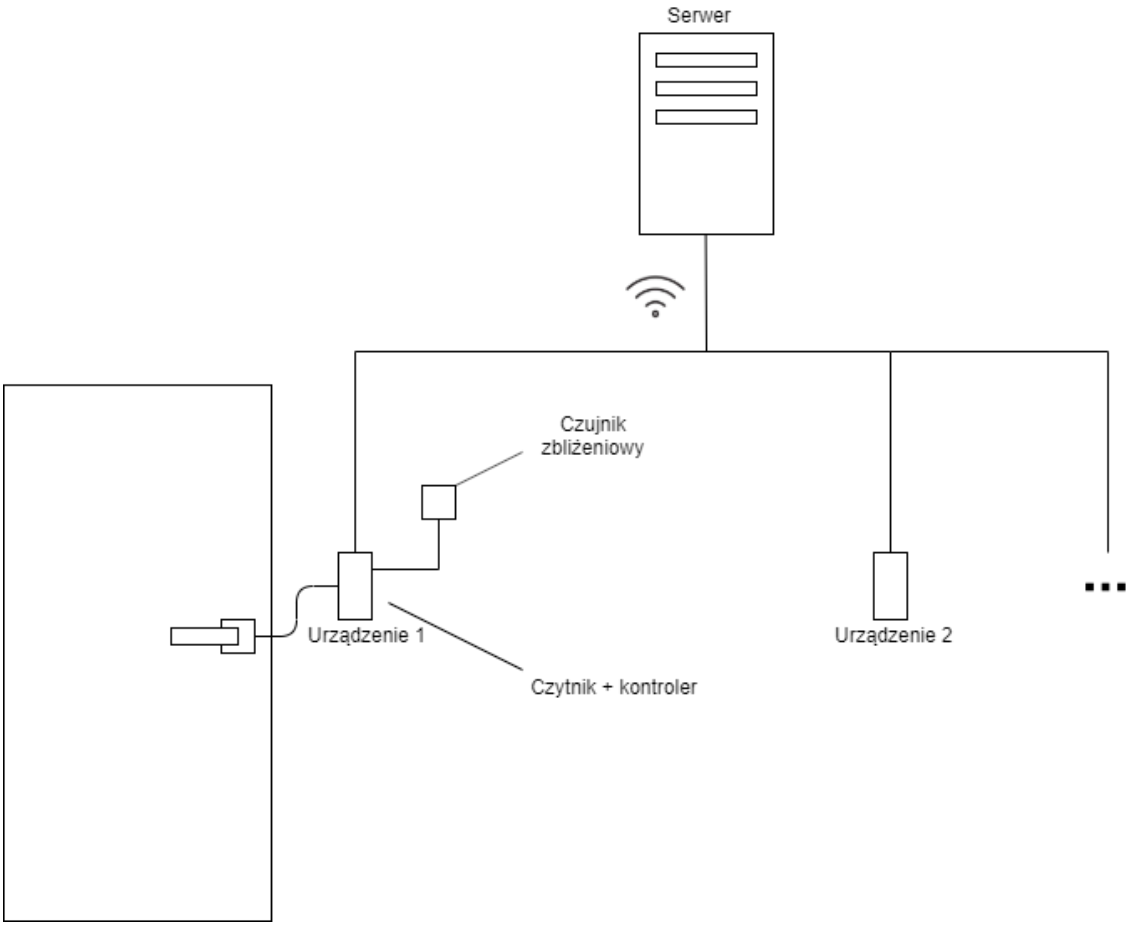
Podsystemy te istnieją w ramach komponentów sprzętowych. Są to:

1. Komponent sterujący zamkiem (inaczej: kontroler, układ zamka),
2. Komponent serwera.

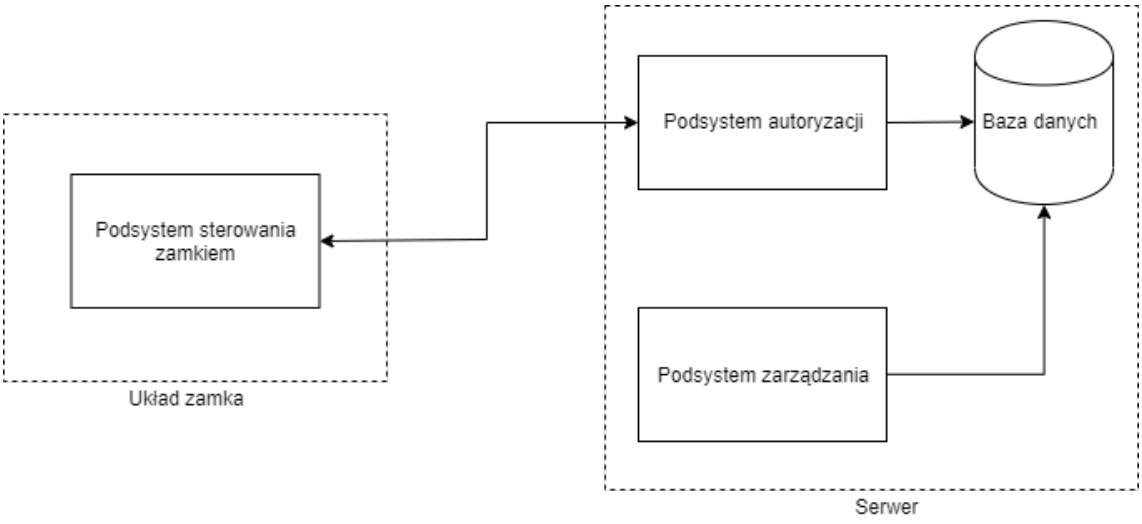
Komponenty te zostały krótko omówione w kolejnych punktach. Ogólna sprzętowa architektura systemu z podziałem na komponenty sprzętowe oraz przynależne im podsystemy przedstawiona została na rysunku 3.2.

3.1.1 Komponent sterujący zamkiem

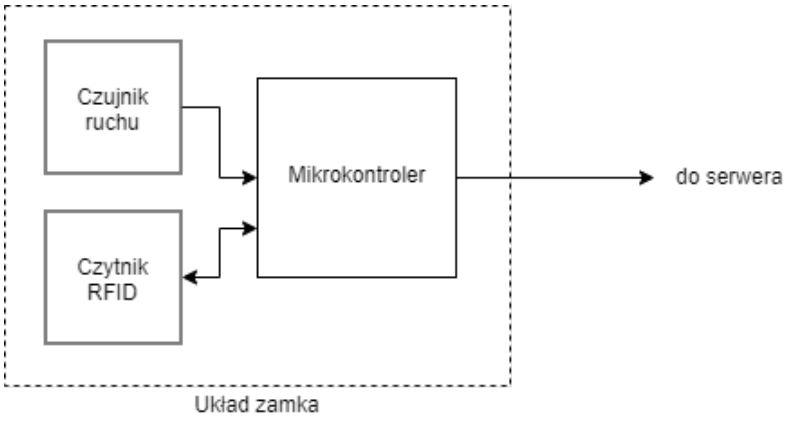
Komponent sterujący zamkiem składa się z mikrokontrolera, czujnika ruchu oraz czytnika RFID. Mikrokontroler odpowiada za sterowanie peryferiami, zarządza ich zasilaniem, inicjuje i przeprowadza bezprzewodową komunikację z serwerem i steruje samym zamkiem na podstawie otrzymanych od serwera danych. Podsystem sterowania zamkiem zlokalizowany jest w całości w tym komponencie (patrz rysunek 3.2). Architektura układu zamka została przedstawiona na rysunku 3.3.



Rysunek 3.1: Koncept systemu kontroli dostępu



Rysunek 3.2: Architektura systemu



Rysunek 3.3: Architektura układu zamka

3.1.2 Serwer główny

W ramach komponentu serwera działają dwa podsystemy funkcjonalne: podsystem autoryzacji, odpowiedzialny za podjęcie decyzji o przyznaniu lub odmowie dostępu na podstawie danych odebranych od podsystemu sterowania zamkiem, oraz podsystem zarządzania, odpowiedzialny za zbieranie oraz prezentację danych użytkownikowi.

Baza danych

Częścią komponentu serwera jest baza danych. Nie jest jednak konieczne, aby pozostawała ona fizycznie na tej samej maszynie. W przypadku całkowitego rozdzielenia serwera danych od serwera autoryzacji skalowalność systemu znacząco wzrośnie.

Podsystem autoryzacji

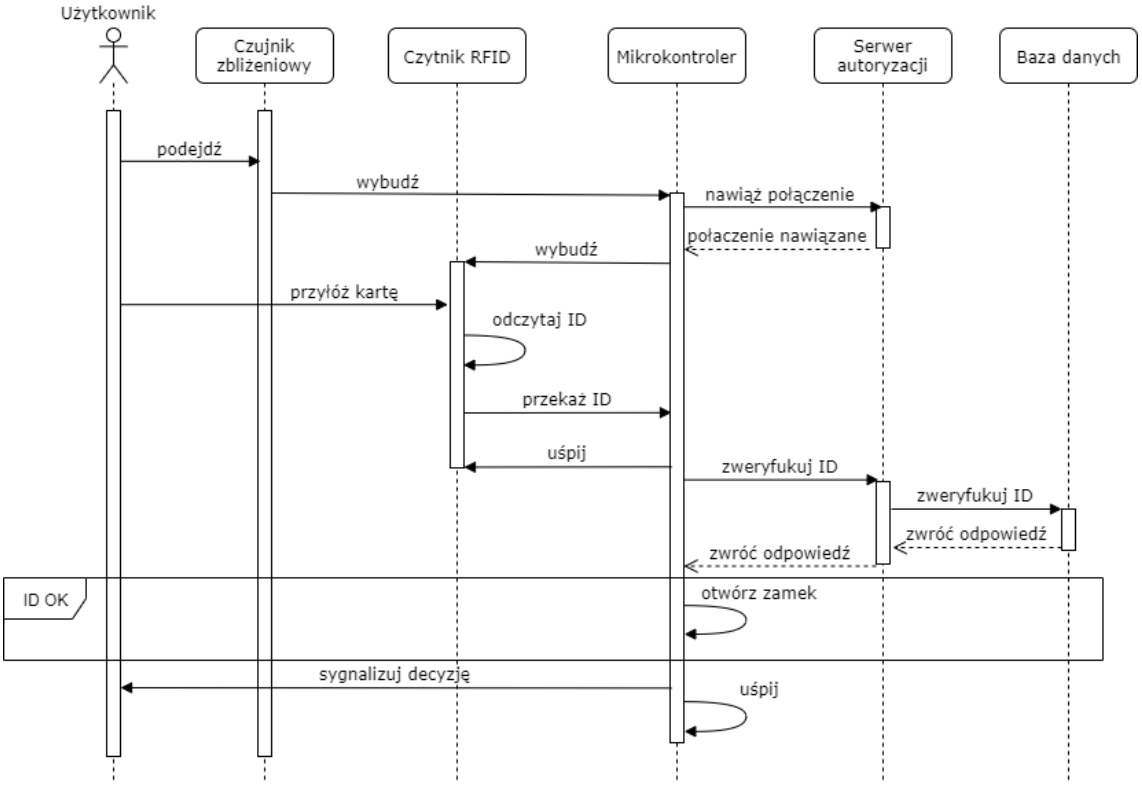
Zadaniem podsystemu autoryzacji jest podjęcie decyzji o przyznaniu bądź odmowie dostępu na podstawie otrzymanych danych. Podsystem komunikuje się z bazą danych w celu uzyskania informacji na temat autoryzowanych kart.

Podsystem zarządzania

Zadaniem podsystemu zarządzania jest umożliwienie użytkownikowi systemu wglądu do danych takich jak historia prób dostępu, zbiór zamków, kart oraz powiązań między nimi, oraz stan poszczególnych zamków.

3.2 Zasada działania

Kontroler wbudowany w zamek pozostaje uśpiony do momentu wykrycia ruchu w pobliżu przez wbudowany czujnik ruchu. Po wybudzeniu nawiązuje bezpieczne połączenie z serwerem autoryzacji, jednocześnie zasilając czytnik RFID oraz oczekując na zbliżenie do niego karty. Gdy karta



Rysunek 3.4: Diagram sekwencji ukazujący zasadę działania systemu

zostanie zbliżona, kontroler przesyła odczytany z niej numer identyfikacyjny do serwera, korzystając z nawiązanego wcześniej połączenia. Serwer podejmuje decyzję, którą jest przyznanie bądź odmowa dostępu, porównując odebrany numer identyfikacyjny z zawartością bazy danych, a następnie przesyła informację zwrotną do kontrolera. Jeżeli podjęto decyzję o przyznaniu dostępu, kontroler wysyła sygnał otwarcia zamka oraz sygnalizuje powodzenie. Jeżeli podjęto decyzję o odmowie dostępu, kontroler sygnalizuje niepowodzenie. Diagram sekwencji przedstawiony jest na rysunku 3.4.

Rozdział 4

Implementacja

4.1 Uproszczenia

W ramach niniejszej pracy stworzony został prototyp końcowego rozwiązania. Niektóre z opisywanych w rozdziale 3 funkcjonalności nie zostały zaimplementowane. Zostawiono jednak możliwość rozbudowy systemu.

Opisywane rozwiązanie nie obejmuje implementacji mechanizmu opuszczenia strefy chronionej systemem kontroli dostępu. W zależności od potrzeb końcowego użytkownika, możliwe rozwiązanie to montaż dodatkowego czytnika po przeciwnej stronie drzwi i połączenie go z kontrolerem wejścia w przypadku gdy wymagana jest obustronna kontrola dostępu bądź zastosowanie przycisku którego naciśnięcie powoduje zwolnienie zamka w przypadku gdy wymagana jest tylko kontrola wejścia do chronionego obszaru.

W sytuacjach awaryjnych, jakimi jest brak zasilania bądź brak połączenia z serwerem **wymyslic co**. Szczegółowy opis tych zagadnień znajduje się **gdziee?**.

Implementacja prototypu obejmowała stworzenie pojedynczego układu zamka. Ze względu na prototypowy charakter pracy, nie przetestowano działania systemu z większą liczbą zamków. Nie ma jednak powodów by twierdzić, że system nie działałby poprawnie z większą liczbą zamków. Wystarczającym rozszerzeniem byłaby modyfikacja oprogramowania serwera umożliwiająca obsługę kilku klientów jednocześnie. **czy to pisac?**

4.2 Układ sterowania zamkiem

Prototyp układu sterowania zamkiem powstał w oparciu o platformę ESP32-DevKitC-32D z wbudowanym modułem ESP-WROOM-32D.

4.2.1 Platforma

ESP32-DevKitC jest produkowaną przez firmę Espressif platformą z wbudowanym modułem ESP32-WROOM-32D. Rdzeniem modułu jest układ z rodziny ESP32 (ESP32-D0WD) wyposa-

żony w dwa rdzenie CPU, które mogą być kontrolowane niezależnie od siebie [4]. Moduł integruje Bluetooth, Bluetooth Low Energy oraz WiFi, a także szeroki zakres peryferiów: czujniki dotyku, czujniki pola magnetycznego, interfejs karty SD, Ethernet, SPI (ang. *Serial Peripheral Interface*), UART (ang. *Universal Asynchronous Receiver-Transmitter*), I^2S (ang. *Inter-IC Sound*) i I^2C (ang. *Inter-Integrated Circuit*) [4].

ESP32 działa w oparciu o system operacyjny freeRTOS.

ESP32 oferuje efektywną i elastyczną technologię zarządzania energią. Istnieje pięć predefiniowanych stanów energetycznych. Dodatkowo umożliwia korzystanie z niskoenergetycznego koprocesora Ultra-Low-Power (ang. *ULP co-processor*), podczas gdy główne jednostki pozostają w trybie głębokiego uśpienia (ang. *Deep-sleep mode*). [5]

4.3 Problemy

Konfiguracja WiFi? Sygnalizacja stanu baterii? Bezpieczeństwo komunikacji zarządzanie stanami energetycznymi Enkrypcja flash mozna cos z technical reference manual

Bibliografia

[1] Polski Komitet Normalizacyjny, *Technika informatyczna. Zabezpieczenia w systemach informatycznych. Terminologia*, Marzec 2002.

[2] British Security Industry Association, *A specifier's guide to access control systems*, Kwiecień 2016.

[3] Roger sp. z o.o. sp. k., *Przewodnik po systemie RACS 5.* v5.3 (dostęp 20.10.1019).

[4] Espressif Systems, *ESP32-WROOM-32D & ESP32-WROOM-32U Datasheet*, 2018. Version 1.7.

[5] Espressif Systems, *ESP32 Technical Reference Manual*, 2018. Version 4.0.