

System kontroli obecności na podstawie elektronicznych legitymacji studenckich

(Students attendance verifying system with the use of electronic student's
card)

Dawid Szczyrk

Praca magisterska

Promotor: dr Jakub Michaliszyn

Uniwersytet Wrocławski
Wydział Matematyki i Informatyki
Instytut Informatyki

7 września 2020

Streszczenie

Projekt wykonany w ramach tego opracowania przedstawia realizację narzędzia umożliwiającego weryfikację uczestników wykładu na podstawie Elektronicznej Legitymacji Studenckiej.

Poniższa praca referuje proces od analizy problemu i postawienia wymagań do realizacji finalnej wersji wielokomponentowego projektu. Na efekt ostateczny składają się aplikacje wykorzystujące technologie webowe, oparte na popularnych frameworkach języka PHP oraz niskopoziomowe elektroniczne urządzenie zaprojektowane i wykonane na potrzeby tego projektu z wykorzystaniem platformy Arduino.

Pierwszym z elementów składających się na finalne rozwiązanie jest urządzenie elektroniczne - weryfikator, udostępniające zrozumiały interfejs użytkownika i realizujące zadania związane ze zbieraniem danych od uczestników wykładu. Zostało ono wykonane w oparciu o płytkę Arduino Uno rozszerzoną o dodatkowe komponenty w tym czytnik RFID i USB Host Shield. Całość układu, wraz z interfejsem do komunikacji z użytkownikiem, została połączona przy pomocy płytki stykowej i opakowana w sposób umożliwiający sprawne użytkowanie oraz wygodny transport.

Dodatkowo w ramach referowanego projektu wykonano internetową aplikację - elektroniczny dziennik - umożliwiającą katalogowanie zebranych przy pomocy weryfikatora obecności. Użytkownikowi umożliwiono zarejestrowanie indywidualnego konta w serwisie, w którego kontekście możliwe jest tworzenie struktury wykładów i zajęć odpowiadającej rzeczywistemu kalendarzowi prowadzącego. Aplikacja została wykonana przy użyciu frameworka języka PHP - Yii2. Wirtualny dziennik nie przechowuje informacji o studentach i do poprawnego działania wymaga dostępu do serwisu udostępniającego takie dane.

Podczas pracy nad projektem nie było możliwości podłączenia się do żadnego istniejącego systemu uczelnianego udostępniającego dane studentów. Z tego powodu, jako element projektu, została stworzona aplikacja - w oparciu o framework Symfony4 - umożliwiająca pobranie danych studenta i udostępniająca w tym celu RESTowe API.

Obie stworzone aplikacje wraz z połączonymi z nimi bazami danych osadzone zostały w chmurze w sposób zapewniający bezpieczeństwo i niezawodność.

Within the following project, a student attendance verification system with usage of Electronic Students Card (ESC) was developed.

The presented work describes a process from problem analysis and demands defining to developing the final version of a multi-component project. The final system consists of Internet applications for collecting and managing students presence data, and an electronic device made for this project with the usage of the Arduino platform.

The electronic device - the verifier - provides a comprehensive user interface and is responsible for collecting data about student presences. The final circuit was made based on the Arduino Uno board, extended with plenty of additional parts such as an RFID module and USB Host Shield. All interconnected parts were put in a plastic box to make it comfortable for use and transportation.

For managing data collected by the verifier, an internet application was developed. It allows a user to create an account, and manage presences data in its context. It is possible to create a composition of lectures and classes, which corresponds with the real calendar of a lecturer. It was developed with the usage of the PHP framework - Yii2.

It was designed not to relate to concrete student's data management system, to be flexible about a university system it is connected with.

Additionally, a system which allows correlation of Electronic Student Card UID with information about students was developed. It takes the role of student data management system, and provides REST API, to retrieve demanded information. It was created based on the PHP framework - Symfony4.

Both created services along with data bases connected with each of them were deployed in the cloud system with respect to proper security and reliability standards.

Spis treści

1. Wprowadzenie	7
2. Analiza problemu	9
2.1. Przegląd obecnego sposobu sprawdzania obecności	9
2.2. Istniejące i możliwe realizacje zagadnienia	10
2.2.1. Podłączenie czytnika RFID bezpośrednio do komputera . . .	10
2.2.2. Podłączenie przy pomocy kabla ethernetowego	11
2.2.3. Samodzielny czytnik	12
2.2.4. Aplikacja internetowa	12
2.2.5. Urządzenie rejestrujące obecności za pośrednictwem sieci bez- przewodowej	12
2.3. Określenie wymagań wobec projektu	13
3. Określenie struktury projektu	15
4. Realizacja	17
4.1. Weryfikator - czytnik legitymacji studenckich	17
4.1.1. Zastosowana platforma i peryferia	17
4.1.2. Konstrukcja	18
4.1.3. Działanie	20
4.1.4. Napotkane problemy	23
4.1.5. Inne koncepcje weryfikatora	25
4.2. Elektroniczny dziennik	26
4.3. Baza studentów	29

4.3.1. Funkcjonowanie	30
4.3.2. Udostępnione API	30
4.4. Propozycja wdrożenia systemu	31
4.5. Narzędzie wykorzystane w trakcie realizacji	32
5. Możliwość dalszego rozwoju systemu	33
5.1. Powiązania pomiędzy instancjami wykładu	33
5.2. Zautomatyzowana weryfikacja	33
5.3. Integracja z uczelnianym systemem	34
5.4. Udostępnienie systemu studentom	34
5.5. Informowanie zainteresowanych o obecnościach	34
5.6. Platforma do szybkiego reagowania	34
6. Podsumowanie	37
Bibliografia	39

Rozdział 1.

Wprowadzenie

Zgodnie z ustępem 3 paragrafu 2 zarządzenia nr 116/2020 rektora Uniwersytetu Wrocławskiego [9] podczas wszystkich zajęć na uczelni, które odbywają się w formie stacjonarnej lub hybrydowej obligatoryjne jest prowadzenie listy obecności uczestników zajęć.

Panująca na świecie pandemia COVID-19 zmusiła ludzi do porzucenia wielu do tej pory dobrze sprawdzających się rozwiązań na rzecz takich, które pomogą zapobiec rozprzestrzenianiu się wirusa. Gospodarki i codzienne życie ludzi zostały przedstawione na tryby tzw. nowej normalności.

W niemniejszym stopniu obecna sytuacja dotknęła pracy uniwersytetów. Po okresie zdalnego nauczania, wraz z nowym rokiem akademickim tradycyjne formy nauczania wracają do sal wykładowych, a troska o bezpieczeństwo studentów i pracowników uniwersytetu narzuca reorganizację życia akademickiego.

Jednym z elementów funkcjonowania instytucji naukowych, który powinien zostać dostosowany do nowych wymogów sanitarnych, jest prowadzenie listy obecności na zajęciach stacjonarnych. Obecna forma realizowana poprzez podawanie sobie przez studentów kartki, na której spisane zostają ich dane, prowokuje dodatkowe niebezpieczeństwo zakażenia wirusem.

Dodatkowym motywatorem, zachęcającym do usprawnienia obecnego rozwiązania, jest cytowane na początku zarządzenie rektora Uniwersytetu Wrocławskiego ustalające, że od semestru zimowego 2020 na wszystkich prowadzonych zajęciach obowiązkowe jest zbieranie listy obecności.

Względy zdrowotne nie są jedynym uzasadnieniem konieczności optymalizacji identyfikowania osób biorących udział w zajęciach. Obecna forma tego procesu jest uciążliwa, zajmuje kilka pierwszych minut zajęć, a studenci się rozpraszają podając sobie listę obecności. Istotnym czynnikiem, który należy wziąć pod uwagę jest również ochrona danych osobowych, do której w dzisiejszym świecie przykładą się coraz większą wagę.

W dobie współczesnych zdobyczy technologicznych można uznać za zaskakujące, że wciąż trwamy przy tym procesie. Wydawać by się mogło, że obecne podej-

ście jest tak zakorzenione w akademickiej kulturze, że nie ma możliwości go zmienić. Istnieją jednak opracowania, które wskazują, że warto jest wdrażać nowoczesne rozwiązania, ponieważ ma to bezpośrednie przełożenie na prędkość sprawdzania obecności [7]. Zostało dodatkowo sprawdzone [1], że obecność ma wprost proporcjonalny wpływ na wyniki w nauce i odsetek uczniów porzucających studia przed ich ukończeniem. Wskazane zostało, że sprawdzanie obecności ma znaczenie nie tylko jako forma przymusu, ale również jako wyraz troski uczelni o swoich studentów i ma wpływ na ich morale.

Rozdział 2.

Analiza problemu

2.1. Przegląd obecnego sposobu sprawdzania obecności

W celu doprecyzowania wymagań stawianych przed projektowanym systemem postanowiono rozważyć proces weryfikowania obecności na zajęciach prowadzonych przez Uniwersytet Wrocławski

Sprawdzanie listy obecności jest w dużej mierze uzależnione od preferencji prowadzącego i zwyczajów panujących na konkretnym wydziale - przykładowo obecność może być potwierdzona słownie - poprzez kolejne wywołanie osób z listy albo pisemnie - poprzez udostępnienie listy, na którą uczestnicy będą zobowiązani się wpisać.

Dla uproszczenia dalszych rozważań przyjęto za ogólnie stosowaną metodę pisemną - która według obserwacji autora jest stosowana częściej - i na tej podstawie wyodrębnić czynności, które składają się na wypełnienie listy obecności podczas zajęć.

Zbieranie informacji o obecności studentów na wykładzie jest czynnością na pozór oczywistą, po bliższym przyjrzeniu się całej procedurze okazuje się jednak, że daje się ona rozłożyć na jeszcze prostsze elementy.

- Przygotowanie kartki z listą obecności (przypisanie listy obecności do zajęć których będzie ona dotyczyła).
- Udostępnienie kartki uczestnikom oraz wpisywanie się na listę.
- Weryfikacja poprawności zebranej listy poprzez przeliczenie osób obecnych na zajęciach.
- Przeniesienie zebranych danych do uczelnianego systemu.

Powyższy schemat zbierania listy obecności podatny jest na dodatkowe błędy. Nie trudno wyobrazić sobie sytuację w której student intencjonalnie podał nie swoje

dane w celu zaliczenia obecności innej osobie. Kolejnym czynnikiem, który może doprowadzić do błędów na ostatecznej liście obecności jest błąd ludzki podczas przenoszenia danych z kartki do uczelnianego systemu komputerowego. Taki błąd trudno jest od razu wychwycić ze względu na to, że studenci zazwyczaj nie przeglądają na bieżąco list obecności dostępnych np. na USOSie.

Pierwszym elementem nadającym się do usprawnienia jest samo tworzenie listy obecności z informacją na temat zajęć, których taka lista będzie dotyczyła. Fizyczna lista, poza czasem poświęconym na jej stworzenie, musi być po odbytych zajęciach przechowywana - co stwarza ryzyko jej zgubienia. Dodatkowo istnieje prawdopodobieństwo, że trafi w niepowołane ręce i ktoś wpisze na nią dodatkowe nazwiska. Do tego wszystkiego dochodzi jeszcze aspekt ekologiczny, ponieważ każda kolejna kartka generuje wymagające utylizacji śmieci.

Również udział studentów w rejestrowaniu własnej obecności może ulec optymalizacji. Wpisanie własnego imienia i nazwiska, a czasem numeru albumu zabiera czas, naraża na upublicznienie dane osobowe i utrudnia studentowi śledzenie wykładu.

Weryfikacja poprawności listy jest nie tylko pracochłonna, ale również podatna na błędy. Czas poświęcony na policzenie uczestników rośnie wprost proporcjonalnie do ich liczby. Dodatkowo prowadzący zajęcia może się pomylić lub ktoś może dopisać się do listy już po tym sprawdzeniu.

Z całą pewnością usprawnienia wymaga proces przenoszenia danych z fizycznego nośnika do uczelnianego systemu komputerowego. Problemem jest nie tylko to, że podczas wpisywania obecności do komputerowego systemu można popełnić błąd, ale również to, że jest to proces czasochłonny.

2.2. Istniejące i możliwe realizacje zagadnienia

2.2.1. Podłączenie czytnika RFID bezpośrednio do komputera

Popularnym pomysłem usprawniającym system weryfikacji obecności jest skorzystanie technologii RFID (Radio-frequency identification). Wykorzystuje ona pole elektromagnetyczne do śledzenia na niewielkie odległości tagów (etykiet) RFID - małych transponderów fal radiowych zdolnych do przechowywania danych umożliwiających zdalną identyfikację [8]. Tagi często mają formę kart, breloków lub innych łatwych w transporcie i przechowywaniu przedmiotów.

W opracowaniu [6] przedstawiono projekt weryfikatora obecności zrealizowany przy pomocy radio technologii. Każdemu studentowi został przypisany tag z unikatowym identyfikatorem. System składa się z czytnika etykiet podłączonego do komputera przy użyciu portu szeregowego oraz aplikacji komputerowej, zdolnej do rozpoznawania zbliżonych do czytnika tagów i zapamiętywania którzy studenci zeskanowali swoje karty w trakcie zajęć.

Ciekawym pomysłem przedstawionym w tym projekcie jest przekazanie osobnego tagu prowadzącemu zajęcia. Zbliżenie tej etykiety na początku i na końcu zajęć do czytnika wyznacza ramy czasowe, podczas których obecność może zostać zaliczona studentom. Dodatkowo zastosowano tutaj podejście, w którym uczestnik powinien rejestrować swoje pojawienie się, jak i opuszczenie zajęć - jest to odstępstwo od tradycyjnej formy zbierania obecności.

W projekcie można zaobserwować kilka wad. Wykorzystany czytnik RFID jest urządzeniem w całości dostarczonym przez producenta. Można spodziewać się że jest to rozwiązanie drogie, a samego urządzenia nie będzie dało się rozszerzyć o dodatkowe funkcjonalności.

Taka architektura pociąga za sobą konieczność ciągłego połączenia z komputerem oraz dodatkowego okablowania. Może to powodować problemy logistyczne, jeśli trzeba korzystać z systemu w różnych salach.

Sama aplikacja komputerowa katalogująca zebrane obecności również poddana jest ograniczeniom. Korzystanie z tego systemu możliwe jest wyłącznie na komputerach, na których zainstalowano taką aplikację, co jest rozwiązaniem uciążliwym. Baza danych zapamiętująca obecności współdzielona jest pomiędzy poszczególne instancje aplikacji na różnych komputerach, jest więc ona udostępniona publicznie, co ułatwia nieautoryzowany dostęp.

2.2.2. Podłączenie przy pomocy kabla ethernetowego

W opracowaniu opisanym w pracy [4] zaproponowano podobną realizację, tym razem w oparciu o bezpośrednie podłączenie czytnika do internetu kablem RJ45. Wykorzystywane urządzenie jest stworzone na bazie Arduino Uno rozszerzonym o moduł RFID i gniazdo pozwalające podłączyć kabel ethernetowy.

Zaproponowany projekt rozwiązuje problem konieczności korzystania z komputera w bezpośrednim połączeniu z czytnikiem, a wybrany układ elektroniczny pozwala rozszerzyć urządzenie o dodatkowe funkcjonalności. Łączność internetowa pozwala na natychmiastowe odnotowywanie obecności w bazie, co na pewno jest wygodnym rozwiązaniem.

W treści opracowania nie został poruszony problem połączenia obecności z zajęciami, na których została ona odnotowana. W przypadku rozszerzenia systemu o kolejne czytniki podłączone do sieci i korzystania z wielu urządzeń jednocześnie, nie będzie możliwości rozszyfrowania, z jakich zajęć pochodzą wpływające do serwera dane.

Jedynym możliwym sposobem na komunikację urządzenia z użytkownikiem jest w tym wypadku buzzer, co może okazać się niewystarczające do wyrażenia stanu urządzenia. W razie kłopotów z łącznością albo anteną RFID nie ma możliwości wygodnego sygnalizowania problemu.

2.2.3. Samodzielny czytnik

W cytowanym we wstępie opracowaniu [7], w celu rozwiązania powyższego problemu zaproponowano wykorzystanie z wyświetlacza LCD, z którego użytek robi opisany w tej pracy układ elektroniczny. Przedstawione w pracy urządzenie poza czytnikiem RFID, zdolne jest również do wyświetlania treściwych komunikatów potwierdzających udane odnotowanie karty studenta.

Trudno w tym wypadku dyskutować jednak z innymi rozwiązaniami technicznymi zawartymi w tej pracy, ponieważ motywem przewodnim tego opracowania jest pokazanie, że sprawdzanie obecności przy pomocy tagów RFID przebiega szybciej niż w klasycznym podejściu.

2.2.4. Aplikacja internetowa

To najprostsze rozwiązanie składające się z jednolitego systemu, w którym jednocześnie można zbierać obecności uczestników wykładu, oraz je przechowywać i przeglądać. Jej niewątpliwym plusem jest całkowite wyeliminowanie problemu związanego z przenoszeniem danych do systemu katalogującego obecności, ponieważ dane wprowadzane są wprost do systemu. Identyfikacja konkretnych zajęć, w ramach których rejestrowana jest obecność, odbywałaby się na początku zajęć poprzez wejście w kontekst odpowiedniego wykładu w aplikacji. Obecność uczestników na zajęciach byłaby sprawdzana przez prowadzącego i od razu wprowadzana do systemu.

2.2.5. Urządzenie rejestrujące obecności za pośrednictwem sieci bezprzewodowej

W przypadku tego rozwiązania mikrokontroler zastalby rozszerzony o moduł do bezprzewodowej łączności z internetem, a stworzona aplikacja udostępniałaby interfejs do odnotowywania obecności.

Na etapie planowania tego rozwiązania wyniknęły komplikacje. Ten sposób wysyłania danych do aplikacji katalogującej obecności wymagałby umożliwienia powiązania obecności z zajęciami, na których zostały zebrane.

Wymagałoby to dołączenia dodatkowego interfejsu, który pozwalałby wprowadzać takie dane, co jeszcze bardziej komplikowałoby projektowane urządzenie. Dodatkowo ograniczyłoby to zbiór układów scalonych, z których można by skorzystać, ponieważ musiałby on posiadać wystarczającą ilość pamięci, pinów i innych potrzebnych peryferiów.

2.3. Określenie wymagań wobec projektu

W poprzednim rozdziale wspomniano o wielu możliwych realizacjach problemu zbierania obecności, co jest tylko niewielkim wycinkiem możliwych do wykonania projektów. W opracowaniu [5] wspomniano o wielu innych przedsięwzięciach, z których na wyróżnienie zasługują:

- Skorzystanie z telefonu komórkowego i łączności bluetooth w celu odnotowania obecności.
- Wykorzystanie odcisku palca do dodatkowego potwierdzenia tożsamości studenta.
- Użycie kamery i rozpoznawania twarzy w celu identyfikacji wchodzących na wykład studentów.

Analiza powyższych rozwiązań wraz z ich mocnymi i słabymi stronami pozwoliła wyłonić zbiór wymagań wobec projektowanego systemu. Wymagania zostały dobrane pod kątem poprawienia wydajności klasycznego sposobu weryfikowania obecności, co zostało rozważone w rozdziale 2.1, oraz możliwości jakie dają współczesne technologie, które zostały opisane powyżej.

Urządzenie powinno udostępniać następujące funkcjonalności:

1. Zarejestrowanie obecności uczestnika zajęć przy pomocy tagu RFID.
2. Wyświetlanie jasnych komunikatów odnośnie stanu urządzenia.
3. Powiązanie obecności z zajęciami, podczas których zostały zebrane.
4. Potwierdzenie tożsamości uczestnika odnotowującego swoją obecność.
5. Katalogowanie zebranych danych i generowanie raportów podsumowujących.
6. Wygodne przeniesienie obecności zebranych przez czytnik do aplikacji przechowującej dane.

Rozdział 3.

Określenie struktury projektu

Finalnie zdecydowano się jednoznacznie oddzielić sposób zbierania danych od ich przechowywania i przetwarzania.

Realizacja projektu opiera się na fakcie, że polskie uczelnie powszechnie korzystają z Elektronicznych Legitymacji Studenckich (ELS), które zawierają wbudowany tag RFID.

Komponent umożliwiający studentowi odnotowanie swojej obecności na wykładzie - weryfikator - został oparty o platformę Arduino. Urządzenie zostało rozszerzone o moduły umożliwiające realizację założeń z poprzedniego rozdziału.

Dodatkowo częścią urządzenia będzie zegar RTC umożliwiający zapamiętanie godziny, o której odnotowane zostały obecności, a więc powiązanie ich z konkretnymi zajęciami, oraz wyświetlacz LCD + Buzzer, pozwalające na wygodne korzystanie z samodzielnego urządzenia.

Sposobem na potwierdzenie tożsamości studenta będzie w wypadku realizowanego projektu porównanie zdjęcia na legitymacji z twarzą osoby, która zbliża ją do czytnika. Za tę weryfikację odpowiedzialny będzie prowadzący.

Rolę oprogramowania odpowiedzialnego za katalogowanie zebranych przez weryfikator danych w omawianym systemie będzie pełnić ogólnodostępna aplikacja internetowa - elektroniczny dziennik, umożliwiający założenie konta i zarządzanie zebranymi obecnościami w kontekście całego przedmiotu i w kontekście pojedynczych zajęć. Dodatkowo ma on umożliwiać generowanie raportów ze zagregowanymi danymi tak, aby dało się łatwo prześledzić obecności w kontekście całego semestru.

Wirtualny dziennik zaprojektowano w taki sposób, żeby był niezależny od danych studentów. Dzięki takiemu podejściu w łatwy sposób można przełączyć cały system na korzystanie z baz danych na różnych uczelniach. Uniknie się także konieczności przechowywania wrażliwych danych w systemie.

Ze względu na to, że na etapie realizowania założonego projektu nie uzyskano dostępu do serwisu udostępniającego dane wrocławskich studentów, została stwo-

rzona dodatkowa aplikacja, niezależna od innych części projektu.

Umożliwia ona powiązanie danych pobranych z legitymacji studenckiej z danymi pozwalającymi na identyfikację jej posiadacza. Jest to aplikacja rozłączna względem systemu zarządzającego obecnościami osób uczestniczących w zajęciach, wystawiająca RESTowe API.

Rozdział 4.

Realizacja

4.1. Weryfikator - czytnik legitymacji studenckich

Zgodnie z wymaganiami projektowane urządzenie powinno udostępniać co najmniej następujące możliwości:

- Możliwość podłączenia zewnętrznego nośnika danych.
- Stworzenie pliku, na którym zapamiętani zostaną uczestnicy zajęć.
- Zebranie informacji z elektronicznej legitymacji studenckiej, potwierdzające obecność uczestników.
- Wyświetlanie informacji o stanie urządzenia, w szczególności sukcesu odczytania danych z legitymacji.
- Zapamiętanie czasu, w którym zebrane zostały obecności.

Dodatkowo cała elektronika powinna zostać schowana wewnątrz plastikowego opakowania, a zasilanie dostarczane za pomocą kabla podłączonego do sieci elektrycznej. Opakowanie powinno zostać wyposażone w otwory na kabel zasilający, zewnętrzny nośnik danych oraz wyświetlacz. Czytnik kart RFID powinien być tak zlokalizowany, aby umożliwić łatwe zebranie danych z ELS.

4.1.1. Zastosowana platforma i peryferia

Arduino to cała platforma programistyczna umożliwiająca łatwe projektowanie i testowanie układów składających się z wielu elektronicznych modułów. Podstawą każdego projektu Arduino jest układ elektroniczny oparty na mikroprocesorze. Pod egidą tego systemu udostępniony jest cały wachlarz wersji takich układów, różniących się rodzajem kontrolera i udostępnionymi peryferiami (przykładowo: slot na kartę SD, gniazdo RJ-45, wbudowany wyświetlacz, czy moduł WIFI). Do wyboru

użytkownika pozostaje cała gama wersji płytek drukowanych spod znaku Arduino. Dodatkowo platforma udostępniona jest na licencji open hardware, co sprawiło, że z projektem związana jest olbrzymia międzynarodowa społeczność entuzjastów elektroniki. Częścią platformy jest również środowisko programistyczne umożliwiające wgrywanie własnych programów na podłączoną do komputera płytkę.

Ciekawą opcją udostępnioną użytkownikom platformy jest możliwość skonstruowania własnej płytki z procesorem na bazie powszechnie dostępnych schematów gotowych układów. Jest to korzystne rozwiązanie, kiedy projektantowi zależy na ograniczeniu kosztów układu. W referowanym rozwiązaniu skorzystano jednak z jednej z gotowych płytek.

Podstawą projektowanego weryfikatora została płytka Arduino Uno oparta na mikroprocesorze AVR ATmega328. Kontroler w tym układzie jest bardzo prosty, posiada ograniczone zasoby, co wymusza dodatkowy wysiłek włożony w zarządzanie pamięcią i czasem procesora. Kontroler jest wyposażony w następujące zasoby:

- 32kB Flash - przestrzeń na kod programu.
- 2kB SRAM zajmowane przez pamięć operacyjną.
- porty SPI, I2C, szeregowy.
- Jednostka obliczeniowa o częstotliwości zegara 20MHz.

Dodatkowo, w celu zapewnienia wszystkich wymaganych funkcjonalności przez projektowany weryfikator, skorzystano z następujących dodatkowych modułów:

- Czytnik RFID - do odczytywania danych z legitymacji studenckiej wyposażonej w interfejs zbliżeniowy. Czytnik podłączony jest przez port szeregowy.
- USB Host Shield - dodające gniazdo USB, umożliwiające podłączenie pendriva, korzystający z drugiego portu SPI.
- Wyświetlacz LCD wraz z potencjometrem do ustawiania kontrastu, przekazujący użytkownikowi informacje na temat stanu urządzenia.
- RTC - zegar czasu rzeczywistego z baterią do zapamiętywania czasu zbierania danych, korzystający z interfejsu I2C.
- Buzzer piezo wydający dźwiękowe sygnały w razie sukcesu.

4.1.2. Konstrukcja

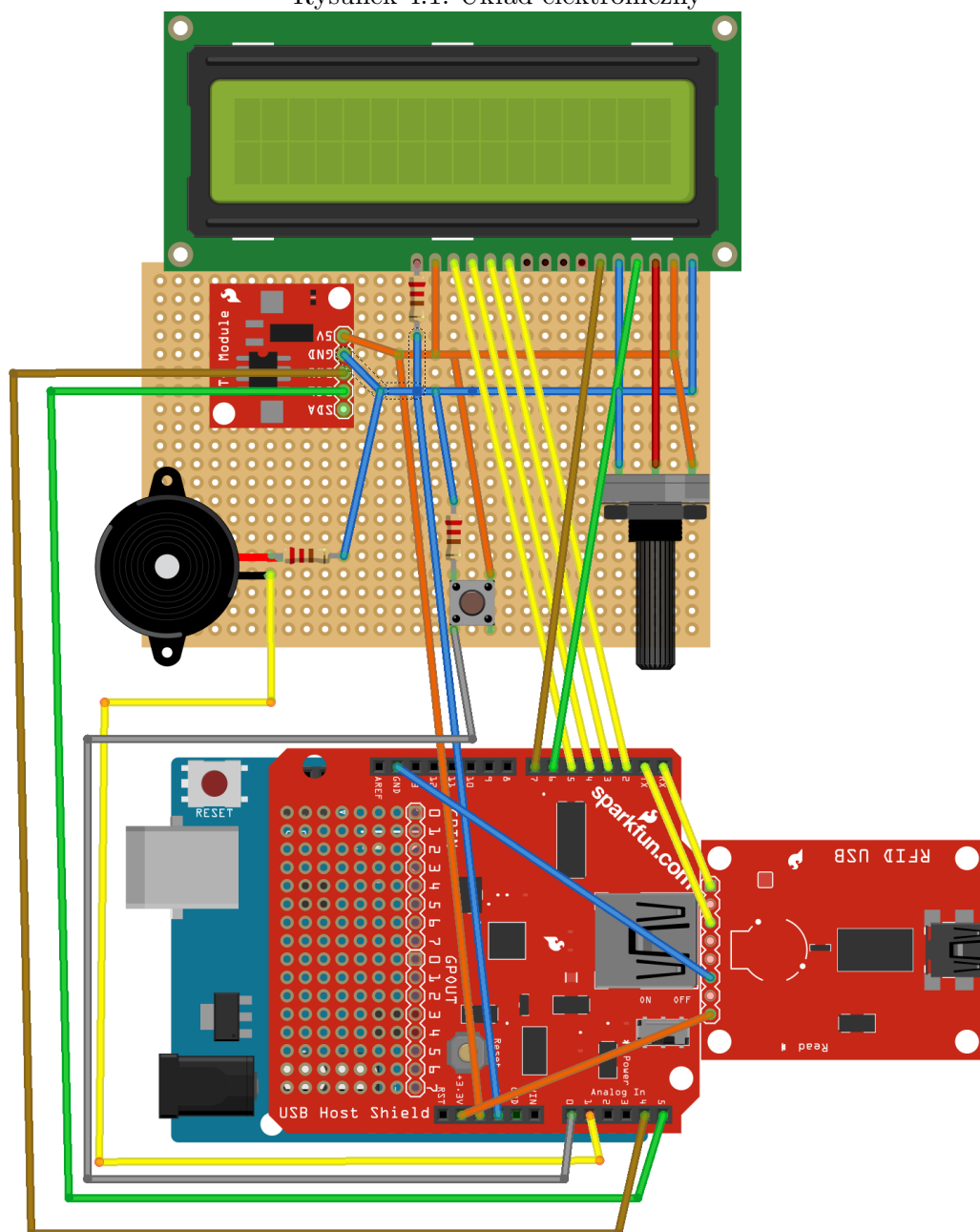
Do skonstruowania ostatecznego układu z zebranych elementów użyto dodatkowo:

- Jednej dwustronnej płytki stykowej.

- Trzech rezystorów 220 Ohm.
- kilkudziesięciu kabli różnej długości.
- Jednego przycisku do resetowania zegara.

Cały układ został osadzony w plastikowym opakowaniu z wywierconymi otworami

Rysunek 4.1: Układ elektroniczny



fritzing

Rysunek 4.2: Gotowe urządzenie



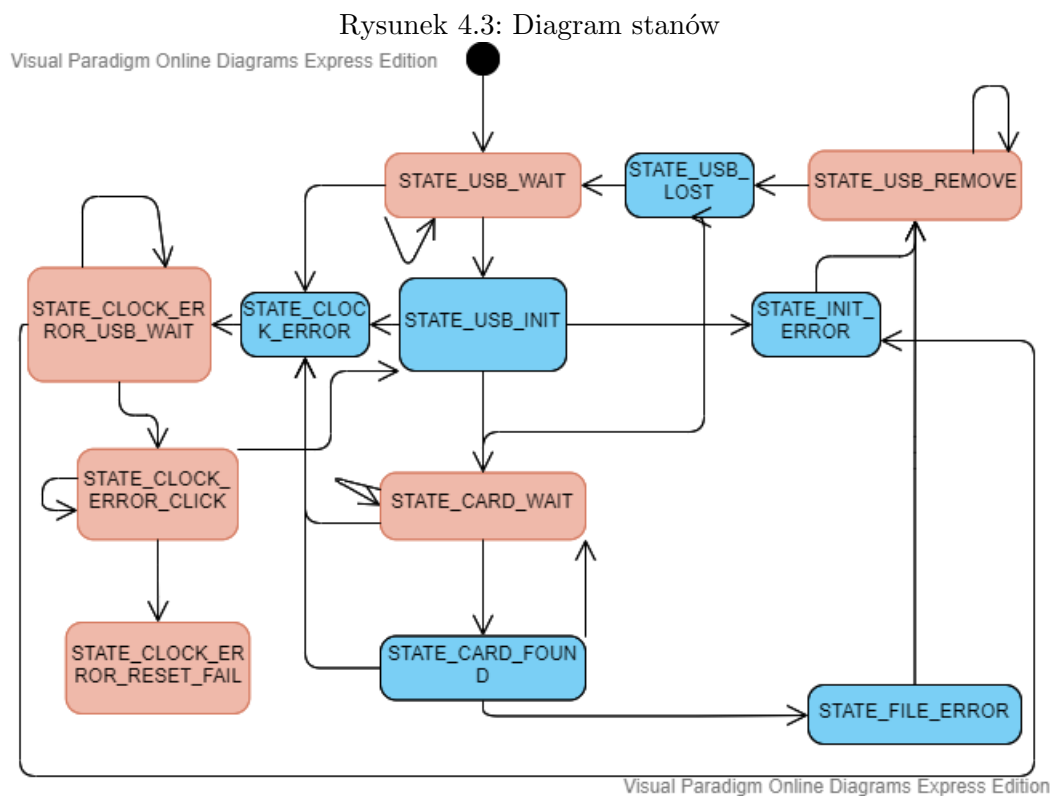
4.1.3. Działanie

Osią działania zaprojektowanego weryfikatora jest interakcja z dwoma zewnętrznymi urządzeniami. Jednym z nich jest nośnik danych, na którym zapisane zostaną obecności uczestników zajęć. W realizowanym projekcie rolę tę pełni pendrive sformatowany w systemie FAT. W zależności od tego, czy w danym momencie pendrive jest podłączony, urządzenie jest w stanie oczekiwania na drugie z zewnętrznych narzędzi - Elektroniczną Legitymację Studencką. Dodatkowo weryfikator jest zdolny do wyświetlania komunikatów o swoim stanie na ekranie LCD i wydawania sygnałów dźwiękowych przy pomocy brzęczka. Częścią urządzenia jest również zegar RTC, który pozwala śledzić aktualną godzinę. Weryfikator monitoruje swój własny stan i jest zdolny do wykrywania błędów takich jak:

- Błąd Inicjalizacji podłączonego pendrive'a.
- Błąd zapisu odczytanych danych na nośniku.
- Błąd zegara RTC - spowodowanego najczęściej rozładowaną baterią.

Kod weryfikatora projektowano z myślą o tym, żeby łatwo dało się przedstawić przebieg programu na diagramie. Struktura kodu jest przemyślana w taki sposób, żeby podczas jednego przebiegu pętli głównej wykonywał się jedynie kod powiązany z aktualnym stanem urządzenia. Taki układ nie tylko pozwala zwięźle opowiadać o działaniu urządzenia, ale również ułatwia testowanie poprawności podczas pisania kodu i montowania urządzenia.

Weryfikator w danej chwili może znajdować się w jednym z 12 stanów. Na przedstawionym diagramie stany oczekujące na zdarzenie przedstawiono kolorem kremowym, a stany przejściowe kolorem niebieskim:



- STATE_USB_WAIT - oczekiwanie na pendrive - ekran wyświetla informację - "Insert pendrive". Próba inicjalizacji nośnika zajmuje około 5 sekund dlatego wyświetlany czas jest aktualizowany z opóźnieniem.
- STATE_USB_INIT - inicjalizacja pendriva - po odnalezieniu pendriva wyświetlana jest informacja "USB Inserted". W przypadku błędu inicjalizacji - przejście do stanu STATE_INIT_ERROR, w razie sukcesu na podstawie aktual-

nego czasu stworzona i zapamiętana zostaje nazwa YY-MM-DD-hh_mm_ss dla pliku, który będzie przechowywał zebrane uidy.

- STATE_CARD_WAIT - oczekiwanie na kartę RFID - ekran: "Scan Card". W razie wykrycia odłączenia pendriva przejście do stanu STATE_USB_LOST. W przypadku wykrycia karty, ale błędu w odczycie (np. ze względu na zbyt szybkie odsunięcie karty) wyświetlenie informacji: Read error.
- STATE_CARD_FOUND - zapisywanie Uidu do pliku - otwarcie pliku o zapamiętanej nazwie zapisanie do niego odczytanego Uidu. W razie błędu przy zapisie przejście do stanu STATE_FILE_ERROR, w przypadku sukcesu sygnał dźwiękowy, wyświetlenie informacji "Read Success" i powrót do stanu STATE_CARD_WAIT.
- STATE_INIT_ERROR - błąd inicjalizacji pendriva - ekran: "Init Error".
- STATE_USB_REMOVE - czekanie na odłączenie pendriva. Wyświetlacz: "Reinsert USB". W razie wykrycia odłączenia pendriva przejście do stanu STATE_USB_LOST.
- STATE_USB_LOST - odłączono pendrive - ekran: "USB removed", sygnał dźwiękowy oraz przejście do stanu STATE_USB_WAIT.
- STATE_FILE_ERROR - błąd zapisu do pliku - ekran: "Open file error", przejście do stanu STATE_USB_REMOVE.
- STATE_CLOCK_ERROR - błąd zegara - w razie wykrycia problemów z zegarem w którymś ze stanów [STATE_USB_WAIT, STATE_CARD_WAIT, STATE_CARD_FOUND, STATE_USB_INIT, STATE_USB_REMOVE] sterowanie przechodzi do tego stanu. Wyświetlona zostaje informacja: "Clock Error", następnie sterowanie przechodzi do STATE_CLOCK_ERROR_USB_WAIT.
- STATE_CLOCK_ERROR_USB_WAIT - oczekiwanie na pendrive z czasem - wyświetlacz "Insert pendrive with time". Sterowanie pozostaje w tym stanie, do czasu kiedy na zewnętrznym nośniku wykryty zostanie plik o nazwie tdav, który w pierwszym wierszu będzie zawierał datę w formacie "YYYY/MM/DD hh:mm:ss". W przypadku wykrycia poprawnego pliku program zapamiętuje datę z pliku tdav i przechodzi w stan STATE_CLOCK_ERROR_CLICK.
 - W razie błędu przy inicjalizacji pendriva program przechodzi do stanu STATE_INIT_ERROR.
 - W razie wykrycia pendrive i nie wykrycia pliku o nazwie tdav wyświetlona zostaje informacja "Upload time tdav".
 - W razie złego formatu pierwszej linijki w pliku tdav wyświetlona zostaje informacja: "Bad date format".
- STATE_CLOCK_ERROR_CLICK - oczekiwanie na reset - wyświetlacz: "Click to reset". Sterowanie pozostaje w tym stanie, do czasu kiedy zostanie przyciśnięty guzik resetu. Po naciśnięciu guzika na zegarze zostaje ustawiona zapamiętana data, wyświetlony zostaje komunikat "Time set", a sterowanie prze-

chodzi w stan STATE_USB_INIT. Jeśli podczas ustawiania czasu na zegarze wystąpi błąd program przechodzi w stan STATE_CLOCK_ERROR_RESET_FAIL.

- **STATE_CLOCK_ERROR_RESET_FAIL** - błąd resetowania czasu. Wyświetlacz: "Clock Reset Fail". Ze względu na brak możliwości ustawienia poprawnego czasu jest to stan, z którego urządzenie nie może wrócić do poprawnego funkcjonowania.

4.1.4. Napotkane problemy

Dwa moduły korzystające z interfejsu SPI

Podczas wstępnej fazy planowania podstawą weryfikatora miała być płytka Arduino Leonardo.

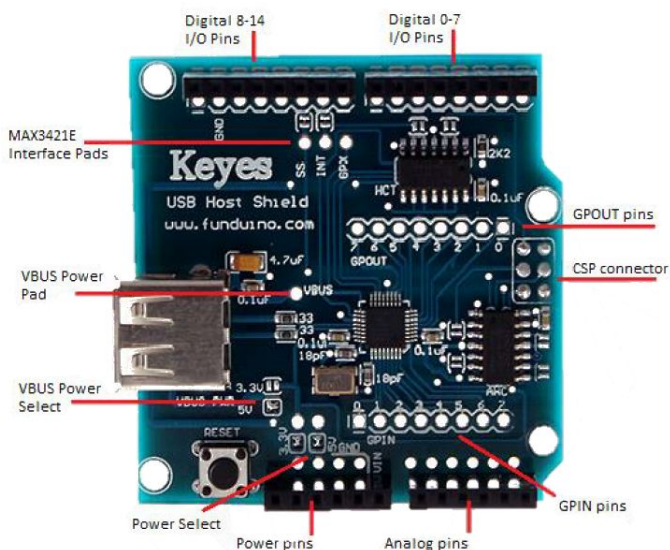
Podobnie jak w ostatecznej wersji miała ona zostać rozszerzona o USB Host Shield oraz moduł RFID - oba używają interfejsu SPI. Każdy z tych komponentów osobno współpracował poprawnie z Arduino Leonardo. Problemy pojawiły się, kiedy połączono wszystko w jedną całość w celu zapisywania odczytanych danych z ELS na podłączonym pendrivie.

Podczas montowania układu okazało się, że w tej wersji płytki piny interfejsu SPI znajdują się w magistrali ICSP, która była już zajęta przez moduł USB w taki sposób, że nie było możliwości podłączenia tam innych kabli.

Próba dolutowania kabli do magistrali CSP na płycie USB Host Shield (z shielda wystają jedynie milimetrowe pinu CSP), zakończyła się przepaleniem połączeń wewnętrznych tego układu i w konsekwencji jego uszkodzeniem.

W celu rozwiązania problemu z portem SPI ostatecznie wykorzystano wersję UNO, która interfejs SPI ma doprowadzony również na piny 10-13.

Rysunek 4.4: Układ USB Host shield ze wskazaniem na zakończenia magistrali CSP



Problemy z odczytaniem danych z ELS

W początkowej wersji urządzenie korzystało z modułu RFID - MFRC-522. Ten komponent bez zarzutów współpracował z załączonymi w zestawie tagami, jednak bardzo słabo wykrywał Elektroniczną Legitymację Studencką. Odczytanie Uidu z ELS zajmowało zazwyczaj parę minut. Żeby rozwiązać ten problem, zmieniono moduł RFID na taki o lepszy, zasięgu - PNS532. Pierwsze próby zwiastowały pełny sukces - próby odczytania danych z ELS przebiegały bez zarzutu.

Problem pojawił się jednak przy współpracy nowego modułu z resztą układu. Jak już zostało wcześniej wspomniane, Arduino Uno posiada jeden port SPI, do którego można podłączyć więcej urządzeń. Niestety Arduino było w stanie współpracować tylko z jednym z dwóch komponentów - albo USB Host shield, albo modulem PNS532. Ostatecznie okazało się jednak, że moduł PNS532 udostępnia również inne porty, dzięki czemu udało się go podłączyć przy pomocy portu szeregowego.

Wypełniona pamięć operacyjna

W miarę dołączania kolejnych komponentów do układu, tzn. zegara RTC, brzęczka oraz wyświetlacza LCD, zaczęły pojawiać się problemy z pamięcią.

Pierwsza skończyła się pamięć operacyjna, której kontroler posiada jedynie 2KB. Objawiało się to nagłym zawieszaniem się wykonywania programu bez jednoznacznego określenia przyczyny.

Udało się rozwiązać ten problem dzięki większej dyscyplinie w korzystaniu z pamięci. Ograniczono liczbę zmiennych globalnych, a największy efekt przyniosło przeniesienie wykorzystywanych w programie napisów z pamięci operacyjnej do pamięci flash, do czego służy dyrektywa PROGMEM.

Pamięć flash jest przeznaczona do przechowywania kodu programu i nie ma do niej swobodnego dostępu, jak w przypadku pamięci operacyjnej. Korzystanie z niej w do przechowywania stałych jest uciążliwe, ponieważ każdy bajt danych musi być odczytywany osobno, jednak dzięki temu nie było potrzeby przechowywania wszystkich łańcuchów znaków jednocześnie w pamięci SRAM.

Wypełniona pamięć flash

Przeniesienie łańcuchów znaków do pamięci flash, chociaż poprawiło wydajność pamięci operacyjnej, to spowodowało wyczerpanie przestrzeni przeznaczonej na kod programu.

Pamięć flash jest bardziej pojemna niż SRAM, ponieważ w tym wypadku jest to aż 32KB do dyspozycji programisty, jednak duża liczba bibliotek do obsługi peryferiów doprowadziła do wyczerpania się również tej przestrzeni.

Ułatwieniem w przypadku optymalizowania wykorzystania pamięci flash jest to, że przestrzeń zajmowana przez kod programu jest stała po kompilacji. Nie ma

więc obawy, że w trakcie przebiegu programu nastąpi nagły wzrost i przekroczenie pojemności. Wystarczy dostosować się do limitu 32 KB.

Problem został przezwyciężony poprzez ograniczenie liczby funkcji, które zadeklarowano w programie, oraz schowanie komunikatów wysyłanych na serial monitor wewnątrz dyrektyw preprocesora `#if DEBUG serial.println("SETUP"); #endif`. Dzięki temu można było łatwo wyłączyć kod programu odpowiedzialny za debugowanie.

Moduł WIFI

W pierwszej wersji planowanego weryfikatora miał on się łączyć z siecią za pomocą modułu WIFI. Wielu problemów przysporzył jednak układ ESP8266, odpowiedzialny za tę łączność. Po wgraniu sterownika do tego układu przestawał on być wykrywany przez komputer i Arduino.

Pomimo wykorzystania kilku takich układów za każdym razem pojawiał się ten sam problem. Ostatecznie zrezygnowano z wykorzystania modułu ESP8266 ze względu na zmianę koncepcji.

4.1.5. Inne koncepcje weryfikatora

Na etapie projektowania weryfikatora, jako jego podstawa brany był pod uwagę układ Raspberry Pi. Ostatecznie zrezygnowano z tego pomysłu, ze względu na to, że takie urządzenie mogłoby wymagać utrzymywania systemu operacyjnego w aktualnej wersji. Za wykorzystaniem Arduino przemawia również cena takiego układu i fakt, że jest on bardzo dobrze znany studentom Instytutu Informatyki UW r z zajęć Systemów Wbudowanych.

Projektując układ należało również podjąć decyzję z jakiego nośnika skorzystać do przenoszenia danych z weryfikatora do aplikacji zarządzającej obecnościami. Poza wykorzystaniem w ostatecznym rozwiązaniu pendrivem brano również pod uwagę skorzystanie z karty SD

Ze względu na większą dostępność i łatwiejsze podłączenie klasycznego pendrive'a do komputera (nie każdy komputer posiada slot na kartę SD), zdecydowano się na tę właśnie możliwość. Później okazało się, że ta decyzja miała swoje konsekwencje.

Po pierwsze USB Host Shield zajął magistralę ICSP, będącą jedynym wyjściem pinów interfejsu SPI w układzie Arduino Leonardo, co w konsekwencji doprowadziło do zmiany wersji płytki na UNO.

Kolejnym utrudnieniem, spowodowanym przez korzystanie z pendriva, były problemy z dostępnością biblioteki obsługującej pamięć w tej formie. Podstawowa biblioteka obsługująca układ USB Host Shield nie przewiduje wykorzystania złącza USB do podłączenia pamięci masowej.

Ostatecznie skorzystano z mniej popularnej biblioteki do obsługi tego narzędzia - UsbFat[21], która jednak okazała się być słabo opisana.

4.2. Elektroniczny dziennik

W celu wygodnego przetwarzania zebranych danych o obecnościach stworzona została aplikacja internetowa - elektroniczny dziennik. W serwisie użytkownik może założyć konto, w jego kontekście stworzyć strukturę prowadzonych przez siebie zajęć i uzupełniać listę obecnych na nich studentów.

Dziennik umożliwia przeglądanie obecności studentów, którzy wzięli udział w zajęciach oraz wygenerowanie raportu w formacie CSV ze zagregowanymi obecnościami.

Struktura dziennika

Użytkownikowi serwisu po założeniu konta i zalogowaniu ukazuje się lista instancji wykładów, które są przypisane do jego konta i na których może dokonać standardowych operacji przeglądania/edytowania/usuwania/dodawania. Instancja wykładu składa się z nazwy, opisu, listy uczestników oraz listy zajęć w jej ramach. Instancję wykładu można rozumieć jako zajęcia prowadzone przez jednego prowadzącego z grupą studentów w ramach jednego przedmiotu.

Do instancji wykładu zostaje przypisana grupa studentów, którzy są zapisani na zajęcia prowadzone przez użytkownika w ramach wykładu. Przykładową listą uczestników będzie więc jedna grupa studentów uczestniczących w ćwiczeniach prowadzonych przez jednego pracownika uniwersytetu w ramach jednego przedmiotu. Dodatkowo, generowany raport z obecności na jednej instancji wykładu będzie odnosił się tylko do studentów znajdujących się na tej liście.

Każda instancja wykładu posiada skończony zbiór zajęć, których pojedyncza instancja składa się z daty i godziny oraz przypisanej do niej listy obecności. Taka instancja może być rozumiana jako pojedyncze zajęcia jednej grupy studentów. Na listę obecności zajęć mogą zostać wpisani studenci, którzy nie są wpisani na listę uczestników instancji wykładu. Będą widoczni w przeglądzie konkretnych zajęć w graficznym interfejsie dziennika, jednak nie zostaną wzięci pod uwagę przy generowaniu raportu dla instancji wykładu.

Posługując się przykładem jednego przedmiotu, prowadzonych w ramach pojedynczego semestru, struktura w dzienniku będzie wyglądała następująco: zajęcia w ramach przedmiotu będą rozdzielone pomiędzy konta wykładowcy i wszystkich ćwiczeniowców prowadzących zajęcia.

Wykładowca stworzy na swoim koncie w elektronicznym dzienniku instancję wykładu, przypisane do niego zostaną wszystkie wykłady, a listą uczestników będą

wszyscy studenci zapisani na ten przedmiot. Lista obecności pojedynczych zajęć będzie więc składać się ze wszystkich studentów, którzy w trakcie odbywania się wykładu w sali Instytutu Informatyki przyłożą swoją legitymację do weryfikatora.

Ćwiczeniowcy na swoich kontach utworzą osobne instancje wykładu, przypiszą do nich zajęcia odpowiadające prowadzonym przez nich cotygodniowym ćwiczeniom oraz dodadzą grupę studentów, którzy zapisali się do ich grupy.

Pojedynczy przedmiot prowadzony w ramach jednego semestru zostanie więc podzielony na tyle instancji wykładu w elektronicznym dzienniku, ilu jest prowadzących i wykładowców. Każdy z nich będzie zbierał obecności tylko w ramach prowadzonych przez siebie zajęć.

Jeśli użytkownik elektronicznego dziennika w ramach jednego przedmiotu prowadzi wiele różnych zajęć. np. wykład i ćwiczenia albo ćwiczenia z różnymi grupami studentów, powinien on przypisać do swojego konta kilka instancji wykładu z przypisanymi do niej grupami studentów oraz instancjami prowadzonych przez niego zajęć z tą grupą.

Interfejs użytkownika

Interfejs użytkownika elektronicznego dziennika jest prosty i składa się tylko z elementów umożliwiający tworzenie struktury instancji wykładów i zajęć oraz zarządzaniem obecnościami. Wygląd strony został oparty na frontendowym freamworku Bootstrap[10]. Podstrony zostały ostyleowane w sposób zapewniający przejrzystość i stosunkowo nowoczesny wygląd.

Cały interfejs aplikacji został zrealizowany w języku angielskim i na chwilę obecną nie ma możliwości przełączenia się na język polski.

Przegląd instancji wykładów

Główną podstroną widoczna dla użytkownika po zalogowaniu się na konto jest przegląd instancji wykładów przypisanych do niego. Z tego poziomu mogą zostać wykonane standardowe funkcje CRUD[22].

Formularz dodawania nowej instancji wykładu umożliwia załączenie pliku, na podstawie którego zostanie zainicjalizowana grupa uczestników instancji wykładu. Plik powinien zawierać listę numerów albumu studentów wypisanych po przecinku.

Inicjalizacja listy zajęć jest możliwa w jednym z trzech trybów - pojedynczym, cotygodniowym lub comiesięcznym. W razie wybrania którejś z dwóch ostatnich opcji formularz umożliwi podanie początkowej i końcowej daty, a do wykładu zostaną przypisane zajęcia odpowiednio co siedem i co 30 dni od pierwszej z nich. Formularz zakłada, że wszystkie zajęcia odbywać się będą o tej samej godzinie. Użytkownik będzie miał możliwość zmiany godziny w przeglądzie poszczególnych zajęć.

Podgląd pojedynczej instancji wykładu

Po wejściu w przegląd instancji wykładu aplikacja wyświetla informacje o jej nazwie i opisie. Dodatkowo w dwóch domyślnie zwiniętych listach wyświetlona zostaje lista obecności i lista zajęć. Użytkownik ma możliwość dodawania/usuwania elementów tych list. W przypadku, kiedy student posiadał już zaliczone obecności w ramach zajęć przyporządkowanych do tej instancji wykładu, a zostanie usunięty z listy uczestników, jego uczestnictwo zostanie zinterpretowane jako udział wolnego słuchacza w zajęciach.

W tym widoku użytkownik dostaje również możliwość wygenerowania raportu z obecnościami w formacie CSV.

Podgląd pojedynczych zajęć

Ostatnim istotnym widokiem jest przegląd pojedynczych zajęć. Użytkownik otrzymuje możliwość zmodyfikowania ich daty i godziny oraz wyświetlenia i zarządzania listą obecności. Lista podzielona jest na dwie części - studentów którzy są uczestnikami instancji wykładu oraz wolnych słuchaczy. Każdy wiersz na pierwszej z list pokolorowany jest na czerwono lub zielono w zależności od tego, czy dany uczestnik był obecny na zajęciach.

Interfejs umożliwia w tym widoku wysłanie na serwer pliku z obecnościami, które zostały wygenerowane przez weryfikator.

Dodatkowe widoki

Aplikacja udostępnia dodatkowo widoki informacyjne związane z funkcjonowaniem serwisu - Kontakt/Opis oraz związane z funkcją logowania/rejestracji. Te części aplikacji są uproszczone i w razie uruchomienia systemu w wersji produkcyjnej będą wymagały uzupełnienia.

Połączenie z bazą studentów

Jak zostało określone podczas definiowania wymagań wobec projektu, dziennik elektroniczny jest niezależny od danych dotyczących studentów i nie przechowuje ich w żadnej formie.

Podczas dodawania studentów do listy uczestników wykładu albo listy obecności na zajęciach aplikacja odwołuje się do zewnętrznego serwisu udostępniającego dane studentów. Korzystając z podanych przez użytkownika informacji identyfikujących

studenta - numeru albumu albo UIDu karty magnetycznej, odpytuje zewnętrzną aplikację poprzez udostępnione API. Kiedy dane studenta zostaną poprawnie pobrane, dziennik zapamiętuje jedynie identyfikator studenta w zewnętrznym systemie. Przy każdym żądaniu wyświetlenia danych studentów aplikacja wykorzystuje zapamiętany identyfikator do wysłania zapytania do zewnętrznego serwisu.

Takie podejście ma zasadnicze korzyści. Dzięki zapamiętywaniu zewnętrznego identyfikatora, aplikacja może uniknąć zapamiętywania wrażliwych danych. Pozwala to znacząco ograniczyć straty nawet w przypadku naruszenia bezpieczeństwa serwisu. Dodatkowo taka architektura jest przygotowaniem systemu do współpracy z rzeczywistymi źródłami danych o studentach i wpięcia do cyfrowego systemu istniejącej uczelni.

Przegląd technologii

Aplikacja została napisana we frameworku Yii2[14], będącym rozszerzeniem języka PHP. Cała architektura opiera się na modelu MVC. W ramach definiowania modeli i łączenia ich z bazą korzystano ze wzorca ActiveRecord, a kod związany z przetwarzaniem innych źródeł danych w serwisie wydzielono do osobnych serwisów w ramach aplikacji.

W projekcie frontendu korzystano z frameworka Bootstrap[10] oraz gotowych komponentów[11][12][13] wyświetlających edytowalne pola z datą i godziną.

Dane wygenerowane w trakcie funkcjonowania aplikacji przechowywane są w relacyjnej bazie danych operującej na systemie PostgreSQL[16].

Gotowa aplikacja została uruchomiona w środowisku najnowszej wersji PHP - 7.4.

Do zarządzania zależnościami serwisu wykorzystano system do zarządzania pakietami Composer[15].

4.3. Baza studentów

Baza studentów jest aplikacją internetową, umożliwiającą zarządzanie danymi studentów i udostępniającą API. Jej zadaniem jest imitowanie systemu istniejącej uczelni i umożliwienie pobrania szczegółowych danych studenta po numerze albumu i identyfikatorze przypisanym do Elektronicznej Legitymacji Studenckiej.

Aplikacja została napisana w technologii Symfony4[19] z biblioteką Doctrine[17] w roli ORMa pośredniczącego w komunikacji z bazą danych w systemie PostgreSQL. Do stworzenia interfejsu umożliwiającego zarządzanie danymi studentów wykorzystany został framework Bootstrap.

4.3.1. Funkcjonowanie

Ze względu na fakt, że aplikacja ma za zadanie jedynie imitować działający system i umożliwić działanie elektronicznego dziennika, funkcjonalności realizowane przez aplikację ograniczone zostały do minimum.

Zarządzanie informacjami o studentach

Administrator systemu może zalogować się na stworzone w systemie konto i wykonać na danych studentów standardowe operacje CRUD. Dodatkowo użytkownik ma możliwość wysłania na serwer pliku w formacie JSON ze zbiorczymi danymi studentów, które ma zamiar dodać do systemu. Studenci dodani w kontekście jednego konta, są dostępni tylko z perspektywy tego konta. Pozwala to na stworzenie w aplikacji odrębnych przestrzeni odpowiadających systemom różnych instytucji, które chciałyby korzystać z takiego serwisu.

Przechowywane dane studentów:

- user_id - identyfikator użytkownika bazy danych.
- album_no - numer albumu studenta, unikalny w kontekście użytkownika który stworzył dandy rekord.
- name - imię.
- surname - nazwisko.
- start_year - rok rozpoczęcia studiów.
- semestr - aktualny semestr studiowania.
- card_uid - identyfikator ELS z której korzysta student, unikalny w kontekście użytkownika który stworzył dandy rekord.

4.3.2. Udostępnione API

Aplikacja udostępnia API w architekturze REST[23]. Do authoryzacji zapytań o dane studentów używany jest metoda HTTP Basic. Zautoryzowany użytkownik ma dostęp do tylko tych rekordów, które zostały utworzone w kontekście jego konta.

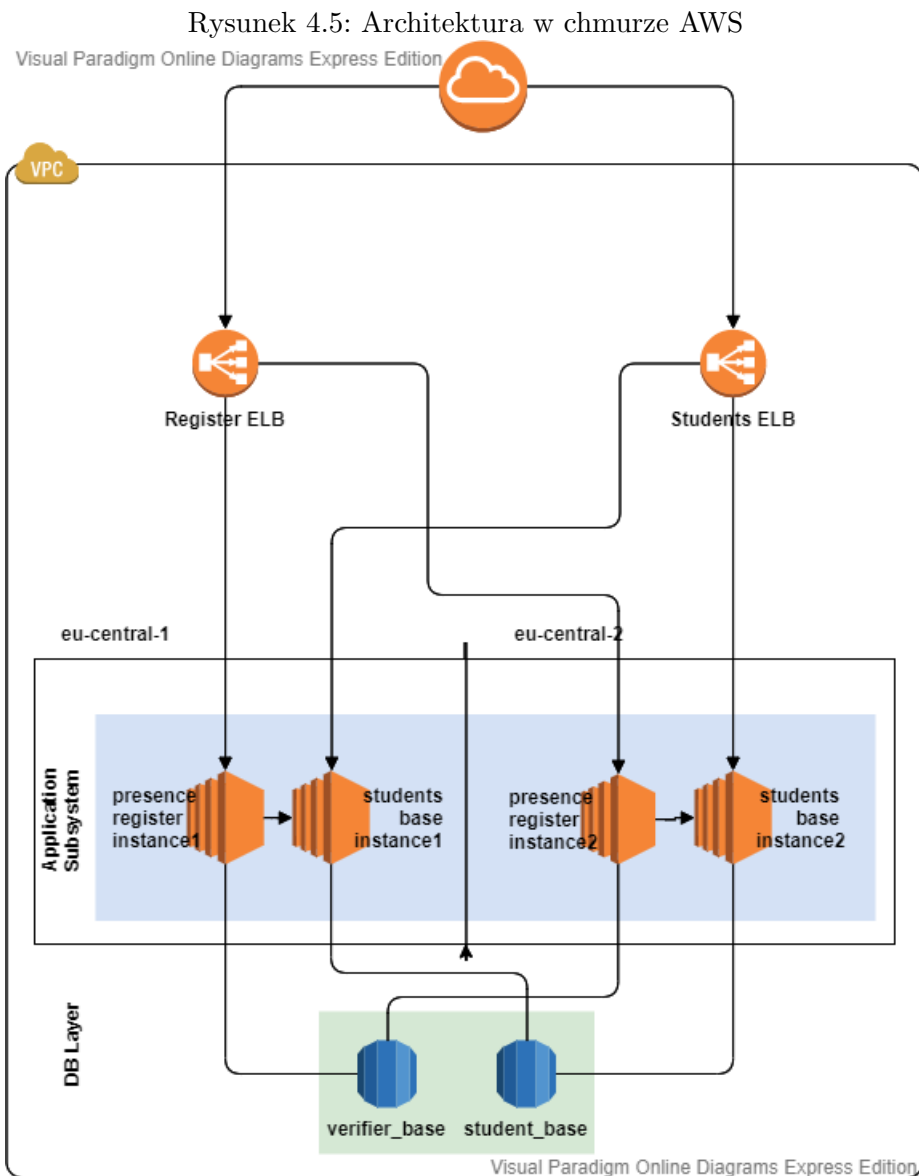
Lista przekazanych w żądaniu parametrów powinna być zakodowana base64, a dla parametrów, dla których w bazie nie istnieje rekord zwracana jest pusta tablica.

Możliwe requesty:

- GET: /api/students
- GET: /api/students/id/id

- GET: /api/students/card_id/card_uid
- GET: /api/students/album_no/album_no

4.4. Propozycja wdrożenia systemu



W celu prezentacji gotowego rozwiązania cały system został wdrożony na platformę przygotowaną przez Amazona - AWS[20] udostępniającą część swoich funkcjonalności na rok za darmo w ramach programu AWS Free Tier.

Zaproponowana architektura to przykład trójwarstwowego podejścia do wdrażania systemów korzystających z równoważenia obciążenia, serwerów uruchomionych aplikacji i baz danych.

Każda z aplikacji utworzona jest w dwóch instancjach w różnych sieciach. Do

obu serwisów przydzielony jest Load Balancer, który równoważy ruch pomiędzy istniejącymi instancjami. W przypadku braku dostępności któregoś z serwerów, na których uruchomione zostały aplikacje, cały ruch przekazywany jest do drugiego z nich.

W celu zapewnienia bezpieczeństwa, bazy danych znajdują się w osobnych sieciach, do których dostęp został umożliwiony jedynie z sieci, w których znajdują się aplikacje dziennika elektronicznego i bazy studentów.

Dodatkowo aplikacje pobierają informacje o swojej konfiguracji ze zmiennych środowiskowych serwera, na którym zostały uruchomione. Są to informacje o sposobie połączenia z bazą danych, a w przypadku dziennika elektronicznego również odnośnik i dane do logowania do aplikacji bazy studentów.

4.5. Narzędzie wykorzystane w trakcie realizacji

- PhpStorm - środowisko programistyczne ułatwiającego programowanie w PHP.
- GIT - system kontroli wersji.
- HeidiSQL - Klient bazy danych.
- Postman - platforma do testowania API.
- AWS console - narzędzie do zarządzania zasobami w chmurze AWS.
- Arduino IDE - środowisko umożliwiające pisanie kodu i wgrywanie go na kontroler.
- Putty - narzędzie do łączności ze zdalnym serwerem wykorzystujące protokół SSH.
- Xdebug - rozszerzenie PHP umożliwiające debugowanie.
- Profiler wbudowany w Symfony4/Yii2.
- Visual paradigm - narzędzie do projektowania diagramów.
- Frizing - narzędzie do projektowania diagramów obwodów.

Rozdział 5.

Możliwość dalszego rozwoju systemu

5.1. Powiązania pomiędzy instancjami wykładu

Dziennik elektroniczny na aktualnym stadium rozwoju nie jest świadomy powiązania pomiędzy instancjami wykładu wchodzącymi w skład jednego rzeczywistego przedmiotu. Każdy prowadzący tworzy odrębną strukturę zajęć na swoim koncie i brakuje informacji na temat tego, w ramach jakiego przedmiotu są te zajęcia prowadzone.

Dzięki rozszerzeniu aplikacji o taką wiedzę, elektroniczny dziennik byłby w stanie generować raport podsumowujący dla całego przedmiotu, agregując statystyki obecności na wykładzie i ćwiczeniach dla każdego studenta. Dodatkowo można byłoby zautomatyzować procedurę odrabiania zajęć na innych ćwiczeniach.

Takie rozwiązanie wymagałoby szczególnej ostrożności, ponieważ informacje z różnych kont byłyby wzajemnie widoczne. Aktualnie taka sytuacja nie występuje.

5.2. Zautomatyzowana weryfikacja

Mankamentem zaprezentowanego w powyższej pracy podejścia jest konieczność manualnej weryfikacji, czy osoba zbliżająca legitymację do czytnika jest rzeczywiście jej właścicielem. W opracowaniu [2] przedstawiono projekt udostępniania informacji o studencie w oparciu o kartę RFID oraz dodatkową weryfikację poprzez sprawdzenie linii papilarnych. W systemie weryfikującym obecność na zajęciach można byłoby skorzystać z podobnego rozwiązania.

Innym dającym się zastosować podejściem jest system do rozpoznawania twarzy.

5.3. Integracja z uczelnianym systemem

Projektowany system od początku miał na celu integrację z zewnętrznym źródłem informacji o studentach. Bazę studentów, która w projekcie jest osobną aplikacją, łatwo można by zastąpić przez akademicką platformę. Kolejnym polem do integracji jest system logowania. Korzystanie z konta z USOSa byłoby ułatwieniem dla korzystających z aplikacji pracowników i studentów oraz pozwoliłoby uniknąć przechowywania w systemie wrażliwych danych związanych z utworzonymi kontami.

5.4. Udostępnienie systemu studentom

Rozwinięciem systemu byłoby udostępnienie studentom funkcjonalności zalogowania się i wglądu do ich aktualnych statystyk związanych z obecnościami. Istotnym problemem byłoby tworzenie kont przypisanych do właściwej osoby. Można byłoby to rozwiązać poprzez integrację z uczelnianym systemem do logowania albo udostępniając studentom konta zakładane przez administratora, który zajmowałby się potwierdzeniem tożsamości.

5.5. Informowanie zainteresowanych o obecnościach

W cytowanym we wstępie opracowaniu [1] wskazane jest, że sprawdzanie obecności ma znaczenie nie tylko jako forma przymusu, ale również jako wyraz troski uczelni o swoich studentów. Wskazane jest, że ‘wczesna interwencja’ w przypadku opuszczania przez ucznia zajęć, może zapobiec przerwaniu przez niego studiów. Nasałwa to bardzo wiele możliwości rozwoju aplikacji weryfikującej obecności. Referowaną platformę można by wyposażyć w możliwość informowania studenta o tym, że limit jego nieobecności na pewnych zajęciach jest bliski wyczerpania się.

Możliwe stałoby się automatyczne informowanie organów uczelnianych o kłopotach studenta na podstawie jego absencji.

5.6. Platforma do szybkiego reagowania

Idąc tym tropem, integrując uczelniane systemy, udostępniając studentom wgląd w ich obecności i umożliwiając interakcje poprzez kanały takie jak mail czy sms, można z prostej aplikacji stworzyć rozbudowaną platformę do monitorowania wyników studenta i adekwatnego reagowania w przypadku wykrycia potencjalnych problemów. Wiążąc informacje na temat tego, na jakim etapie studiów znajduje się student z jego aktualnymi wynikami, byłoby możliwe automatyczne dopasowanie

pomocy, takiej jak rozmowa z pracownikiem uczeni odpowiedzialnym za studentów, czy zaproponowanie dodatkowych zajęć.

Rozdział 6.

Podsumowanie

Powyższa praca w kompleksowy sposób przedstawia proces od projektowania do wdrożenia systemu do monitorowania obecności studentów na zajęciach uniwersyteckich.

System jest zrozumiały i łatwy w obsłudze, jednak ze względu na to, że jak dotąd nie został włączony w istniejącą architekturę cyfrową żadnego uniwersytetu, może wymagać dostosowania.

Projekt pozwala na prowadzenie kontroli obecności na wielu zajęciach jednocześnie i wygodne przetwarzanie zebranych danych.

Na tle przytoczonych w rozdziale 2 przykładów innych realizacji podobnych systemów, opisany powyżej projekt jest przedstawiony w sposób najbardziej kompleksowy.

Bibliografia

- [1] Debbie Bevitt and Chris Baldwin and Jane Calvert, *Intervening Early: Attendance and Performance Monitoring as a Trigger for First Year Support in the Biosciences* 2016, Bioscience Education <https://doi.org/10.3108/beej.15.4>
- [2] Asiya R. Shaikh, Dipali.S.Sahane, Pradip V.Wagh *RFID and FINGERPRINT based Students Database System* 2020 <https://www.irjet.net/archives/V7/i4/IRJET-V7I4445.pdf>
- [3] Vishal Bhalla and Tapodhan Singla and Ankit Gahlot and Vijay Gupta *Bluetooth Based Attendance Management System* 2013 <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.645.1573>
- [4] Oo, Zaw Lin and Win Lai, Theint and Than, Maung Maung *Web Server Base RFID Attendance Record Systems* 2018 https://www.researchgate.net/publication/333115623_Web_Server_Base_RFID_Attendance_Record_System/comments
- [5] Patel, Unnati and Swaminarayan, Priya *Computer Science and Management Studies Development of a Student Attendance Management System Using RFID and Face Recognition: A Review* 2014, International Journal of Advance Research in Computer Science and Management Studies https://www.researchgate.net/publication/325819350_Computer_Science_and_Management_Studies_Development_of_a_Student_Attendance_Management_System_Using_RFID_and_Face_Recognition_A_Review
- [6] Arulogun, Oladiran and Olatunbosun, Adeboye and A., Fakolujo and Olayemi Mikail, Olaniy *RFID-Based Students Attendance Management System* 2013, International Journal of Engineering and Scientific Research https://www.researchgate.net/publication/235598499_RFID-Based_Students_Attendance_Management_System
- [7] Shoewu, Oluwagbemiga and Mekanjuola, N. and Ajasa, Abiodun and Oluwafemi J., Ayangbekun *Design and Implementation of an Rfid Based Automated Students Attendance System R BASAS* 2015, JOURNAL OF ADVANCEMENT IN ENGINEERING AND TECHNOLOGY

https://www.researchgate.net/publication/235598499_RFID-Based_Students_Attendance_Management_System

- [8] https://en.wikipedia.org/wiki/Radio-frequency_identification
- [9] ZARZĄDZENIE Nr 116/2020 Rektora Uniwersytetu Wrocławskiego z dnia 3 września 2020 r https://bip.uni.wroc.pl/download/attachment/25560/nr_116_2020_zarzadzenie_funkcjonowanie-uwr-w-zwiazku-z-covid_19.pdf
- [10] <https://getbootstrap.com/>
- [11] <https://github.com/kartik-v/yii2-widget-timepicker>
- [12] <https://github.com/2amigos/yii2-date-time-picker-widget>
- [13] <https://github.com/2amigos/yii2-date-picker-widget>
- [14] <https://www.yiiframework.com/>
- [15] <https://getcomposer.org/>
- [16] <https://www.postgresql.org/>
- [17] <https://www.doctrine-project.org/>
- [18] <https://symfony.com/>
- [19] https://en.wikipedia.org/wiki/Representational_state_transfer/
- [20] https://en.wikipedia.org/wiki/Amazon_Web_Services
- [21] <https://github.com/greiman/UsbFat>
- [22] <https://pl.wikipedia.org/wiki/CRUD>
- [23] https://en.wikipedia.org/wiki/Representational_state_transfer