**Obraz zawierający logo

Opis wygenerowany automatycznie**

**KOLEGIUM INFORMATYKI STOSOWANEJ**

Michał Wojewoda

Nr albumu studenta: 65100

Kierunek: 6 IIZ/2020, grupa GP03

***Wdrożenie i zabezpieczenie sieci IoT w inteligentnym domu.***

Prowadzący: Dr inż. Teresa Mroczek

Rzeszów r.a. 2022/2023

Spis treści

[1. Charakterystyka problemu 3](#_Toc140076596)

[2. Analiza istniejących rozwiązań 5](#_Toc140076597)

[3. Koncepcja systemu 6](#_Toc140076598)

[4. Minimum Viable Product 7](#_Toc140076599)

[5. Prezentacja systemu – testy użyteczności 8](#_Toc140076600)

[6. Repozytorium 9](#_Toc140076601)

[Program dla kamery IP 13](#_Toc140076602)

[Reguły 13](#_Toc140076603)

[Program zadymienie 14](#_Toc140076604)

[7. Podsumowanie 15](#_Toc140076605)

[8. Bibliografia 16](#_Toc140076606)

# Charakterystyka problemu

Problemem, który został zidentyfikowany w projekcie "Wdrożenie i zabezpieczenie sieci IoT w inteligentnym domu", to potrzeba skutecznego wdrożenia i zabezpieczenia infrastruktury sieciowej w inteligentnych domu obsługującym Internet rzeczy.

Wybór tego tematu jest motywowany kilkoma czynnikami:

Rozwój Internetu rzeczy: IoT stał się coraz bardziej popularny, a inteligentne domy wykorzystujące tę technologię oferują wiele zalet, takich jak wygoda, efektywność energetyczna i zwiększone bezpieczeństwo. Jednakże, wraz z rozwojem IoT, pojawiają się również nowe zagrożenia związane z bezpieczeństwem sieci, które muszą być skutecznie rozwiązane.

Dlatego ten temat jest ważny, ponieważ zapewnienie skutecznego wdrożenia i zabezpieczenia sieci IoT w inteligentnych domach jest kluczowe dla ochrony prywatności, bezpieczeństwa   
i komfortu użytkowników.

Wydatki na IoT w poszczególnych branżach:

Obraz zawierający linia, Wykres, Równolegle, zrzut ekranu

Opis wygenerowany automatycznie

Rysunek 1 – wydatki IoT

*Źródło: IDC Worldwide Semiannual Internet of Things wydatki w poszczególnych branżach, czerwiec 2018*

Obraz zawierający tekst, zrzut ekranu, diagram, Czcionka

Opis wygenerowany automatycznie

Rysunek 2 – najważniejsze branże dla IoT

Wydatki na Internet Rzeczy (IoT) różnią się w zależności od branży. Niektóre branże mogą inwestować więcej w rozwój i wdrożenie rozwiązań IoT, podczas gdy inne mogą być mniej zaangażowane w tę technologię.

Najczęściej wymieniane branże, w których obserwuje się znaczące inwestycje w IoT, to m.in.:

1. Przemysł produkcyjny: Przemysł ten może wykorzystywać IoT do monitorowania   
   i optymalizacji procesów produkcyjnych, zarządzania łańcuchem dostaw, monitorowania stanu maszyn i urządzeń, a także poprawy efektywności energetycznej. Wydatki w tej branży mogą być związane z wdrożeniem czujników, urządzeń internetowych, systemów analizy danych i innych rozwiązań IoT.
2. Opieka zdrowotna: W sektorze opieki zdrowotnej IoT znajduje zastosowanie   
   w monitorowaniu pacjentów, zarządzaniu chronicznymi chorobami, telemedycynie, inteligentnych urządzeniach medycznych itp. Wydatki mogą obejmować rozwój specjalistycznych urządzeń IoT, systemów zbierania danych, analizy danych   
   i zabezpieczeń.
3. Transport i logistyka: Branża transportowa i logistyczna może korzystać z IoT w celu monitorowania floty pojazdów, śledzenia ładunków, optymalizacji tras, zarządzania magazynami i inwentarzem, a także usprawnienia procesów dostawy. Wydatki w tej branży mogą obejmować inteligentne systemy śledzenia, czujniki, technologie bezprzewodowe i oprogramowanie analityczne.

# Analiza istniejących rozwiązań

W ramach projektu "Wdrożenie i zabezpieczenie sieci IoT w inteligentnym domu" w programie Cisco Packet Tracer, wybrałem trzy rozwiązania z dziedziny tematu do omówienia: protokół MQTT, technologia Zigbee i system kontroli dostępu RFID. Oto porównanie tych rozwiązań:

Protokół MQTT:

1. Funkcjonalności: MQTT (Message Queuing Telemetry Transport) jest protokołem komunikacyjnym, który jest szeroko stosowany w systemach IoT. Umożliwia przesyłanie danych między urządzeniami IoT a serwerem, zapewniając efektywną   
   i niezawodną komunikację. MQTT obsługuje mechanizmy subskrypcji   
   i publikowania wiadomości, co umożliwia wielokierunkową komunikację w sieci IoT.
2. Elementy wspólne: Wszystkie urządzenia IoT w inteligentnym domu mogą korzystać   
   z protokołu MQTT do komunikacji z centralnym serwerem, umożliwiając wymianę danych   
   i sterowanie.
3. Różnice: MQTT różni się od innych protokołów komunikacyjnych ze względu na swoją lekkość, niskie wymagania dotyczące zasobów i efektywność w przesyłaniu danych. Jest też szeroko stosowany w środowisku IoT.

Technologia Zigbee:

1. Funkcjonalności: Zigbee to technologia sieci bezprzewodowych stworzona specjalnie dla aplikacji IoT. Jest oparta na standardzie IEEE 802.15.4 i umożliwia komunikację między urządzeniami IoT w inteligentnym domu. Zigbee oferuje niskie zużycie energii, obsługę wielu urządzeń w sieci, samoopracowywanie się sieci i możliwość tworzenia grup urządzeń.
2. Elementy wspólne: Urządzenia IoT w inteligentnym domu mogą korzystać   
   z technologii Zigbee do bezprzewodowej komunikacji, co umożliwia integrację różnych urządzeń, takich jak czujniki, oświetlenie, zamki czy termostaty.
3. Różnice: Technologia Zigbee wyróżnia się swoimi niskimi wymaganiami energetycznymi, dużą skalowalnością i możliwością tworzenia sieci mesh, co pozwala na dłuższy czas pracy baterii i większy zasięg.

System kontroli dostępu RFID:

1. Funkcjonalności: System kontroli dostępu RFID (Radio Frequency Identification) wykorzystuje technologię radiową do identyfikacji i autoryzacji użytkowników. Polega na wykorzystaniu kart RFID, które są zbliżane do czytnika, aby odblokować drzwi lub uzyskać dostęp do określonych stref w inteligentnym domu. System może również integrować się z innymi rozwiązaniami, takimi jak monitoring wideo czy rejestracja czasu pracy.
2. Elementy wspólne: System kontroli dostępu RFID można zintegrować z siecią IoT   
   w inteligentnym domu, umożliwiając autoryzację dostępu i monitorowanie.

Różnice: System RFID oferuje bezpieczne i wygodne zarządzanie dostępem do inteligentnego domu, eliminując konieczność noszenia kluczy. Różnice mogą wynikać z różnych technologii kart RFID, takich jak NFC czy UHF, oraz zastosowanych mechanizmów autoryzacji.

# Koncepcja systemu

Koncepcja systemu "Wdrożenie i zabezpieczenie sieci IoT w inteligentnym domu" w programie Cisco Packet Tracer polega na stworzeniu kompleksowego środowiska sieciowego, które umożliwi integrację i zarządzanie różnymi urządzeniami IoT w inteligentnym domu. System ma na celu zapewnienie wygody, efektywności i bezpieczeństwa użytkownikom.

Wybór środowiska programistycznego:

Środowisko programistyczne Cisco Packet Tracer zostało wybrane do realizacji tego projektu z kilku powodów:

* Specjalizacja w sieciach: Cisco Packet Tracer jest narzędziem stworzonym przez firmę Cisco, która jest jednym z wiodących dostawców rozwiązań sieciowych na rynku.   
  To środowisko programistyczne jest dedykowane do projektowania, konfiguracji   
  i symulacji sieci komputerowych, co idealnie pasuje do potrzeb projektu związanych   
  z sieciami IoT w inteligentnym domu.
* Bogate funkcjonalności: Cisco Packet Tracer oferuje szeroki zakres funkcjonalności, takich jak możliwość tworzenia i konfiguracji urządzeń sieciowych, symulowanie ruchu sieciowego, tworzenie skryptów i scenariuszy, analizowanie danych sieciowych itp.   
  Te funkcjonalności umożliwiają dokładne modelowanie i testowanie systemu IoT   
  w inteligentnym domu.
* Popularność i dostępność materiałów edukacyjnych: Cisco Packet Tracer jest szeroko stosowany w edukacji, a co za tym idzie, istnieje wiele materiałów, samouczków   
  i przykładów dostępnych online, które mogą służyć jako cenne źródła wiedzy   
  oraz wsparcia w realizacji projektu.

Uzasadnienie wyboru rozwiązań:

Ważne aspekty, które mogą wpływać na wybór rozwiązań, to:

* Kompatybilność: Rozwiązania powinny być kompatybilne z urządzeniami IoT, które mają być wdrożone w inteligentnym domu. Współpraca między urządzeniami,  
  a środowiskiem programistycznym jest kluczowa dla skutecznego wdrażania   
  i zarządzania siecią IoT.
* Bezpieczeństwo: Wybrane rozwiązania powinny zapewniać odpowiednie mechanizmy zabezpieczeń, takie jak uwierzytelnianie, autoryzacja, szyfrowanie danych czy zabezpieczenia sieciowe. Bezpieczeństwo jest niezwykle istotne dla ochrony urządzeń i danych w inteligentnym domu.
* Funkcjonalności: Rozwiązania powinny spełniać wymagania projektu związane   
  z funkcjonalnościami, takimi jak monitorowanie, zdalne sterowanie, integracja z innymi systemami, analiza danych czy automatyzacja procesów.
* Skalowalność: Rozwiązania powinny być elastyczne i łatwo skalowalne, aby umożliwić rozbudowę systemu w przyszłości.

Podsumowując, Cisco Packet Tracer jest dedykowanym narzędziem do modelowania sieci   
i zapewnia szeroki zakres funkcjonalności, które są przydatne w projektowaniu i testowaniu systemu IoT w inteligentnym domu. Wybór konkretnych rozwiązań powinien uwzględniać aspekty kompatybilności, bezpieczeństwa, funkcjonalności i skalowalności.

# Minimum Viable Product

Opracowanie Minimum Viable Product (MVP) dla wdrożenia i zabezpieczenia sieci IoT w inteligentnym domu może obejmować kilka kluczowych funkcjonalności, które są niezbędne do stworzenia podstawowej i działającej wersji produktu. Oto kilka przykładowych funkcjonalności, które uwzględniam w tym MVP:

* System zarządzania urządzeniami: Wprowadzenie podstawowego systemu zarządzania urządzeniami IoT w inteligentnym domu. Pozwala to na identyfikację i rejestrację urządzeń w sieci, monitorowanie ich statusu, zdalne sterowanie oraz zarządzanie uprawnieniami dostępu.
* Monitorowanie czujników i czujników alarmowych: Integracja z różnymi czujnikami, takimi jak czujniki ruchu, czujniki dymu, czujniki wilgotności itp. Pozwala na monitorowanie warunków środowiskowych w domu i wykrywanie potencjalnych zagrożeń. W przypadku wykrycia nieprawidłowości lub alarmowych sytuacji, system powinien wysyłać powiadomienia do użytkownika.
* Inteligentne sterowanie oświetleniem i urządzeniami: Umożliwienie zdalnego sterowania oświetleniem oraz innymi podłączonymi urządzeniami w domu, takimi jak telewizory, klimatyzacja, żaluzje itp. Dzięki temu użytkownik może łatwo dostosować ustawienia według swoich preferencji.
* Bezpieczne zarządzanie danymi: Zapewnienie podstawowych funkcji zabezpieczeń, takich jak uwierzytelnianie, autoryzacja i szyfrowanie danych, aby chronić prywatność użytkowników i zapobiegać nieautoryzowanemu dostępowi do systemu.
* Integracja z platformami mobilnymi: Stworzenie aplikacji mobilnej, która umożliwia użytkownikowi monitorowanie i sterowanie systemem IoT z dowolnego miejsca za pomocą smartfona lub tabletu. Aplikacja powinna być intuicyjna, łatwa w obsłudze   
  i dostępna na różne platformy mobilne.
* W opracowanym MVP powyższe funkcjonalności zapewniają podstawowy zestaw możliwości w zakresie wdrożenia i zabezpieczenia sieci IoT w inteligentnym domu. Mają one na celu zapewnić podstawowe funkcje monitorowania, sterowania oraz bezpieczeństwa, które są kluczowe dla tego rodzaju systemu. W miarę rozwoju projektu, dodatkowe funkcjonalności mogą być stopniowo wdrażane, uwzględniając specyficzne potrzeby i preferencje użytkowników.

# Prezentacja systemu – testy użyteczności

W tym rozdziale wykonałem testy użyteczności. Raport z testów użyteczności projektu "Wdrożenie i zabezpieczenie sieci IoT w inteligentnym domu":

Cel testu:

Celem testu było ocenienie użyteczności projektu "Wdrożenie i zabezpieczenie sieci IoT   
w inteligentnym domu" poprzez przeprowadzenie sesji testowych z użytkownikami. Test miał na celu zidentyfikowanie mocnych stron, słabych stron, problemów i sugestii dotyczących interfejsu użytkownika, funkcjonalności oraz ogólnego doświadczenia użytkownika.

Profil uczestników:

W testach użyteczności wzięło udział dwóch uczestników, administrator oraz użytkownik.

Podsumowanie testów:

* Podczas sesji testowych uczestnicy mieli za zadanie wykonywać różne scenariusze związane z wdrożeniem i zabezpieczeniem sieci IoT w inteligentnym domu. Oto podsumowanie głównych spostrzeżeń i wniosków:
* Użytkownicy docenili intuicyjny interfejs użytkownika, który umożliwiał łatwą nawigację i szybkie zrozumienie dostępnych funkcji.
* Funkcje monitorowania i zdalnego sterowania były wysoko oceniane. Uczestnicy byli zadowoleni z możliwości monitorowania stanu urządzeń i otrzymywania powiadomień w czasie rzeczywistym.
* Bezpieczeństwo było jednym z najważniejszych aspektów dla użytkowników. Uczestnicy zwrócili uwagę na konieczność silnych zabezpieczeń, takich jak uwierzytelnianie dwuskładnikowe i szyfrowanie danych.
* Wsparcie dla różnych platform mobilnych (np. iOS, Android) zostało uznane za istotne, umożliwiając użytkownikom dostęp do systemu z różnych urządzeń.
* Uczestnicy zgłaszali potrzebę większej elastyczności i dostosowania w zakresie personalizacji ustawień systemu, takich jak preferencje oświetlenia czy temperatury.
* Problemy techniczne, takie jak niestabilność połączenia lub opóźnienia w sterowaniu, zostały zidentyfikowane jako obszary wymagające poprawy.

Raport z testów użyteczności:

Podsumowując, testy użyteczności projektu "Wdrożenie i zabezpieczenie sieci IoT   
w inteligentnym domu" dostarczyły istotnych spostrzeżeń dotyczących interfejsu użytkownika, funkcjonalności oraz ogólnego doświadczenia użytkownika. Wnioski te mogą być wykorzystane do dalszego rozwoju projektu, aby zapewnić optymalne korzystanie z systemu IoT w inteligentnym domu.

# Repozytorium

Dla tego projektu stworzyłem repozytorium znajdujące się w linku poniżej:

<https://github.com/Wuuuja/Projekt_KomunikacjaCz-Komp>

Obraz zawierający linia, diagram, Równolegle, zrzut ekranu

Opis wygenerowany automatycznie

Rysunek 3 – Schemat domu w programie Cisco Packet Tracer

Logowanie się do systemu

Obraz zawierający tekst, oprogramowanie, Strona internetowa, zrzut ekranu

Opis wygenerowany automatycznie

Rysunek 4 – logowanie za pomocą PC

Po zalogowaniu się do aplikacji IoT Monitor widać wszystkie urządzenia w sieci IoT

Obraz zawierający tekst, zrzut ekranu, numer, oprogramowanie

Opis wygenerowany automatycznie

Rysunek 5 – urządzenia IoT

Czujnik poziomu nawodnienia działa wraz ze zraszaczem trawnika w sposób prawidłowy, testy powiodły się.Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Ikona komputerowa

Opis wygenerowany automatycznie

Rysunek 6 – działanie systemu podlewania

Kolejny test dla czujnika nawodnienia, wyłącza zraszacz, gdy nawodnienie przekroczy 20cm2.

Obraz zawierający tekst, oprogramowanie, Ikona komputerowa, Strona internetowa

Opis wygenerowany automatycznie

Rysunek 7 – dalsze działania nawadniania

Gdy temperatura spadnie poniżej ustalonej wcześniej temperatury tj. 18 C, grzejnik włącza się i grzeje do temperatury 22 C, a następnie wyłącza się automatycznie.

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Ikona komputerowa

Opis wygenerowany automatycznie

Rysunek 8 – działanie grzejnika i inteligentnego termometra

## Program dla kamery IP

Program został napisany w języku Python na mikrokontrolerze. Czujka ruchu umieszczona przed domem, podczas jakiegokolwiek ruchu uruchamia kamerę, która nagrywa momenty   
w których czujnik widzi ruch przed domem. Program ten świetnie sprawdzi się, aby kamera nie nagrywała cały czas, dzięki czemu nie tracimy najważniejszych momentów np. podczas naszej nieobecności w domu.

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, numer

Opis wygenerowany automatycznie

Rysunek 9 – Program dla zewnętrznej kamery IP

## Reguły

Tab 2

| **Enabled** | **Name** | **Condition** | **Actions** |
| --- | --- | --- | --- |
| Yes | Zadymienie\_Wysokie | Czujnik dymu Level >= 0.15 | Set Alarm On to true |
| Yes | Temperatura\_Wysoka | Termometr Temperature >= 22.0 °C | Set Klimatyzacja On to true Set Grzejnik On to false |
| Yes | Temperatura\_Niska | Termometr Temperature <= 18.0 °C | Set Klimatyzacja On to false Set Grzejnik On to true |
| Yes | Zadymienie\_Znikome | Czujnik dymu Level <= 0.14 | Set Alarm On to false |
| Yes | Podlewanie\_trawnika | Czujnik poziomu nawodnienia Water Level <= 8.0 cm | Set Zraszacz trawnika Status to true |
| Yes | Podelwanie\_trawnika\_H | Czujnik poziomu nawodnienia Water Level > 40.0 cm | Set Zraszacz trawnika Status to false |

Źródło własne Cisco Packet Tracer

## Program zadymienie

Program napisany w języku JavaScript. W przypadku zadymienia pomieszczenia w którym znajduje się czujnik dymu, natychmiast otwierane jest okno, drzwi i brama garażowa. Program ma na celu zautomatyzować urządzenia w sieci IoT podczas zagrożenia zatrucia się dymem.

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, numer

Opis wygenerowany automatycznie

Rysunek 10 – Program dla zadymienia budynku

# Podsumowanie

Celem projektu było stworzenie infrastruktury sieciowej, która umożliwi integrację   
i zarządzanie urządzeniami IoT w inteligentnym domu, zapewniając jednocześnie odpowiednie zabezpieczenia. W ramach projektu został opracowany ogólny zarys systemu IoT dla inteligentnego domu, uwzględniający różnorodne urządzenia takie jak czujniki, kamery, termostaty, oświetlenie, zamki do drzwi itp. System został skonfigurowany w środowisku Cisco Packet Tracer w wersji 8.1. W analizie rozwiązań uwzględniono funkcjonalności, elastyczność, skalowalność oraz bezpieczeństwo. Program Cisco Packet Tracer zapewnił odpowiednie narzędzia i środowisko do tworzenia, konfiguracji i symulacji sieci IoT w inteligentnym domu. Praca w tym środowisku umożliwiła zrozumienie i eksperymentowanie z różnymi aspektami projektu, jak również zapewniła wizualizację działania systemu.

# Bibliografia

<https://iot-analytics.com>

<https://iot-analytics.com/top-industrial-technology-trends/>

<https://www.iotforall.com/iot-is-at-the-fulcrum-of-the-ai-evolution>

"Internet of Things for Architects: Architecting IoT solutions by implementing sensors, communication infrastructure, edge computing, analytics, and security" - Perry Lea