

UNIWERSYTET GDAŃSKI

Wydział Matematyki, Fizyki i Informatyki

Specyfikacja systemu kamer Smarthome.

Autorzy:

Mateusz Domino,

Dominik Krakowski,

Michał Kopczewski.



Gdańsk 2024.

1. Spis treści

1. Spis treści.....	2
Cel dokumentu	3
1. Zakres produktu	3
2. Opis ogólny systemu	3
3. Wymagania funkcjonalne.....	3
3.1 Rejestracja i logowanie użytkownika	3
3.2 Zarządzanie urządzeniami.....	3
3.3 Monitoring i powiadomienia	4
3.4 Zasilanie awaryjne.....	4
3.5 Tryb offline/online.....	4
3.6 Użytkownicy.....	4
3.7 Diagramy Use-Case.....	5
4. Wymagania нефункционалне	17
4.1 Wydajność.....	17
4.2 Bezpieczeństwo	17
4.3 Niezawodność	17
4.4 Użyteczność	17
4.5 Skalowalność.....	18
Wymagania sprzętowe:.....	18
Urządzenie z kamerą	18
Serwer główny	18
Wymagania minimalne	18
Wymagania zalecane	18
Ograniczenia prawne.....	19
Monitoring obejmuje wyłącznie teren prywatny	19
Monitoring obejmuje również obszar publiczny	19
Monitoring obejmuje teren prywatny innych podmiotów prawnych	19

Cel dokumentu

Dokument stanowi jedyne źródło wymagań aplikacji. Stanowi podstawę specyfikacji oprogramowania oraz urządzeń na którym będzie ono zainstalowane. Dokument przeznaczony głównie dla zespołu deweloperskiego zajmującego się wytwarzaniem oprogramowania.

1. Zakres produktu

System monitoringu wizyjnego instalowany w celu ochrony osób i mienia. System ma umożliwiać podgląd na żywo kamer lub/i odtworzenie ich historycznych nagrań. Zabezpieczenia tego typu znacznie zwiększają szansę identyfikacji i odnalezienia sprawców potencjalnego włamania.

2. Opis ogólny systemu

Na system składa się:

- Komputer główny, będący jednostką centralną, decyzyjną
- Router integralny do komputera głównego, zapewniający połączenie bezprzewodowe między urządzeniami systemu w sieci lokalnej, odrębnej od i niedostępnej dla internetu zewnętrznego
- Każde połączone urządzenie, np. kamera, czujnik

3. Wymagania funkcjonalne

3.1 Rejestracja i logowanie użytkownika

3.1.1: System powinien umożliwiać użytkownikom logowanie i rejestrację przy pierwszym uruchomieniu.

3.1.2: Autoryzacja użytkownika musi być chroniona co najmniej hasłem, pinem lub innym

3.2 Zarządzanie urządzeniami

3.2.1: Użytkownik powinien mieć możliwość dodawania, usuwania i konfigurowania kamer oraz czujników.

3.2.2: System powinien automatycznie wykrywać nowe urządzenia po ich podłączeniu do sieci lokalnej systemu.

3.2.3: Urządzenia powinny komunikować się z serwerem za pomocą protokołu zabezpieczonego, np. TLS.

3.3 Monitoring i powiadomienia

3.3.1: System powinien rejestrować wideo.

3.3.2: System powinien wysyłać powiadomienia na urządzenia mobilne w przypadku wykrycia zdarzeń.

3.3.3: Powiadomienia powinny zawierać opis zdarzenia.

3.4 Zasilanie awaryjne

3.4.1: Każde urządzenie (czujniki i kamery) oraz główny komputer powinny być wyposażone w akumulatory pozwalające na działanie przez co najmniej 12 godzin w razie awarii zasilania.

3.4.2: System powinien powiadomić użytkownika o przejściu na zasilanie awaryjne.

3.4.3: Po powrocie zasilania sieciowego system powinien automatycznie wrócić do zasilania z sieci oraz naładować akumulatory.

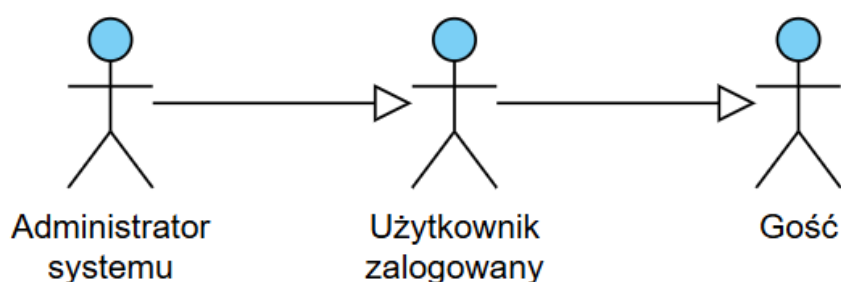
3.5 Tryb offline/online

3.5.1: Domyślny tryb działania to offline, z przechowywaniem danych lokalnie na komputerze połączonym z kamerą lub podłączonym do niego nośniku.

3.5.2: Użytkownik może ręcznie przełączyć system w tryb online, umożliwiając synchronizację danych z chmurą lub aktualizacje.

3.5.3: Dane przesyłane do chmury muszą być szyfrowane za pomocą co najmniej protokołu AES.

3.6 Użytkownicy



3.7 Diagramy Use-Case

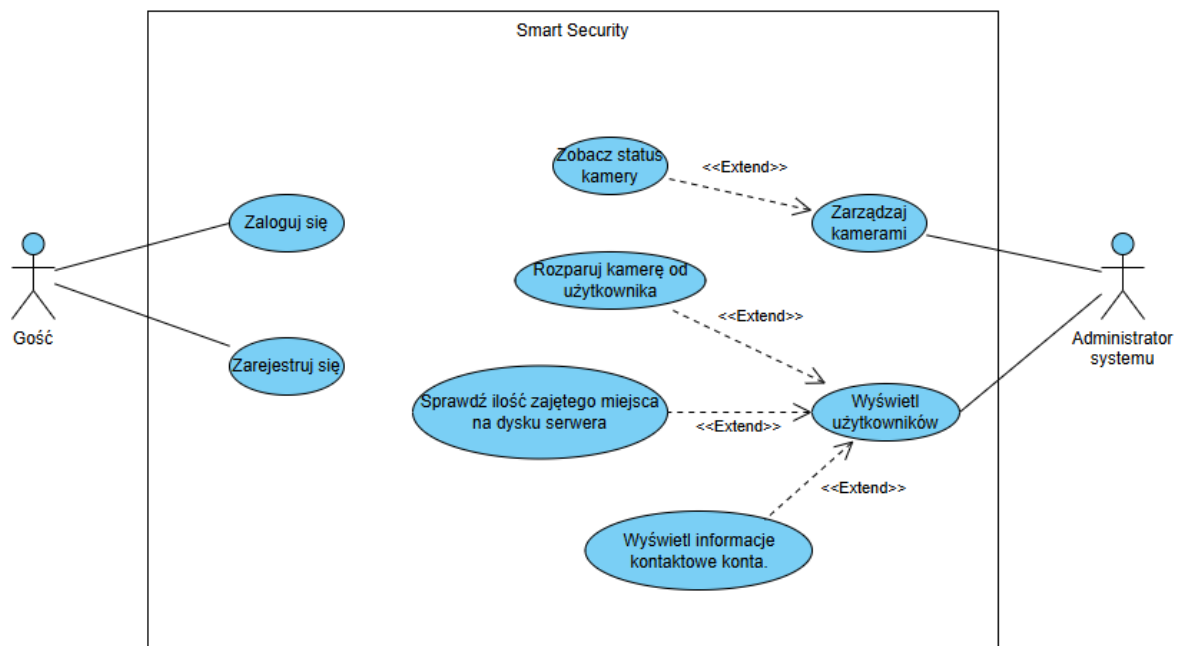


Diagram przypadków użycia dla użytkownika niezalogowanego (gościa) oraz administratora systemu. Super-użytkownik nie posiada dostępu do podglądu kamer oraz nie może przeglądać zapisów z nich.

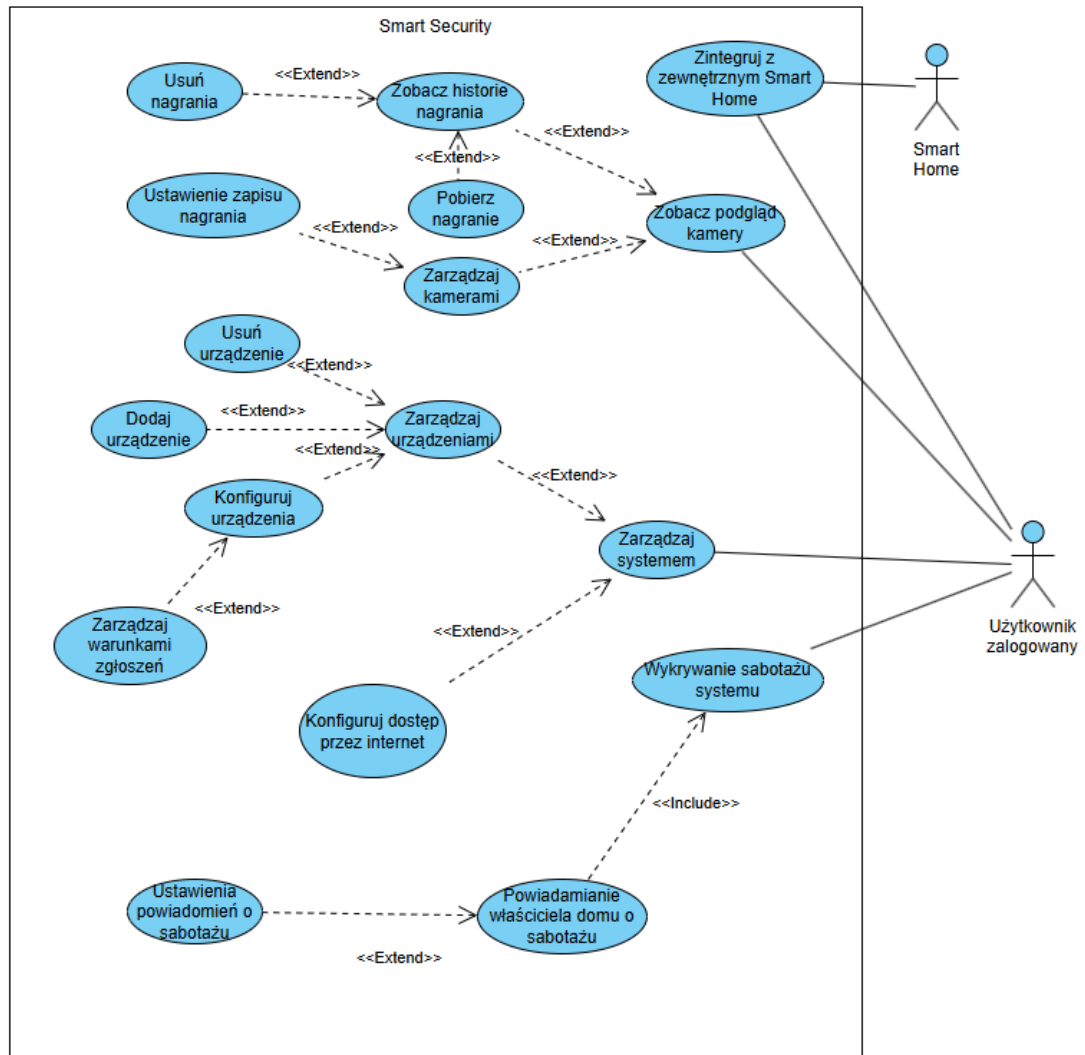


Diagram użycia dla użytkownika zalogowanego.

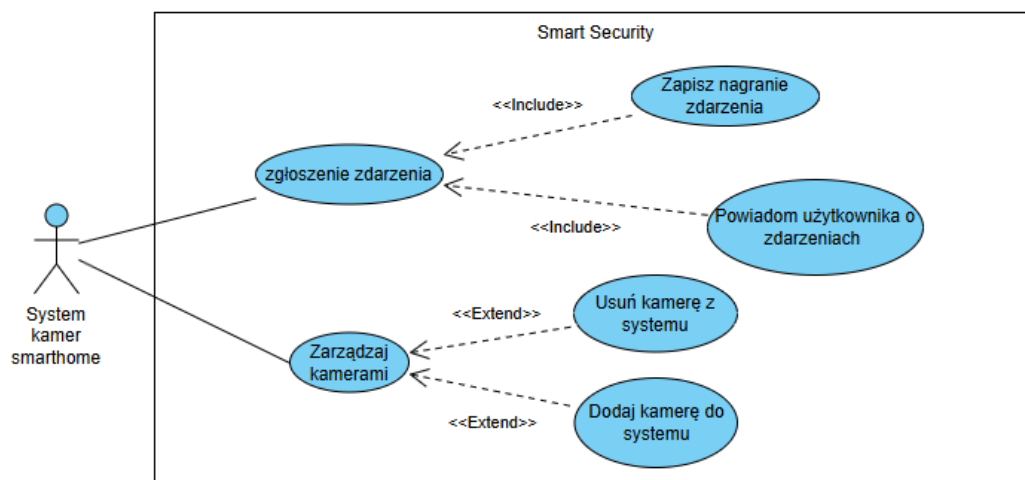


Diagram użycia dla systemu kamer.

ID:	A-1
Nazwa:	Logowanie użytkownika
Aktorzy główni:	Gość
Aktorzy pomocniczy:	Brak
Poziom:	Gościa
Priorytet:	P2
Opis:	Użytkownik uruchamia aplikację w telefonie i loguje się do systemu.
Wyzwalacze:	1. Przycisk “zaloguj się”
Warunki początkowe:	Brak
Warunki końcowe:	Zalogowany użytkownik
Scenariusz Główny:	<ol style="list-style-type: none"> 1. Użytkownik otwiera aplikację 2. Aplikacja wyświetla ekran zawierający: <ol style="list-style-type: none"> a. Pole Adres e-mail, b. Pole Hasło.
Scenariusz alternatywne	Użytkownik podał niepoprawne dane logowania.
Rozszerzenia:	Brak
Wyjątki	Brak
Dodatkowe wymagania	Brak

ID:	A-2
Nazwa:	Rejestracja użytkownika
Aktorzy główni:	Gość
Aktorzy pomocniczy:	Brak
Poziom:	Gościa
Priorytet:	P2
Opis:	Użytkownik uruchamia aplikację w telefonie i rejestruje się do systemu.
Wyzwalacze:	1. Kliknięcie przycisku “Zarejestruj się” w ekranie logowania
Warunki początkowe:	Brak
Warunki końcowe:	Zarejestrowany użytkownik
Scenariusz Główny:	<ol style="list-style-type: none"> 1. Użytkownik otwiera aplikację 2. Aplikacja wyświetla ekran zawierający: <ol style="list-style-type: none"> a. Pole Adres e-mail, b. Pole Adres Kontaktowy, c. Pole Imię, d. Pole Nazwisko, e. Pole Hasło, f. Pole Powtórz hasło.
Scenariusz alternatywne	<p>Użytkownik podaje email, który jest już powiązany z pewnym kontem w systemie.</p> <p>Użytkownik podaje inne hasło w polu “Powtórz hasło” niż w polu “Hasło”.</p>
Rozszerzenia:	Brak
Wyjątki	Brak
Dodatkowe wymagania	Brak

ID:	C-1
Nazwa:	Zarządzanie kamerami w systemie.
Aktorzy główni:	Administrator systemu
Aktorzy pomocniczy:	Brak
Poziom:	Administradora
Priorytet:	P0
Opis:	Administrator loguje się do systemu i ma możliwość zarządzania kamerami w systemie.
Wyzwalacze:	Wejście do panelu zarządzania kamerami.
Warunki początkowe:	Administrator musi być zalogowany.
Warunki końcowe:	Lista kamer w systemie.
Scenariusz Główny:	<ol style="list-style-type: none"> 1. Administrator wchodzi na stronę zarządzania kamerami 2. Wyświetlana jest lista kamer z możliwością wyszukania po id.
Scenariusz alternatywne	Brak
Rozszerzenia:	<ol style="list-style-type: none"> 1. Administrator może wybrać opcję “zobacz status kamery”: <ol style="list-style-type: none"> a. Wyświetlany jest właściciel kamery wraz z informacjami kontaktowymi b. Wyświetlana jest informacja odnośnie wykorzystanego miejsca dyskowego przez kamerę. c. Wyświetlana jest informacja o ostatnich zdarzeniach. 2. Administrator może wybrać opcję “Rozparuj kamerę od użytkownika”: <ol style="list-style-type: none"> a. Użytkownik dostaje informację o rozparowaniu kamery wraz z odpowiednim uzasadnieniem, b. Kamera jest usuwana z konta użytkownika, jej zapis jest trzymany na serwerze w razie odwołania do decyzji.
Wyjątki	Brak
Dodatkowe wymagania	Typ konta super-użytkownika.

ID:	C-2
Nazwa:	Wyświetlenie użytkowników systemu.
Aktorzy główni:	Administrator systemu
Aktorzy pomocniczy:	Brak
Poziom:	Administradora
Priorytet:	P2
Opis:	Administrator loguje się do systemu i ma możliwość wyświetlenia użytkowników systemu.
Wyzwalacze:	Wejście do panelu zarządzania użytkownikami.
Warunki początkowe:	Administrator musi być zalogowany.
Warunki końcowe:	Lista użytkowników systemu.
Scenariusz Główny:	<ul style="list-style-type: none"> • Administrator wchodzi na stronę zarządzania użytkownikami, • Wyświetlana jest lista użytkowników.
Scenariusz alternatywne	Brak
Rozszerzenia:	<ol style="list-style-type: none"> 1. Administrator może wybrać opcję "Sprawdź ilość zajętego miejsca na dysku serwera". <ol style="list-style-type: none"> a. Wyświetlane jest podsumowanie z informacją o łącznym użyciu miejsca dyskowego. 2. Administrator może wybrać opcję "Wyświetl informacje kontaktowe konta". <ol style="list-style-type: none"> a. Wyświetlane są pełne dane potrzebne do kontaktu z użytkownikiem.
Wyjątki	Brak
Dodatkowe wymagania	Typ konta super-użytkownika.

ID:	B-1
Nazwa:	Zintegruj system ze Smarthome.
Aktorzy główni:	Użytkownik
Aktorzy pomocniczy:	Smart Home
Poziom:	Użytkownika zalogowanego
Priorytet:	P1
Opis:	Możliwość integracji systemu kamer z już istniejącym systemem smart home. Zdarzenia z czujników smart home mają moc sterować nagrywaniem. Przykładowo przemieszczenie telefonu właściciela domu poza jego obszar w trakcie dopuszczonych godzin wcześniej obsługujące włącznik światła będzie mogło również włączać nagrywanie.
Wyzwalacze:	Przycisk „Zintegruj ze smart home”
Warunki początkowe:	Użytkownik musi być zalogowany.
Warunki końcowe:	System monitoringu jest zintegrowany ze smart home
Scenariusz Główny:	Użytkownik zalogowany może w ustawieniach obu systemów je ze sobą zintegrować.
Scenariusz alternatywne	brak
Rozszerzenia:	brak
Wyjątki	brak
Dodatkowe wymagania	W domu musi być zainstalowany osobny system smart home

ID:	B-2
Nazwa:	Zobacz podgląd kamery
Aktorzy główni:	Użytkownik
Aktorzy pomocniczy:	Brak
Poziom:	Użytkownika
Priorytet:	P0
Opis:	Użytkownik loguje się do systemu i ma możliwość podglądu obrazu z kamery.
Wyzwalacze:	1. Kliknięcie przycisku “Zobacz podgląd kamery”
Warunki początkowe:	Użytkownik musi być zalogowany i posiadać kamerę dodaną do swojego profilu.
Warunki końcowe:	Wyświetlenie obrazu z kamery.
Scenariusz Główny:	<ol style="list-style-type: none"> Po zalogowaniu użytkownik wybiera określoną kamerę. Użytkownik wybiera przycisk Zobacz podgląd kamery. Obraz jest wyświetlany.
Scenariusz alternatywne	Kamera jest niedostępna.
Rozszerzenia:	<ol style="list-style-type: none"> Użytkownik może wybrać opcję “Zobacz historie nagrania”: <ol style="list-style-type: none"> Wyświetlana jest lista nagrań z kamery Użytkownik może wybrać opcję “Usuń nagrania”: <ol style="list-style-type: none"> System usuwa wybrane nagrania z systemu.
Wyjątki	Brak

Dodatkowe wymagania	Brak
---------------------	------

ID:	B-3
Nazwa:	Wykrywania sabotażu systemu.
Aktorzy główni:	Użytkownik
Aktorzy pomocniczy:	System kamer smarthome.
Poziom:	Użytkownika
Priorytet:	P1
Opis:	System wykrywa sabotaż kamery bądź szkodliwe działania w obrębie działania urządzenia oraz zbyt długi brak komunikacji centralnego serwera z kamerą.
Wyzwalacze:	Brak
Warunki początkowe:	Następuje niepożądane zdarzenie.
Warunki końcowe:	Kamera zapisuje nagrania zdarzenia oraz powiadamia użytkownika.
Scenariusz Główny:	<ol style="list-style-type: none"> 1. Kamera wykrywa niepożądane zdarzenie. 2. Kamera włącza nagrywanie zapisu. 3. Kamera przekazuje do systemu wystąpienie zdarzenia 4. Kamera przekazuje nagranie zdarzenia do serwera.
Scenariusz alternatywne	Brak
Rozszerzenia:	<ol style="list-style-type: none"> 1. Możliwość zmiany ustawień powiadomień o sabotażu. <ol style="list-style-type: none"> a. Możliwość wyłączenia powiadomień, b. Możliwość ustawienia powiadomień według priorytetu.
Wyjątki	Brak

Dodatkowe wymagania	Brak
---------------------	------

ID:	B-4
Nazwa:	Zarządzaj systemem kamer.
Aktorzy główni:	Użytkownik
Aktorzy pomocniczy:	Brak
Poziom:	Użytkownika
Priorytet:	P0
Opis:	Użytkownik loguje się do systemu, po czym może zobaczyć listę swoich urządzeń oraz nimi zarządzać: usuwać, dodawać oraz konfigurować.
Wyzwalacze:	Wejście do panelu zarządzania systemem.
Warunki początkowe:	Użytkownik musi być zalogowany do systemu.
Warunki końcowe:	Wyświetlenie listy urządzeń i przedstawienie dostępnych operacji na nich.
Scenariusz Główny:	<ol style="list-style-type: none"> 1. Wyświetlana jest lista urządzeń. 2. Użytkownik wybiera określone urządzenie. 3. Użytkownik wykonuje wybraną operację na urządzeniu.
Scenariusz alternatywne	Brak kamer dodanych do profilu użytkownika.
Rozszerzenia:	<ol style="list-style-type: none"> 1. Zarządzanie kamerami <ol style="list-style-type: none"> a. Wyświetlenie dostępnych operacji: b. Usuń urządzenie:

	<ul style="list-style-type: none"> i. Użytkownik może usunąć kamerę ze swojego profilu. ii. Usuwane są zapisy nagrań oraz historia zdarzeń. c. Dodaj urządzenie: <ul style="list-style-type: none"> i. Użytkownik może dodać nowe urządzenie do swojego profilu. d. Konfiguruj urządzenie: <ul style="list-style-type: none"> i. Ustawianie parametrów wykrywania zdarzeń oraz sposobu zapisywania nagrań. e. Konfiguruj dostęp przez internet: <ul style="list-style-type: none"> i. Zmienienie opcji zdalnego dostępu do kamery.
Wyjątki	Brak
Dodatkowe wymagania	Brak

ID:	SH-1
Nazwa:	Zgłoszenie zdarzenia przez system.
Aktorzy główni:	System kamer smarthome.
Aktorzy pomocniczy:	Brak
Poziom:	System kamer smarthome
Priorytet:	P0
Opis:	Kamera zgłasza wystąpienie incydentu do systemu, system zapisuje obraz z kamery oraz powiadamia użytkownika.
Wyzwalacze:	Brak.
Warunki początkowe:	Wystąpiło zdarzenie niepożądane.
Warunki końcowe:	Zapisano zdarzenie w systemie, jeśli włączone są powiadomienia to system również informuje użytkownika.
Scenariusz Główny:	<ul style="list-style-type: none"> 2. Kamera wykrywa incydent oraz rozpoczyna nagrywanie. 3. Kamera wysyła informacje o zdarzeniu do systemu. 4. System zapisuje zdarzenie oraz informację na jego temat. 5. (Opcjonalnie) system powiadamia użytkownika o incydencie rozpoznanym przez kamerę.
Scenariusz alternatywne	Kamera ma wyłączone zgłaszania incydentów.
Rozszerzenia:	Brak

Wyjątki	Brak
Dodatkowe wymagania	Brak

ID:	B-5
Nazwa:	Zarządzanie kamerami przez System.
Aktorzy główni:	System kamer smarthome.
Aktorzy pomocniczy:	Użytkownik.
Poziom:	System kamer smarthome
Priorytet:	P0
Opis:	Zarządzanie kamerami na żądanie użytkownika systemu.
Wyzwalacze:	Wykonanie odpowiedniej operacji przez użytkownika.
Warunki początkowe:	Przyjęto określone działanie.
Warunki końcowe:	Zmieniona konfiguracja kamery/kamer.
Scenariusz Główny:	<ol style="list-style-type: none"> 1. Użytkownik wysyła żądanie o zmienieniu listy kamer. 2. System przyjmuje żądanie. 3. System wykonuje określoną operację.
Scenariusz alternatywny	Niepoprawna operacja.
Rozszerzenia:	<ol style="list-style-type: none"> 1. Usuń kamerę <ol style="list-style-type: none"> a. Usunięcie kamery z bazy danych b. Usunięcie zapisu z kamer na serwerze. 2. Dodaj kamerę <ol style="list-style-type: none"> a. Sprawdzenie dostępności danej kamery. b. Przypisanie kamery do profilu użytkownika. c. Dodanie jej do listy kamer.
Wyjątki	Brak
Dodatkowe wymagania	Brak

4. Wymagania niefunkcjonalne

4.1 Wydajność

4.1.1: System musi być w stanie przetwarzać i przechowywać dane z co najmniej 8 kamer i 16 czujników jednocześnie.

4.1.2: Opóźnienie działania nie może przekraczać 10 sekund od momentu inicjacji zdarzenia.

4.2 Bezpieczeństwo

4.2.1: Dane przechowywane lokalnie i w chmurze muszą być zabezpieczone.

4.2.2: Uwierzytelnianie komunikacji między urządzeniami musi być zabezpieczone co najmniej protokołem TLS.

4.2.3: System musi zapewniać regularne aktualizacje zabezpieczeń, jeśli ustawienia na to pozwalają.

4.2.4: Jeśli przez określony czas nie ma połączenia między skonfigurowaną kamerą a serwerem zostaje to odnotowane jako potencjalny sabotaż kamery.

4.3 niezawodność

4.3.1: System musi działać bez przerwy przez co najmniej 95% czasu operacyjnego.

4.3.2: Każde urządzenie musi powiadamiać o spadku poziomu naładowania akumulatora poniżej 20%.

4.3.3: W przypadku fatalnego błędu system powinien się zrestartować.

4.4 użyteczność

4.4.1: Interfejs użytkownika musi być intuicyjny, z prostymi instrukcjami do konfiguracji urządzeń.

4.4.2: Użytkownik powinien mieć dostęp do podglądu i historii zdarzeń.

4.5 Skalowalność

4.5.1: System powinien umożliwiać dodanie dodatkowych kamer i czujników bez konieczności przeprowadzania innych modyfikacji.

Wymagania sprzętowe:

Urządzenie z kamerą

Ze względu na bardzo ograniczone zastosowanie urządzenia wymagania minimalne są takie same jak zalecane.

- 4 rdzeniowe CPU
- 1 GB RAM
- 32 GB ROM
- Dowolna dystrybucja Linux w najnowszej wersji
- Kamera 1 mpx
- Łączność z internetem 100 Mb/s (opcjonalnie)
- Opcjonalnie większy dysk/zewnętrzna pamięć w przypadku chęci przechowywania większej ilości historycznych danych.

Serwer główny

System musi być skalowalny, więc centralna maszyna musi być dostosowana mn. do ilości użytkowników, ilości i rozdzielczości kamer itd.

Wymagania minimalne

- 4 rdzeniowe CPU
- 4 GB RAM DDR3
- 128GB ROM typu SSD (system)
- Windows/Linux w najnowszej wersji
- Łączność z internetem 1000 mb/s
- 1TB ROM HDD (dane z kamer)
- UPS zdolny zasilać urządzenie przez min 12h.

Wymagania zalecane

- 20 rdzeniowy Intel Xeon/Porównywalny procesor AMD
- 128GB RAM DDR4
- 128 GB ROM typu SSD (system)
- Macierz dyskowa 24 dyski HDD po 5TB RAID 5 (dane z kamer)
- 10 Gigabit Ethernet
- Windows/Linux w najnowszej wersji
- UPS zdolny zasilać maszynę przez 30 min w celu bezpiecznego jej wyłączenia.

Ograniczenia prawne

Głównym przepisem ograniczającym możliwość przetwarzania danych z systemu monitoringu wizyjnego jest Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), w dalszej części zwane **RODO**. Zgodnie z kodeksem Cywilnym wizerunek stanowi dobro osobiste człowieka a jego naruszenie może wiązać się z konsekwencjami prawnymi.

Opisywany system jest dozwolony do użytku prywatnego, nota prawna dla podmiotów prawnych będzie się znacząco różnić.

Współmałżonek/współwłaściciel musi zostać poinformowany o monitoringu i wyrazić na niego zgodę.

Monitoring obejmuje wyłącznie teren prywatny

Instalacja monitoringu wizyjnego jest legalna na posesjach prywatnych w Polsce jest legalna i nie wymaga umieszczania żadnej informacji o tym pod warunkiem że system nie narusza prywatności innych osób. Zarejestrowane dane mogą być wykorzystywane do celów osobistych.

Monitoring obejmuje również obszar publiczny

System może obejmować również obszar poza posesją np. chodnik. Sama obserwacja na żywo bez zapisu ani przetwarzania danych jest legalna. Aby legalnie rejestrować/przetwarzać na użytek prywatny te dane wystarczy umieścić znak z informacją o monitoringu w widocznym miejscu. Na takim znaku musi być wskazany administrator danych, zazwyczaj jest to właściciel posesji. Na życzenie osób zarejestrowanych na monitoringu należy im udostępnić obraz na którym zostały zarejestrowane.

Monitoring obejmuje teren prywatny innych podmiotów prawnych

Jeśli system monitoringu obejmuje teren prywatny innej osoby należy wystąpić z prośbą do właściciela terenu o pozwolenie na nagrywanie, najlepiej pisemne.

Powyżej wymienione przepisy dotyczą wyłącznie rejestracji oraz przetwarzania danych na użytek własny. Domyślnym zastosowaniem systemu jest zapewnienie bezpieczeństwa osób i mienia dlatego w tym dokumencie nie są umieszczone informacje prawne dot. Udostępniania zapisanego materiału. Przed publikacją nagrań należy zapoznać się z aktualnymi przepisami.

Jako twórcy systemu zapewniamy że powyższe noty prawne są aktualne w momencie publikacji oprogramowania oraz wszelkich jego aktualizacji. Nie gwarantujemy że system będzie zawsze legalny.

