Funkcjonalność aplikacji

Aplikacja ma służyć do bezpiecznego dzielenia się między sobą poufnymi plikami. Po wysłaniu na serwer plików zaszyfrowanych za pomocą klucza symetrycznego, użytkownik będzie mógł ustawić termin wygaśnięcia pliku oraz zarządzać listą osób uprawnionych do jego odczytu. Służący do tego klucz symetryczny zostanie wtedy zaszyfrowany i przekazany według protokołu Diffiego-Hellmana.

1. Audytowanie

Administrator ma dostęp do danych audytowych przechowywanych w bazie danych oraz dostarczanych przez serwer aplikacji w postaci logów systemowych. Logi systemowe są dostępne dla administratora z poziomu aplikacji. Dane audytowe przechowują informacje na temat zdarzeń zachodzących w aplikacji. Zawierają dane o krytycznych funkcjach systemu: logowaniu, wylogowaniu, nieudanych próbach logowania, wyjątkach, wywoływanych metodach, a także o zmianach dokonywanych w bazie danych. Jest to szczególnie ważne w przypadku niniejszej aplikacji ze względu na jej poufny charakter. Dostęp do danych audytowych posiada jedynie administrator.

Funkcje bezpieczeństwa realizowane w ramach audytowania

- FAU_GEN.1
- FAU_GEN.2
- FAU_ARP.1.1
- FAU_ARP.1.2
- FAU_SAR.1.1
- FAU_SAR.1.2
- FAU_SAR.2.1
- FAU_STG.1.1
- FAU_STG.2.1

2. Weryfikacja i uwierzytelnianie

System posiada mechanizm kontroli dostępu. Do wykonania jakiejkolwiek akcji, wymaga od użytkownika uwierzytelnienia się poprzez zalogowanie do aplikacji. W systemie zdefiniowane są dwie role - administrator oraz użytkownik. Żaden użytkownik nie posiada uprawnień do otwierania dokumentów dla niego nieprzeznaczonych. Tylko administrator ma prawo do przeglądania wszystkich dokumentów w bazie (bez uprawnień do ich otwierania i wyświetlania) oraz dostęp do danych audytowych. W przypadku, gdy system wykryje podejrzane zachowanie, jakim są wielokrotne, nieudane próby zalogowania, blokuje użytkownikowi dostęp do konta na 1 godzinę (dla danej sesji - nie dla danego konta).

Funkcje bezpieczeństwa realizowane w ramach weryfikacji i uwierzytelniania

- FAU_SAR.2.1
- FDP_ACC.1.1
- FDP_ACF.1.1
- FDP_ACF.1.2
- FIA_AFL.1.1

- FIA_AFL1.2
- FIA_UAU.1.1
- FIA_UAU.1.1
- FIA_UID.1.1
- FMT_SMR.1.1
- FMT_SMR.1.2
- FMT_SMR.2.1
- FMT_SMR.2.2

3. Przypadki użycia

UC1 - Rejestracja

Jeśli użytkownik nie posiada jeszcze konta w systemie, przy pierwszym kontakcie z aplikacją powinien się zarejestrować. Dzięki temu podczas użytkowania aplikacji system będzie mógł dokonać jego identyfikacji i potwierdzić tożsamość.

1. Wymagania: brak
2. Scenariusz główny:

- Przeglądarka wyświetla formularz logowania - obok znajduje się opcja "Register"
- Użytkownik wybiera opcję "Register"
- Przeglądarka ładuje ekran rejestracji z trzema polami - prosi o podanie identyfikatora (loginu), założenie hasła i powtórzenie go
- Użytkownik wpisuje poprawne dane do formularza logowania
- Użytkownik wybiera opcję "Submit"
- System tworzy nowe konto i przenosi użytkownika do ekranu logowania

3. Scenariusz alternatywny 1:

- Przeglądarka wyświetla formularz logowania - obok znajduje się opcja "Register"
- Użytkownik wybiera opcję "Submit"
- Przeglądarka ładuje ekran rejestracji z trzema polami - prosi o podanie identyfikatora (loginu), założenie hasła i powtórzenie go
- Użytkownik podaje zajęty lub niepoprawny identyfikator (login)
- System wyświetla komunikat o wprowadzeniu błędnych danych

4. Scenariusz alternatywny 2:

- Przeglądarka wyświetla formularz logowania - obok znajduje się opcja "Register"
- Użytkownik wybiera opcję "Submit"
- Przeglądarka ładuje ekran rejestracji z trzema polami - prosi o podanie identyfikatora (loginu), założenie hasła i powtórzenie go
- Użytkownik podaje identyfikator (login) i hasło, jednak niepoprawnie je powtarza
- System wyświetla komunikat z prośbą o ponowne powtórzenie hasła

Funkcje bezpieczeństwa realizowane przez UC1

- FIA_UID.1.1

UC2 - Logowanie

Po połączeniu się z serwerem i otwarciu aplikacji w przeglądarce, użytkownik musi się zalogować do systemu. Ma to na celu identyfikację i potwierdzenie tożsamości osoby korzystającej z aplikacji. Zalogowanie się jest konieczne - niezalogowany użytkownik nie może wykonać w systemie żadnych operacji.

1. Wymagania: brak
2. Scenariusz główny:

- Przeglądarka wyświetla formularz logowania
- Użytkownik wpisuje poprawne dane do formularza logowania
- Użytkownik wybiera opcję “Submit”
- System sprawdza poprawność danych i wyświetla główny widok aplikacji

3. Scenariusz alternatywny 1:

- Przeglądarka wyświetla formularz logowania
- Użytkownik wpisuje niepoprawne dane do formularza logowania
- Użytkownik wybiera opcję “Submit”
- System wyświetla komunikat o wprowadzeniu błędnych danych

4. Scenariusz alternatywny 2:

- Przeglądarka wyświetla formularz logowania
- Użytkownik niepoprawnie wpisuje dane do formularza logowania
- Użytkownik wybiera opcję “Submit”
- System wyświetla komunikat o błędnym wypełnieniu formularza

5. Scenariusz alternatywny 3:

- Przeglądarka wyświetla formularz logowania
- Użytkownik wpisuje poprawny login, ale niepoprawne hasło do formularza logowania
- Użytkownik wybiera opcję “Submit”
- System wyświetla komunikat o wprowadzeniu błędnych danych
- Użytkownik 2 razy ponownie wpisuje niepoprawne hasło
- Po 3-krotnej próbie podania niepoprawnego hasła system blokuje użytkownikowi dostęp do konta na 1 godzinę (dla danej sesji - nie dla konta)

Funkcje bezpieczeństwa realizowane przez UC2

- FIA_UID.1.1
- FAU_GEN.1.1
- FAU_GEN.2.1
- FAU_ARP.1.1
- FAU_ARP.1.2
- FDP_ACC.1.1
- FDP_ACF.1.1
- FDP_ACF.1.2
- FIA_AFL.1.1
- FIA_AFL.1.2

- FIA_UAU.1.1
- FIA_UAU.1.2
- FIA_UID.1.1
- FMT_SMR.1.1
- FMT_SMR.1.2
- FMT_SMR.2.1
- FMT_SMR.2.1

UC3 - Wysyłanie dokumentu

1. Wymagania: użytkownik musi być zalogowany
2. Scenariusz główny:

- Użytkownik wybiera zakładkę "DOCUMENTS SHARING APP"
- Pojawia się pole wyboru pliku
- Użytkownik przeciąga i upuszcza odpowiedni dokument (rozszerzenie *.txt) w polu wyboru pliku
- Użytkownik podaje klucz symetryczny, którym zostanie zaszyfrowany dokument
- Użytkownik wybiera opcję "Save and continue"
- Dokument zostaje załadowany

3. Scenariusz alternatywny 1:

- Użytkownik wybiera zakładkę "DOCUMENTS SHARING APP"
- Pojawia się pole wyboru pliku
- Użytkownik klika w pole wyboru pliku
- Pojawia się systemowe okno wyboru pliku
- Użytkownik wybiera odpowiedni dokument (rozszerzenie *.txt)
- Użytkownik podaje klucz symetryczny, którym zostanie zaszyfrowany dokument
- Użytkownik wybiera opcję "Save and continue"
- Dokument zostaje załadowany

4. Scenariusz alternatywny 2:

- Użytkownik wybiera zakładkę "DOCUMENTS SHARING APP"
- Pojawia się pole wyboru pliku
- Użytkownik przeciąga i upuszcza dokument o błędnym rozszerzeniu w polu wyboru pliku
- Użytkownik podaje klucz symetryczny, którym zostanie zaszyfrowany dokument
- Użytkownik wybiera opcję "Save and continue"
- System wyświetla komunikat o niepowodzeniu ze względu na nieprawidłowe rozszerzenie pliku

UC4 - Przeglądanie własnych dokumentów

1. Wymagania: użytkownik musi być zalogowany
2. Scenariusz główny:

- Użytkownik wybiera zakładkę "My documents"
- Wyświetlona zostaje lista załadowanych wcześniej przez użytkownika dokumentów

UC5 - Udostępnianie dokumentów

1. Wymagania: użytkownik musi być zalogowany
2. Scenariusz główny:

- Użytkownik wybiera zakładkę "My documents"
- Wyświetlona zostaje lista załadowanych wcześniej przez użytkownika dokumentów
- Użytkownik wybiera opcję "Share document" przy jednym z załadowanych wcześniej przez siebie dokumentów
- Użytkownik wpisuje identyfikator (login) użytkownika, któremu chce udostępnić wybrany plik
- Użytkownik zatwierdza operację przyciskiem "Share"
- Wybrany dokument zostaje udostępniony odpowiedniemu użytkownikowi

3. Scenariusz alternatywny:

- Użytkownik wybiera zakładkę "My documents"
- Wyświetlona zostaje lista załadowanych wcześniej przez użytkownika dokumentów
- Użytkownik wybiera opcję "Share document" przy jednym z załadowanych wcześniej przez siebie dokumentów
- Użytkownik wpisuje niepoprawny identyfikator (login) użytkownika, któremu chce udostępnić wybrany plik
- Użytkownik zatwierdza operację przyciskiem "Share"
- System powiadamia użytkownika, że użytkownik o podanym loginie nie istnieje

UC6 - Przejście do kolejnego stanu udostępniania dokumentu

1. Wymagania: użytkownik musi być zalogowany
2. Scenariusz główny:

- Użytkownik2 wybiera zakładkę "Shares"
- Stan udostępniania zmienia się z State1 na State2
- Użytkownik1 podaje hasło do pliku
- Użytkownik1 wybiera "Submit"
- Stan udostępniania zmienia się z State2 na State3
- Użytkownik2 odczytuje plik

3. Scenariusz alternatywny 1:

- Użytkownik2 wybiera zakładkę "Shares"
- Stan udostępniania zmienia się z State1 na State2
- Użytkownik1 podaje hasło do pliku
- Użytkownik1 wybiera "Submit"
- Stan udostępniania zmienia się z State2 na State3
- Użytkownik2 odczytuje plik
- Użytkownik1 wprowadza czas wygaśnięcia pliku
- Po określonym czasie plik zostaje usunięty dla obu użytkowników

Funkcje bezpieczeństwa realizowane przez UC3

- FCS_CKM.1
- FCS_CKM.2

- FCS_CKM.3
- FCS_CKM.4
- FCS_COP.1

UC7 - Wylogowanie

1. Wymagania: użytkownik musi być zalogowany
2. Scenariusz główny:

- Użytkownik wybiera opcję "Log Out"
- Użytkownik zostaje wylogowany
- System przenosi użytkownika do ekranu logowania

UC8 - Wyświetlenie logów systemowych

1. Wymagania: użytkownik musi być zalogowany jako administrator
2. Scenariusz główny:

- Użytkownik wybiera opcję "Logs"
- Pojawia się lista logów systemowych

Funkcje bezpieczeństwa realizowane przez UC8

- FAU_GEN.1.1
- FAU_GEN.1.2
- FAU_SAR.1.1
- FAU_SAR.1.2
- FAU_SAR.2.1

UC9 - Przeglądanie bazy dokumentów

1. Wymagania: użytkownik musi być zalogowany jako administrator
2. Scenariusz główny:

- Użytkownik wybiera opcję "Shares"
- Wyświetlona zostaje lista dokumentów dostępnych w bazie

4. Charakterystyka użytkowników aplikacji

1. Użytkownicy

Główna grupa korzystających z systemu. Używają oni aplikacji do dzielenia się plikami, ufając w bezpieczeństwo procesu. Nie mają dokładnej wiedzy na temat mechanizmów, na których oparte jest działanie systemu.

Wykorzystywane funkcje:

- Rejestracja;
- Logowanie;
- Wysyłanie dokumentów;
- Przeglądanie własnych dokumentów;

- Udostępnianie dokumentów (w tym ustalenie terminu wygaśnięcia, nadanie uprawnień dostępu, nadanie symetrycznego klucza szyfrującego);
- Odczytywanie udostępnionych dokumentów.

2. Administrator

Użytkownik zarządzający systemem. Nadzoruje on pracę systemu oraz działania użytkowników. Czuwa nad bezpieczeństwem. Posiada szerszą wiedzę na temat specyfiki działania systemu. Wychwytuje niepożądane akcje użytkowników i zachowania aplikacji. Ma dostęp do bazy danych.

Wykorzystywane funkcje:

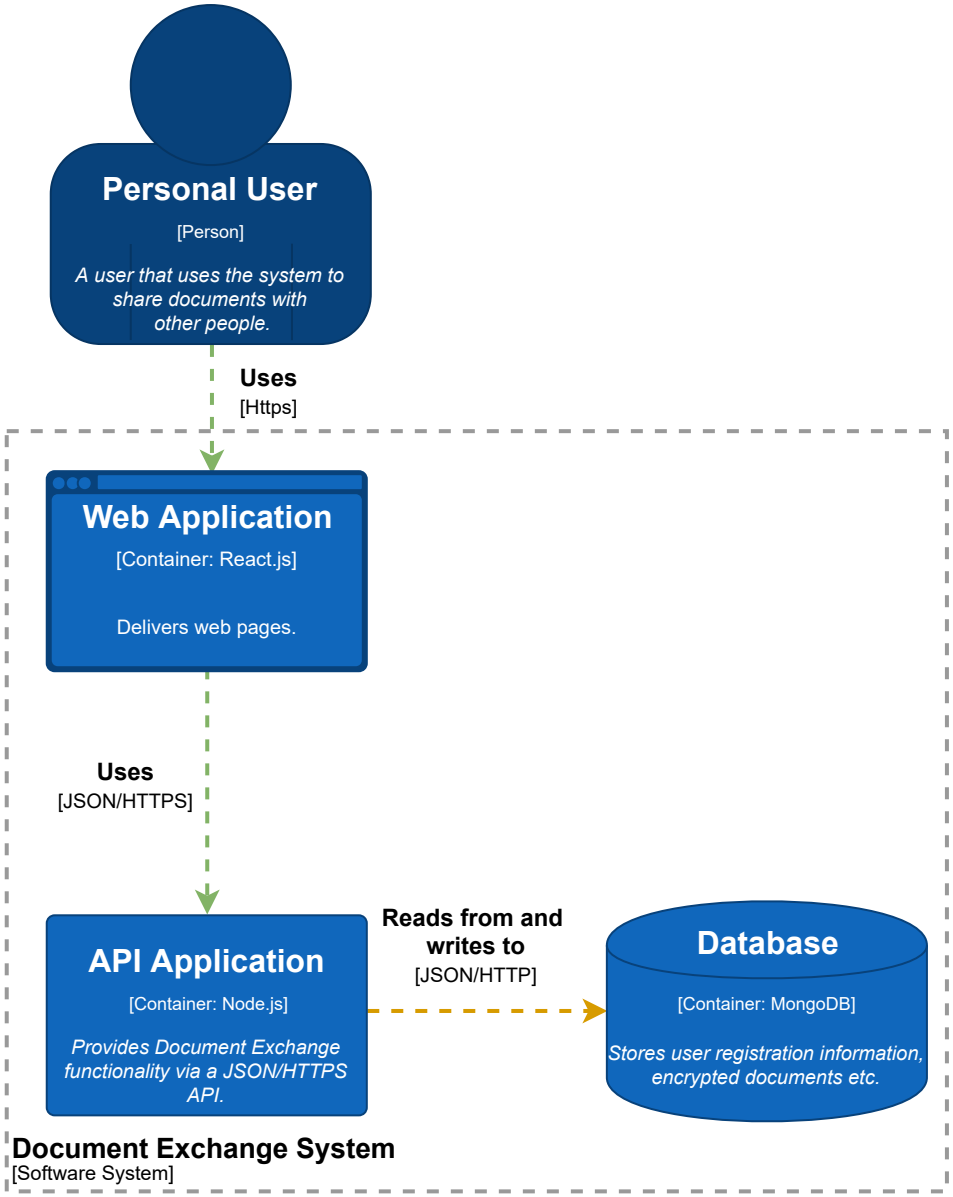
- Logowanie;
- Wyświetlanie logów systemowych z serwera;
- Przeglądanie bazy dokumentów (bez uprawnień do ich otwierania i wyświetlania).

5. Wykorzystanie aplikacji

Aplikacja będzie wykorzystywana przez użytkowników na co dzień do dzielenia się między sobą plikami. Ma za zadanie umożliwiać to w sposób bezpieczny i poufny. Główne funkcjonalności systemu to wysyłanie plików na serwer, zarządzanie plikami i dostępem do nich oraz wymiana zaszyfrowanych kluczy dostępu.

6. Sposób realizacji aplikacji

Ogólna charakterystyka: Aplikacja webowa z dostępem przez przeglądarkę
Platforma: Ubuntu 14.04, chmura Microsoft Azure
Język programowania: JavaScript
Front-end: React.js
Back-end: Node.js
Bazy danych: MongoDB
Format wymiany danych: JSON
Protokół internetowy: HTTPS



Container diagram for the Document Exchange System