Академија струковних студија Шумадија
Одсек Крагујевац

Студијски програм: Информатика
Предмет: Пројектовање информационих система

ПРЕДЛОГ РЕШЕЊА

- Евиденција долазака за изборни предмет–

Предметни наставник:

Саша Стаменовић

Студент:

Светлана Ђурђевић 147/2022
Драгољуб Мијаиловић 004/2023
Ђорђе Мајсторовић 005/2023

Крагујевац 2024.

Садржај:

Contents

1. Увод

Циљ овог документа је да представи свеобухватан и јасан план за развој система „MojePrisustvo“, који ће омогућити аутоматизовану евиденцију присуства студената, као и генерисање извештаја и управљање корисницима. Систем ће у великој мери побољшати ефикасност рада професора, администрације и студената, кроз кориснички интерфејс који је интуитиван и лак за коришћење, али истовремено обезбеђује и сигурну размену података. Овај систем има за циљ да поједностави и убрза процес управљања присуством, чиме ће се значајно смањити административни рад и смањити могућност грешака у евиденцији.

2. Архитектура система

Предложено решење за систем „MojePrisustvo“ засновано је на модерној веб архитектури, која ће бити проширена мобилним апликацијама за студенте и професоре. Ова архитектура ће омогућити лак и брз приступ систему са било ког уређаја (рачунар, мобилни телефон или таблет), чиме ће се осигурати велика доступност и флексибилност. Основни делови архитектуре су:

2.1 Кориснички интерфејс (UI)

Кориснички интерфејс биће развијен као респонзивна веб апликација, што значи да ће систем бити доступан преко веб претраживача (попут Google Chrome, Firefox, Edge, Safari) и такође ће имати мобилне апликације за платформе iOS и Android. Интерфејс ће бити једноставан и пријатан за коришћење, с минималним бројем корака потребних за обављање задатака.

- Професори ће имати могућност да уносе присуство студената на свим наставним јединицама (предавања, вежбе), као и да додају напомене о изостанцима и оправдањима, те генеришу различите врсте извештаја за своје предмете.

- Студенти ће моћи да прегледају своје податке о присуству, као и да генеришу извештаје који се односе на њихов статус присуства и њихове оцене.
- Администратори ће имати пун приступ свим подацима и моћи ће да управљају корисничким налозима, као и да одржавају и ажурирају базу података.

2.2 Серверска компонента (Back-end)

Систем ће бити развијен као микросервисна архитектура, што значи да ће се састојати од више независних сервиса који комуницирају међусобно преко API интерфејса. Главни делови серверске компонента су:

- Управљање подацима: Главни сервис који обрађује све податке о присуству студената, изостанцима, као и извештајима и корисничким налозима. Овај сервис ће такође бити одговоран за синхронизацију података између различитих делова система.
- API интерфејс: Интерфејс који омогућава комуникацију са другим системима универзитета, као и за размену података са другим апликацијама или платформама, као што су академски портали.
- Безбедност: Модул који је одговоран за сигурност података, укључујући шифровање података, аутентификацију корисника (провера идентитета) и ауторизацију (управљање правима приступа).

2.3 База података

Систем ће користити релациону базу података која ће чувати све податке о студентима, присуству, предметима, извештајима и корисницима. База података ће бити оптимизована за брзо чување и извлачење података, што ће омогућити лаку обраду и брзи приступ информацијама. За ову сврху препоручује се коришћење база података као што су PostgreSQL или MySQL.

- Модел података: У систему ће бити дефинисани основни ентитети као што су студенти, професори, предмети, изостанци и извештаји. Сви ови подаци ће бити ускладиштени у посебним табелама које су међусобно повезане.

- Безбедност података: Сви осетљиви подаци, као што су лични подаци студената и професора, биће шифровани користећи AES алгоритам. Приступ бази података ће бити строго контролисан и ограничен само на овлашћене кориснике.

2.4 API интеграција

Систем ће бити у могућности да се интегрише са другим постојећим академским и административним системима преко RESTful API интерфејса. Ова интеграција ће омогућити аутоматско ажурирање података о студентима и њиховим активностима, као и размену података између система у реалном времену, што ће повећати оперативну ефикасност.

3. Функционалности система

Систем ће подржавати различите функционалности, као што су:

3.1 Унос података о присуству

Једна од основних функција система је омогућавање професорима да на једноставан и брз начин уносе податке о присуству студената на наставним активностима. Ова функционалност подразумева:

- Преглед листе студената: Професори ће имати приступ ажурираној листи студената за сваку наставну јединицу.
- Различите опције за означавање присуства: Биће омогућено да се присуство означи у више категорија, као што су „Присутан“, „Изостао“ и „Оправдано одсутан“.
- Аутоматско ажурирање: Сви унети подаци биће одмах синхронизовани са базом података, омогућавајући њихов преглед у реалном времену.
- Интеграција са QR кодом или NFC технологијом: Систем може подржавати опције за скенирање студената ради брже евиденције.

Ова функционалност значајно ће смањити време потребно за обраду података и смањити могућност грешака приликом уноса.

3.2 Генерисање извештаја

Систем ће омогућити креирање различитих типова извештаја који ће задовољити потребе корисника на индивидуалном и групном нивоу. Ова функционалност укључује:

- Параметри извештаја: Професори и студенти ће моћи да дефинишу параметре извештаја, као што су временски периоди (недеља, месец, семестар), наставне јединице или групе студената.
- Индивидуални извештаји:
    - Студенти ће имати могућност да генеришу извештаје о свом присуству и учинку.
    - Професори ће моћи да добију детаљне извештаје за сваког студента, укључујући историју присуства и напомене.
- Колективни извештаји:
    - Професори ће моћи да генеришу извештаје за целе групе, који ће приказивати укупну статистику о присуству.
    - Администратори ће моћи да креирају извештаје о укупној активности у систему.
- Експорт у различите формате: Систем ће подржавати експорт извештаја у формате као што су PDF, Excel или CSV, чиме ће се олакшати њихово дељење и даља анализа.

Ови извештаји ће бити корисни за праћење напретка студената и ефикасности наставног процеса, као и за доношење административних одлука.

3.3 Управљање корисницима

Управљање корисничким налозима је још једна кључна функционалност система, која ће бити доступна искључиво администраторима. Овај модул омогућава:

- Креирање корисничких налога: Администратори ће моћи да креирају налоге за професоре, студенте и друге кориснике.

- Додела права и улога: Сваки кориснички налог биће повезан са одређеном улогом (студент, професор, администратор), чиме ће се регулисати права приступа.
- Управљање привилегијама: Биће могуће одредити прецизне привилегије за сваку улогу, укључујући приступ извештајима, базама података и административним функцијама.
- Ревидирање и ажурирање налога: Администратори ће имати могућност да ажурирају податке о корисницима, ресетују лозинке или деактивирају налоге у случају потребе.
- Праћење активности корисника: Систем ће евидентирати све важне активности корисника како би се обезбедила транспарентност и сигурност.

4. Безбедност

4.1 Заштита података о личности

Систем ће бити у складу са свим важећим регулативама, као што су:

- Закон о заштити података о личности (ЗЗПЛ) Републике Србије, који дефинише обавезе у погледу чувања и обраде личних података.
- GDPR (General Data Protection Regulation), уколико је систем намењен за међународне институције.

Осетљиви подаци, као што су лични подаци студената, професора и администратора, биће шифровани како током складиштења тако и приликом преноса између клијента и сервера. Подаци ће се чувати у строго контролисаном окружењу са ограниченим приступом.

4.2 Аутентификација и ауторизација

Систем ће користити OAuth 2.0 протокол за проверу идентитета корисника. Овај приступ подразумева:

- Вишефакторску аутентификацију (MFA): Корисници ће имати могућност да поред лозинке користе додатне мере провере, као што су SMS кодови или апликације за аутентификацију.
- Роле-базирана контрола приступа (RBAC): Права приступа биће ограничена у складу са улогом корисника (професор, студент, администратор).

4.3 Шифровање података

Сви осетљиви подаци биће шифровани коришћењем AES-256 алгоритма, који представља један од најпоузданијих стандарда у области информационе безбедности. Шифровање ће се примењивати:

- На податке који се чувају у бази података.
- На податке који се преносе преко мреже путем TLS (Transport Layer Security) протокола.

4.4 Мониторинг и детекција претњи

Систем ће укључивати модул за праћење активности, који ће омогућити:

- Детекцију и спречавање неовлашћених покушаја приступа.
- Логовање активности корисника ради праћења злоупотреба или аномалија.
- Редовне безбедносне провере, укључујући аутоматизоване алате за тестирање на рањивости.

5. Процес имплементације

5.1 Развој и имплементација

Имплементација ће бити подељена у шест кључних фаза:

1. Планирање и анализа захтева (1 месец):

- Идентификација свих функционалних и нефункционалних захтева.
- Анализа постојећих процеса у установама које ће користити систем.
- Утврђивање ризика и њихово ублажавање.

2. Дизајн архитектуре и интерфејса (1 месец):
   - Разрада техничке архитектуре система.
   - Развој иницијалних прототипа корисничког интерфејса и њихово тестирање са корисницима.

3. Развој серверске и клијентске компоненте (3 месеца):
   - Израда серверског дела система који обухвата базе података, API интерфејс и модул за безбедност.
   - Развој клијентског дела, укључујући веб и мобилне апликације.

4. Тестирање функционалности и безбедности (1 месец):
   - Тестирање свих модула система како би се осигурало да испуњавају захтеве.
   - Извођење безбедносних провера и симулација потенцијалних напада.

5. Интеграција са постојећим системима (1 месец):
   - Постављање механизама за размену података са другим академским и административним платформама.
   - Успостављање протокола за одржавање података у реалном времену.

6. Прилагођавање и оптимизација (1 месец):
    - На основу повратних информација од корисника, систем ће бити оптимизован ради побољшања брзине, стабилности и употребљивости.

5.2 План имплементације у академским установама

- Обука корисника:
    - Професори, студенти и администратори ће проћи кроз серију обука за коришћење система.
    - Припремљени приручници и видео упутства.
- Фаза тестирања:
    - Увођење система у неколико пилот група, уз праћење перформанси и прикупљање повратних информација.

6. Планирање тестова

Систем „MojePrisustvo“ биће подвргнут темељним тестовима како би се осигурала његова функционалност, безбедност и перформансе.

6.1 Функционално тестирање

Фокус ће бити на верификацији свих функционалности система:

- Евиденција присуства.
- Генерисање извештаја.
- Управљање корисничким налозима.
- Кориснички интерфејс (веб и мобилни).
- Аутентификација и ауторизација корисника.

6.2 Безбедносно тестирање

Безбедносно тестирање ће укључивати:

- Penetration Testing: Провера отпорности система на нападе.
- Евалуација шифровања: Осигуравање да су сви подаци правилно шифровани.
- Стрес тестирање безбедности: Тестирање отпорности на масовне неовлашћене покушаје приступа.

6.3 Тестирање перформанси

Систем ће бити тестиран под различитим условима оптерећења:

- Нормално оптерећење: Тестирање са очекиваним бројем корисника.
- Екстремно оптерећење: Тестирање са значајно повећаним бројем корисника и акција у кратком временском периоду.
- Скалабилност: Провера могућности проширења система без нарушавања перформанси.

6.4 Континуирано тестирање

Током рада система, континуирано ће се изводити:

- Аутоматизовани тестови функционалности након ажурирања.
- Редовни безбедносни тестови.
- Мониторинг перформанси ради идентификације потенцијалних проблема.