SVEUČILIŠTE U SPLITU

FAKULTET ELEKTROTEHNIKE, STROJARSTVA I BRODOGRADNJE

SEMINARSKI RAD IZ KOLEGIJA „UGRADBENI RAČUNALNI SUSTAVI“

**IDEJNO RJEŠENJE SUSTAVA ZA EVIDENCIJU OSOBA I PRAĆENJE KORIŠTENJA RESURSA**

**Božo Božinović**

**Mislav Ivanda**

**Mateo Medak**

**Ana Žuljević**

Split, veljača 2023.

Sadržaj

[1 Uvod 1](#_Toc127443868)

[2 Korisnički zahtjevi 2](#_Toc127443869)

[2.1 Funkcionalni zahtjevi 2](#_Toc127443870)

[2.1.1 Student 2](#_Toc127443871)

[2.1.2 Profesor 2](#_Toc127443872)

[2.1.3 Administrator 2](#_Toc127443873)

[2.2 Nefunkcionalni zahtjevi 3](#_Toc127443874)

[3 Arhitektura sustava 4](#_Toc127443875)

[3.1 Ideja 4](#_Toc127443876)

[3.2 Moduli sustava i korištene tehnologije 4](#_Toc127443877)

[3.3 Mrežna arhitektura sustava 7](#_Toc127443878)

[3.4 Rad sustava u određenim situacijama 9](#_Toc127443879)

[3.5 Zadovoljenje nefunkcionalnih zahtjeva 10](#_Toc127443880)

[4 Primjer korištenja 12](#_Toc127443881)

[5 *Proof of concept* 13](#_Toc127443882)

[5.1 Sistemska podrška 13](#_Toc127443883)

[5.2 Aplikacijski server i baza podataka 15](#_Toc127443884)

[5.3 Klijentska aplikacija 16](#_Toc127443885)

[5.3.1 Zajedničke opcije 16](#_Toc127443886)

[5.3.2 Profesorske opcije 17](#_Toc127443887)

[5.3.3 Studentove opcije 19](#_Toc127443888)

[PRILOZI 21](#_Toc127443889)

[Kazalo slika 21](#_Toc127443890)

# Uvod

Posljednjih nekoliko desetljeća pojmovi restrukturiranja i racionalizacije poslovanja sve se češće spominju i integriraju u poslovne planove svih poslovnih subjekata. Razlog tome leži u povećanoj volatilnosti svjetskog tržišta koje se sve češće susreće s gospodarskim krizama. Stoga je za održavanje konkurentnosti kako na lokalnom tako i na globalnom tržištu nužno održavati profitabilnost tvrtke.

Jednako kao što kupac želi dobiti što bolju vrijednost za uloženi novac tako i vlasnici tvrtki žele dobiti što bolju produktivnost od svojih zaposlenika za uplaćeni iznos plaće. Krajnji cilj je postizanje što veće stope efikasnosti radnika, ali i upravljanja ostalim resursima.

Stoga je cilj ovog seminarskog rada prezentirati idejno rješenje sustava koji bi omogućio praćenje vremena koje član određenog subjekta zaista provodi na predodređenom mjestu te istovremeno praćenje zauzetosti prostorija koje također pretežno predstavljaju važan resurs.

Iako na tržištu već postoje sustavi sa identičnim ciljem nijedan od njih ne garantira ispravnost pohranjenih podataka. Primjerice, sustavi koji zadani problem rješavaju korištenjem RFID kartica nisu imuni na ilegalnu evidenciju osobe izvršenu od strane druge osobe te često podaci pohranjeni u sustavu ne odgovaraju stvarnim podacima. Jedini način detekcije ilegalne evidencije u zadanim sustavima je određena vrsta manualne kontrole koja iziskuje dodatne resurse odnosno taj proces nije automatiziran.

Stoga je osnovni cilj prezentiranog sustava osiguranje konzistentnosti između stanja u realnom svijetu i stanja u sustavu.

S obzirom na problematiku koju sustav treba riješiti, područje njegove primjene je zaista široko. Jedno od područja primjene je praćenje evidencije prisutnosti studenata na fakultetu pa će stoga zadani primjer biti uzet kao referenca prilikom opisivanja rada sustava i definiranja njegove arhitekture. Referenciranje na određeni primjer i dalje ne umanjuje općenitost sustava već samo služi za njegov plastičniji opis primjene u praksi. Primjena sustava na nekom drugom primjeru bi zapravo odgovarala matematičkom slučaju u kojem imamo istu kompleksnost jednadžbe, ali različita imena varijabli. Ta različitost varijabli najviše će utjecati na vrstu podataka koje je potrebno evidentirati.

Na početku će biti navedeni korisnički zahtjevi za sustav i to kroz podjelu na funkcionalne i nefunkcionalne zahtjeve. Nakon toga biti će prikazano idejno rješenje sustava kroz opis njegove arhitekture i potrebnih tehnologija uz navođenje njihove konkretne primjene na zadani sustav. Na kraju će biti naveden primjer korištenja sustava.

# Korisnički zahtjevi

Razlikujemo 3 vrste korisnika sustava: **student, profesor, administrator**.

Za svaku od prethodno navedenih uloga potrebno je definirati različite funkcionalne zahtjeve zbog različitosti vrsta podataka kojima je potrebno pristupiti.

## Funkcionalni zahtjevi

### Student

* Evidentiranje vlastite prisutnosti
* Pregled vlastite evidencije prisutnosti po predmetima
* Pregled vlastite evidencije prisutnosti po vremenskom intervalu
* Usporedba ostvarene stope dolaznosti s vrijednostima potrebnima za izlazak na kolokvij/ispit po predmetima
* Obavijest o uspješnom/neuspješnom pokušaju evidencije
* Obavijest u slučaju nedolaska na nastavu
* Obavijest u slučaju niske stope dolaznosti
* Obavijest o ispunjavanju obvezne stope dolaznosti

### Profesor

* Evidentiranje vlastite prisutnosti
* Manualna evidencija prisutnosti studenta
* Pregled prisutnosti studenata u realnom vremenu s izlistanim podacima prisutnih studenata
* Pregled vlastite evidencije prisutnosti po predmetima
* Pregled vlastite evidencije po vremenskom intervalu
* Pretraga studenata po imenu, predmetu, grupi
* Sortiranje studenata po abecednom redu, prisutnosti
* Obavijest o uspješnom/neuspješnom pokušaju evidencije
* Obavijest o odlasku studenta s nastave
* Obavijest o slučaju ilegalne evidencije s imenima studenata
* Prosječno trajanje nastave unutar određene prostorije
* Prosječno trajanje nastave za pojedini predmet
* Evidencija broja sati rada po predmetima i razdobljima

### Administrator

* Pregled evidencije prisustva u realnom vremenu
* Pregled evidencije prisustva po prostoriji
* Pregled evidencije prisustva po profesoru
* Pregled evidencije prisustva po studentu
* Pregled evidencije prisustva po vremenskom intervalu
* Pregled evidencije prisustva po predmetu
* Sortiranje predmeta/profesora po postotku prisutnosti
* Unos postotka kojim je zadovoljena prisutnost
* Ispis studenata koji nisu zadovoljili potreban postotak prisutnosti
* Uvid u način evidencije prisutnosti koji može biti manualan od strane profesora ili automatiziran putem sustava
* Obavijest o neodržanom nastavnom satu
* Obavijest o greškama u radu sustava s relevantnim informacijama
* Obavijest o detektiranim sigurnosnim prijetnjama s relevantnim informacijama

## Nefunkcionalni zahtjevi

* **Sigurnost**: osjetljivi podaci ne smiju biti pohranjeni u izvornom obliku. Podaci između modula sustava moraju se razmjenjivati isključivo u enkriptiranoj formi.
* **Pouzdanost:** sustav treba spriječiti moguće računalne napade, a u slučaju mogućeg propusta ispravno ih detektirati i poduzeti odgovarajuće radnje.
* **Točnost:** sustav mora evidentirati prisutnost u rezoluciji od 1 minute.
* **Tehnologije:** sustav treba koristiti tehnologije čija starost iznosi minimalno 10 godina zbog izbjegavanja mogućih još neotkrivenih sigurnosnih propusta novijih tehnologija.
* **Uporabljivost:** zahtjevi za korištenje sustava trebaju biti ispunjeni za barem 95% studenata u anketi provedenoj na uzorku od 500 studenata.
* **Općenitost:** sustav treba biti dizajniran na način da se može primijeniti na druga područja primjene unutar zadane domene uz minimalne preinake.
* **Cijena:** prosječna cijena instalacije opreme sustava u prostorijama ne smije biti veća od 2000 kuna.
* **Usklađenost sa zakonima:** sustav mora koristiti osobne podatke sukladno GDPR regulativi.

# Arhitektura sustava

## Ideja

Arhitektura sustava bit će kompleksnija od trenutnih sustava za praćenje evidencije zbog povećanih zahtjeva koje je potrebno zadovoljiti. Međutim, dio koji se tiče interakcije korisnika sa sustavom ostat će vrlo sličan onome iz trenutnih sustava.

Prva radikalna razlika u odnosu na trenutne sustave biti će zamjena kartica, tokena i sličnih predmeta mobilnim uređajem. Budući da gotovo svi korisnici sa sobom uvijek imaju mobilni uređaj moguće ga je iskoristiti kao sredstvo identifikacije te za aktivno sudjelovanje u radu sustava čime prethodno navedeni predmeti postaju beskorisni, a korištenje sustava postaje jednostavnije za korisnika zbog rasterećenja potrebne opreme.

## Moduli sustava i korištene tehnologije

Budući da će mobilni uređaj imati interakciju sa sustavom prirodni zaključak je kreiranje i instalacija **mobilne aplikacije** u kojoj će biti definirani procesi interakcije. Dakle, osnovna pretpostavka sustava(koje je ujedno razumna i ostvariva u praksi) odnosi se na zahtjev za posjedovanjem uređaja i instalirane mobilne aplikacije.

Mobilna aplikacija treba biti razvijena za **Android** i **iOS** platformu kako bi se u potpunosti iskoristile prednosti razvoja aplikacije za *native* arhitekture.

Također, mobilna aplikacija treba sadržavati što manje aplikacijske logike zbog mogućih manipulacija s programskim kodom aplikacije koji bi mogli utjecati na ispravnost rada sustava budući da se ona ne izvršava u kontroliranom okruženju već na proizvoljnom mobilnom uređaju koji također može biti u posjedu potencijalnog napadača. Za razliku od mobilne aplikacije, aplikacijski server se nalazi u kontroliranom okruženju u kojem je integritet sustava zagarantiran.

Zaključujemo da tehnologije koje ćemo koristiti za realizaciju zahtjeva pouzdane evidencije prisutnosti moraju biti kompatibilne sa prosječnim mobilnim uređajem današnjice. Zbog toga je za potrebe ovog sustava odabrana **NFC** tehnologija.

NFC tehnologija odabrana je zbog svoje široke rasprostranjenosti na svim novijim mobilnim uređajima te zbog potrebne interakcije između mobilnog uređaja korisnika i sustava. Primjerice, očitavanje QR koda ili RFID kartice podrazumijeva samo 1 aktivnu stranu koju predstavlja sustav koji ih očitava. Drugim riječima, sustav ne može ni na koji način narediti RFID kartici ili QR kodu da izvrše određenu operaciju jer za to nisu sposobni[[1]](#footnote-1). S druge strane, korištenjem NFC tehnologije sustav će moći „narediti“ mobilnom uređaju kroz sučelje aplikacije izvršavanje određenih radnji.

Sada je potrebno razraditi što je potrebno „narediti“ mobilnom uređaju kako bi realizirali pouzdanu evidenciju pristupa.

Budući da stanje sustava mora odgovarati realnom stanju nužno je prikupljati informacije u realnom vremenu i to na automatiziran način bez zamaranja korisnika. Realizaciju ovog zahtjeva najlakše je zadovoljiti korištenjem određene bežične tehnologije koja bi idealno trebala imati domet samo unutar cijele prostorije. Ukoliko je korisnik unutar prostorije odnosno unutar dometa mreže tada njegov mobilni uređaj ima pristup mreži te se može evidentirati njegovo prisustvo. Kada korisnik nije unutar prostorije tada on nije unutar dometa mreže te se može evidentirati njegova odsutnost.

Odabir bežične mrežne tehnologije sveo se na 2 moguća izbora: WiFi ili Bluetooth.

Sagledavajući prednosti i mane odabir je pao na **WiFi** tehnologiju iz nekoliko razloga:

* Bluetooth bi zahtijevao uparivanje mobilnog uređaja s baznom stanicom prilikom prvog korištenja što bi iziskivalo dodatnu interakciju korisnika
* Upoznatost osoba s WiFi tehnologijom i protokolima Interneta je znatno raširenija nego što je to kod Bluetooth-a zbog čega je sustav jednostavniji za razumijevanje i održavanje.

Dakle, zaključujemo da će svaka prostorija trebati imati instaliranu WiFi pristupnu točku i to na onom mjestu na kojem se realizira najbolja pokrivenost signalom.

Ovdje nailazimo na 2 moguća problema:

1. Što ukoliko je prostorija toliko velika da u određenim dijelovima nema WiFi signala? -> Unutarnji domet WiFi mreže u prostoriji bez prepreka s *Line-of-Sight* može sezati sve do 90 metara. Ukoliko to nije dovoljno, tada je najbolje rješenje za zadanu prostoriju realizirati **WiFi mesh** koji će realizirati pokrivenost u svim dijelovima te predstavlja kvalitetniju i skuplju opciju u odnosu na koriptenje WiFi extendera(mesh koristi isit SSID kao i mreža dok extender dodaje nastavak na SSID što bi uzrokovalo dodatne probleme i komplikacije u sustavu)
2. Može li 1 WiFi bazna stanica izdržati toliki broj povezanih osoba? -> Korištenjem **dual band** baznih stanica moguće je ostvariti i do preko 250 konekcija.

Kompatibilnost mobilnih uređaja i WiFi protokola je neupitna. Također, korištenjem WiFi protokola koristimo blagodati Interneta što se odnosi na potrebnu opremu za instalaciju i moguće potrebne protokole.

Za potrebe ispitivanja prisutnosti mobilnog uređaja korisnika na mreži WiFi pristupne točke u prostoriji najbolje nam odgovara poznata **ping** naredba. Dakle, naš sustav bi trebao u određenim vremenskim intervalima provjeravati prisutnost određenog korisnika na način da izvršava ping naredbu na IP adresu korisnika.

Dakle, da bi sustav mogao pingati mobilni uređaj on mora imati određenu IP adresu odnosno mora biti spojen na mrežu zadane WiFi pristupne točke. Također, potrebno je odrediti na koju pristupnu točku se mobilni uređaj treba spojiti

Upravo je to uloga aplikacije i NFC protokola.

Prvi korak je otvaranje mobilne aplikacije te prijava korištenjem primjerice AAI korisničkog računa pri čemu postupak autentifikacije realiziramo preko specificiranog API-a. Nakon uspješne prijave znamo kojem korisniku pripada mobilni uređaj te aplikacija aktivira NFC na mobilnom uređaju. Korisnik prislanja mobitel na NFC čitač koji se nalazi u prostoriji.

Ovdje treba navesti važan zahtjev sustava: **svakom NFC čitaču treba pridružiti naziv prostorije u kojoj se nalazi, a svaka WiFi pristupna točka će imati SSID koji također odgovara prostoriji u kojoj se nalazi.**

Na ovaj način će čitač znati na koju pristupnu točku se uređaj korisnika treba spojiti te će mu korištenjem NFC protokola „narediti“ spajanje na zadanu WiFi pristupnu točku sa svim potrebnim podacima. Nakon uspješnog spajanja na mrežu, aplikacija će čitaču poslati **IP i MAC adresu** koje će biti spremljene u sustavu zajedno sa vremenom upisa. Nakon izvršenih operacija, čitač će zvučnim signalom i bojom obavijestiti korisnika o uspješnosti postupka.

Iz opisa rada čitača zaključujemo da on mora biti spojen s **aplikacijskim serverom** kako bi mogao pretraživati i spremati podatke. Logika aplikacijskog servera biti će implementirana u **Node.js** okruženju korištenjem **express** programskog okvira dok će aplikacijski server u produkciji biti *host-an* na **Linux** serveru s **Ubuntu** distribucijom. Za potrebe implementacije web servera biti će korišten **Apache** web server kojim će se realizirati poveznica između aplikacijskog servera i ostalih modula sustava.

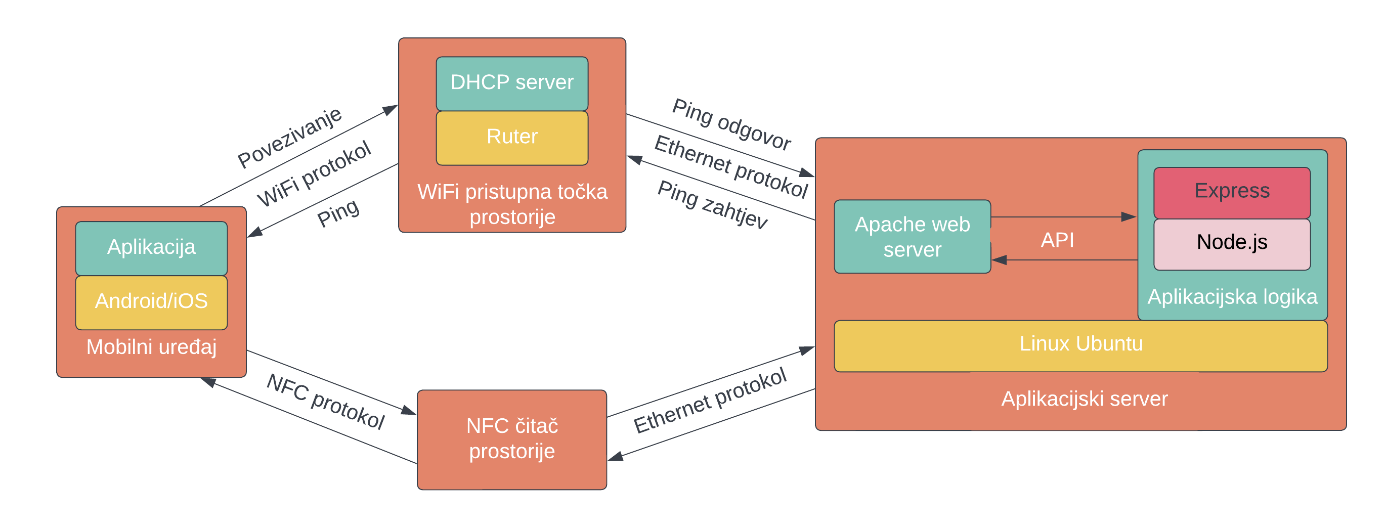
Za potrebe dodjele IP adresa biti će korišten automatski postavljen **DHCP** server koji se odvija na samoj WiFi pristupnoj točki.

Također, aplikacija će morati detektirati slučaj prijave profesora koji bi trebao **prethoditi prijavi ostalih studenata** kako bi mogli inicirati sesiju predmeta koji je upisan u rasporedu za tu prostoriju u tom terminu. U tom slučaju, čitač mora proslijediti zadanu naredbu aplikacijskom serveru zajedno s podacima prijavljenog profesora.

U slučaju da nema inicirane sesije predmeta, odnosno profesor nije prethodno odradio očitavanje, sustav treba odbaciti sve moguće prijave i otkazati spajanja na pristpnu točku

Nakon ulaska svih osoba u prostoriju sve osobe bi trebale biti spojene na pristupnu točku prostorije. Na strani aplikacijskog servera inicijalizirana je sesija koja će u intervalima od primjerice 1 minute izvršavati **ping** naredbu prema IP adresama svih uređaja koje su prethodno zapisane u sustavu.

Arhitektura sustava zajedno s korištenim tehnologijama prikazan je na slici Slika 3‑1:

****

Slika ‑ Arhitektura sustava i korištenih tehnologija

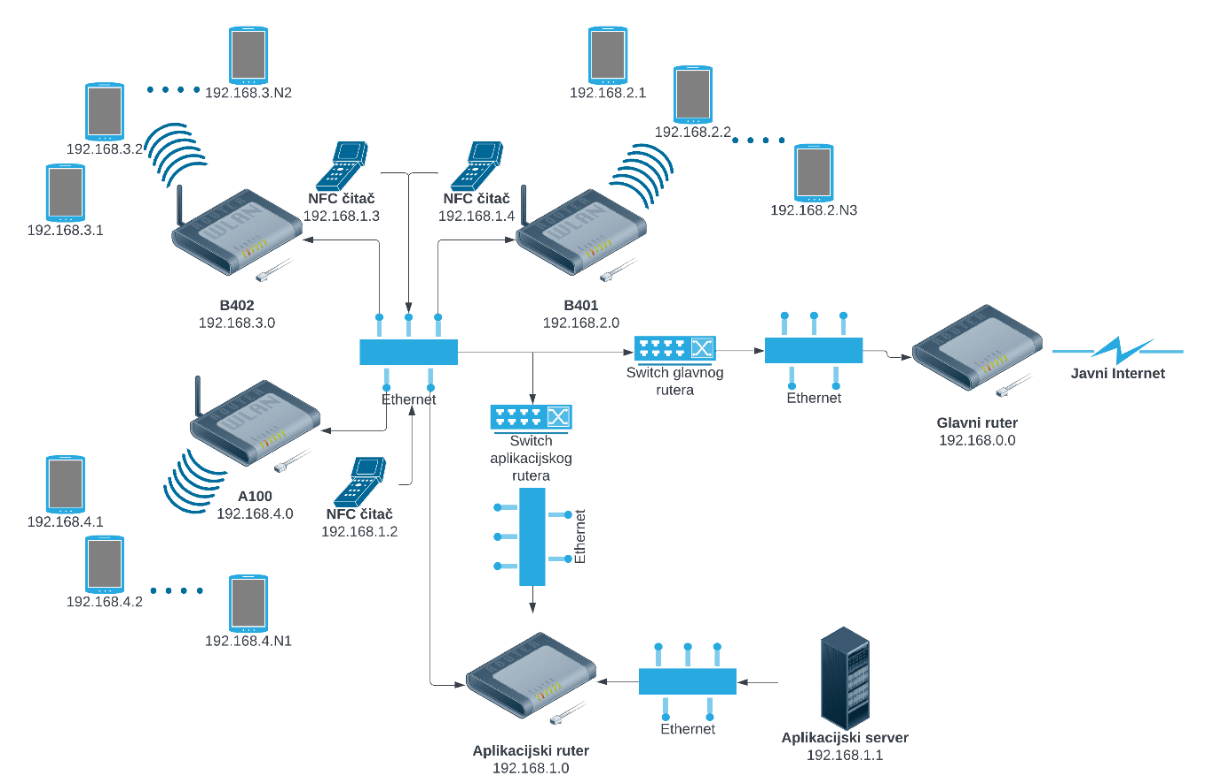
## Mrežna arhitektura sustava

Međutim, znamo da svi uređaji koji se nalaze „iza“ mrežnog rutera imaju **privatne IP adrese.** Znamo da su privatne IP adrese jedino validne unutar LAN mreže te da uređaj koji se nalazi izvan LAN-a ne može poslati paket na privatnu IP adresu.

Da bi aplikacijski server mogao izvršiti ping naredbu nad mobilnim uređajem u nekoj od prostorija potrebno je definirati određenu topologiju pod mreže kroz podjelu na podmreže i definiranje potrebnih mrežnih maski iz kojih proizlaze određena ograničenja sustava.

Za privatne adrese ćemo koristiti 192.168. klasu

Mrežna arhitektura sustava prikazan je na slici Slika 3‑2:



Slika ‑ Mrežna arhitektura sustava

Dakle, cijeli sustav povezan je na 1 glavni ruter preko kojeg je moguć pristup Internetu izvan lokalne mreže pri čemu se za te potrebe koristi NAT protokol. Glavni ruter definira 192.168.0.0/16 IP adrese navedeno u CIDR notaciji.

Glavni ruter kao *defualt gateway* ima IP adresu 192.168.0.0 dok će ruter aplikacijskog servera imati adresu 192.168.1.0 ,a ostale pristupne točke po prostorijama koja zapravo predstavljaju rutere na mrežnoj razini će imati adrese 192.168.2.0, 192.168.3.0 itd. pri čemu redoslijed pridjeljivanja IP adresa nije bitan.

Iz ovakve dodjele IP adresa proizlazi važno ograničenje sustava: **sustav može istovremeno pokrivati najviše 255 prostorija**.

Nadalje, svaki od prethodno navedenih rutera definira vlastitu podmrežu u kojoj on predstavlja *default gateway* na koji se spajaju svi ostali uređaji koji zapravo predstavljaju mobilne uređaje korisnika. Zadani ruteri će definirati 192.168.[1-255].0/24 IP adrese pri čemu će njihova adresa biti 192.168.[1-255].0. Također, uočimo da su na aplikacijski ruter povezani aplikacijski server te NFC čitači svih prostorija zbog potrebne komunikacije između njih i aplikacijskog servera.

Za potrebe ostvarenja komunikacije na podatkovnoj i fizičkoj ISO-OSI razini se koristi **Ethernet** protokol odnosno ethernet kabeli s RJ45 konektorom.

Iz ovakve dodjele IP adresa proizlazi drugo važno ograničenje sustava: **sustav može evidentirati najviše 255 korisnika unutar prostorije**.

Na ovaj način moguće je realizirati ping naredbu aplikacijskog servera na neki od mobilnih uređaja u određenoj prostoriji.

Postupak ćemo ilustrirat na konkretnom primjeru:

Budući da je aplikacijski server jedini uređaj povezan na ruter njegova IP adresa će biti 192.168.1.1. Recimo da želimo pingati uređaj s adresom 192.168.4.5.

1. Aplikacijski server će prvo provjeriti postoji li na njegovoj lokalnoj mreži uređaj s IP adresom 192.168.4.5. Korištenjem mrežne maske zaključit će da zadani uređaj pripada nekoj drugoj mreži te će proslijediti paket na *default gateway*
2. *Default gateway* će primiti paket te će izvršiti jedinu moguću operaciju: proslijediti će paket na glavni ruter jer je jedino s njim povezan. Za ostvarenje zadane konekcije WAN port rutera povezujemo s LAN portom glavnom rutera
3. Glavni ruter će primiti paket i na njega primijeniti mrežnu masku. Nakon primjene zaključit će da paket treba proslijediti na ruter koji definira mrežu s 192.168.4.0/24 IP adresama.
4. Ruter s adresom 192.168.4.0 predstavlja ruter ciljane prostorije. Budući da su na njega povezani svi uređaji s dodijeljenim IP adresama ruter će znati kojem mobilnom uređaju je potrebno proslijediti paket.
5. Ukoliko je mobilni uređaj spojen na mrežu -> ping će uspjeti -> korisnik je prisutan
6. Ukoliko mobilni uređaj nije spojen na mrežu -> ping neće uspjeti -> korisnik nije prisutan
7. Paket s informacijom o ishodu će se na ekvivalentan način propagirati natrag do aplikacijskog servera

Također, važno je spomenuti da se na glavnom ruteru postavlja **IP filtriranje** pomoću kojeg je jedino aplikacijskom serveru dopuštena komunikacija izvan privatne mreže kako bi se priječilo korištenje pristupnih točaka u prostorijama za pristup Internetu što bi uzrokovalo prijenos velike količine podataka i zagušenje mreže, a posljedično tome i pad performansi sustava.

## Rad sustava u određenim situacijama

Slučajevi pauze između više sati predavanja će također biti ispravno detektirani od strane sustava i neće uzrokovati nepredviđene rezultate. Sustav će detektirati odsutnost studenata tijekom pauze, a nakon povratka mobilni uređaji studenata će se **automatski spojiti** na zadanu pristupnu točku te će sustav nakon toga ispravno evidentirati prisutnost.

Međutim, iako se mobilni uređaji korisnika automatski povezuju na prethodno korištenu pristupnu točku **sustav neće evidentirati prisutnost studenta bez NFC očitavanja.**

Završetak sesije predmeta inicira se nakon što profesor ponovno izvrši NFC očitavanje ili ukoliko na pristupnoj točki nije povezan niti jedan uređaj(svi pingovi neuspješni). Nakon toga, aplikacijski server prestaje s izvršavanjem ping naredbe te podatke o parovima IP i MAC adresa za sesiju može izbrisati.

Konačno, iz vrste podataka koje sustav pohranjuje zaključujemo da ćemo moći detektirati potencijalne pokušaje **ilegalne evidencije**. Primjerice, ukoliko se neka osoba odluči na proceduru u kojoj će evidentirati sebe, odjaviti se s aplikacije, prijaviti se s AAI podacima druge osobe te ponovno izvršiti evidenciju sustav će ovaj pokušaj detektirati **jer će za identičnu MAC adresu u bazi biti pohranjene 2 ili više IP adresa.**

Ukoliko govorimo o izrazito naprednom korisniku koji će prilikom drugog pokušaja promijeniti MAC adresu i dalje će sustav biti u mogućnosti izvršiti **samo jednu ping** naredbu pa će neka od osoba i dalje ostati neevidentirana.

Jedini slučaj u kojem sustav može zapisati djelomično netočnu informaciju je sljedeći: korisnik izvrši NFC očitavanje, ali nije prisutan unutar učionice već se nalazi izvan učionice unutar dometa pristupne točke. Sustav će registrirati korisnika kao prisutnog što i nije potpuno pogrešno budući da korisnik uistinu jest bio prisutan, ali izvan prostorije. Zbog ograničenog WiFi dometa izvan prostorije vjerojatnost da će se netko odlučiti na stajanje neposredno ispred prostorije je jako mala i pomalo zabrinjavajuća.

## Zadovoljenje nefunkcionalnih zahtjeva

* **Sigurnost**: komunikacija između modula sustava odvija se preko standardiziranih protokola koji su ujedno i jedni od najkorištenijih protokola na globalnoj razini čime je pouzdanost postupaka enkripcije i dekripcije zagarantirana. Najveća ranjivost sustava leži u oslanjanju na bežične komunikacijske kanale koji su znatno ranjiviji od žičnih kanala. Kod WiFi protokola govorimo o 2 najčešća i najopasnija napada:

1. **Deauthentication attack:** korištenjem bilo kojeg MacOs ili Linux računala moguće je odspojiti bilo koji uređaj povezan na određenu WiFi pristupnu točku te bi u tom slučaju svi korisnici bili neevidentirani. Međutim, na tržištu su dostupna rješenja i to u vidu korištenja **Encryption of Management Frames** opcije
2. **Radio jamming:** odašiljanjem signala identične frekvencije kanala koji koristi određena WiFi pristupna točka moguće je izvršiti DoS napad u kojem se nijedan korisnik ne bi mogao spojiti na pristupnu točku te bi svi ostali neevidentirani. U ovom slučaju moguće je koristiti **WiFi blocker** uređaj koji će vršiti prevenciju zadanih napada(skuplje) ili instalirati softver za detekciju(jeftinije) koji će detektirati napad pri čemu sustav mora odlučiti na koji način reagirati u tom slučaju.

* **Pouzdanost:** U slučaju nefunkcioniranja sustava NFC čitač će zvučnim signalom i bojom korisniku dati do znanja da sustav nije u funkciji, ali će profesor nakon što sustav ponovno bude u funkciji moći ručno upisati vlastitu prisutnost i prisutnost studenata.
* **Točnost:** aplikacijski server odašilje ping zahtjeve u intervalima od 1 minute nakon iniciranja sesije
* **Tehnologije:** sve korištene tehnologije zahtijevaju ovaj zahjtev
* **Uporabljivost:** gotovo svaki prosječni Android ili Iphone mobitel posjeduje NFC tehnologiju koja je jedini uvjet koji uređaj treba imati za korištenje sustava.
* **Općenitost:** arhitektura sustava može se preslikati na sva ostala područja unutar zadane domene. Jedina promjena se može odnositi na promjenu aplikacijske logike u kojoj primjerice u određenim kompanijama neće biti potrebe za rolom koja je u našem slučaju odgovara profesoru već će biti dovoljno korištenje rola studenta/zaposlenika i administratora.
* **Cijena:** oprema svake prostorije sastoji se od:

1. **Dual band WiFi pristupna točka:** Netgear WiFi 6 AX1800 Dual Band Access Point -> 150 eura
2. **NFC čitač:** ACR1252U USB NFC Reader III -> 50 eura
3. **Ethernet kabeli:** zbog male količine podataka koji se prenose dovoljno je koristit Cat5e Shielded kabel. Uzmimo da duljina kabela potrebnog za povezivanje čitača i pristupne točke u prosjeku iznosi 20 metara -> 4 eura

Povećanje cijene moguće je u slučaju velikog broja prostorija koja zahtijevaju instalaciju WiFi mesh infrastrukture te u ovisnosti o opciji korištenja WiFi blocker uređaja. Također, u ovisnosti o topologiji postojeće mrežne infrastrukture moguće je variranje u korištenju određenih mrežnih uređaja.

* **Usklađenost sa zakonima:** korisnicima sustava će biti ponuđen formular u kojem trebaju izreći suglasnost s korištenjem njihovih osobnih podataka od strane sustava.

# Primjer korištenja

1. Profesor izvršava početno NFC očitavanje u kojem čitač prosljeđuje dobivene podatke na aplikacijski server koji zaključuje da je riječ o profesoru te inicira sesiju
2. Čitač prosljeđuje aplikaciji na profesorovom mobilnom uređaju podatke za spajanja ne pristupnu točku
3. Profesorov mobilni uređaj se spaja na zadanu pristupnu točku
4. Aplikacija mobilnog uređaja šalje dobivenu privatnu IP adresu i svoju MAC adresu čitaču koji ih prosljeđuje na aplikacijski server koji ih sprema u sustav i povezuje s profesorom
5. Čitač zvučnim signalom i bojom izvještava profesora o uspješnosti operacije
6. Studenti ulaze u prostoriju te izvršavaju NFC očitavanje s jednakim postupcima kao u koracima 2 – 5
7. Aplikacijski server izvršava ping naredbu svako 60 sekundi na svim pohranjenim IP adresama u sustavu te u ovisnosti o odgovoru evidentira prisutnost
8. Profesor završava sa satom te prilikom izlaska iz prostorije izvršava drugo NFC očitavanje. Aplikacijski server prekida dosadašnju sesiju te briše sve podatke vezane uz sesiju. Podaci od evidenciji su prethodno već spremani tijekom cijele sesije.

# *Proof of concept*

Budući da realizacija zadanog rješenja u produkciji zahtijeva prilično veliku infrastrukturu, za početak je potrebno kreirati i testirati *proof-of-concept* rješenje čija je svrha potvrda prethodno navedenih koncepata i ideje projekta nakon čega je moguće ići u stvarnu, produkcijsku realizaciju.

## Sistemska podrška

Za realizaciju sistemskog aspekta *proof of concept* rješenja korišteni su sljedeći hardverski resursi:

* **Raspberry Pi 4 Model B 4GB RAM**
* **32GB SD kartica** kao medij pohrane za Raspberry Pi računalo
* Raspberry Pi metalna kutija za prenosivost
* Raspberry Pi 4 ventilator: postavljen na metalnu kutiju za potrebe hlađenja. **Crvena** žica spojena je na RasppberryPi **pin 2** za napajanje od 5V dok je **crna** žica spojena na **pin 6** uzemljenje(GND)
* Napajanje korištenjem adaptera električne energije za održavanje randog napona u intervalu 4.75V - 5.25V koji je predviđen za Raspberry Pi računalo

Za realizaciju NFC aspekta planirana je nabava **Adafruit PN532 NFC/RFID controller breakout board - v1.6** . Planirano je fizičko spajanje zadane pločice na Raspberry Pi i to na sljedeći način:

* PN532 SCK → RPi GPIO 11 (SPI\_CLK)
* PN532 MISO → RPi GPIO 09 (SPI\_MISO)
* PN532 MOSI → RPi GPIO 10 (SPI\_MOSI)
* PN532 SSEL → RPi GPIO 08 (SPI\_CE0\_N)
* PN532 3.3v → RPi 3.3v (multiple pins)
* PN532 GND → RPi GND (multiple pins)

Komunikacija između Raspberry Pi računala i NFC pločice odvijala bi se preko SPI sučelja uz korištenje **libnfc**biblioteke.

Međutim, zbog problema u isporuci nismo bili u mogućnosti koristiti zadanu pločicu pa je NFC dio komunikacije *hard* kodiran. Budući da se NFC dio prvenstveno odnosi na poboljšanje *user experience* dijela njegovo odsustvo ne utječe na ispitivanje valjanosti predloženog rješenja.

Slika na kojoj se prikazuje na zatvorenom, elektronički, prilagodnik

Opis je automatski generiran

Slika 5‑1 Raspberry Pi server

Slika na kojoj se prikazuje na zatvorenom, prilagodnik

Opis je automatski generiran

Slika 5‑2 Raspberry Pi server portovi(1)

Slika na kojoj se prikazuje prilagodnik

Opis je automatski generiran

Slika ‑ Raspberry Pi server portovi(2)

## Aplikacijski server i baza podataka

Aplikacijski server i baza podataka instalirani su na Raspberry Pi računalu na koje je instaliran **Raspbian GNU/Linux verzija 10 (*codename buster*)** operacijski sustav.

Instalirano je **Node.js** okruženje verzije **10.24.0**.

Popis *dependencies*-a koje je potrebno instalirati za pokretanje aplikacijskog servera:

* ***Bcrypt***: lozinke u bazi podataka ne pohranjujemo u *plaintext-u* već pohranjujemo *hash*-iranu kombinaciju *plaintext* lozinke i soli(*salt*).
* ***Dotenv***: učitavanje *environment* varijabli iz *.env* datoteke u globalni *process.env* objekt za njihovo korištenje u kodu.
* ***Express***: programski okvir za razvoj aplikacijskog servera
* ***Morgan***: *logger* za sadržajno ispisivanje ishoda HTTP zahtjeva upućenih prema serveru
* ***Winston***: *logger* za potrebe ispisivanja rezultata i *debug* na serveru
* ***Pg***: modul za pristup PostgreSQL bazi podataka potreban Sequelize modulu
* ***Ping***: realizacija *ping* naredbe za praćenje prisutnosti
* ***Sequelize***: ORM alat koji služi kao poveznica između aplikacijskog servera i baze podataka.

Instaliran je ***PostgreSQL*** DBMS verzije **11.18** za bazu podataka.

Za GUI pristup bazi podataka dodatno je instalirana ***PgAdmin3*** klijentska aplikacija.

Zbog problema pristupa Raspberry Pi računalu izvan LAN-a u kojem se nalazi i nemogućnosti korištenja statičke IP adrese korišteno je **PiTunnel** rješenje koje po principu sličnom VPN serveru dodjeljuje Raspberry Pi računalu javnu domenu te pruža *out of the box* uslugu tuneliranja prometa na server.

## Klijentska aplikacija

Za *proof-of-concept* potrebe razvijena je samo Android verzija aplikacije.

Aplikacija je razvijena u **Android Studio IDE** korištenjem programskog jezika **Java**.

Kreirani su osnovni moduli aplikacije potrebni za dokazivanje *proof-of-concept* rješenja:

* Autentikacija kao student ili kao profesor
* Pregled ostvarenog prisustva po predmetima za studenta i profesora
* Registracija/otvaranje sesije predmeta za profesora
* Registracija studenta za evidenciju
* Zatvaranje sesije predmeta za profesora

Aplikaciju je moguće pokrenuti na stvarnom Android uređaju ili korištenjem emulatora unutar Android Studio IDE.

### Zajedničke opcije

A picture containing diagram

Description automatically generated

Slika ‑ Početno sučelje

Graphical user interface

Description automatically generated with low confidence

Slika ‑ Forma za prijavu

### Profesorske opcije

A picture containing diagram

Description automatically generated

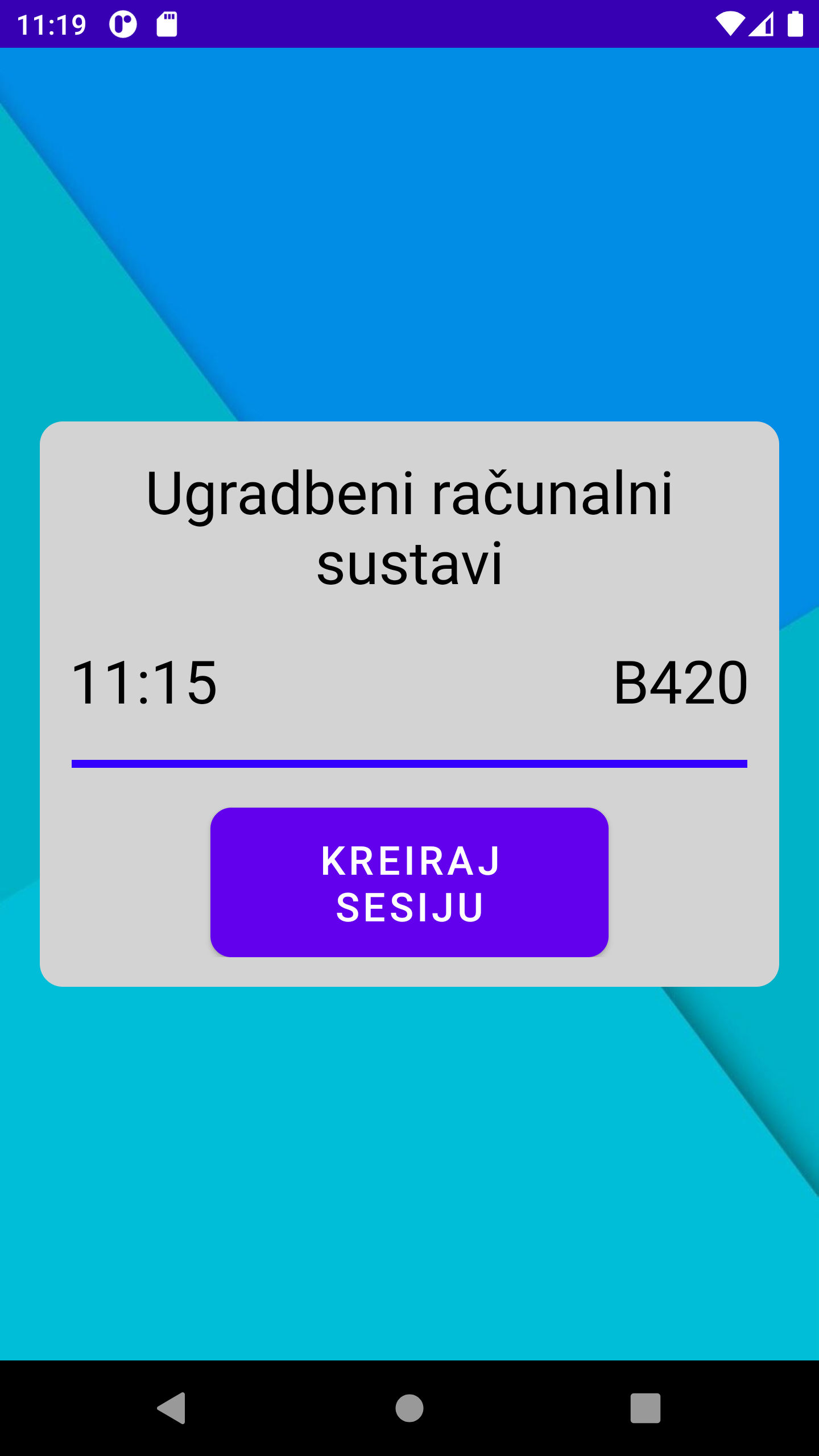
Slika ‑ Početno sučelje profesora

Graphical user interface, application

Description automatically generated

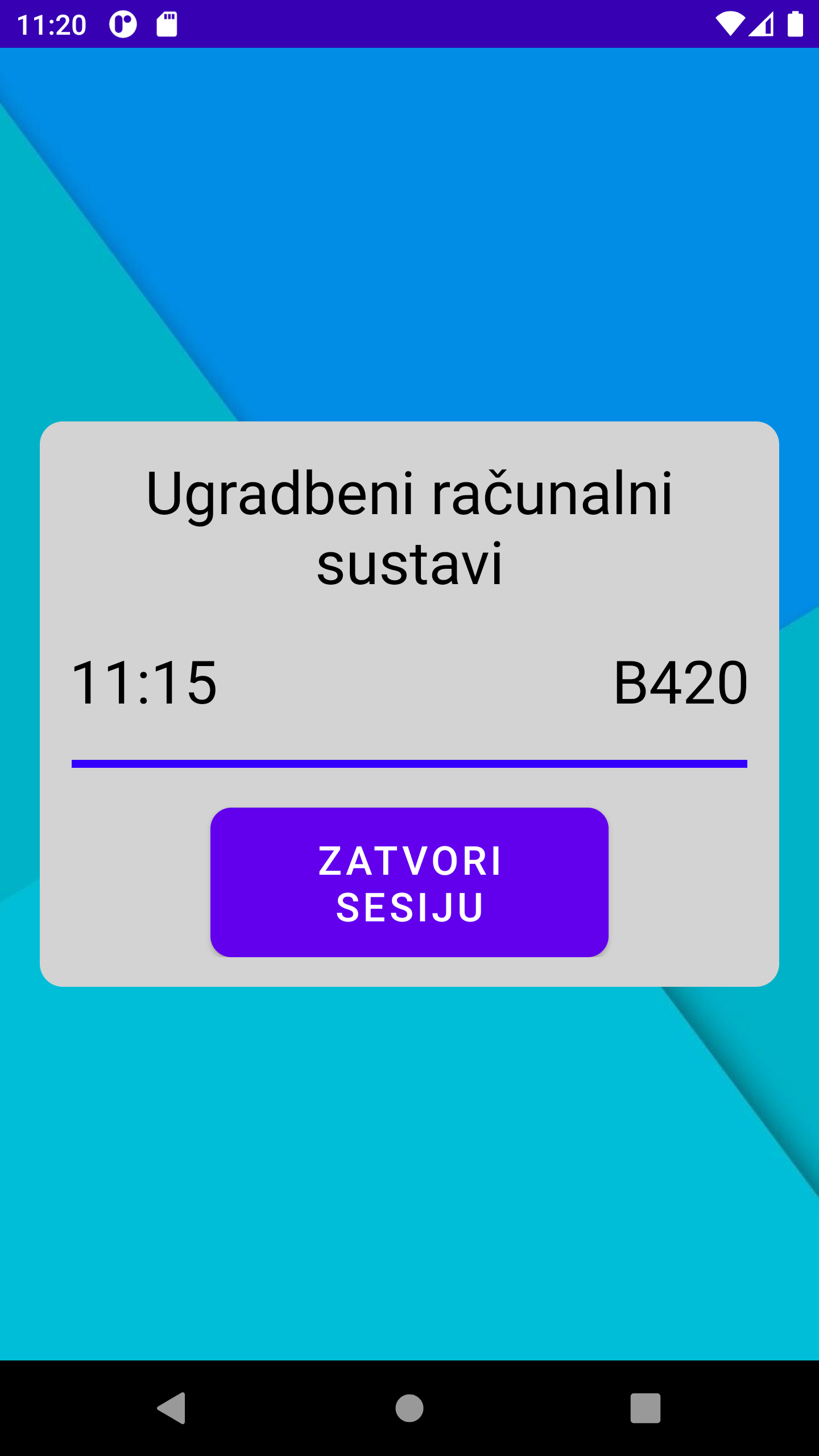
Slika ‑ Pregled prisutnosti

profesora



Slika ‑ Profesor - registracija

početka nastave



Slika ‑ Profesor - kraj nastave

### Studentove opcije

A picture containing diagram

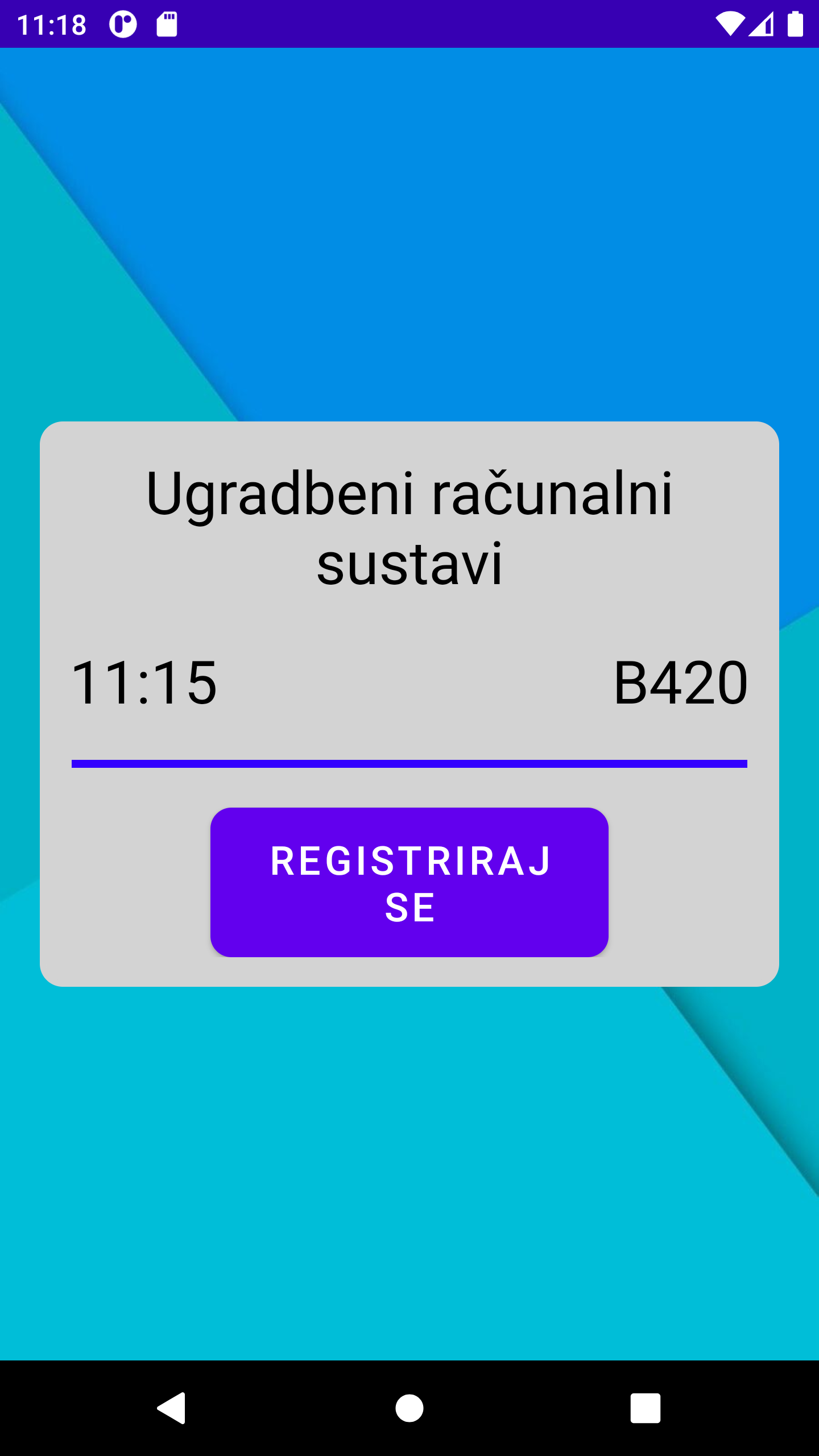
Description automatically generated

Slika ‑ Početno sučelje studenta

Graphical user interface, application

Description automatically generated

Slika ‑ Pregled prisutnosti - student



Slika ‑ Registracija studenta

# PRILOZI

## Kazalo slika

[Slika 3‑1 Arhitektura sustava i korištenih tehnologija 7](#_Toc127443891)

[Slika 3‑2 Mrežna arhitektura sustava 8](#_Toc127443892)

[Slika 5‑1 Raspberry Pi server 14](#_Toc127443893)

[Slika 5‑2 Raspberry Pi server portovi(1) 14](#_Toc127443894)

[Slika 5‑3 Raspberry Pi server portovi(2) 15](#_Toc127443895)

[Slika 5‑4 Početno sučelje 16](#_Toc127443896)

[Slika 5‑5 Forma za prijavu 17](#_Toc127443897)

[Slika 5‑6 Početno sučelje profesora 17](#_Toc127443898)

[Slika 5‑7 Pregled prisutnosti 18](#_Toc127443899)

[Slika 5‑8 Profesor - registracija 18](#_Toc127443900)

[Slika 5‑9 Profesor - kraj nastave 19](#_Toc127443901)

[Slika 5‑10 Početno sučelje studenta 19](#_Toc127443902)

[Slika 5‑11 Pregled prisutnosti - student 20](#_Toc127443903)

[Slika 5‑12 Registracija studenta 20](#_Toc127443904)

1. Doduše, kod QR koda mogućnost postoji ukoliko je QR kod aktivan unutar određene aplikacije sustava, ali je u tom slučaju za potrebnu aktivnost potrebna internetska povezanost korisnika što je u našem slučaju prevelik zahtjev zbog praktičnosti. Također, funkcionalnost ovog sustava bi bilo moguće izvesti korištenjem principa skeniranja QR koda, ali u tom slučaju žrtvovala bi se mogućnost olakšanog održavanja sustava i nemogućnosti integracije sustava čitača s određenim vanjskim servisima za provjeru validnosti. Također, omogućilo bi se spajanje korisnika na WiFi pristupnu točku bez potrebe za validacijom postojanja sesije. [↑](#footnote-ref-1)