

MULTIFAKTORSKA AUTENTIFIKACIJA I KONTROLA PRISTUPA ZASNOVANA NA INTEGRACIJI SENZORA I BIOMETRIJE

MULTIFACTOR AUTHENTICATION AND ACCESS CONTROL BASED ON SENSOR INTEGRATION AND BIOMETRICS

Miljana Stefanov, *Fakultet tehničkih nauka, Novi Sad*

Oblast – ELEKTROTEHNIKA I RAČUNARSTVO

Kratak sadržaj – U ovom radu predstavljen je dizajn multifaktorskog sistema za autentifikaciju i kontrolu pristupa, koji kombinuje senzore pokreta, biometriju i prepoznavanje glasa. Sistem omogućava dva nivoa verifikacije – PIN ili otisak prsta i prepoznavanje glasa – pre odobrenja pristupa ili aktiviranja alarma.

Ključne reči: Multifaktorska autentifikacija, verifikacija

Abstract – This paper presents the design of a multifactor authentication and access control system that combines motion sensors, biometrics, and voice recognition. The system provides two levels of verification – PIN or fingerprint, and voice recognition – before granting access or activating an alarm.

Keywords: Multifactor authentication, verification

1. UVOD

Pojam bezbednosti je individualan i zavisi od potreba svakog pojedinca. Dok je nekima dovoljno da zaključaju vrata i ostave rezervni ključ komšiji, drugi se oslanjaju na napredna tehnološka rešenja. U prošlosti, kuće su čuvalе životinje poput pasa, dok se danas sve više oslanjamo na moderne tehnologije i senzore. Vremenom, sa promenom društvenih i tehnoloških okolnosti, menja se i samo shvatanje termina "bezbednost".

Savremeni senzori omogućavaju praćenje doma u realnom vremenu i slanje obaveštenja u slučaju neuobičajene aktivnosti. Ovo rešenje doprinosi osećaju sigurnosti, kako u kućama tako i u stanovima, posebno za ljude koji nemaju želju ili mogućnost da drže životinje kao čuvarе.

U ovom radu prikazan je primer implementacije sigurnosnog sistema za kontrolu ulaska u dom.

2. OPIS SISTEMA

Cilj ovog istraživanja je dizajn i implementacija sigurnosnog sistema za automatsko upravljanje vratima, koji omogućava višestepenu autentifikaciju korisnika.

Fokus je na sigurnosti i efikasnosti kroz integraciju senzora i mikrokontrolera.

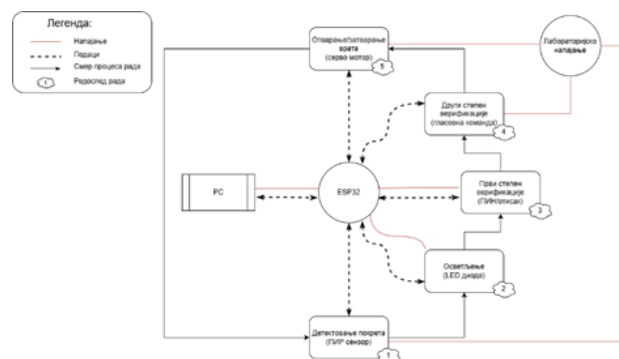
NAPOMENA:

Ovaj rad proistekao je iz master rada čiji mentor je bio dr Jovan Bajić, vanr. prof.

Sistem omogućava pristup samo ovlašćenim korisnicima koristeći sledeće korake:

- 1. Detekcija korisnika** – PIR senzor registruje pokret i aktivira LED diodu.
- 2. Prvi stepen verifikacije** – Korisnik unosi PIN ili skenira otisak prsta.
- 3. Drugi stepen verifikacije** – Aktivira se senzor za prepoznavanje glasa.
- 4. Otvaranje vrata** – Ako su oba koraka uspešna, vrata se otvaraju; u suprotnom, aktivira se alarm i šalje obaveštenje preko Telegram aplikacije.
- 5. Napajanje i kontrola** – Sistemom upravlja ESP32 mikrokontroler, dok laboratorijsko napajanje omogućava rad komponenti.

Blok šema koja se nalazi na slici broj 1, prikazuje strukturu sistema, uključujući linije napajanja, tok podataka i redosled aktivacije komponenti.



Slika 1. Rezultati simulacije

3. PREGLED KOMPONENTI SISTEMA

3.1. ESP32

ESP32 može označavati sam čip ili razvojnu ploču, koja je praktičnija za učenje i testiranje. Najčešće se koristi razvojne ploče, poput ESP32 DEVKIT DOIT, koje uključuju USB interfejs, regulatore napona i lako dostupne GPIO pinove. Izgled mikrokontrolera dat je na slici broj 2.



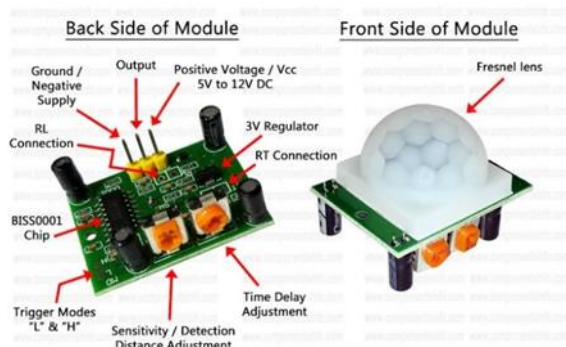
Slika 2. ESP32 DEVKIT [1]

Ovaj mikrokontroler ima dvostruko jezgro, integrisani *Wi-Fi* i *Bluetooth*, što ga čini idealnim za *IoT* projekte. Podržava različite komunikacione interfejsse (*UART*, *SPI*, *I²C*, *PWM*, *ADC*, *DAC*) i omogućava efikasno upravljanje resursima. Njegova niska potrošnja energije (*deep sleep*, *light sleep režimi*) pogodna je za baterijski napajane uređaje.

ESP32 podržava razvojna okruženja poput *Arduino IDE*, *MicroPython* i *ESP-IDF*. Fleksibilni *GPIO* pinovi omogućavaju prilagođavanje projektima, uključujući promenu podrazumevanih *I²C* pinova (*GPIO 21 – SDA*, *GPIO 22 – SCL*). Zbog ovih karakteristika, ESP32 je jedno od najpopularnijih rešenja za automatizaciju, pametne uređaje i senzorske mreže.

3.2. PIR senzor

PIR senzor detektuje infracrveno zračenje koje emituju sva tela na temperaturama iznad apsolutne nule. Sastoji se od piroelektričnog senzora, koji registruje promene u infracrvenom spektru i Frenelovih sočiva, koja povećavaju domet i širinu vidnog polja. Prikazan je na slici broj 3.



Slika 3. Izgled PIR senzora sa donje i gornje strane [2]

Što se tiče podešavanja senzora, postoje dva potencijometra. Jedan potencijometar vezan je za osetljivost. Ukoliko se pomera u smeru kazaljke na satu onda se povećava osetljivost, suprotno se smanjuje. Drugi potencijometar vezan je za vremensko odlaganje, odnosno koliko dugo izlaz ostaje u visokom stanju nakon detekcije (1s-3min). Postoje i dva režima rada, *single* i *multiple trigger mode*. U projektu je izabran *single trigger mode*.

U ovom projektu, PIR senzor detektuje prisustvo osobe ispred vrata i aktivira LED diodu za osvetljenje. Kada se pokret registruje, sistem prelazi na sledeći nivo verifikacije korisnika.

3.3. OLED displej

OLED displej ZJY096I0400WG11 je ekran dijagonale 0,96 inča sa *I²C* interfejsom i rezolucijom 128x64 piksela. Izgled datog displeja dat je na slici broj 4.



Slika 4. Izgled OLED displeja [3]

Zahvaljujući tome što svaki piksel samostalno emituje svetlost, ima visok kontrast i malu potrošnju energije. U

ovom radu koristi se za prikaz informacija korisniku – kao što su status sistema i rezultati verifikacije – čime omogućava jasan uvid u tok procesa autentifikacije. Komunikacija sa ESP32 mikrokontrolerom ostvaruje se putem *I²C* protokola, korišćenjem samo dve linije: *SDA* (za podatke) i *SCL* (za taktnu sinhronizaciju).

3.4. Tastatura

U ovom sistemu, 4x4 membranska tastatura predstavlja jednu od dve ponuđene metode za prvi stepen verifikacije. Na slici broj 5 prikazan je izgled iskorišćene tastature sa pripadajućim rasporedom pinova



Slika 5. Izgled 4x4 tastature u rasporedu pinova [4]

Zbog svoje otpornosti na vlagu, masnoću i mehaničku pouzdanost, odabrana je umesto osetljivih *touch* ekrana, koji u realnim uslovima mogu da dovedu do grešaka pri unosu. Tastatura funkcioniše po principu presecanja redova i kolona: kada korisnik pritisne taster, zatvara se kontakt između određenog reda i kolone, što mikrokontroler prepoznaje putem programske logike koja sekvencijalno aktivira izlazne linije i očitava ulazne. Na osnovu aktivnog spoja, određuje se koji je taster pritisnut i taj unos se dalje koristi u procesu autentifikacije.

3.5. Senzor za skeniranje otiska prsta

Senzor za otisak prsta koristi se kao alternativa tastaturi za prvi stepen verifikacije korisnika. Na slici broj 6 prikazan je izgled korišćenog senzora.



Slika 6. Izgled senzora za skeniranje otiska prsta [5]

U pitanju je optički skener koji snima otisak i upoređuje ga sa prethodno sačuvanim šablonima radi potvrde identiteta. Karakteriše ga brz odgovor (manje od 1 sekunde), kapacitet od 162 otiska i nizak procenat grešaka pri prepoznavanju. U ovom radu povezan je sa ESP32 mikrokontrolerom putem *TTL* serijske komunikacije i omogućava sigurnu, brzu i jednostavnu biometrijsku autentifikaciju korisnika.

3.6. Senzor za prepoznavanje fraza

U završnoj fazi verifikacije koristi se senzor za prepoznavanje fraza, čime se sistemu dodaje drugi

sigurnosni sloj – glasovna potvrda identiteta. Ugrađeni modul omogućava *offline* rad, bez potrebe za internet konekcijom i prepoznaje do 17 korisnički definisanih komandi. Izgled datog senzora dat je na slici broj 7.



Slika 7. Izgled senzora za prepoznavanja fraza [6]

Dati senzor je povezan sa ESP32 mikrokontrolerom putem *I²C* protokola, što omogućava jednostavno proširenje sistema bez zauzimanja velikog broja pinova. Zahvaljujući integriranom zvučniku, korisniku se pruža povratna audio informacija, dok kompaktnost i pristupačnost modula čine ga pogodnim za upotrebu u pametnim sistemima kontrole pristupa.

4. POVEZIVANJE KOMPONENTI

Za pravilno funkcionisanje sistema bilo je neophodno pažljivo definisati povezivanje svake komponente sa odgovarajućim *GPIO* pinovima na ESP32 mikrokontroleru. Sve komponente, uključujući senzore, tastaturu, displej i servo motor, imaju dodeljene pinove u skladu sa funkcionalnim zahtevima sistema. Posebno su konfigurisani *GPIO* 33 i *GPIO* 32 kao *SDA* i *SCL* linije za *I²C* komunikaciju, zahvaljujući fleksibilnosti ESP32 i biblioteci *Wire*, koja omogućava redefinisane pinova. U tabeli 1 dat je pregled načina povezivanja iskorišćenih uređaja sa odgovarajućim *GPIO* pinovima.

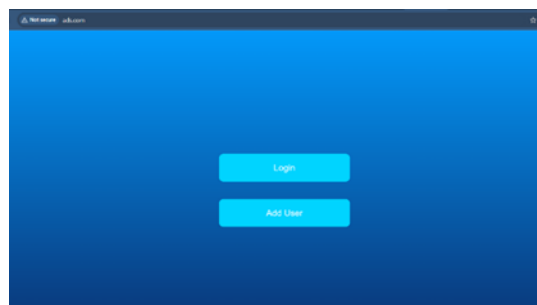
Tabela 1. Komponente i odgovarajući *GPIO* pinovi

Uređaj	Pin na ESP32
Tastatura – redovi (R1, R2, R3, R4)	<i>GPIO</i> 13,12,14,27
Tastatura – kolone (C1, C2, C3, C4)	<i>GPIO</i> 26,25,15,2
<i>PIR</i> sensor	<i>GPIO</i> 23
Servo motor	<i>GPIO</i> 18
Senzor otiska prsta (TX - RX)	<i>GPIO</i> 17 (RX2), <i>GPIO</i> 16 (TX2)
Senzor za prepoznavanje fraza (<i>I²C</i>)	<i>GPIO</i> 33 (<i>SDA</i>), <i>GPIO</i> 32 (<i>SCL</i>)
<i>OLED</i> displej (<i>I²C</i>)	<i>GPIO</i> 21 (<i>SDA</i>), <i>GPIO</i> 22 (<i>SCL</i>)
<i>LED</i> dioda	<i>GPIO</i> 5

5. WEB STRANICA

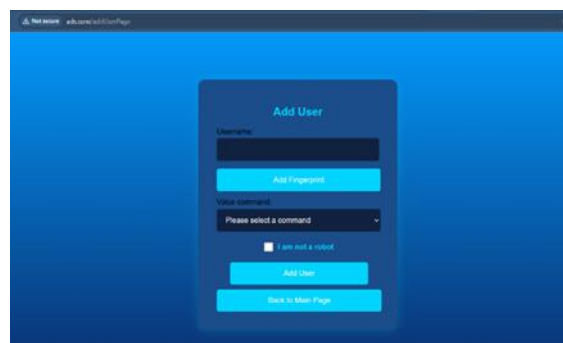
Za potrebe upravljanja korisnicima i verifikacije identiteta, razvijen je jednostavan *web* interfejs koji omogućava lokalni pristup stranici putem *IP* adrese koju ESP32 dobija

nakon povezivanja na mrežu. Pristupom početnoj stranici korisniku se nude dve osnovne opcije: prijava na sistem i kreiranje novog naloga i to je prikazano na slici broj 8.



Slika 8. Glavni meni

Na slici ispod, označenom pod brojem 9 prikazana je stranica za kreiranje naloga.



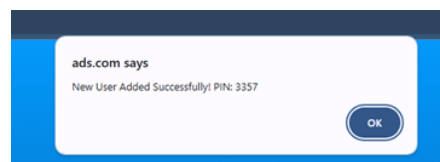
Slika 9. Stranica za dodavanje novog korisnika

Prilikom kreiranja naloga, korisnik unosi korisničko ime i registruje svoj otisak prsta kao jedan od načina verifikacije. Da bi unos bio validan, mora ispuniti određena pravila. Sistem automatski proverava da li već postoji korisnik sa unetim imenom i prikazuje poruku u slučaju neuspešnog unosa. Interfejs prikazuje sve faze registracije otiska prsta – od početnog očitavanja, preko validacije, do završetka procesa – uz jasan prikaz statusa i poruka korisniku. U sklopu registracije, korisnik bira i frazu iz ponuđene liste komandi koja se kasnije koristiti za glasovno prepoznavanje. Spisak fraza je dat na slici broj 10.



Slika 10. Lista dostupnih komandi

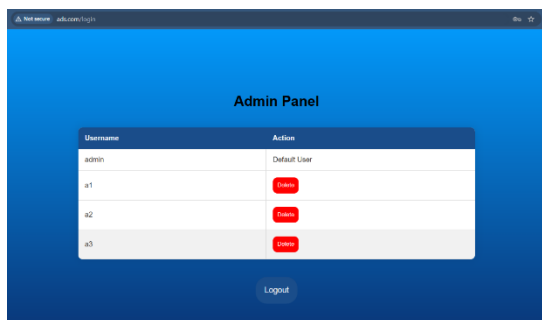
PIN se korisniku dodeljuje automatski nakon uspešne registracije, kako bi se obezbedila jedinstvenost i izbegle greške pri izboru. Kraj uspešne registracije prikazan je na slici broj 11.



Slika 11. Uspešno dodat korisnik

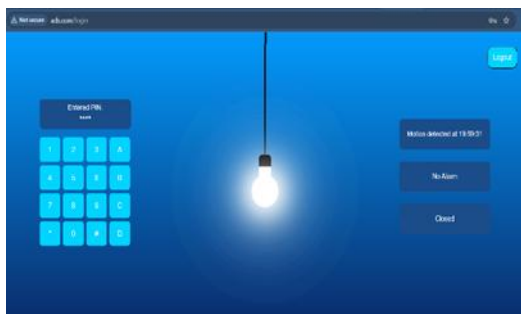
Pored opcije za kreiranje naloga, interfejs sadrži i deo za prijavu korisnika. Nakon uspešnog logovanja, korisnik biva preusmeren na odgovarajuću stranicu u zavisnosti od privilegija: administrativni panel za administratora ili korisnički prikaz za običnog korisnika.

Na administratorskoj stranici, prikazanoj na slici broj 12, prikazana je lista svih registrovanih korisnika sa mogućnošću njihovog brisanja. Ova funkcionalnost omogućava jednostavno upravljanje bazom korisnika.



Slika 12. Izgled admin stranice

Na korisničkoj stranici, prikazanoj na slici broj 13, vizuelno se prikazuje ponašanje sistema u realnom vremenu: kada PIR senzor detektuje pokret, ispisuje se vreme detekcije; kada se unosi PIN kod, unosi se i na ekranu; kada se aktivira LED dioda, pali se sijalica; a tokom rada servo motora, status vrata se menja. Ako su oba koraka verifikacije uspešno završena, servo motor automatski otvara vrata. U suprotnom, nakon tri neuspešna pokušaja, aktivira se alarm, a sistem korisniku automatski šalje obaveštenje o pokušaju neovlašćenog pristupa putem Telegram aplikacije. Na ovaj način, korisnički interfejs pruža jasnu i intuitivnu vizualizaciju toka autentifikacije i rada sistema, dok se bezbednosne informacije prenose u realnom vremenu.



Slika 13. Izgled korisničkog interfejsa

6. ZAKLJUČAK

Ovaj rad prikazuje multifaktorski sistem za autentifikaciju i kontrolu pristupa, zasnovan na pristupačnim komponentama i praktičnoj web aplikaciji koja omogućava uvid u rad sistema u realnom vremenu. U slučaju neovlašćenog pristupa, korisnik se automatski obaveštava putem Telegram aplikacije.

Poseban fokus je na mogućnostima daljeg razvoja sistema. Planirane nadogradnje uključuju opciju da korisnici samostalno menjaju korisničko ime i šifru, uz proveru da ime nije već zauzeto. Razmatra se i dodavanje provere već registrovanih otisaka prstiju, što bi omogućilo bolje upravljanje nalogom. Predložena je i mogućnost izmene

glasovnih komandi, kao i proširenje liste dostupnih fraza. Pored toga, sistem bi mogao da komunicira i bez interneta, putem GSM modula za slanje SMS poruka ili automatski poziv hitnim službama u slučaju opasnosti. Kao moguće unapređenje sistema predlaže se dodavanje dodatnih senzora i aktuatora, što bi povećalo bezbednost ne samo vrata, već i celog objekta. Na taj način se otvara mogućnost razvoja sistema za sigurnost stambenih prostora.

7. LITERATURA

- [1] <https://randomnerdtutorials.com/getting-started-with-esp32/> (pristupljeno u oktobru 2025.)
- [2] <https://www.componentsinfo.com/hc-sr501-module-pinout-datasheet/> (pristupljeno u oktobru 2025.)
- [3] <https://www.az-delivery.de/en/products/0-96zolldisplay> (pristupljeno u oktobru 2025.)
- [4] <https://lastminuteengineers.com/arduino-keypad-tutorial/> (pristupljeno u oktobru 2025.)
- [5] <https://learn.adafruit.com/adafruit-optical-fingerprint-sensor> (pristupljeno u oktobru 2025.)
- [6] https://wiki.dfrobot.com/SKU_SEN0539-EN_Gravity_Voice_Recognition_Module_I2C_UART_target_0 (pristupljeno u oktobru 2025.)

Kratka biografija:



Miljana Stefanov rođena je u Vršcu 2000. god. Master rad na Fakultetu tehničkih nauka iz oblasti Primenjena elektronika odbranila je 2025.god.
Kontakt: miljana.s2609@gmail.com