Otvoreni okvir za upravljanje korisničkim računima u Oracle DBMS

Nikšić, Goran

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Goran Nikšić

OTVORENI OKVIR ZA UPRAVLJANJE KORISNIČKIM RAČUNIMA U ORACLE DBMS

ZAVRŠNI SPECIJALISTIČKI RAD

Varaždin, 2024.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Goran Nikšić

Matični broj: 0016024549

Studij: specijalistički poslijediplomski studij Upravljanje sigurnošću i revizija IS-a

OTVORENI OKVIR ZA UPRAVLJANJE KORISNIČKIM RAČUNIMA U ORACLE DBMS

ZAVRŠNI SPECIJALISTIČKI RAD

Mentori:

doc. dr.sc. Igor Tomičić

prof. dr.sc. Miroslav Bača

Varaždin, ožujak 2024.

PODACI O SPECIJALISTIČKOM ZAVRŠNOM RADU

I. AUTOR

Ime i prezime	Goran Nikšić
Datum i mjesto rođenja	13.05.1982.
Naziv fakulteta i datum diplomiranja	Fakultet organizacije i informatike, 16.04.2024.
Sadašnje zaposlene	Časnik Oružanih snaga Republike Hrvatske

II. ZAVRŠNI RAD

Naslov	Upravljanje korisničkim računima u Oracle DBMS
Broj stranica, slika, tabela, priloga, bibliografskih podataka	broj stranica: 88, broj slika: 4, broj tabela: 3, broj bibliografskih podataka: 35
Znanstveno područje, smjer i disciplina iz koje je postignut akademski stupanj	Informacijske znanosti, Upravljanje sigurnošću i revizija informacijskih sustava
Mentor i voditelj rada	doc. dr. sc. Igor Tomičić
Fakultet na kojem je rad obranjen	Fakultet organizacije informatike
Oznaka i redni broj rada	USIRIS-20

III. OCJENA I OBRANA

Datum prihvaćanja teme od Fakultetskog vijeća	19.10.2023.
Datum predaje rada	08.02.2024.
Datum sjednice FV-a na kojoj je prihvaćena pozitivna ocjena rada	21.03.2024.
Sastav Povjerenstva koje je rad ocijenilo	1. Prof. dr. sc. Ivan Magdalenić, predsjednik 2. Doc. dr. sc. Igor Tomičić, mentor i član 3. Izv. prof. dr. sc. Zlatko Stapić, član
Datum obrane	16.04.2024.
Sastav Povjerenstva pred kojim je rad obranjen	1. Prof. dr. sc. Ivan Magdalenić, predsjednik 2. Doc. dr. sc. Igor Tomičić, mentor i član 3. Izv. prof. dr. sc. Zlatko Stapić, član
Datum promocije	

Hvala mojoj obitelji, Ivani, Irini i Franku.

Goran Nikšić

Izjava o izvornosti

Izjavljujem da je moj završni specijalistički rad izvorni rezultat mojeg rada te da se u izradi istoga nisam koristio drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada su korištene etički prikladne i prihvatljive metode i tehnike rada.

Potpis autora

Sažetak

U ovom radu predstavljen je otvoreni okvir za upravljanje korisničkim računima u kontekstu relacijske baze podataka. Istraživanje je bilo usmjereno na izradi i primjeni predmetnog okvira s ciljem omogućavanja precizne kontrole nad korisničkim pristupom i ovlastima. Istaknuti su ključni izazovi u očuvanju integriteta, povjerljivosti i dostupnosti podataka poznatih kao CIA trokut.

Predmet istraživanja bio je predstaviti ključne trendove u području kontrole pristupa podacima te predstaviti prilagodljivi okvir za upravljanje korisničkim računima. Istraživanje obuhvaća modele kontrole pristupa podacima i razvoj predmetnog okvira, a kroz studiju slučaja ističe se njegova primjena unutar vojne organizacije.

Rad se sastoji od teorijskog pregleda, analize postojećih modela kontrole pristupa podacima, razvoja prilagodljivog okvira i njegove primjene unutar Oracle DBMS uz integraciju sa studijom slučaja unutar vojne organizacije. Očekivani rezultati ovog rada su doprinos unapređenju kontrole pristupa podacima i korisničkih računa.

Ključne riječi: Kontrola pristupa podacima, korisnički računi, baza podataka, CIA trokut, modeli kontrole, podaci

Sadržaj

1. Uvod

Danas, u uvjetima brzih tehnoloških promjena i ovisnosti o informacijsko-komunikacijskim tehnologijama, upravljanje korisničkim računima i pravima pristupa podacima jedno je od ključnih pitanja u postizanju ravnoteže između tri ključna načela sigurnosti – povjerljivosti, integriteta i dostupnosti (CIA trokut).

Poznavanje važnosti CIA trokuta kao temelja sigurnosti podataka od izuzetne je važnosti za svaku organizaciju koja nastoji očuvati povjerljivost, integritet i dostupnost podataka. U tom kontekstu, ovaj rad istražuje razvoj i implementaciju otvorenog okvira za upravljanje korisničkim računima usmjerenog na postizanje i održavanje dva načela CIA trokuta – očuvanja povjerljivosti i integriteta podataka.

Kroz analizu literature, razvoj metodologije i studiju slučaja, rad se bavi pitanjima vezanim uz kontrolu prava pristupa i očuvanja integriteta podataka pružajući uvid u složenost upravljanja korisničkim računima. Razmatranje rezultata implementacije otvorenog okvira unutar studije slučaja pruža uvid u njegovu učinkovitost i potencijal za primjenu. Ovaj rad bavi se različitim čimbenicima upravljanja korisničkim računima uzimajući u obzir potrebu za skalabilnim, sigurnim i prilagodljivim rješenjima.

1.1 Predmet istraživanja

U suvremenom informacijskom okruženju pristup podacima i ovlasti u bazi podataka od iznimne su važnosti za organizacije. Nužnost zaštite podataka postavlja se kao veliki izazov pred organizacije. U tom kontekstu ključno je istražiti načine kako organizacije mogu odgovoriti na ovaj izazov posebice razmatrajući upravljanje korisničkim računima kao ključnu komponentu sigurnosnih strategija.

Kroz kontekst digitalne transformacije svijet se transformira pod utjecajem digitalnih inovacija, od automatizacije do umjetne inteligencije. Organizacije su suočene s potrebom prilagodbe i usklađivanja s tehnološkim trendovima, ali istovremeno moraju osigurati da transformacija ne ugrozi sigurnost podataka.

Upravljanje kontrolom pristupa podacima ključni je instrument organizacija pri ostvarivanju ravnoteže između sigurnosti i funkcionalnosti. Ovaj rad temelji se na analizi ključnih aspekata upravljanja korisničkim računima, modela zaštite podataka te razvoja otvorenog okvira za upravljanje korisničkim računima. Rad je orijentiran prema strategijama, procesima i tehnologijama koje omogućavaju učinkovito upravljanje korisničkim računima u organizaciji uz naglasak na autentifikaciji, autorizaciji i praćenju korisničkih aktivnosti radi povećanja razine sigurnosti podataka.

Uz analizu različitih modela zaštite podataka proučava se razvoj otvorenog okvira za upravljanje korisničkim računima s naglaskom na arhitekturi, funkcionalnostima i implementaciji. Ovaj pristup razvoju otvorenog okvira postavlja se kao skalabilno, fleksibilno i sigurno rješenje.

Uključivanjem studije slučaja koja prikazuje stvarnu implementaciju otvorenog okvira, istraživanje ilustrira konkretnu primjenu razvijenog rješenja u odabranoj organizaciji. Kroz studiju slučaja istraživanje daje uvid u konkretne izazove, rješenja i rezultate primjene otvorenog okvira. Kroz studiju slučaja povezan je teorijski pristup sa stvarnim praktičnim iskustvom.

1.2 Motivacija za istraživanje

Ovo istraživanje ima korijene u osobnom iskustvu u području razvoja informacijskih sustava te izazova povezanih s kontrolom i osiguravanjem prava pristupa podacima. Iskustva stečena tijekom godina rada jasno su utjecala na motivaciju i potrebu za provođenjem ovog istraživanja.

Ključni čimbenici za provedbu ovog istraživanja su:

- Dinamika suvremenog poslovnog okruženja
- Povećana složenost upravljanja kontrolom pristupa podacima
- Rastući zahtjevi za zaštitom podataka
- Potreba za standardizacijom procesa pri upravljanju kontrolom pristupa podacima

Upravljanje korisničkim računima i pravima pristupa podacima nosi sa sobom određene izazove. U ovom poglavlju istaknuti su najvažniji izazovi iz kojega proizlazi potreba za razvojem otvorenog okvira za upravljanje korisničkim računima. Neki od tih izazova su:

- Sigurnost podataka – Osiguravanje da pristup podacima bude siguran i zaštićen od neovlaštenog pristupa.
- Složenost organizacija – U današnjim organizacijama s velikim brojem korisnika i različitim potrebama upravljanje korisničkim računima postaje znatno složenije.
- Dinamičnost radne snage – Česte promjene radne snage uključujući nova zapošljavanja, otkaze i promocije kao i nova radna mjesta zahtijevaju brze i učinkovite procese administracije računa.
- Standardizacija procesa – Nedostatak standardiziranih procesa za upravljanje korisničkim ulogama, administraciju korisničkih prava i upravljanje revizijom može rezultirati povećanjem rizika.
- Revizija i praćenja prava pristupa – Potreba za uspostavom redovite revizije prava pristupa s ciljem smanjenja rizika od neovlaštenog pristupa podacima.

S obzirom na rastući broj korisnika, složenost zahtjeva za pravima pristupa kao i dinamične promjene u organizacijama, razvoj otvorenog okvira za upravljanje korisničkim računima postaje neizbježan korak prema unapređenju sigurnosti i učinkovitosti organizacijskih procesa.

U konačnici, razvoj ovakvog okvira odražava predanost organizacije unapređenju svojih praksi upravljanja korisničkim računima i pravima pristupa što rezultira jačom sigurnošću podataka, poboljšanom operativnom učinkovitošću te sposobnošću suočavanja s dinamičnim izazovima modernog poslovnog okruženja.

1.3 Ciljevi istraživanja

Cilj istraživanja je prepoznati ključne izazove i ograničenja postojećih modela kontrole pristupa podacima s fokusom na model temeljen na ulogama u relacijskoj bazi podataka. Provedena analiza istraživanja u posljednjih pet godina pruža uvid u trenutačna stanja, trendove i nedostatke u kontroli pristupa podacima postavljajući temelj za razvoj proširenog modela.

Cilj razvoja otvorenog okvira je odgovoriti na prepoznate izazove kroz sustav koji omogućuje standardizaciju procesa, jedinstvenu kontrolu pristupa, reviziju i praćenje prava pristupa te prilagodljivost promjenama unutar organizacije. Implementacijom otvorenog okvira organizacijama se otvara mogućnost za sljedeće:

- Povećanje sigurnosti – Standardizirani procesi omogućuju dosljednu primjenu sigurnosnih politika smanjujući rizik od neovlaštenog pristupa podacima.
- Učinkovito upravljanje promjenama – Dinamičnost radne snage zahtijeva brze i precizne procese dodjele i povlačenja prava pristupa.
- Osiguravanje dosljednosti i transparentnosti – Standardizacija procesa osigurava dosljednost u kreiranju korisničkih računa i dodjeli prava pristupa dok transparentnost omogućava praćenje aktivnosti i promjena.
- Prilagođavanje organizaciji – Otvoreni okvir omogućava organizacijama prilagodbu procesa upravljanja korisničkim računima prema organizacijskim i poslovnim potrebama.
- Automatizirati reviziju i praćenje - Otvoreni okvir podržava automatiziranu reviziju prava pristupa, čime olakšava otkrivanje i rješavanje bilo kakvih nesukladnosti ili sigurnosnih prijetnji.
- Prilagoditi se specifičnim potrebama organizacije - Otvoreni okvir omogućuje organizacijama prilagodbu procesa upravljanja korisničkim računima prema vlastitim specifičnim zahtjevima i poslovnim potrebama.

Jedan od ciljeva istraživanja je i prikaz proširenog modela kontrole pristupa podacima kroz studiju slučaja. Svrha studije slučaja je detaljno analizirati dizajn i implementaciju predmetnog modela pružajući dublje razumijevanje funkcionalnosti, prednosti i praktične primjene. Cilj je bolje razumjeti koje konkretne prednosti prošireni model donosi u odnosu na postojeće modele.

Konačni cilj ovog istraživanja je pružiti duboko razumijevanje dizajna i implementacije otvorenog okvira za upravljanje korisničkim računima. Ovaj cilj je usmjeren na stvaranje temeljitog uvida u

tehničke, funkcionalne i sigurnosne aspekte otvorenog okvira pružajući potpuno razumijevanje njegove primjenjivosti i prednosti u stvarnom okruženju.

Kroz postizanje ovih ciljeva istraživanje ima ambiciju doprinijeti razvoju naprednih metoda kontrole pristupa podacima u relacijskim bazama podataka.

1.4 Stručni i društveni doprinos

Stručni i društveni doprinos ovog rada očituje se u području kontrole prava pristupa podacima i upravljanja korisničkim računima. Kroz ovaj rad planirano je ostvarivanje doprinosa koji će obuhvatiti područje teorije i prakse.

U kontekstu stručnog doprinosa cilj ovog rada je proširiti trenutačno razumijevanje upravljanja korisničkim računima i modela kontrole pristupa podacima kroz analizu izazova i razvoj sveobuhvatnog pristupa upravljanju korisničkim računima. Stručni doprinos proizlazi iz prepoznavanja najboljih praksi, alata i strategija s ciljem podržavanja organizacije u učinkovitom upravljanju pravima pristupa podacima i osiguranju integriteta podataka. Stručni doprinos ostvaruje se kroz prepoznavanje ključnih čimbenika uspješnog upravljanja korisničkim računima čime se unapređuje praksa u području informacijske sigurnosti.

Uz stručni, rad ima i društveni doprinos. Implementacija održivog i sigurnog okvira može pridonijeti općoj informacijskoj sigurnosti. Društveni doprinos proizlazi iz razvoja alata i proširenja postojećih modela koji potiču odgovorno ponašanje s podacima što u konačnici dovodi do stvaranja povjerenja između organizacija i njihovih korisnika.

Osim toga, rad ima namjeru dodatnog obrazovanja i razvoja svijesti o važnosti informacijske sigurnosti. Kroz dostupnost rezultata istraživanja i prikaz implementacije razvijenog okvira planira se pridonijeti edukaciji osoblja povezanih s područjem informacijske sigurnosti.

Istraživanje prikazano u ovom radu teži pridonijeti raspravi u području informacijske sigurnosti pružajući nove perspektive, teorijski okvir i metodologije za daljnja istraživanja.

2. Definiranje osnovnih pojmova

U ovom poglavlju definirani su osnovni pojmovi važni za specijalistički rad. Dana je definicija informacijske sigurnosti kao krovne discipline i pojmovi pristup podacima, model kontrole pristupa podacima, autentifikacija, autorizacija, povjerljivost podataka i integritet podataka.

2.1 Pojam informacijske sigurnosti

Informacijska sigurnost, kao ključni aspekt u suvremenom informacijskom društvu, definira se kroz različite perspektive koje naglašavaju zaštitu podataka, privatnosti, integriteta i dostupnosti informacija.

„Informacijska sigurnost je stanje povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom potporom za poslove planiranja, provedbe, provjere i dorade mjera i standarda.“ [1]

Tako Europsko vijeće [2] definira informacijsku sigurnost kao povjerenje da će takvi sustavi štititi podatke koje obrađuju i da će funkcionirati onako kako trebaju, kada trebaju i uz kontrolu zakonitih korisnika. Učinkovitom informacijskom sigurnošću moraju se osigurati odgovarajuće razine tajnosti, cjelovitosti, dostupnosti, nepobitnosti i autentičnosti.

Prema Zakonu o informacijskoj sigurnosti, informacijska sigurnost ima sljedeće značenje:
„Informacijska sigurnost je stanje povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda.“ [3]

Tako prema američkom Nacionalnom institutu za standarde i tehnologije (NIST), informacijsku sigurnost definiramo kao zaštitu informacija i informacijskih sustava od neovlaštenog pristupa, korištenja, otkrivanja, prekida, modifikacije ili uništenja kako bi se osigurao integritet, povjerljivost i dostupnost [4].

2.2 Pojam pristupa podacima

Pristup podacima odnosi se na mogućnost dohvaćanja i korištenja podataka pohranjenih u bazi podataka ili drugom sustavu za pohranu. Obuhvaća niz aktivnosti uključujući dohvaćanje podataka, upravljanje, analizu i zaštitu. Cilj pristupa podacima je pružiti pojedincima i organizacijama mogućnost pristupa ili dohvaćanja podataka pohranjenih unutar repozitorija kako bi ih korisnici mogli dohvatiti, premjestiti ili manipulirati njima u širokom rasponu slučajeva upotrebe.

U praksi pristup podacima može uključivati niz tehnologija, alata i procesa. Prema opće prihvaćenoj definiciji pristup podacima može uključivati korištenje sustava za upravljanje bazom podataka za pohranjivanje i dohvaćanje podataka, implementaciju mjera sigurnosti podataka za zaštitu od neovlaštenog pristupa i korištenje alata za analizu podataka za vizualizaciju, obradu i otključavanje uvida [5].

2.3 Pojam modela kontrole pristupa podacima

Model za kontrolu pristupa podacima je sustav ili okvir u kojemu su definirana pravila i mehanizmi za upravljanjem pristupom korisnika ili entiteta određenim podacima ili resursima. Model omogućava organizacijama da postave granice i odrede tko, kako i u kojim uvjetima može pristupiti određenim podacima. Osnovna svrha modela za kontrolu pristupa podacima je zaštita povjerljivosti, integriteta i dostupnost podataka. Primjenom određenog modela osigurava se sigurnost podataka i umanjuje rizik neovlaštenog pristupa ili zlouporabe.

2.4 Pojam autentifikacije i autorizacije

Kao osnovnu definiciju autentifikacije i autorizacije možemo se poslužiti sljedećom tvrdnjom:
„Autentifikacija je proces kojim se utvrđuje korisnikov identitet, dok se autorizacijom utvrđuju dozvoljene radnje korisnika (obično se dodjeljuju uloge koje imaju dozvole).“ [6]
Iako postoje brojne definicije navedenih pojmova, u daljnjem tekstu poslužiti ćemo se definicijama NIST-a:

- „Autentifikacija je provjera identiteta korisnika, procesa ili uređaja, često kao preduvjet za omogućavanje pristupa resursima u informacijskom sustavu.“ [7]
- „Autorizacija je proces provjere da je tražena radnja ili usluga odobrena za određeni entitet.“ [8]

2.5 Pojam povjerljivosti i integriteta podataka

Prema NIST-u povjerljivost podataka je definirana kao svojstvo da podaci ili informacije nisu dostupni ili otkriveni neovlaštenim osobama ili procesima [9].

Prema NIST-u definicija integriteta podataka glasi:
„Integritet (cjelovitost) podataka odnosi se na to jesu li podaci promijenjeni između dva vremena (npr. između vremena kada su podaci stvoreni, pohranjeni i/ili poslani i vremena kada su podaci dohvaćeni i/ili primljeni).“ [10]

3. Teorijski okvir

U modernom informacijskom dobu, u uvjetima neprestanog generiranja, dijeljenja i pohrane podataka, sigurnost je ključni prioritet za organizacije svih veličina i domena [11]. Jedna od temeljnih sastavnica sigurnosti podataka je kontrola pristupa, sustav koji omogućuje upravljanje tko može pristupiti određenim resursima i na koji način.

U ovom poglavlju prikazan je teorijski okvir za kontrolu pristupa kroz osnovne koncepte, standarde i trendove koji oblikuju ovu sastavnicu informacijske sigurnosti dok je pregled modela kontrole pristupa dan u 4. poglavlju ovog rada.

Kontrola pristupa uključuje niz mehanizama i pristupnih politika oblikovanih s ciljem osiguravanja da samo ovlaštene osobe ili sustavi mogu pristupiti određenim podacima ili resursima. Predmetni mehanizmi uključuju autentifikaciju, proces koji potvrđuje identitet korisnika ili sustava te autorizaciju, proces koji određuje koja prava pristupa korisnik ili sustav ima nakon što je autentificiran.

Pored modela kontrole pristupa važno je spomenuti i niz standarda i regulativa vezanih uz kontrolu pristupa podacima poput ISO 27001, GDPR i drugih. Navedene regulative postavljaju smjernice za upravljanje pristupom podacima kako bi se osigurala usklađenost i zaštita privatnosti.

Svrha ovog poglavlja je omogućiti čitatelju da stekne cjelovitu sliku kompleksnih izazova i rješenja u upravljanju pravima pristupa kao i da postavi scenu za vlastito istraživanje i doprinos ovom ključnom području informacijske sigurnosti.

3.1 Povijesna okosnica

Povijesna okosnica pruža uvid u evoluciju računalne sigurnosti kroz vrijeme. Kroz povijesnu okosnicu prikazane su ključne točke u razvoju sigurnosti računalnih sustava, razvoju sigurnosnih modela, napretku tehnologije, regulativnim okvirima te naprednim tehnikama autentifikacije. Razumijevanje povijesnih aspekata pomaže nam pri razumijevanju konteksta u kojem su se razvijale tehnike upravljanja pravima pristupa i kako su se iste prilagođavale promjenama u tehnologiji i regulatornom okruženju. Kao ključne točke u razvoju sigurnosti možemo istaknuti:

- **Rani razvoj sigurnosti računalnih sustava** – Počeci razvoja sigurnosti računalnih sustava vezani su uz pojavu prvih računalnih sustava. U to vrijeme osnovni koncepti sigurnosti bili su usmjereni na fizičku kontrolu pristupa računalima i osnovne kontrole pristupa. Ovi sustavi nisu imali složene mehanizme autentifikacije i autorizacije kakve danas poznajemo, ali su postavili temelje za razvoj modernih sigurnosnih praksi i standarda.
- **Razvoj modela za kontrolu pristupa podacima** – Tijekom vremena došlo je do razvoja različitih modela s ciljem poboljšanja kontrole pristupa i zaštite podataka. Diskrecijski i mandatorni model postavili su temelje za modernu kontrolu pristupa podacima.
- **Napredak tehnologije** – Razvoj tehnologije, posebice interneta i mobilnih uređaja promijenio je način na koji koristimo računalne sustave i pristupamo podacima. Distribuirani sustavi, cloud tehnologija i široki spektar softverskih rješenja postavili su nove izazove za sigurnost podataka potičući razvoj naprednih tehnika upravljanja pravima pristupa kako bi se osigurala zaštita osjetljivih podataka.
- **Regulatorni okviri** – Uvođenje regulatornih okvira poput Opće uredbe o zaštiti podataka (GDPR) u Europi ili Health Insurance Portability and Accountability Act (HIPAA) u SAD-u postavilo je stroge zahtjeve za sigurno upravljanje pravima pristupa podacima i zaštitu privatnosti korisnika. Uvođenjem ovih okvira organizacije su potaknute da pažljivije razmatraju vlastite prakse u upravljanju pravima pristupa podacima i osiguraju usklađenost s regulatornim zahtjevima.
- **Napredne tehnike autentifikacije** – Razvoj biometrijskih tehnologija kao što su prepoznavanje otisaka prstiju, prepoznavanje lica i skeniranje rožnice omogućio je naprednije metode autentifikacije korisnika. Uz navedeno, implementacija dvofaktorske autentifikacije i korištenje pametnih kartica odnosno tokena dodatno su poboljšali sigurnost autentifikacijskih procesa. Navedene tehnike omogućavaju organizacijama

osiguravanje pouzdane identifikacije korisnika i sprječavanje neovlaštenog pristupa sustavima i podacima.

3.2 Osnovni koncepti kontrole pristupa

Osnovni koncept kontrole pristupa podrazumijeva definiranje pravila i mehanizama kojima se određuje tko ima pravo određenim resursima kao što su podaci, datoteke, mrežni resursi ili informacijski sustavi. Kontrola pristupa osigurava da samo ovlaštene osobe ili entiteti mogu pristupiti određenim podacima ili resursima dok se neovlašteni pristup sprječava ili ograničava.

Kontrola pristupa obično uključuje sljedeće sastavnice:

- **Identifikacija i autentifikacija** – Proces koji potvrđuje identitet korisnika ili entiteta koji pokušava pristupiti sustavu ili resursima. Identifikacija je proces prepoznavanja korisničkog identiteta dok je autentifikacija proces provjere je li identitet korisnika valjan.
- **Autorizacija** – Proces dodjele prava pristupa nakon što je korisnik uspješno autentificiran. Autorizacija određuje što ovlašteni korisnici mogu raditi unutar sustava ili s određenim resursima kao što su čitanje, pisanje, izmjena ili brisanje podataka.
- **Provjera pristupa** – Proces provjere prava pristupa tijekom korištenja sustava ili resursa. Ova provjera osigurava da se prava pristupa dinamički prilagođavaju promjenama u okolini ili zahtjevima korisnika.
- **Nadzor i praćenje** – Zapisivanje i praćenje svih aktivnosti vezanih uz pristup resursima ili izvođenje radnji unutar sustava. Ova sastavnica omogućava reviziju aktivnosti, prepoznavanje neovlaštenih pokušaja pristupa te osigurava usklađenost s regulativama i sigurnosnim standardima.
- **Politike sigurnosti** – Skup pravila, postupaka i smjernica kojima je definiran način upravljanja pravima pristupa, identifikacije, autentifikacije i autorizacije unutar organizacije ili informacijskog sustava. Politike sigurnosti mogu se temeljiti na regulatornim zahtjevima, poslovnim potrebama ili sigurnosnim standardima.

Kontrola pristupa ima ključnu ulogu u zaštiti informacijskih resursa od neovlaštenog pristupa, manipulacije ili krađe te osigurava integritet, povjerljivost i dostupnost podataka u organizaciji ili sustavu.

3.3 Autentifikacija i autorizacija

U suvremenim informacijskim sustavima, autentifikacija i autorizacija ključni su koncepti koji osiguravaju sigurnost informacija i pristup resursima. Proces autentifikacije odnosno potvrde identiteta vrši se kroz različite metode poput zaporki, biometrije ili dvofaktorske autentifikacije s ciljem osiguravanja da samo ovlašteni korisnici dobiju pristup.

Nakon autentifikacije, autorizacija određuje što ovlašteni korisnik smije raditi unutar sustava. Autorizacija se temelji na unaprijed postavljenim pravilima i politikama. Autorizacija definira dopuštene radnje, resurse ili podatke na koje korisnik ima pravo pristupa na temelju njegove uloge ili dodijeljenih prava.

Iako autentifikacije i autorizacije imaju različite svrhe, procesi su međusobno povezani i često se provode zajedno. Autentifikacija osigurava identitet korisnika dok autorizacija definira što taj identitet može učiniti nakon što je potvrđen. U suvremenim informacijskim sustavima procesi autentifikacije i autorizacije igraju ključnu ulogu u sigurnosti podataka. Primjena naprednih tehnika osigurava najviše sigurnosne standarde u digitalnom okruženju.

S obzirom na temu rada i predstavljeni studiju slučaja, važno je spomenuti i upravljanje korisničkim računima u kontekstu Oracle DBMS. U Oracle DBMS postoji nekoliko razina autentifikacije i autorizacije koje omogućuju organizacijama fleksibilnost i prilagodbu sigurnosnim potrebama. Ovaj rad prvenstveno je usmjeren na lokalnu autentifikaciju i autorizaciju.

U ovom poglavlju razmotrene su razine autentifikacije i autorizacije dostupne u Oracle DBMS :

1. **Lokalna autentifikacija i autorizacija:**
   - *Lokalna autentifikacija:* Na ovoj razini autentifikacije korisnički identitet i pristupni podaci (npr. zaporke) pohranjuju se i upravljaju unutar samog Oracle DBMS. Korisnici moraju koristiti te podatke kako bi se autentificirali i pristupili resursima unutar baze podataka.
   - *Lokalna autorizacija:* Lokalna autorizacija uključuje dodjelu privilegija i prava pristupa unutar Oracle DBMS. Administratori baze podataka određuju korisničke uloge i privilegije različitim resursima. Ova razina autorizacije oslanja se na upravljanje korisnicima i pravima unutar baze podataka.
2. **Centralizirana autentifikacija i lokalna autorizacija:**

- *Centralizirana autentifikacija:* U ovom scenariju autentifikacija se centralizira putem vanjske usluge, kao što je direktorij. Korisnici se autentificiraju izvan Oracle DBMS (npr. putem usluge direktorija) prije nego što dobiju pristup resursima unutar baze podataka.
- *Lokalna autorizacija:* Unutar baze podataka i dalje se upravlja autorizacijom odnosno dodjelom privilegija i prava pristupa.

3. **Centralizirana autentifikacija i autorizacija:**
   - *Centralizirana autentifikacija:* Korisnici se autentificiraju putem centralizirane usluge kao što je navedeno u prethodnom scenariju.
   - *Centralizirana autorizacija:* Autorizacija se također provodi putem vanjskog sustava. Ovaj scenarij omogućava potpunu centralizaciju upravljanja pravima pristupa i kontrolom nad korisnicima.

3.4 Upravljanje korisničkim računima

U kontekstu baze podataka upravljanje pravima pristupa ključna je sastavnica sigurnosti podataka uključujući i Oracle DBMS. Tako upravljanje korisničkim računima možemo shvatiti kao sustavni pristup stvaranju, konfiguriranju, praćenju i održavanju korisničkih računa. Ovaj proces uključuje definiranje identiteta korisnika, autentifikaciju, autorizaciju te dodjelu privilegija i prava korisnicima. Upravljanje korisničkim računima također obuhvaća zatvaranje ili deaktivaciju računa kada više nisu potrebni.

Svrha upravljanja korisničkim računima je mnogostruka i ima ključnu ulogu u sigurnosti i integritetu podataka unutar Oracle DBMS-a. Upravljanje korisničkim računima možemo podijeliti na:

- **Osiguravanje sigurnosti podataka** – Upravljanje korisničkim računima može osigurati da samo ovlašteni korisnici imaju pristup podacima, čime se sprječava neovlašteni pristup i zloupotreba podataka.
- **Precizna kontrola prava i privilegija korisnika** – Kroz upravljanje korisničkim računima, administratori mogu precizno definirati što svaki korisnik može raditi unutar baze podataka, čime se primjenjuje princip „najmanjih privilegija“ i smanjuje rizik od zloupotrebe.
- **Praćenje aktivnosti korisnika** – Upravljanje korisničkim računima omogućava praćenje pristupa, izmjena i ostalih aktivnosti nad podacima što je od suštinskog značaja za forenzičku analizu i otkrivanje sigurnosnih incidenata.

- **Administracijsku učinkovitost** – Upravljanje korisničkim računima pojednostavljuje administriranje računa kao što su dodjela i ukidanje prava, brisanje neaktivnih korisničkih računa te praćenje promjena.
- **Usklađivanje sa standardima i regulativama** – Upravljanje korisničkim računima pomaže organizacijama pri usklađivanju sa specifičnim sigurnosnim standardima i regulativama koje se primjenjuju na njihovu industriju.

Svrha upravljanja korisničkim računima, izuzev osiguravanja kontrole pristupa, očituje se i u održavanju integriteta, dostupnosti i povjerljivosti podataka unutar baze podataka. Upravljanje korisničkim računima čini temeljnu komponentu sigurnosne politike i prakse za organizacije koje koriste Oracle DBMS.

3.5 Politike sigurnosti

Politike sigurnosti definiraju smjernice, pravila i procedure koje organizacija provodi kako bi zaštitila svoje podatke, resurse i sustave od različitih prijetnji. Razvoj, primjena i provedba politika sigurnosti ključni su koraci u osiguravanju integriteta, povjerljivosti i dostupnosti podataka. Kao ključne elemente politika sigurnosti možemo navesti:

- **Ciljevi sigurnosti** – Politike sigurnosti trebaju jasno odražavati ciljeve organizacije u vezi s informacijskom sigurnošću. To može biti zaštita osjetljivih podataka, sprječavanje neovlaštenog pristupa sustavu ili osiguravanje kontinuiteta poslovanja u slučaju incidenta.
- **Odgovornosti i ovlasti** - Politike sigurnosti trebaju jasno odrediti odgovornosti i ovlasti svih dionika unutar organizacije u vezi s implementacijom i provedbom sigurnosnih mjera. To uključuje upravljanje sigurnošću, IT osoblje, menadžment i sve ostale korisnike sustava.
- **Proceduralne smjernice** – Politike sigurnosti trebaju sadržavati detaljne proceduralne smjernice o sigurnosnim postupcima i praksama koje treba slijediti unutar organizacije. To može uključivati postupke autentifikacije, upravljanje zaporkama, pravila pristupa, postupke zaštite podataka i sl.
- **Standardi i regulative** – Politike sigurnosti trebaju biti usklađene s relevantnim standardima i regulativama u industriji i/ili zakonodavstvu. To uključuje GDPR, HIPAA,

ISO 27001 kao i druge standarde i regulative vezane uz zaštitu privatnosti i sigurnost podataka.

- **Obuka i osvještavanje** – Politike sigurnosti trebaju sadržavati smjernice o obuci i osvještavanju zaposlenika o sigurnosnim praksama i politikama organizacije. Obuka bi trebala biti redovita i prilagođena sudionicima s ciljem osiguravanja sposobnosti prepoznavanja i sprječavanja sigurnosnih prijetnji.
- **Praćenje i revizija** – Politike sigurnosti trebaju uključivati mehanizme za praćenje, reviziju i poboljšanje sigurnosnih postupaka. To uključuje redovito praćenje sigurnosnih događaja, provođenje revizije sigurnosnih postupaka i mjera te reagiranje na incidente i prijetnje.
- **Kontinuirano poboljšanje** – Politike sigurnosti trebaju promicati kulturu kontinuiranog poboljšanja sigurnosnih praksi i mjera. Svaka organizacija bi trebala redovito vršiti reviziju i unaprjeđivati vlastite politike sigurnosti s ciljem uspješnog odgovora na novonastale prijetnje i izazove u području informacijske sigurnosti.

3.6 Primjeri primjene sigurnosnih koncepata

Primjeri primjene sigurnosnih koncepata pružaju praktične ilustracije kako teorijski koncepti sigurnosti mogu biti primijenjeni u stvarnom svijetu što doprinosi razumijevanju njihove važnosti i učinkovitosti u zaštiti informacijskih sustava. Integracija poglavlja o primjerima primjene sigurnosnih koncepata unutar teorijskog okvira dodatno obogaćuje razumijevanje čitatelja o konkretnim primjenama teorijskih koncepata sigurnosti.

U daljnjem tekstu navedeno je nekoliko primjera primjene sigurnosnih koncepata:

- **Višefaktorska autentifikacija (MFA)** – Implementacijom višefaktorskih autentifikacija za pristup korisničkom računu osigurava se da korisnik mora pružiti nekoliko dokaza identiteta poput zaporke i jednokratnog koda poslanog na korisnikov mobilni uređaj kako bi se prijavio u sustav. Primjenom višefaktorskih autentifikacija povećava se razina sigurnosti pristupa i sprječava neovlašteni pristup čak i u slučaju kompromitirane zaporke.
- **Enkripcija podataka** – Enkripcija podataka koristi se za zaštitu osjetljivih podataka tijekom prijenosa i pohrane. Primjerice, korištenjem SSL/TLS enkripcije prilikom prijenosa podataka putem interneta i AES enkripcija za pohranu osjetljivih podataka u bazi podataka. Enkripcija podataka u bazi podataka sprječava neovlašteni pristup podacima u slučaju kompromitacije fizičkog medija na kojemu se nalazi baza podataka.
- **Politike pristupa temeljene na ulogama (RBAC)** – Implementacijom RBAC modela na temelju uloga korisnika („administrator“, „zaposlenik“, „gost“) određuje se koja uloga ima pristup određenom resursu. Primjerice, samo uloga „administrator“ ima pristup administracijskom sučelju sustava.
- **Nadzor i upravljanje događajima (SIEM)** – SIEM sustav prikuplja, analizira i izvještava o sigurnosnim događajima unutar sustava kao što su pokušaji neuspješnih prijava, sumnjive aktivnosti ili pokušaji neovlaštenog pristupa. Implementacija SIEM sustava omogućava brzo otkrivanje i reakciju na sigurnosne prijetnje.
- **Pravilna konfiguracija sigurnosnih postavki** – Redovitom provjerom i ažuriranjem sigurnosnih postavki svojih sustava organizacija osigurava usklađenost s najnovijim sigurnosnim standardima i najboljim praksama. To uključuje konfiguraciju vatrozida, antivirusne zaštite, politika vezanih uz zaporke i drugih sigurnosnih postavki prema potrebi.

4. Analiza modela za kontrolu pristupa podacima

U svijetu rastuće digitalizacije i kompleksnih informacijskih sustava, sigurnost i upravljanje korisničkim pristupima odnosno pravima postala su kritična pitanja. Pouzdanost i sigurnost baze podataka smatraju se temeljem informatičke infrastrukture organizacija. Kontrola pristupa, uključujući autentifikaciju i autorizaciju korisnika, ključna je komponenta u očuvanju integriteta i povjerljivosti podataka.

U ovom poglavlju provedena je analiza postojećih rješenja za kontrolu prava pristupa podacima. To uključuje istraživanje modela kontrole pristupa kroz sigurnosne značajke i pravila pristupa.

Svrha ove analize je ostvariti nekoliko ključnih ciljeva. Prvo, omogućeno je razumijevanje različitih modela kontrole pristupa podacima. Drugo, prepoznati su prednosti i nedostaci prisutni u postojećim modelima. Treće, kroz inicijalno predstavljanje otvorenog okvira jasno su određeni dodatna vrijednost i novosti koje ovaj rad donosi.

Analiza postojećih rješenja ključan je korak prema razvoju otvorenog okvira za upravljanje korisničkim računima koje će u jednom dijelu nadmašiti dostupne dosadašnje pristupe. U svijetu brzih tehnoloških promjena i sofisticiranih prijetnji, razumijevanje i optimizacija kontrole pristupa postaje imperativ za organizacije koje žele očuvati sigurnost i povjerljivost podataka.

Ovo poglavlje stvara temelj na kojem se mogu izgraditi novi pristupi upravljanju korisničkim računima te postavlja kontekst za vlastitu istraživačku inicijativu i doprinos ovom području.

4.1 Pregled modela kontrole pristupa

Kako organizacije sve više ovise o svojim informacijskim sustavima, pitanje tko ima pristup podacima postaje od suštinskog značaja. Modeli kontrole pristupa postaju središnji alat za upravljanje ovim pitanjima i osiguravaju da prava osoba u pravo vrijeme dobiva pristup pravim podacima.

U analizi kontrole pristupa podacima susrećemo se s raznovrsnim modelima i pristupima koji se primjenjuju kako bi se osiguralo da samo ovlašteni korisnici dobiju pristup podacima. Ovi modeli se razlikuju u svom pristupu, od tradicionalnih modela do naprednih strategija koje uključuju atribute i dinamičke pristupne politike.

Analiza modela kontrole pristupa omogućiti će temeljit uvid u različite strategije upravljanja pristupom. To uključuje tradicionalne pristupe, pristupe temeljene na ulogama te naprednije modele koji se oslanjaju na atribute.

Kontrola pristupa temeljena na identitetu

Najstariji model kontrole pristupa. Predstavljen je 1969. godine. IBAC [12] se predstavlja matricom kontrole pristupa. Redci matrice pripadaju korisnicima, dok se stupci odnose na objekte. Ćelija (i, j) specificira prava pristupa korisnika i način pristupa objektu j. Pravo pristupa može biti vlasništvo, čitanje, pisanje, izvođenje i slično. Dva modela kontrole pristupa povezana su s IBAC-om su liste kontrole pristupa i liste mogućnosti.

Prednosti:

- Jednostavnost i intuitivnost: IBAC olakšava dodjelu prava pristupa jer se temelji na identitetu korisnika (npr. e-mail adresi). Ovaj model može pojednostaviti administraciju korisničkih računa.
- Precizna kontrola: Model temeljen na identitetu korisnika omogućava preciznu kontrolu prava pristupa korisnika. Svaki korisnik može imati jedinstvene ovlasti.
- Lakša integracija: IBAC se lako integrira s drugim sustavima, kao što su sustavi za upravljanje identitetom (IAM).

Nedostaci:

- Povećan rizik od zlouporabe: Ako korisnikov identitet bude ugrožen (npr. krađa zaporke), to može rezultirati ozbiljnim sigurnosnim problemima.
- Kompleksnost u velikim organizacijama. U velikim organizacijama s mnogo korisnika i resursa, IBAC može postati složen za upravljanje jer svaki korisnik ima jedinstvene ovlasti.
- Održavanje identiteta: Zahtijeva točne informacije o identitetu korisnika, što može biti problem ako se korisnici često mijenjaju.
- Nedostatak kontrole nad atributima: IBAC se zasniva na kontroli identiteta, a ne na atributima korisnika. To može ograničiti kontrolu nad pravima pristupa na temelju drugih činitelja (npr. geografska lokacija, vrijeme, uređaj).

Višerazinske metode i srodni matematički modeli

Godine 1973., Bell i LaPadula [13] oblikovali su višerazinsku metodu pristupa u matematički model. Nazvana je višerazinska zbog više sigurnosnih razina pristupa podacima koji se zasniva na temelju razine odobrenja korisnika i sigurnosne razine pristupanom objektu. U tom modelu opisane su dva osnovna pravila. Pravilo jednostavne sigurnosti * - svojstvo (zvjezdana svojstva). Pravilo jednostavne sigurnosti označava da korisniku na određenoj razini odobrenja nije dopušteno da čita podatke iznad te razine. Zvjezdano svojstvo označava da korisnik ne može pisati u objektu koji je klasificiran ispod njegove razine odobrenja. Model Bell-LaPadula osigurava povjerljivost u sustav.

Biba matematički model objavljen je 1977. godine. U ovom modelu [14] pravilo jednostavne sigurnosti označava da je korisniku dopušteno čitanje podataka koje imaju višu sigurnosnu razinu od njegove razine odobrenja. Zvjezdano svojstvo navodi kako korisnik može pisati u objektu koji je klasificiran ispod njegove razini odobrenja. Važno je međusobno kombinirati ova dva modela kako bi se osigurali povjerljivost i integritet podataka.

Ovi modeli imaju svoje korijene u formalnim matematičkim teorijama i bili su predmetom pažljive analize i rasprave tijekom godina. Unatoč njihovoj povijesnoj važnosti u razumijevanju i primjeni, važno je napomenuti da će u ovom radu analiza prednosti i nedostataka biti izostavljena. Umjesto toga, fokus ovog rada biti će na drugim modelima i njihovoj primjenjivosti u suvremenim okruženjima. Ova odluka proizlazi iz potrebe za specifičnim usmjerenjem rada kao i iz činjenice da je analiza ovih modela već detaljno obrađena u brojnim drugim radovima i izvorima.

Mandatorna kontrola pristupa

Mandatorna kontrola pristupa (MAC) predstavljena je 1983. godine od strane Ministarstva obrane SAD-a [15]. Mandatorna kontrola pristupa [13] temelji se na Bell-LaPadula matematičkom modelu. Prema Carnet-u, MAC kontrola pristupa [16] je oblik kontrole pristupa kod kojeg operacijski sustav ograničava mogućnost subjekta u pristupanju i/ili obavljanju neke akcije nad objektima. U mandatornom modelu subjektima i objektima je dodijeljena skupina sigurnosnih oznaka odnosno klasifikacija te je pristup određenim resursima dozvoljen samo subjektima s dodijeljenom klasifikacijom. Mehanizam nadzora pristupa određenim objektima nameće operacijski sustav i/ili modul za sigurnost jezgre operacijskog sustava. Kad god korisnik ili program pokušaju pristupiti objektu, nameće se autorizacijsko pravilo u ovisnosti o klasifikaciji i odlučuje ima li subjekt pravo pristupa. U skladu s navedenim, svaka se operacija koju korisnik želi izvesti nad nekim objektom testira prema skupini autorizacijskih pravila odnosno sigurnosnoj politici kako bi se utvrdilo je li operacija dozvoljena ili nije.

MAC se koristi zajedno s diskrecijskom kontrolom pristupa (DAC) i primjenjuje se uglavnom u vojnim, vladinim i drugim organizacijama gdje je zaštita podataka ključna. Sigurnosne oznake dodjeljuju se korisnicima i objektima kako bi se uspostavila MAC politika.

Prednosti:

- Visoka razina sigurnosti: MAC pruža iznimno visoku razinu sigurnosti jer se temelji na strogo definiranim sigurnosnim politikama. To sprječava neovlašteni pristup osjetljivim informacijama, njihovo curenje kao i neovlaštene promjene. Ovaj model osigurava pristup podacima samo autoriziranim korisnicima što je ključno za očuvanje povjerljivosti informacija i minimiziranju rizika od sigurnosnih incidenata. Također omogućava bolju kontrolu nad unutarnjim prijetnjama jer čak i autorizirani korisnici ne mogu zaobići sigurnosne politike. Primjenom MAC modela osigurava se dosljedno provođenje sigurnosnih pravila što je od ključne važnosti u organizacijama s visokim sigurnosnim standardima.
- Primjena sigurnosnih politika: Primjena politika u ovom modelu odnosi se na dosljedno provođenje sigurnosnih politika i pravila na razini sustava. To znači da se korisnici i resursi ocjenjuju u skladu s postavljenim politikama, a pristup se dodjeljuje ili odbija sukladno tim pravilima. To osigurava strogo pridržavanje sigurnosnih standarda, smanjujući rizik od neovlaštenog pristupa i kršenja sigurnosnih pravila u organizaciji.

- Zaštita od unutarnjih prijetnji: Ovakva zaštita postiže se time što ni autorizirani korisnici ne mogu zaobići sigurnosne politike. To sprječava zlonamjerne aktivnosti unutar organizacije, umanjuje rizik od potencijalnih prijetnji iznutra te osigurava dosljednost sigurnosnih pravila i propisa.
- Odgovarajući za visoko sigurnosna okruženja: Prednost ovog modela leži u njegovoj sposobnosti apsolutne sigurnosti i stroge kontrole nad pristupom podacima. U takvim okruženjima MAC model osigurava da samo najmanji broj autoriziranih korisnika ima ovlasti za pristup i manipulaciju tim podacima. Ovo je ključno za očuvanje povjerljivosti i sigurnosti podataka te umanjenju rizika od curenja osjetljivih informacija. U okruženjima gdje su sigurnosni standardi vrlo visoki i gdje se bave visoko povjerljivim informacijama, MAC model se često smatra najprikladnijim i najučinkovitijim izborom za zaštitu podataka.

Nedostaci:

- Nedostatak fleksibilnosti: MAC model, iako pruža visoku razinu sigurnosti, često je ograničavajući faktor za korisnike. Ovisnost o administratorskim odlukama često može ometati produktivnost, posebice u okolinama gdje su promjene u pristupu česte ili gdje je potrebna brza prilagodba poslovnim potrebama.
- Složenost upravljanja: Upravljanje sigurnosnim politikama i klasifikacijom podataka u okviru MAC modela zahtijeva specijaliziranog osoblje i posebno znanje. Održavanje ovakvog sustava može biti vrlo izazovno, s visokim troškovima administracije. Ovo može rezultirati potrebom za dodatnim resursima, čime se povećavaju operativni troškovi organizacije.
- Niski komercijalni slučajevi: Kako je već navedeno, MAC se često primjenjuje u vladinim i vojnim organizacijama, ali ima ograničenu praktičnu primjenu u komercijalnim okruženjima. Kompleksnost i restriktivnost ovog modela često meta poslovnu agilnosti i prilagodbu visoko dinamičkim promjenama na tržištu. Većina tvrtki preferira druge modele zbog njihove prilagodljivosti.
- Nedostatak prilagodljivosti: MAC model nije prilagodljiv promjenama u zahtjevima organizacije ili okruženja. Model je često statičan i ne dopušta brze promjene u politikama pristupa i prilagodbu novim uvjetima. Ovo može predstavljati problem u brzo mijenjajućim industrijama ili okruženjima gdje su promjene poslovnih zahtjeva česte.

Diskrecijska kontrola pristupa

Diskrecijska kontrola pristupa (DAC) predstavljena je zajedno s MAC kontrolom [15]. Temeljna značajka diskrecijske kontrole pristupa je da vlasnik objekta može prenositi pristupna ovlaštenja za taj objekt po diskrecijskom načelu. Vrlo često vlasnik objekta je ujedno i njegov kreator. Pristup objektu s DAC-om regulira se ovisno o identitetu korisnika. DAC pristupne politike imaju najveću primjenu zbog svoje fleksibilnosti. Sam DAC nije dovoljan pri osiguravaju sigurnog sustava zbog čega je ovaj model kontrole pristupa podacima predstavljen zajedno s MAC kontrolom pristupa. Diskrecijska kontrola pristupa primjenjuje se u operativnim sustavima u kombinaciji s drugim modelima kontrole pristupa.

Prednosti:

- Fleksibilnost: DAC pruža iznimnu fleksibilnost jer omogućava vlasnicima resursa kontrolu nad pravima pristupa. To znači da vlasnici resursa mogu prilagoditi prava pristupa kako bi odgovorili na trenutačne zahtjeve. Ova fleksibilnost je ključna u okolinama gdje se zahtjevi često mijenjaju omogućujući brzu prilagodbu.
- Jednostavnost upravljanja: Upravljanje DAC modelom je jednostavno jer vlasnici resursa sami postavljaju i kontroliraju prava pristupa. Ovo smanjuje potrebu za centraliziranom administracijom i olakšava korisnicima samostalno upravljanje pravima pristupa što u konačnici rezultira smanjenim administracijskim opterećenjem.
- Osobni pristup: DAC osigurava da svaki korisnik ima pravo pristupa vlastitim podacima i resursima što je ključna stavka za produktivnost. Osim toga, DAC udovoljava individualnim potrebama, a korisnici mogu pristupiti svojim resursima bez ovisnosti o administratorima.

Nedostaci:

- Sigurnosni rizik: S obzirom na to da korisnici imaju kontrolu nad svojim pravima pristupa, postoji potencijalni rizik od pogrešaka u postavljanju ovlasti ili zlouporabe prava. To može dovesti do ozbiljnih sigurnosnih problema, uključujući neovlašteni pristup resursima i curenje osjetljivih podataka.
- Dosljednost: Nedostatak dosljedne primjene sigurnosnih politika je inherentan u DAC modelu jer ovisi o individualnim odlukama korisnika. Ovakav pristup može rezultirati neusklađenošću u primjeni sigurnosnih pravila i nepredvidivim pristupa resursima što može biti problem.

- Ograničenost: DAC model nije prikladan za okoline gdje je potrebna iznimno visoka razina sigurnosti, kao što su vojne i vladine organizacije koje čuvaju iznimno osjetljive informacije. Nedostatak strogih kontrola i centraliziranog nadzora što ga čini neprikladnim za takve zahtjeve.

Kontrola pristupa temeljena na ulogama

Obitelj modela kontrole pristupa temeljenog na ulogama (RBAC) predstavljena je 1996. godine [17]. RBAC se temelji na Bell-LaPadula matematičkom modelu [13]. Temeljna značajka ovog modela je da su dopuštenja dodijeljena ulogama, a odgovarajuće uloge su dodijeljene korisnicima.

Uloga je radna funkcija unutar neke organizacije. Primjerice korisniku na radnom mjestu „Računovođa“ dodijeljena je uloga „Računovođa“ u softverskom sustavu, a dopuštenja za radno mjesto „Računovođa“ su dodijeljena ulozi „Računovođa“. Rezultat primjene RBAC je pojednostavljeno upravljanje dopuštenjima. Politika RBAC-a je izražena kroz uloge.

Obitelj RBAC modela se sastoji od četiri komponente. Osnovni model je RBAC0. Napredni model, RBAC1, uključuje RBAC0, ali podržava hijerarhije uloga. Napredni model, RBAC2, uključuje RBAC0, ali s dodatnim ograničenjima. Konsolidirani model, RBAC3, uključuje RBAC1 i RBAC2. Osnovni RBAC model, RBAC0 sastoji se od skupa korisnika, skupa uloga i skupa dopuštenja. Korisnik može biti ljudsko biće, robot ili računalo. Uloga je poslovna funkcija u organizaciji. Dopuštenje je pravo pristupa. RBAC podržava značajke kao što su fleksibilnost, skalabilnost, kontrola tijeka rada i razdvajanje dužnosti. RBAC se najčešće koristi u poslovnom softveru. Ovaj model je najpopularniji zbog svoje fleksibilnosti i usmjerenosti na uloge.

Prednosti:

- Jednostavnost upravljanja: RBAC pristup pojednostavljuje upravljanje pravima pristupa jer se zasniva na definiranim ulogama i njihovim pravima. Administratori dodjeljuju korisnicima specifične uloge koje automatski definiraju njihove ovlasti. Ovo smanjuje složenost procesa upravljanja jer administratori ne moraju dodjeljivati pojedinačna prava svakom korisniku.
- Pojačana dosljednost i sigurnost: RBAC model pruža dosljednost u postavljanju prava pristupa. Svi korisnici s istom ulogom imaju identične ovlasti što umanjuje rizik od

ljudskih grešaka pri dodjeli prava. Dosljednost također doprinosi većoj sigurnosti sustava jer se smanjuje mogućnost zlouporabe prava pristupa.

- Osiguranje kontrole prava pristupa: RBAC model omogućava precizno definiranje ovlasti koje su potrebne za izvršavanje određenih zadataka. Ovo se odnosi na dodjelu specifičnih ovlasti potrebnih za korisnikovu radnu funkciju. Ovo osigurava da korisnici dobivaju samo ona prava koja su im potrebna za obavljanje svojih poslovnih zadataka, što također pomaže u smanjenju rizika od neovlaštenog pristupa.
- Skalabilnost: RBAC model je skalabilan i može se primijeniti u organizacijama različitih veličina. Bez obzira na veličinu organizacije, RBAC može pružiti adekvatnu razinu kontrole prava pristupa i jednostavnost upravljanja.

Nedostaci:

- Nedostatak prilagodljivosti: RBAC model može biti manje fleksibilan u usporedbi s drugim modelima kontrole prava pristupa, posebno u dinamičkim okruženjima gdje se zahtjevi često mijenjaju. Ažuriranje i prilagodba uloga mogu biti složeni procesi, a u slučajevima gdje su potrebne brze promjene, RBAC može biti ograničavajući.
- Složenost upravljanja ulogama: U organizacijama s velikim brojem uloga i korisnika, upravljanje i održavanje sustava RBAC može postati izazovno i zahtijevati posebne alate i procese. Administracija i praćenje velikog broja uloga i njihovih prava mogu zahtijevati dodatne resurse.
- Nedostatak kontrole na razini atributa: RBAC se temelji na ulogama, a ne na specifičnim atributima korisnika. To može ograničiti preciznost i kontrolu u situacijama gdje su potrebni dodatni atributi za donošenje odluka o pristupu. Primjerice, RBAC ne može lako razlikovati pristup resursima na temelju specifičnih kontekstualnih atributa kao što su vrijeme, lokacija ili karakteristike korisnika.

Kontrola pristupa temeljena na atributima

Kontrola pristupa temeljena na atributima (ABAC) [18] predstavljena je 2014. godine. Naziv samog modela dolazi od imenice „atribut“ koji je obilježje subjekta i objekta. Subjekt može biti ljudsko biće ili uređaj. Objekt može biti traženi resurs softverskog sustava. Politika u ABAC-u je pravilo koje određuje može li subjekt pristupiti objektu. Uvjeti okoline uključuju vrijeme, datum i mjesto korisnika. ABAC mehanizam kontrolira atribute, uvjete okoline i pristupne politike te donosi odluku o pristupu. ABAC mehanizam kontrole sastoji se od Policy Decision Point i Policy Enforcement Point komponenti. Primjeri atributa subjekta su ime, uloga i posao unutar organizacije. ABAC dozvoljava da subjekti i objekti koji još ne postoje u sustavu budu uključeni u pristupnu politiku. ABAC je skalabilan i fleksibilan model s mogućnošću određivanja preciznih politika. Primjenu ABAC-a je u poslovnom softveru i web servisima.

Prednosti:

- Precizna kontrola pristupa: ABAC model omogućava detaljnu kontrolu pristupa jer uzima u obzir različite atribute kao što su uloga korisnika, karakteristike resursa i kontekst. Ovakva preciznost omogućava organizacijama postizanje visoke razine pristupačnosti, omogućavajući samo potrebne i relevantne ovlasti što povećava sigurnost i smanjuje rizik od zlouporabe prava.
- Prilagodljivost: ABAC je izuzetno prilagodljiv model jer pristup može dinamički odgovoriti na promjene u atributima. To znači da organizacije mogu brzo reagirati na promjene u zahtjevima i poslovnom okruženju bez potrebe za složenim administrativnim procesima. Ovo je ključno u dinamičkim okolinama gdje se zahtjevi često mijenjaju.
- Integracija s vanjskim izvorima: ABAC omogućava integraciju s različitim vanjskim izvorima podataka i politika. To znači da organizacije mogu koristiti vanjske atribute kao što su podaci o vremenu, geolokaciji ili identitetu trećih strana kako bi unaprijedile proces donošenja odluka o pristupu. Ovo omogućava širu primjenu i kontekstualizaciju politika pristupa.

Nedostaci:

- Složenost upravljanja: Upravljanje ABAC modelom može biti složeno jer zahtijeva pažljivo definiranje i održavanje atributa, politika i pravila. Ovo može rezultirati povećanim troškovima administracije kao i potrebom za visoko stručnim osobljem koje je u stanju učinkovito implementirati i održavati kompleksnu infrastrukturu.
- Potreba za naprednim sustavima podrške: ABAC zahtijeva napredne informacijske sustave i alate za učinkovitu primjenu. Organizacije koje nemaju pristup takvim tehnološkim resursima mogu se suočiti s teškoćama u implementaciji ovog modela, uključujući financijske izazove i potrebu za stručnjacima koji razumiju ovu tehnologiju.
- Složenost donošenja odluke: ABAC model može biti izuzetno kompleksan u procesu donošenja odluke o pristupu podacima. Složene politike i različiti atributi prilikom donošenja odluke mogu rezultirati zastojem u procesu donošenja odluke. ABAC model zahtijeva pažljivo planiranje i implementaciju kako bi se osiguralo učinkovito donošenje odluka.

4.2 Otvoreni okvir u istraživanju upravljanja korisničkim računima

Upravljanje korisničkim računima u Oracle DBMS kritičan je aspekt sigurnosti i administracije baze podataka. Kako bi se poboljšala sigurnost, kontrola i učinkovitost, istraživački rad se fokusira na razvoj otvorenog okvira za upravljanje korisničkim računima. Ovo poglavlje pruža teorijski pregled otvorenog okvira, njegove svrhe i uloge u istraživanju upravljanja korisničkim računima u Oracle DBMS.

Definicija

Otvoreni okvir u kontekstu ovog istraživanja odnosi se na razvijeni i prilagodljivi sustav ili arhitekturu koji omogućava učinkovito upravljanje korisničkim računima unutar Oracle DBMS. Otvoreni okvir pruža strukturu i skup alata za provođenje autentifikacije i autorizacije na korisničkim računima. Glavno obilježje ovog okvira je njegova prilagodljivost i sposobnost prilagođavanja specifičnim sigurnosnim potrebama organizacije.

Svrha otvorenog okvira

Predloženi otvoreni okvir za upravljanje korisničkim računima predstavlja prošireno rješenje u odnosu na klasični RBAC model ugrađen u Oracle DBMS pružajući niz prednosti sa svrhom unapređenja i optimizacije procesa upravljanja korisničkim računima.

Glavna obilježja okvira su:

1. **Prilagodljivost i skalabilnost** – Otvoreni okvir omogućava prilagodbu pravila pristupa na temelju specifičnih potreba organizacije što rezultira većom prilagodljivošću samog sustava. Kroz sposobnost prilagodbe i proširivanja pravila pristupa s ciljem odgovora na povećanje broja korisnika ili promjene u organizaciji osigurava se skalabilnost sustava. Ovakav pristup osigurava da sustav može rasti i mijenjati se zajedno s organizacijskim potrebama. Programsko rješenje kao sastavnica otvorenog okvira omogućava jednostavniju administraciju korisničkih računa i korisničkih uloga u odnosu na generičko rješenje unutar Oracle DBMS sustava te precizniju kontrolu pristupa pojedinim sustavima unutar organizacije.

2. **Preciznija kontrola pristupa** – U odnosu na ugrađeni RBAC u Oracle DBMS, otvoreni okvir omogućava precizniju kontrolu pristupa putem dodatnih funkcionalnosti. To znači da organizacija može definirati pristup resursima s većom razinom detalja čime se povećava razina sigurnosti i osigurava da korisnici imaju samo ona prava koja su im uistinu i potrebna. Precizna kontrola pristupa može iskoristiti dodatna obilježja korisnika i/ili okoline kako bi dinamički odredila pristup određenom resursu. Neka od dodatnih obilježja su vremenska kontrola pristupa, lokacijska kontrola pristupa, identitet korisnika, karakteristike uređaja, stanje sustava i dinamička razina ovlasti zasnovana na kontekstu (radno vrijeme zaposlenika).
3. **Standardizacija i jednostavnost upravljanja** – Otvoreni okvir potiče standardizaciju procesa izrade korisničkih računa i dodjeljivanja uloga čime se smanjuje mogućnost ljudske pogreške i povećava administratorska učinkovitost. Centralizirano upravljanje korisničkim računima olakšava praćenje i reviziju prava pristupa. Grafičko sučelje kao sastavnica otvorenog okvira proces izrade korisničkih računa i dodjeljivanja uloga čini znatno jednostavnijim. Grafička reprezentacija podataka, intuitivnost pri korištenju, mogućnost vizualizacije podataka, smanjenje potrebe za učenjem sintakse i vizualna povratna informacija doprinosi jednostavnosti upravljanja.
4. **Praćenje i revizija** – Otvoreni okvir predviđa mogućnost implementacije praćenja korisničke aktivnosti ovisno o organizacijskim potrebama kao i reviziju prava pristupa. Ovakav proaktivni pristup doprinosi povećanju sigurnosti sustava omogućavajući brže prepoznavanje i odgovor na potencijalne prijetnje. Uz standardne mogućnosti praćenja aktivnosti korisnika kao što je prijavljivanje i odjavljivanje korisnika, korištenjem okidača na razini baze podataka i implementacijom dodatnih programskih modula na aplikacijskoj razini moguće je uspostaviti sustav praćenja pristupa osjetljivim podacima, praćenje promjena u konfiguraciji sustava (izmjena sigurnosnih politika) te praćenje vršenja periodičnih revizija

4.3 Odabir odgovarajućeg modela za kontrolu prava pristupa podacima

Odabir odgovarajućeg modela za kontrolu prava pristupa podacima ključan je korak u razvoju sigurnosnih politika i implementaciji sigurnosnih sustava. Različiti modeli pristupa nude različite prednosti i ograničenja, a odabir modela ovisi o nizu parametara. Ovo poglavlje istražuje ključne parametre i čimbenike koji trebaju biti razmotreni pri odabiru modela kontrole pristupa i kako ih povezati s konkretnim potrebama organizacije.

Odabir odgovarajućeg modela je proces koji zahtijeva pažljivo razmatranje kako bi se osiguralo da odabrani model podržava zaštitu podataka i dosljednost s poslovnim ciljevima i regulativama. U ovom poglavlju analiziraju se ključni parametri i čimbenici za odabir modela kontrole pristupa koji se temelje na autorovom profesionalnom iskustvu u implementaciji sigurnosnih politika.

Vrsta podataka i osjetljivost

Prva i osnovna razmatranja u odabiru modela za kontrolu prava pristupa su vrsta podataka i njihova osjetljivost. Treba razmotriti vrste podataka koji će se obraditi, poput osobnih, financijskih, zdravstvenih i drugih osjetljivih informacija. Temeljem navedenog, odabire se model koji najbolje štiti ove podatke.

Poslovne potrebe i fleksibilnost

Drugi ključni parametar je poslovna agilnost i potrebe organizacije. Potrebno je razmotriti koliko često se poslovni zahtjevi mijenjaju i koliko brzo je potrebno prilagoditi prava pristupa. Ovdje su razmatrana dva ključna modela kontrole prava pristupa podacima u relacijskoj bazi podataka, a to su Attribute-Based Acces Control (ABAC) i Role-Based Access Control (RBAC). ABAC omogućava detaljnu kontrolu pristupa temeljenu na atributima kao što su vlasništvo podataka, vrijeme i lokacija. S druge strane, RBAC pojednostavljuje upravljanje pravima grupiranjem korisnika u uloge. Pri odabiru modela potrebno je istražiti njihove prednosti, ograničenja i prilagodljivost u odnosu na specifične poslovne zahtjeve.

Sigurnosni standardi i regulative

Važno je razmotriti relevantne sigurnosne standarde i regulative koje organizacija mora zadovoljiti. Na primjer vojne organizacije mogu biti obavezne koristiti strože modele poput RBAC ili MAC, kako bi se uskladile sa specifičnim zahtjevima sigurnosti.

Broj korisnika i resursa

Veličina i kompleksnost sustava imaju veliku ulogu u odabiru modela. Velike organizacije s mnogo korisnika i resursa mogu zahtijevati skalabilan model, dok se manje organizacije mogu osloniti na jednostavnije modele.

Administrativni resursi

Troškovi upravljanja sigurnosnim modelima također su ključni parametar. Organizacija bi trebala prije odluke o implementaciji određenog modela razmotriti dostupne administrativne resurse i budžet za implementaciju i održavanje odabranog modela.

Složenost implementacije

Složenost implementacije modela prava pristupa može odstupati ovisno o veličini organizacije, složenosti njezinih operacija i razini automatizacije. U malim organizacijama s jasno definiranim procesima, implementacija može biti relativno jednostavna. No u velikim organizacijama ili organizacijama s visokom dinamikom promjena, implementacija i održavanje modela za kontrolu prava pristupa podacima može biti znatno složenije i zahtijevati specijalizirane alate i resurse kao i ljudske potencijale.

Revizija

Revizija pristupnih prava osigurava sigurnost, dosljednost i usklađenost u upravljanju pravima pristupa. Pomaže u otkrivanju neovlaštenih pristupa, sprječava sigurnosne prijetnje i osigurava usklađenost organizacije s internim pravilima i vanjskim regulativama. Uz navedeno, revizija doprinosi optimizaciji resursa i pravilnom upravljanju promjenama u organizaciji.

4.4 RBAC u Oracle DBMS: Upravljanje pristupom podacima i kontrola korisničkih računa

Kako se dio otvorenog okvira za upravljanje korisničkim računima temelji na RBAC modelu unutar Oracle DBMS-a, u ovom poglavlju prikazane su ključne funkcionalnosti predmetnog modela:

Funkcionalnost – RBAC model unutar Oracle DBMS pruća niz funkcionalnosti za upravljanje pravima pristupa podacima. Integracija ovog modela omogućava korištenje isprobanih mehanizama za administraciju korisničkih prava što čini temelj za pouzdan sustav upravljanja korisničkim računima.

Sigurnost podataka – Mogućnost implementacije naprednih sigurnosnih značajki pridonosi osiguravanju visoke razine sigurnosti podataka štiteći ih od neovlaštenog pristupa i manipulacije. Sigurnost podataka [19] pridonosi povjerenju u upravljanju korisničkim računima u otvorenom okviru kroz sljedeće aspekte:

- **Prilagodljivost i skalabilnost** – RBAC model omogućava prilagodbu prava pristupa prema potrebama organizacije. Prilagodljivost potrebama organizacije vrlo je važna za razvoj otvorenog okvira koji podržava različite organizacijske strukture i potrebe. Nadalje, sposobnost skaliranja prava pristupa s rastućim brojem korisnika ili organizacijskim promjenama doprinosi dugoročnoj učinkovitosti otvorenog okvira.
- **Razvoj specifičnih pravila** – Otvoreni okvir može koristiti fleksibilnost RBAC modela za razvoj specifičnih pravila pristupa koja odražavaju pravila organizacije. Ovim pristupom postiže se prilagođeno upravljanje korisničkim računima koje u potpunosti odražava poslovne potrebe.
- **Najbolje prakse** – Integracijom RBAC modela unutar otvorenog okvira iskorištavaju se najbolje prakse koje su već ugrađene u Oracle DBMS. Predmetnom integracijom smanjuje se potreba za eksperimentiranjem i osigurava se stabilnost i pouzdanost otvorenog okvira.

Važnost RBAC modela unutar Oracle DBMS očituje se u kombinaciji funkcionalnih, sigurnosnih i praktičnih elemenata koji pružaju osnovu za izgradnju stabilnog, prilagodljivog i učinkovitog sustava za upravljanje korisničkim računima.

5. Pregled literature i postojećih rješenja

U današnjem digitalnom dobu, gdje organizacije prikupljaju i obrađuju velike količine podataka, zaštita podataka postaje imperativ. „Rizici od cyber prijetnji, zlouporabe podataka i neovlaštenog pristupa nikada nisu bili veći“ [11]. Upravljanje zaštitom podataka postaje ključno za očuvanje povjerenja korisnika, zakonitost poslovanja i sigurnost informacija.

Ovo poglavlje posvećeno je razmatranju koncepta upravljanja zaštitom podataka i ključnih aspekata. Kroz rezultate provedenog istraživanja predstavljeni su prepoznate prednosti, izazovi i ograničenja pojedinih modela kontrole pristupa podacima. Uz prepoznavanje prednosti, izazova i ograničenja pojedinih modela, cilj istraživanja bio je prepoznati najnovije trendove u području upravljanja pristupom podacima.

Kroz analizu članaka razmotreno je kako organizacije koje posluju u različitim sektorima pristupaju izazovima zaštite podataka.

U vremenima gdje su podaci srce poslovanja, upravljanje njihovom zaštitom postaje nužnost, a dubinsko razumijevanje ovog koncepta ključno za osiguravanje sigurnosti, povjerenja i usklađenosti.

5.1 Provedeno istraživanje na temu upravljanja zaštitom podataka

U ovom poglavlju predstavljeni su rezultati provedenog istraživanja koje je bilo usmjereno na pretraživanje citatnih baza podataka. Svrha istraživanja bila je razumjeti trenutačne prakse u području upravljanja sigurnošću podataka i identificirati najučinkovitije strategije koje organizacijama omogućuju da se uspješno nose s izazovima sigurnosti podataka.

Temeljem analize prikupljenih radova objavljenih u posljednjih pet godina utvrđeno je kako su autori prepoznali problem koji se odnosi na dvije sastavnice CIA trokuta, a to su integritet i povjerljivost podataka odnosno povećanje razine zaštite integriteta i povjerljivosti podataka u relacijskoj bazi podataka.

Poglavlje započinje pregledom relevantne literature i istraživačkih radova koji su doprinijeli razumijevanju i razvoju koncepta upravljanja zaštitom podataka. Nakon pregleda literature istraženi su primjeri najboljih praksi i praktičnih iskustava na temelju prikazanih implementacija. Kroz ovaj proces, postignut je dublji uvid u izazove i potencijalne pristupe koji su relevantni za različite sektore i industrije.

Ciljevi istraživanja

Cilj istraživanja bio je stjecanje dubljeg uvida u stanje kako postojeći modeli kontrole pristupa podacima funkcioniraju u stvarnom svijetu. Također istražuje se kako se te kontrole primjenjuju u različitim sektorima s ciljem razumijevanja specifičnih izazova i potreba tih sektora. Procjena rizika u upravljanju pravima igra ključnu ulogu u razvoju strategija za smanjenje potencijalnih prijetnji i osiguranje sigurnosti podataka. S obzirom na navedeno, ciljeve istraživanja možemo podijeliti na sljedeće kategorije:

- Analiza učinkovitosti kontrole pristupa
- Procjena rizika u upravljanju pravima
- Razvoj modela kontrole pristupa
- Primjena kontrole u specifičnim sektorima
- Revizija i praćenje pristupa podacima

Metodologija istraživanja

Istraživanje je provedeno kroz nekoliko koraka:

1. Identifikacija ključnih citatnih baza podataka: Prvi korak u istraživanju bio je prepoznati relevantne citatne baze podataka koje sadrži članke i radove iz područja upravljanja kontrolom pristupa podacima. Ovdje su korištene baze „IEEE Xplore“, „ScienceDirect“, „Scopus“ i „Web of Science“.

2. Definiranje ključnih pojmova za pretraživanje: Za pretraživanje citatnih baza definirane su ključne riječi koje su relevantne za istraživanje, uključujući „data access management“, „data confidentiality“, „database access controle“, „database atuhorization“, „database role management“, „database security“, „role based access control“.

3. Pretraživanje citatnih baza: Kroz pretraživanje citatnih baza izvršeno je pretraživanje koristeći definirane ključne riječi kako bi se identificirali ključni relevantni članci i radovi. Pretraživanje je obuhvatilo članke objavljene unutar posljednjih pet godina (2017. – 2022.) kako bi se osigurala aktualnost istraživanja.

4. Odabir relevantnih članaka: Nakon pretraživanja odabranih citatnih baza odabrani su članci koji su najrelevantniji za temu istraživanja, uzimajući u obzir kvalitetu i sadržaj svakog članka. Nakon što su u prethodnim koracima jasno definirani kriteriji za ocjenu relevantnosti članaka kao što su vremenski okvir, vrsta izvora i ključne riječi, odabir članaka je izvršen prema sljedećim koracima:

- Pregled naslova i sažetaka: Proces odabira započeo je pregledom naslova i sažetaka svih članaka koji su se pojavili tijekom pretraživanja citatnih baza podataka. Cilj ovog koraka bio je brzo procijeniti osnovnu relevantnost svakog članka.
- Dubinska analiza članaka: Nakon pregleda naslova i sažetaka, članci koji su se činili potencijalno relevantnima, pažljivo su proučeni u potpunosti. Analizirani su ciljevi istraživanja, metodologija, ključne spoznaje i relevantnost u kontekstu istraživanja kontrole pristupa podacima.
- Konačni odabir: Na temelju pregleda i analize, odabrani su članci koji su najbolje odgovarali postavljenim kriterijima i bili najrelevantniji za istraživanje. Konačni odabir obuhvatio je članke koji su bili dalje analizirani u svrhu izvlačenja ključnih spoznaja.

Analiza i interpretacija rezultata

U ovom poglavlju predstavljeni su ključni rezultati provedenog istraživanja u vezi kontrole pristupa podacima temeljenom na analizi relevantnih članaka. U tablici 1 predstavljen je sažet pregled rezultata.

Citatna baza podataka	Broj članaka
IEEE	9
Science direct	8
Scopus	11
Web of Science	31
Ukupno	59

Tablica 1: Rezultati pretraživanja citatnih baza podataka (Izvor: autorov doprinos)

Nakon pretraživanja citatnih baza podataka proveden je proces pročišćavanja prikupljenih članaka kako bi osigurao da istraživanje bude što preciznije i relevantnije. Proces pročišćavanja uključivao je primjenu sljedećih kriterija:

- Eliminacija duplikata (9 članaka isključeno): Prvi korak pročišćavanja bio je prepoznavanje i eliminacija svih članaka koji su se pojavili više puta u različitim izvorima. Kako su točnost i relevantnost ključni aspekti, svi duplikati su isključeni kako bi se izbjegla ponavljanja i nepotrebna analiza.
- Ocjenjivanje prikladnosti (34 članka isključeno): Nakon eliminacije duplikata proces je nastavljen kroz ocjenjivanje svakog članka kako bi se utvrdila prikladnost i značaj za istraživanje. Ovdje je istaknuta važnost odabira članaka koji su dubinski relevantni za temu kontrole pristupa podacima kao i vremenski okvir u kojem su članci nastali, a pokazali su se kao rezultati pretraživanja bez obzira na vremenske kriterije pretraživanja.

Cilj procesa pročišćavanja bio je osiguravanje da se u analizu uključe samo članci visokog značaja što pridonosi pouzdanosti i preciznosti zaključaka istraživanja o kontroli pristupa podacima. Analizirajući sličnosti i razlike, kao i teme te područja koja članci pokrivaju, članci su razvrstani u tri skupine:

1. skupina – Teorijski okvir (1 članak)
2. skupina - Razrada modela kontrole pristupa podacima (9 članaka)
3. skupina - Implementacija modela kroz studije slučaja (6 članaka)

Rezultati istraživanja

U prvoj skupini članaka [20] autorica se bavi teorijskim okvirom kontrole pristupa podacima. Teorijskim okvirom obuhvaćeni su osnovni koncepti kao što su povjerljivost, integritet i dostupnost podataka, povijesni pregled, zaštita podataka, politike zaštite podataka, autorizacija pristupa podacima i modeli kontrole pristupa podacima. Uz osnovne koncepte, autorica se bavi opisivanjem i proučavanjem najzastupljenijih modela kontrole pristupa podacima kao što su diskrecijski model (DAC), mandatorni model (MAC) i model grupa i uloga (RBAC).

Razvoj informacijske tehnologije kao i rastući izazovi u području informacijske sigurnosti doveli su do razvoja brojnih modela kontrole pristupa podacima. Modeli se međusobno razlikuju po dizajnu, složenosti i područjima primjene. Kroz teorijsku osnovu i povijesni pregled modela kontrole pristupa podacima, u ovoj skupini autorica se bavi i analizom i međusobnom usporedbom modela prema nizu parametara kao što su pohranjivanje identiteta korisnika, prijenos (delegiranje) povjerenja, detaljne politike kontrole pristupa, fleksibilnost, područja primjene itd.

U drugoj skupini članaka [21 - 30] autori se bave detaljnom analizom najzastupljenijih modela kontrole pristupa podacima, prvenstveno modelom temeljenom na ulogama (Role Based Access Control). Literatura u ovoj skupini pokriva teme upravljanja rizicima pri implementaciji određenog modela, sigurnosne politike i procedure, zaštita informacijske imovine, sigurnost informacijskih sustava te slojevita zaštita.

Kontrola pristupa je ključni mehanizam za osiguranje integriteta i čuvanje privatnosti u velikim i kritičnim infrastrukturama. Za postizanje visoke razine sigurnosti, neizostavna je provjerena i pouzdana kontrola pristupa.

Analizirajući sigurnosne politike i pravila, osnovnu strukturu pojedinog modela i njegove sastavnice, prednosti, ograničenja, područja primjene kao i moguća proširenja, autori nastoje pronaći najprikladniji model sukladno prepoznatim izazovima i organizacijskim potrebama.

U ovoj skupini članaka, autori temeljem dobivenih rezultata analize pojedinih modela predlažu njegovu primjenu, a s ciljem povećanja povjerljivosti i integriteta podataka.

U trećoj skupini članaka [31 - 35] autori se bave implementacijom modela za kontrolu pristupa podacima. Osnovna pitanja koja se postavljaju u studijama slučaja u analiziranoj literaturi su:
1. Kako uspostaviti visoku razinu sigurnosti baze podataka?
2. Zašto koristiti model kontrole pristupa podacima temeljen na ulogama?

Autori kreću od činjenice da je uspostava visoke razine sigurnosti baze podataka osnovna i vrlo izazovna zadaća. U analiziranoj literaturi autori nastoje odgovoriti na dvije komponente CIA trokuta, a to su povjerljivost i integritet podataka na primjerima iz stvarnog života.

Najzastupljeniji model u analiziranoj literaturi je svakako model kontrole pristupa temeljen na ulogama. Kao osnovne prednosti razmatranog modela navode se sigurnost, fleksibilnost, razdvajanje dužnosti i mogućnost organizacije uloga kroz nasljeđivanje prava i hijerarhiju.

Diskusija

U ovom poglavlju navedeni su zaključci istraživanja o kontroli pristupa podacima temeljenom na analizi prikupljenih članaka kao i preporuke za daljnje istraživanje. Istraživanje je omogućilo dublje razumijevanje ključnih tema u kontroli pristupa podacima, uključujući modele prava pristupa kao i sigurnost podataka.

Ključne spoznaje dobivene iz istraživanja ukazuju na važnost primjene RBAC modela za učinkovitu kontrolu prava pristupa podacima u organizacijama. Također primijećen je interes za modele kontrole prava pristupa zasnovane na atributima te potreba za dinamičkom prilagodbom kontrole prava pristupa podacima. Uz navedeno, naglašena je potreba za snažnijim fokusom na reviziju prava pristupa kako bi se očuvala sigurnost podataka.

Na temelju ovih zaključaka iznesene su preporuke koje imaju značajnu ulogu u daljnjem razvoju otvorenog okvira za upravljanje korisničkim računima:
- Nastavak istraživanja RBAC modela. Buduća istraživanja mogu se orijentirati na unaprjeđenje RBAC modela i razvoj novih tehnika za učinkovitu primjenu.
- Istraživanje modela zasnovanog na atributima. Razmatranje mogućnosti za proširenje kontrole temeljene na atributima i njezine primjene u specifičnim sektorima.
    - Revizija i praćenje prava pristupa. Razvijanje alata i tehnika za učinkovitu reviziju i praćenje prava korisnika radi zaštite podataka.

6. Definiranje značajki okvira

U procesu razvoja otvorenog okvira za upravljanje korisničkim računima ključno je razumjeti i definirati značajke koje će oblikovati funkcionalnost. Kako bi se osigurala dosljednost, sigurnost i učinkovitost, standardizacija je imperativ.

Standardizacija procesa razvoja i revizije korisničkih uloga i kreiranja korisničkih uloga postavlja okvire koji omogućuju jasno definirane smjernice i pravila. To osigurava da se isti standardi primjenjuju na svim razinama i u svim dijelovima sustava.

U ovom kontekstu standardizacija pomaže pri osiguravanju sigurnosti podataka i zaštiti od potencijalnih prijetnji, ali i olakšava upravljanje pravima pristupa, reviziju i nadzor.

Uz standardizaciju, u procesu razvoja otvorenog okvira za upravljanje korisničkim računima, ključno je razumjeti i definirati značajke koje će oblikovati funkcionalnost ovog sigurnosnog alata. Značajke okvira igraju ključnu ulogu u određivanju kako će okvir ispuniti svoju svrhu, unaprijediti sigurnost i administraciju te doprinijeti ostvarenju istraživačkih ciljeva.

U ovom poglavlju predstavljena je definicija i svrha značajki unutar otvorenog okvira i njihova povezanost s istraživanjem upravljanja korisničkim računima.

Ključna karakteristika ovog otvorenog okvira i studije slučaja je standardizacija procesa vezanih uz upravljanje korisničkim računima i usmjerenost na lokalnu autorizaciju i autentifikaciju. Specifičnost ovog pristupa proizlazi iz jedinstvenih zahtjeva, ograničenja i ciljeva istraživanja.

Usmjerenost razvoja okvira na standardizaciju, lokalnu autentifikaciju i autorizaciju ima nekoliko značajnih implikacija:

- **Specifičnost studije slučaja** – Lokalna autentifikacija i autorizacija koriste se u scenarijima gdje se pravima pristupa upravlja unutar samog DBMS-a, bez povezivanja na vanjske usluge ili direktorije. Specifičnost odražava studiju slučaja i cilj istraživanja kroz usredotočenost na aspekte sigurnosti unutar Oracle DBMS sustava.

- **Veća kontrola i ovisnost o DBMS** – Koristeći lokalnu autentifikaciju i autorizaciju osigurava se veća kontrola nad pristupom korisnicima i upravljanjem pravima pristupa unutar baze podataka. Ovakvim pristupom smanjuje se ovisnost organizacije o vanjskim uslugama i osigurava potpuna autonomija nad sigurnošću baze podataka.
- **Proučavanje specifičnih izazova** – Specifičnost lokalne autentifikacije i autorizacije omogućava detaljno proučavanje izazova, prednosti i nedostataka ovakvog pristupa.
- **Praktična implementacija** – Usmjeravanjem na lokalnu autentifikaciju i autorizaciju osigurava se razvoj praktičnih smjernica za implementaciju otvorenog okvira u stvarnim scenarijima. Ovakva implementacija posebno je korisna za organizacije koje žele primijeniti lokalne metode sigurnosti u vlastitim Oracle DBMS okruženjima.

6.1 Standardizacija procesa

U poglavlju o standardizaciji procesa razrade uloga, odobrenja korisničkih računa i revizije korisničkih prava istaknut je vlastiti doprinos. Pristup standardizaciji procesa osmišljen je kako bi unaprijedio ove ključne aspekte upravljanja pravima pristupa podacima. Ovaj doprinos odražava ne samo teorijsko razumijevanje već i praktično iskustvo u implementaciji unutar specifičnog konteksta organizacije.

Nadalje važno je naglasiti da predložene standardizacije nisu generički modeli već rezultat dubinskog razumijevanja potreba organizacije. Ovaj pristup čini osnovu za učinkovito upravljanje pravima pristupa uzimajući u obzir specifičnosti organizacije. Potrebno je istaknuti implementaciju odabranih praksi u stvarnom radnom okruženju čime se dokazuje njihova praktična primjenjivost i usklađenost s organizacijskim zahtjevima.

U sklopu istraživanja o upravljanju korisničkim računima i kontroli prava pristupa važno je opisati ključne procese koji se odnose na sigurnost informacija i kontrolu pristupa. U ovom poglavlju analizirati će se tri osnovna procesa u održavanju sigurnosti i integriteta podataka, a to su: proces razrade uloga, proces odobrenja korisničkog računa i dodjeljivanje određene uloge te proces revizije korisničkih uloga.

U tu svrhu, standardizacija navedenih procesa igra ključnu ulogu. Standardizacija omogućava organizacijama da uspostave jasna pravila, procedure i smjernice za upravljanje korisničkim računima, čime se osigurava dosljednost i sigurnost.

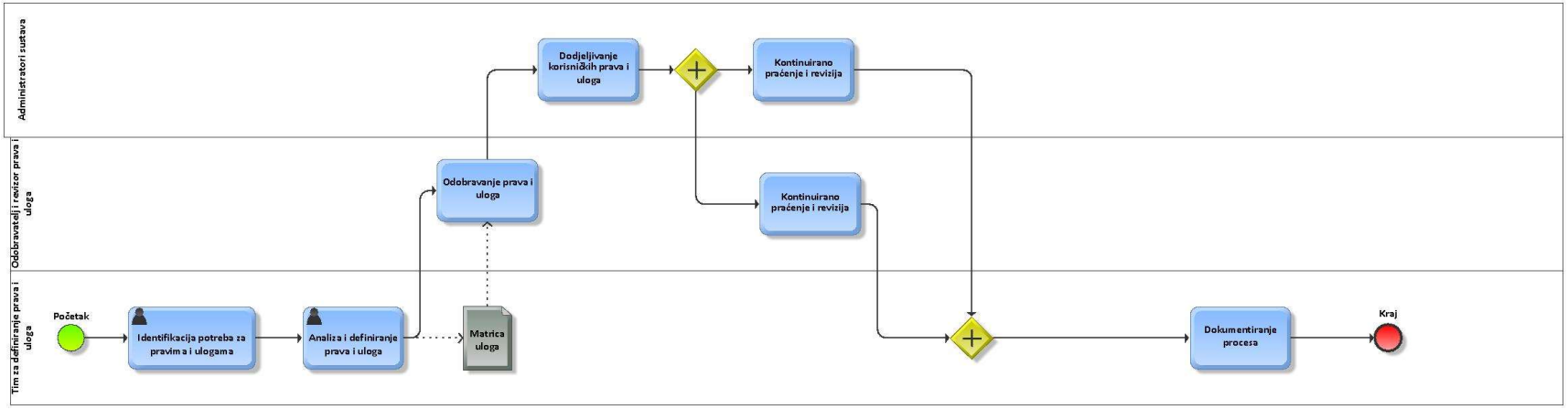
U narednim dijelovima ovog poglavlja biti će razmotreno kako standardizacija procesa može doprinijeti boljem definiranju uloga i odgovornosti u upravljanju korisničkim računima. Također analizirati će se kako standardi mogu osigurati dosljednost u primjeni sigurnosnih politika te kako mogu pomoći u praćenju i reviziji sustava.

6.2 Proces razrade uloga

Proces razrade uloga (slika 1) u upravljanju korisničkim računima od iznimne je važnosti u osiguranju da svaki korisnik ima pristup samo onim resursima koji su nužni za obavljanje njihovih zadataka. Ovaj proces pomaže organizacijama da postignu preciznu kontrolu nad pravima i ovlastima korisnika te osiguraju pridržavanje načela najmanjih privilegija. Ključni koraci u procesu razrade uloga su:

1. **Identifikacija funkcija i zadataka:** Prvi korak u razradi uloga je identifikacija različitih funkcija i zadataka unutar organizacija. To uključuje utvrđivanje specifičnih poslovnih procesa, aplikacija i sustava kojima korisnici moraju pristupiti.
2. **Klasifikacija korisnika:** Nakon što su funkcije i zadaci iz prvog identificirani, korisnici se klasificiraju prema njihovim ulogama i odgovornostima. Na primjer korisnici mogu biti podijeljeni na administratora podataka, menadžera, zaposlenika itd.
3. **Definiranje uloga:** Za svaku klasifikaciju korisnika definiraju se uloge koje odražavaju njihove potrebe za pristupom resursima. Ove uloge trebaju biti jasno opisane i dokumentirane kako bi se izbjegao bilo kakav nesporazum.
4. **Dodjela ovlasti:** Svaka uloga treba imati pripadajuće ovlasti koje definiraju što korisnici mogu ili ne mogu raditi unutar dodijeljene uloge. Ovlasti se dodjeljuju u skladu s poslovnim pravilima i sigurnosnim potrebama.
5. **Revizija i ažuriranje uloga:** Proces razrade uloga nije statičan i zahtijeva redovitu reviziju i ažuriranje. Promjene u organizaciji ili tehnološkim zahtjevima mogu zahtijevati prilagodbu uloga i ovlasti.

Ovaj proces osigurava da svaki korisnik ima pristup samo onim resursima koji su nužni za obavljanje njihovih zadataka, smanjujući rizik od zloupotrebe ovlasti ili sigurnosnih propusta. Pravilno razrađene uloge olakšavaju administraciju korisničkih računa, podržavaju princip najmanjih privilegija i doprinose općoj sigurnosti informacijskog sustava.



Slika 1: Proces razrade korisničkih prava i uloga (Izvor: autorov doprinos)

Matrica korisničkih uloga

Matrica korisničkih uloga predstavlja organizacijski alat u sustavu kontrole pristupa podacima. Svrha matrice uloga je strukturiranje prava i ovlasti uloge unutar informacijskog sustava. U matrici su definirane različite uloge koje korisnici mogu imati povezujući ih s određenim zadacima i/ili funkcionalnostima. Svaka uloga unutar matrice nosi određeni set prava kao što su pravo pristupa podacima, mogućnosti izvršavanja određenih operacija i/ili sudjelovanja u specifičnim procesima sustava. Matrica korisničkih uloga izuzetno je važna u organizacijama gdje je kontrola pristupa podacima od izuzetne važnosti.

Matrica korisničkih uloga mora biti rezultat procesa razrade korisničkih prava i uloga kako bi odražavala zahtjeve i potrebe organizacije. Dinamičnost matrice proizlazi iz stalnih promjena u organizaciji, tehnologiji i/ili zakonodavstvu zbog čega je nužno voditi računa o ažurnosti matrice kako bi odražavala trenutačno stanje i sigurnosne potrebe.

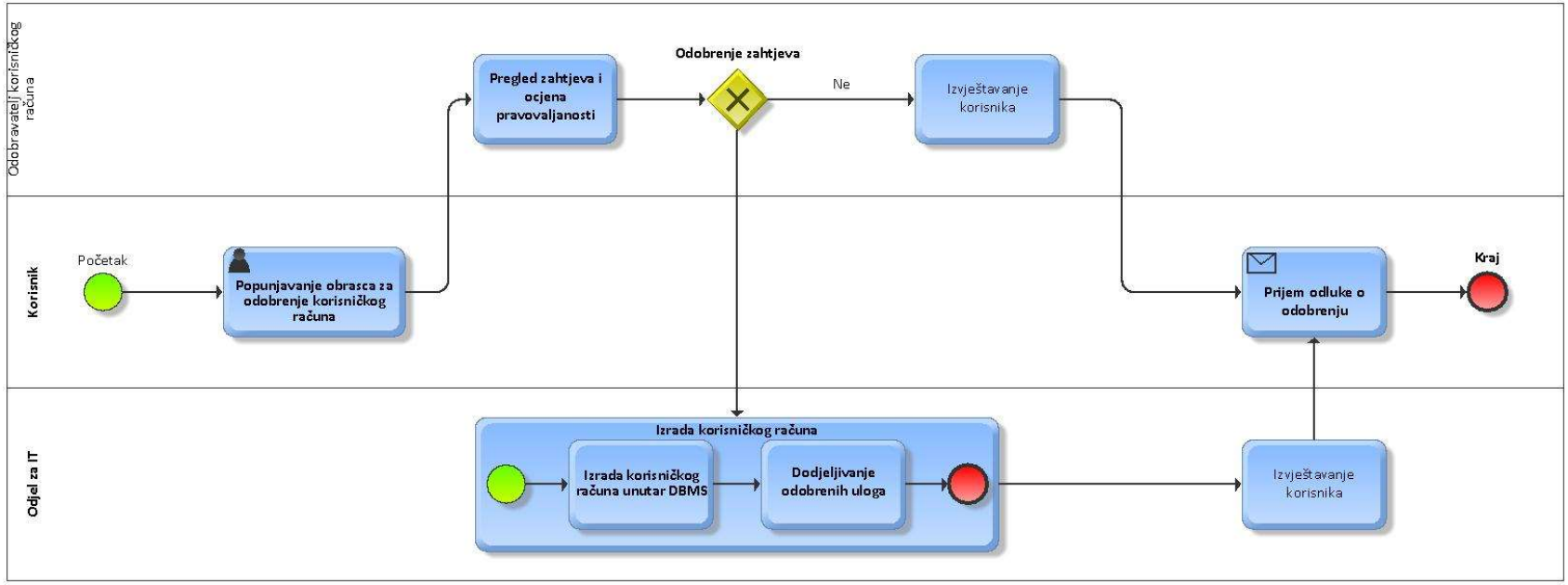
Rola	**KORISNIČKA_ULOGA_1**				**KORISNIČKA_ULOGA_2**				**KORISNIČKA_ULOGA_3**			
Objekt/pravo	Select	Insert	Update	Delete	Select	Insert	Update	Delete	Select	Insert	Update	Delete
Objekt_1	x	x	x	x	x		x		x			
Objekt_2	x	x	x	x	x		x		x			
Objekt_3	x	x	x	x	x		x		x			
Objekt_4	x	x	x	x	x		x		x			

Tablica 2: Matrica korisničkih uloga (Izvor: autorov doprinos)

6.3 Proces odobrenja korisničkih računa

Proces odobrenja korisničkog računa (slika 2) odnosi se na niz koraka i postupaka koje organizacija provodi kako bi omogućila korisnicima pristup informacijskim sustavima. Ovaj proces ima ključnu ulogu u osiguravanju sigurnosti, identifikaciji i kontroli pristupa podacima. Uz navedeno proces osigurava da samo ovlašteni korisnici dobiju pristup sustavima. U ovom poglavlju opisani su koraci u procesu odobrenja korisničkog računa:

1. **Korisnik podnosi zahtjev za korisničkim računom:** Korisnik inicira proces podnošenjem zahtjeva za stvaranjem korisničkog računa kroz popunjavanje standardiziranog obrasca za odobrenje korisničkog računa.
2. **Zahtjev stiže do odobravatelja korisničkog računa:** Nakon što korisnik podnese zahtjev, on stiže do odobravatelja korisničkog računa.
3. **Pregled zahtjeva i ocjena pravovaljanosti:** Odobravatelj korisničkog računa provodi detaljan pregled zahtjeva kako bi provjerio njegovu valjanost i ispravnost.
4. **Odobravatelj donosi odluku:** Na temelju pregleda, odobravatelj donosi odluku o odobrenju ili odbijanju zahtjeva.
5. **Kreiranje korisničkog računa:** Ako je zahtjev odobren, IT odjel kreira korisnički račun za korisnika u sustavu. Kreiranje uključuje dodjelu korisničkog imena, zaporke i odgovarajućih pristupnih prava.
6. **Obavještavanje korisnika:** Korisnika se obavještava o statusu zahtjeva. U slučaju odobrenja, obavještava ga se o kreiranju korisničkog računa, korisničkom imenu i privremenoj zaporci. U slučaju odbijanja, obavještava ga se o razlozima.
7. **Proces završava nakon obavještavanja korisnika o statusu zahtjeva**

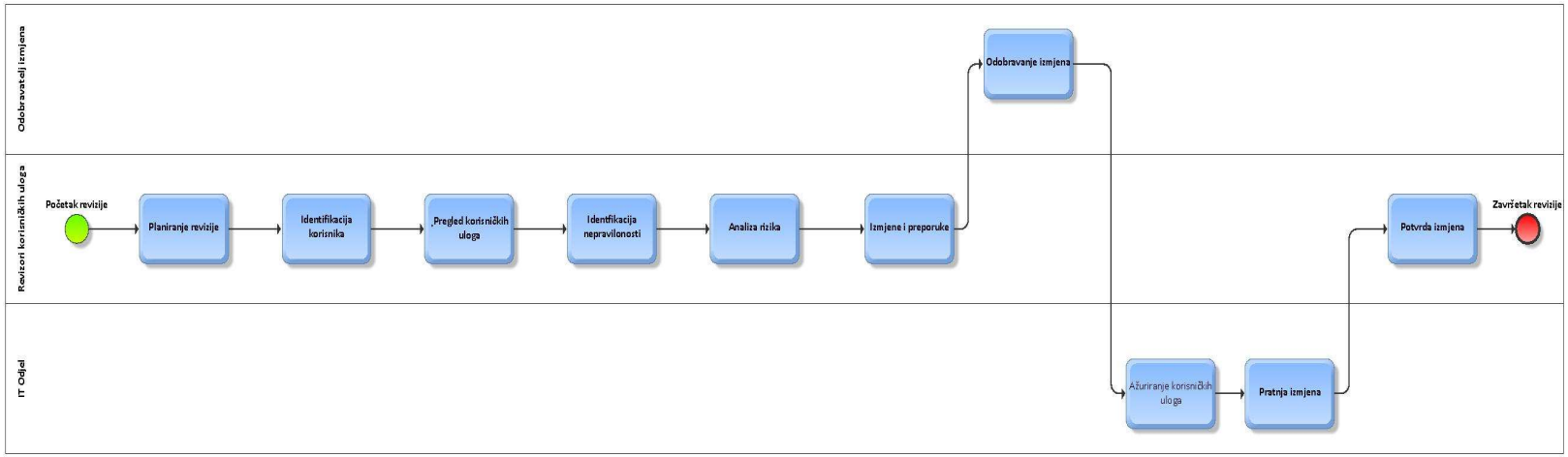


Slika 2: Proces odobrenja korisničkog računa (Izvor: autorov doprinos)

6.4 Proces revizije korisničkih uloga

Proces revizije korisničkih uloga (slika 3) ključan je za održavanje sigurnosti i pravilnog upravljanja korisničkim računima u organizaciji. Revizija osigurava da prava i uloge korisnika odgovaraju njihovim trenutačnim odgovornostima i potrebama, a istovremeno štiti organizaciju od potencijalnih rizika. U ovom poglavlju detaljno je razmotren proces revizije korisničkih uloga kroz ključne korake:

1. **Proces započinje kada tim revizora korisničkih uloga pokreću reviziju korisničkih uloga u sustavu.**
2. **Planiranje revizije:** Revizori planiraju reviziju, definiraju ciljeve, postavljaju raspored i određuju resurse za provođenje revizije.
3. **Identifikacija korisnika:** Revizori identificiraju korisnike i/ili korisničke uloge koji će biti predmet revizije.
4. **Pregled korisničkih uloga:** Revizori prikupljaju podatke o korisničkim ulogama.
5. **Identifikacija nepravilnosti:** Revizori traže nepravilnosti i povrede sigurnosnih standarda u dodijeljenim ulogama.
6. **Analiza rizika:** Na temelju prepoznatih nepravilnosti provodi se analiza kako bi se procijenile posljedice i prioriteti izmjena.
7. **Izmjene i preporuke:** Revizori izrađuju preporuke za izmjene u korisničkim ulogama kako bi se osigurala usklađenost sa sigurnosnim standardima.
8. **Odobravanje izmjena:** Izmjene u korisničkim ulogama moraju biti odobrene od strane nadležnih odobravatelja unutar organizacije.
9. **Ažuriranje korisničkih uloga:** Nakon odobrenja izmjena administratori sustava ažuriraju korisničke uloge.
10. **Pratnja izmjena:** IT odjel prati i provjerava provedbu izmjena u korisničkim ulogama
11. **Završetak revizije:** Revizija završava nakon što su izmjene u korisničkim ulogama provedene i potvrđene.



Slika 3: Proces revizije korisničkih uloga (Izvor: autorov doprinos)

6.5 Moduli i funkcionalnosti otvorenog okvira

Razvoj otvorenog okvira za upravljanje korisničkim računima u Oracle DBMS zahtijeva pažljivo definiranje modula i funkcionalnosti koji će oblikovati njegovu cjelokupnu arhitekturu. U ovom poglavlju predstavljeni su ključni moduli i funkcionalnosti koji čine temelj ovog okvira te njihov doprinos pri ostvarenju istraživačkih ciljeva.

Autentifikacija

Autentifikacija je temeljna funkcionalnost ovog okvira i odnosi se na proces provjere korisničkog identiteta pri pristupu bazi podataka. U okviru autentifikacije definiraju se različite metode provjere identiteta korisnika, uključujući korisničko ime i lozinku, certifikate, biometrijske podatke ili druge tehnike. Autentifikacija osigurava da samo ovlašteni korisnici imaju pristup sustavu.

Autorizacija

Autorizacija je ključna komponenta za kontrolu prava pristupa i privilegija korisnika unutar baze podataka. U okviru autorizacije definiraju se prava pristupa tablicama, shemama, funkcijama i drugim resursima. Ovo omogućava precizno upravljanje ovlastima i ograničava pristup osjetljivim podacima.

Sigurnosne politike

Sigurnosne politike definiraju minimalne zahtjeve i pravila za sigurnosne postavke unutar baze podataka. Moduli za sigurnosne politike omogućavaju postavljanje i primjenu pravila koja se odnose na sigurnosne zahtjeve organizacije. Ovo uključuje pravila za kompleksne lozinke, višestruke razine autentifikacije i zahtjeve za sigurnosne certifikate.

Praćenje aktivnosti korisnika

Praćenje aktivnosti korisnika pruža dublji uvid u kako se korisnici ponašaju unutar baze podataka. Ovaj modul omogućava zapisivanje i analizu svih radnji koje korisnici poduzimaju, što je ključno za otkrivanje neovlaštenih aktivnosti, praćenje promjena i analizu sigurnosnih događaja.

Administracija korisnika

Moduli za administraciju korisnika olakšavaju dodjelu i upravljanje korisničkim ulogama, privilegijama i postavkama korisničkih računa. Ovo omogućava administratorima sustava da učinkovito konfiguriraju i nadziru korisničke račune unutar baze podataka.

Skalabilnost

Skalabilnost pridonosi dugoročnoj funkcionalnosti otvorenog okvira za upravljanje korisničkim računima. Otvoreni okvir dizajniran je s namjerom da se lako prilagodi rastućem broju korisnika kao i organizacijskim promjenama te evoluciji poslovnih zahtjeva. Uz podršku većem broju korisnika važnost skalabilnosti očituje se i u sposobnosti prilagodbe organizacijskim zahtjevima.

Otvoreni okvir omogućava jednostavno dodavanje i/ili mijenjanje korisničkih uloga i prava. Fleksibilnost okvira u prilagodbi promjenama jedna je od ključnih karakteristika skalabilnosti.

6.6 Sigurnosni aspekti

U ovom poglavlju predstavljeni su ključni sigurnosni aspekti unutar okvira koji su od presudne važnosti za osiguranje integriteta, povjerljivosti i dostupnosti baze podataka.

Snažnija autentifikacija

Jača autentifikacija u ovom kontekstu znači korištenje višefaktorskih metoda za provjeru identiteta korisnika. To uključuje nešto što korisnik zna (npr. lozinku), nešto što korisnik ima (npr. sigurnosni token) i nešto što korisnik jest (npr. biometrijske podatka). Ovakav pristup povećava sigurnost jer neovlaštenim korisnicima znatno otežava prijeći navedene prepreke i pristupiti bazi podataka.

Jača autentifikacija je osnovni sigurnosni aspekt koji se odnosi na postupak provjere korisničkog identiteta pri pristupu bazi podataka. U predstavljanju otvorenog okvira, višefaktorska autentifikacija neće biti implementirana već se ostavlja prostor za buduća istraživanja.

Višerazinska zaštita

Ovaj sigurnosni aspekt predstavlja ključan dio sigurnosne strategije za zaštitu baze podataka. Ovaj aspekt istražuje kako se sigurnost može primjenjivati na više razina, počevši od aplikacijske razine i spuštajući se sve do samih podataka unutar baze podataka. Na aplikacijskoj razini sigurnost uključuje provjeru identiteta korisnika, primjenu različitih autentifikacijskih metoda i kontrolu pristupa unutar aplikacije koja koristi bazu podataka. Ovo osigurava da samo ovlašteni korisnici mogu pristupiti aplikaciji, a samim time i bazi podataka.

Na razini baze podataka sigurnost se dodatno pojačava. To uključuje kontrolu pristupa na razini tablica, shema, funkcija, procedura i drugih resursa unutar baze podataka. Administratori baze podataka mogu precizno definirati koje operacije i drugi resursi su dostupni korisnicima ili pojedinim aplikacijama. Ovaj aspekt istraživanja usmjeren je na razumijevanje kako se sigurnost može implementirati na više razina i kako razine međusobno surađuju sa svrhom postizanja potpune zaštite podataka i aplikacija.

Autorizacija i kontrola pristupa

Kontrola pristupa unutar okvira omogućava precizno definiranje tko ima prava pristupa određenim resursima baze podataka. Ovo uključuje kontrolu nad tablicama, shemama, funkcijama i drugim resursima. Svaki korisnik ili skupina korisnika ima dodijeljene određene privilegije, što osigurava da se podaci i funkcionalnosti baze koriste samo onako kako je predviđeno.

Sigurnosne politike

Sigurnosne politike unutar okvira definiraju minimalne sigurnosne zahtjeve i pravila koja korisnici moraju poštivati. Ovo je ključno za usklađenost s regulatornim zahtjevima i internim sigurnosnim standardima. Primjenom tih politika osigurava se dosljednost i sigurno okruženje za bazu podataka.

Praćenje aktivnosti korisnika i sigurnosna pohrana

Praćenje aktivnosti korisnika i zapisivanje sigurnosnih događaja omogućuju detaljan uvid u sve što se događa unutar baze podataka. To uključuje prijave korisnika, promjene u podacima, pokušaje neovlaštenog pristupa i mnoge druge aktivnosti. Analiza ovih zapisa pomaže u otkrivanju sumnjivih aktivnosti i odgovoru na sigurnosne incidente.

Kriptografija i zaštita podataka

Uporaba kriptografije ima ključnu ulogu u osiguravanju sigurnosti podataka pohranjenih u bazi podataka. Oracle DBMS nudi niz mogućnosti za zaštitu podataka [19] od kojih se može izdvojiti:

- **Enkripcija podataka na razini baze podataka** – Ova značajka sprječava potencijalne napadače da „zaobiđu“ bazu podataka i pokušaju čitati podatke izravno iz pohranjenih datoteka. Korisnici koji su autentificirani u bazi podataka i dalje ostvaruju pristup podacima dok se svim drugim korisnicima uskraćuje pristup datotekama pohranjenim na nekom mediju.
- **Enkripcija podataka na razini stupca** – Ova značajka predstavlja mogućnost enkripcije određenih stupaca unutar tablice kao što su brojevi kreditnih kartica i drugi osjetljivi podaci. Značajka omogućava vlasnicima podataka odabir kritičnih stupaca koji sadrže osjetljive podatke te enkripciju istih. Korisnost ovog pristupa očituje se kod velikih baza podataka gdje samo mali broj stupaca mora biti štićen.
- **Enkripcija tabličnog prostora** – Ova značajka omogućava enkripciju čitavog tabličnog prostora (tablespace). Značajka enkriptira cijeli tablični prostor bez obzira na osjetljivosti vrstu podatka. Ova značajka pojednostavljuje proces enkripcije jer nije potrebno označavati određene stupce koje korisnik želi zaštititi. Korisnost značajke posebno se očituje kada baza podataka sadrži veliku količinu osjetljivih podataka koje je potrebno štititi.

Za navedene značajke Oracle DBMS koristi TDE enkripciju (Transparent Dana Encryption) koja omogućava da podaci ostanu zaštićeni i na medijima za sigurnosnu pohranu i na starim (odbačenim) medijima što u konačnici dovodi do sprječavanja neovlaštenog pristupa u slučaju kada se zaobilazi sigurnost na razini baze podataka.

Upravljanje identitetom

Upravljanje identitetom unutar okvira osigurava da svaki korisnik ima jedinstven identitet i da se korisnički računi stvaraju, upravljaju i ukidaju na siguran način. Ovo sprječava dvostruke račune ili neovlašten pristup i osigurava dosljedno upravljanje identitetima.

Kontrola pristupa unutar okvira

Kontrola pristupa unutar okvira postavlja tko ima pravo upravljati sigurnosnim postavkama i privilegijama korisnika. Ovo osigurava da samo odabrani administratori mogu mijenjati sigurnosne postavke, sprječavajući neovlašteno mijenjanje prava pristupa.

Svaki od ovih sigurnosnih aspekata igra ključnu ulogu u zaštiti baze podataka od prijetnji, osiguravajući da samo ovlašteni korisnici imaju pristup podacima i da se podaci čuvaju na siguran način.

7. Razvoj otvorenog okvira

U ovom poglavlju predstavljeni su ključni aspekti razvoja predmetnog okvira pri čemu je razvoj usmjereni na dvije osnovne komponente, tehnologiju i arhitekturu otvorenog okvira. Kroz analizu tehnološkog temelja i arhitekturu predmetnog okvira, otkriti ćemo kako stvaranje ovakvog okvira može poboljšati pristup i upravljanje korisničkim računima dok istovremeno pruža visoku razinu sigurnosti.

Osim tehničkih aspekata u ovom poglavlju razmotrene su i organizacijske koristi te koraci koji su ključni za razvoj okvira koji će odgovarati potrebama i izazovima današnjih organizacija.

7.1 Tehnologija

Za dublje razumijevanje razvoja otvorenog okvira za upravljanje korisničkim računima ključno je predstaviti arhitekturu i tehnologije koje će biti upotrijebljene u njegovoj konstrukciji. Ovo poglavlje pruža uvid u srž tehnološkog okvira koji će osigurati sigurno, učinkovito i skalabilno upravljanje korisničkim pravima.

Na temelju analize potreba organizacije i izazova koje smo identificirali u prethodnim etapama, ključne tehnološke komponente čine Oracle DBMS (sustav za upravljanje bazom podataka) i Oracle ADF Middleware (Oracle Application Development Framework).

Oracle DBMS s dokazanom pouzdanošću pruža sigurno i skalabilno rješenje za pohranu i upravljanje bazom podataka. S druge strane Oracle ADF Middleware omogućava brzu i učinkovitu izradu Java EE aplikacija s bogatim korisničkim sučeljem čime se osigurava intuitivno iskustvo za korisnike i administratore.

U ovom poglavlju analizirana je arhitektura ovih tehnologija, razmotrena integracija i kako ista podržava funkcionalnosti okvira za upravljanje korisničkim računima. Provedena je analiza o tome kako Oracle DBMS omogućava sigurno pohranjivanje osjetljivih informacija, a kako Oracle ADF Middleware omogućava razvoj korisničkog sučelja prilagođenog potrebama organizacije.

S naglaskom na ove ključne tehnologije nastavljena je dubinska analiza s ciljem da korištena arhitektura podržava postavljene ciljeve u vidu sigurnosti, usklađenosti i učinkovitosti pri upravljanju korisničkim računima.

7.2 Arhitektura okvira

Arhitektura okvira temelji se na slojevitoj strukturi koja omogućuje bolju organizaciju i veću učinkovitost u odnosu na klasično upravljanje pravima pristupa temeljeno na ulogama unutar Oracle DBMS. Slojevi, kao ključni element, olakšavaju razdvajanje odgovornosti, podržavaju standardizaciju i omogućuju skalabilnost. Svaki sloj ima svoje specifične funkcionalnosti, od korisničkog sučelja i poslovne logike do sloja podataka i sigurnosnih mehanizama. Kroz ovakvu arhitekturu otvoreni okvir pruža temelje za upravljanje korisničkim računima koji se mogu prilagoditi organizacijskim potrebama.

Slojevi okvira

Slojevi predstavljaju logičku podjelu funkcionalnosti i komponenti unutar sustava. Ovo poglavlje sastoji se od nekoliko dijelova, svaki posvećen određenom sloju.

Aplikacijski sloj

Sloj korisničkog sučelja (UI) predstavlja vanjski sloj u arhitekturi okvira za upravljanje korisničkim računima i omogućava korisnicima interakciju sa sustavom. Ovaj sloj pruža grafičko sučelje koje olakšava korisnicima pristup mogućnosti, pregled i uređivanje korisničkih profila te navigaciju kroz sustav. Osim toga ovaj sloj uključuje mehanizme autentifikacije za provjeru identiteta korisnika pri prijavi, omogućava prikaz obavijesti te poruka. Ovaj sloj ima zadatak stvoriti korisničko iskustvo koje je intuitivno, funkcionalno i privlačno čime se u konačnici olakšava interakcija između korisnika i okvira za upravljanje korisničkim računima.

Sloj poslovne logike

Sloj poslovne logike u arhitekturi upravljanja korisničkim računima osigurava da sve operacije povezane s korisničkim računima budu obavljene na pravi način. To uključuje autentifikaciju, provjeru identiteta korisnika, određivanje njihovih ovlasti, te upravljanje korisničkim računima i ulogama. Nadalje, ovaj sloj implementira poslovna pravila i sigurnosne politike koja određuju tko ima pristup određenim resursima i pod kojim uvjetima.

Ovaj sloj omogućava konfiguraciju i prilagodbu sustava prema specifičnim potrebama organizacije što uključuje postavljanje pravila i parametara koji odražavaju unutarnje procese i zahtjeve. Uz navedeno ovaj sloj može integrirati različite sustave i usluge kako bi omogućio razmjenu podataka i funkcionalnosti između njih.

Kroz ove funkcionalnosti sloj poslovne logike osigurava da se upravljanje korisničkim računima odvija u skladu s definiranim pravilima i standardima, pružajući tako sigurnost, dosljednost i prilagodljivost okvira.

Podatkovni sloj

Podatkovni sloj u arhitekturi okvira predstavlja centralno mjesto za pohranu podataka povezanih s korisničkim računima, korisničkim ulogama i pravima pristupa. Ovaj sloj omogućava pohranu i upravljanje korisničkim podacima čime podržava autentifikaciju i autorizaciju, praćenje te reviziju aktivnosti korisnika. Podatkovni sloj osigurava dosljednost i integritet podataka te omogućava brz pristup i pretraživanje informacija potrebnih za učinkovito upravljanje korisničkim računima.

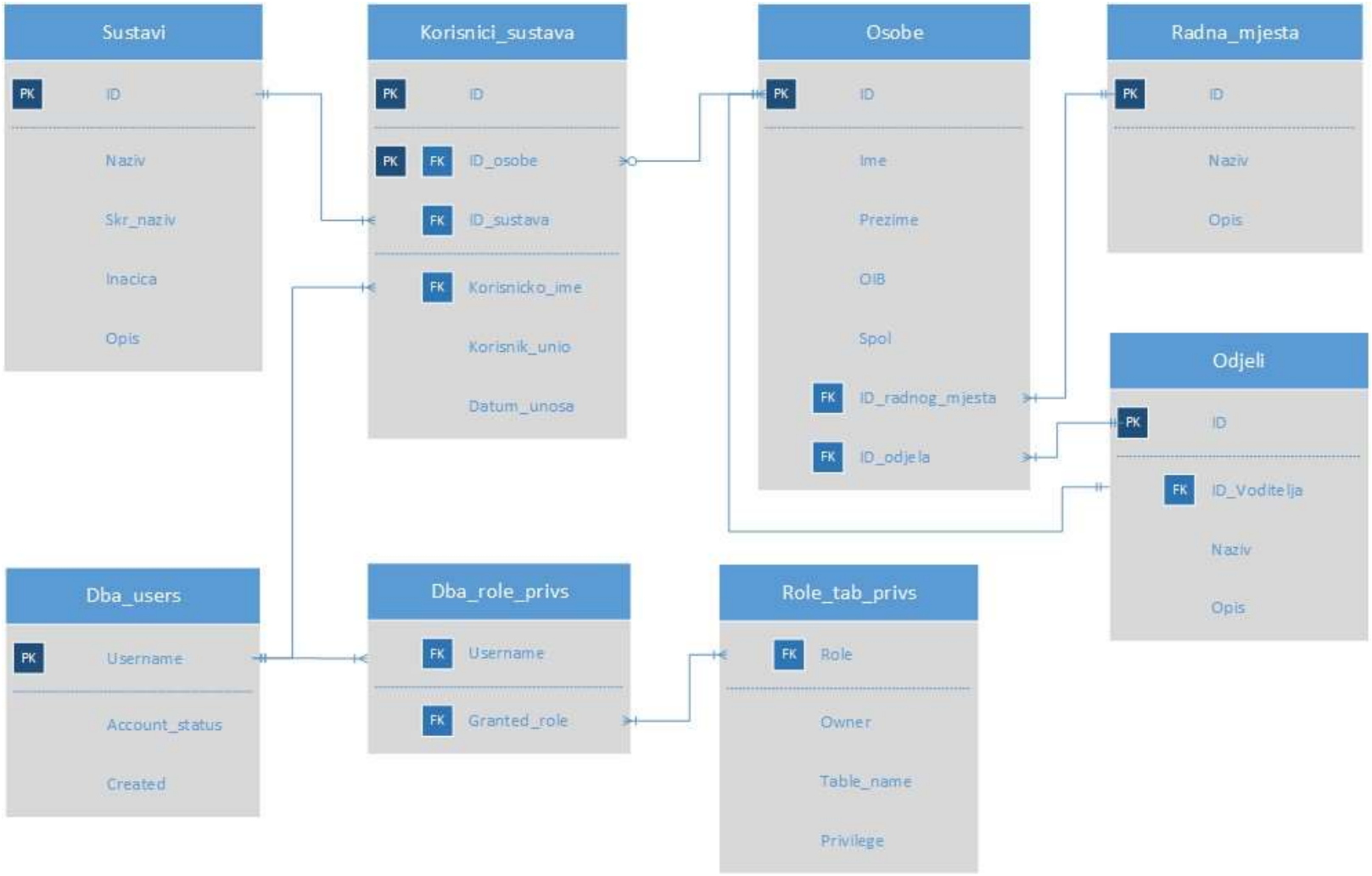
Osim toga podatkovni sloj uključuje tablice koje sadrže podatke o korisnicima, njihovim pravima, povijesti prijava i ostalim relevantnim podacima. Važno je naglasiti da podatkovni sloj također podržava replikaciju i sigurnosne mehanizme kako bi se osigurala dostupnost i zaštita podataka. Ovaj sloj u interakciji je sa slojem poslovne logike i slojem korisničkog sučelja.

U prikazu modela podataka (slika 4), koristi se kombinacija sistemskih i korisničkih tablica kako bismo dobili cjelovitu sliku strukture podatkovnog sloja. Sistemske tablice pružiti će nam informacije o korisničkim računima, ulogama i pravima pristupa dok korisničke tablice omogućavaju proširenje osnovnog modela kontrole pristupa podacima temeljenog na ulogama i samim time podržavaju funkcioniranje otvorenog okvira.

Važno je napomenuti kako prikaz obuhvaća samo ključne entitete i atribute kako bi se očuvala jasnoća i fokus na relevantnim informacijama. Ovdje su osnovni elementi koje ćemo obuhvatiti:

- **Entitet „Sustavi“** predstavlja šifarnik sustava nad kojima organizacija želi uspostaviti kontrolu pristupa podacima. Sadrži jedinstveni identifikator sustava, naziv, skraćeni naziv i opis sustava.
- **Entitet „Osobe“** predstavlja strukturiranu kolekciju podataka o zaposlenim osobama unutar organizacije. Entitet sadrži jedinstveni identifikator, ime, prezime, OIB, oznaku spola, identifikator radnog mjesta kao i identifikator odjela u kojem je zaposlena.
- **Entitet „Radna mjesta“** o radnim mjestima unutar organizacije. Osnovni atributi ovog entiteta su jedinstveni identifikator, naziv i opis radnog mjesta.
- **Entiteti „Odjeli“** obuhvaća ključne podatke o odjelima i/ili sektorima unutar organizacije. Osnovni atributi ovog entiteta uključuju jedinstveni identifikator, identifikator voditelja odjela, naziv odjela i opis odjela.
- **Entitet „Dba_users“** odnosi se na sistemsku tablicu i sadrži ključne podatke o svim korisnicima u bazi podataka. Svaki zapis predstavlja jednog korisnika i uključuje atribute poput korisničkog imena, statusa računa, datuma kreiranja korisničkog računa itd.
- **Entitet „Dba_role_privs“** odnosi se na sistemsku tablicu i sadrži podatke o dodijeljenim privilegijama odnosno ulogama korisnicima u bazi podataka. Svaki redak predstavlja vezu između korisničkog imena i korisničke uloge.
- **Entitet „Role_tab_privs“** sadrži podatke o privilegijama koje su dodijeljene ulogama u kontekstu tablica (objekata) unutar baze podataka. Svaki redak predstavlja vezu između uloge, tablice i dodijeljenih privilegija uključujući podatke o vrsti privilegije, vlasništvu tablice itd.

-



Slika 4: Model podataka otvorenog okvira (Izvor: autorov doprinos)

8. Studija slučaja

U cilju razvoja učinkovitog i prilagodljivog okvira za upravljanje korisničkim računima provedena je studija slučaja usmjerena na izazove s kojim se organizacije danas susreću. Izazovi su povezani sa specifičnim potrebama, prilikama i ograničenjima organizacije. Kroz analizu pravilnosti, procesa i implementiranih rješenja, ova studija slučaja predstavlja učinkoviti pristup upravljanju korisničkim računima.

Nadalje studija slučaja proučava kako integrirati tehnologije, metodologije i najbolje prakse u upravljanju korisničkim računima te kako se ta integracija odražava na ukupnu sigurnost informacijskih sustava.

Kroz ovu studiju slučaja planiramo pridonijeti boljem razumijevanju izazova i rješenja u upravljanju korisničkim računima te pružiti korisne uvide i preporuke koje će biti od značaja za organizacije koje teže unapređenju upravljanja korisničkim računima.

8.1 Opis organizacije i konteksta

U studiji slučaja predstavljena je vojna organizacija koja je sama po sebi složen entitet posvećen zaštiti nacionalnih interesa i sigurnosti. Vojna organizacija obuhvaća raznoliku strukturu organiziranu prema jasnoj hijerarhiji koja uključuje stratešku, operativnu i taktičku razinu.

S obzirom na osjetljivost vojna organizacija postavlja visoke standarde u području kontrole pristupa podacima. Sigurnosni certifikati, stroge pristupne politike i redovite provjere sigurnosnih pravila čine temelj zaštite podataka.

Prema navedenom, ključne aspekte vojne organizacije možemo predstaviti kroz sljedeće kategorije:

- **Zaštita osjetljivih podataka** – Upravljanje korisničkim računima ključno je za osiguranje da pristup podacima imaju samo ovlašteni pojedinci. To je temeljna mjera u zaštiti nacionalnih sigurnosnih interesa.
- **Hijerarhijska struktura** – Vojna organizacija temeljena je na tradiciji vojnog sustava što se reflektira kroz precizan lanac zapovijedanja, u kojem svaki pripadnik obavlja određene dužnosti unutar jasno definiranje hijerarhije.
- **Prilagodba na promjene** – Pri razvoju okvira potrebno je uzeti u obzir dinamičnost vojnih operacija i potrebu za brzom prilagodbom pristupa resursima tijekom kriznih situacija. Visoka razina fleksibilnosti je ključna u osiguravanju učinkovitog upravljanja korisničkim računima u turbulentnim uvjetima.
- **Potreba za diskrecijom i tajnosti** – Učinkovito upravljanje korisničkim računima podrazumijeva da samo ovlaštene osobe imaju pristup osjetljivim operativnim podacima čime se osigurava sigurnost i povjerenje.
- **Standardizacija procesa** – Razvoj otvorenog okvira također mora adresirati potrebu za standardizacijom procesa stvaranja korisničkih računa i dodjeljivanja korisničkih uloga. Ovo je ključno za održavanje konzistentnosti i olakšavanje procesa administracije.

8.2 Prepoznavanje problema i izazova

U specifičnom kontekstu vojne organizacije upravljanje pravima pristupa podacima predstavlja kompleksan izazov s obzirom na zahtjeve vojne organizacije. Brojnost informacijskih sustava, raznolikost zadataka, hijerarhijska struktura te potreba za održavanjem visokih standarda sigurnosti čine upravljanje pravima pristupa ključnim aspektom operativne efikasnosti. Izazovi u ovom području utječu na aspekte sigurnosti podataka, ali i na funkcionalnost sustava i operativne sposobnosti vojnih snaga. Izazovi se ogledaju u potrebi za brzom prilagodbom kao i administraciji korisničkih računa. Ovi izazovi zahtijevaju tehnološke inovacije kao i prilagođavanje organizacijskih procesa kako bi se učinkovito upravljalo korisničkim računima unutar vojnog konteksta.

8.3 Metodologija

U procesu istraživanja i razvoja otvorenog okvira primijenjen je raznolik set metoda u prikupljanju podataka kako bi se dobile dubinske informacije i stvorila jasnu slika o trenutačnom stanju. Za razumijevanje cjelovite slike potrebno je kombinirati nekoliko pristupa. Kombinacijom kvantitativnih i kvalitativnih pristupa te uzimajući u obzir perspektive svih dionika nastoje se prepoznati ključne točke poboljšanja te utvrditi smjernice za razvoj okvira. Korišteni pristupi su:

- **Intervjui** – Pri razgovoru s relevantnim stručnjacima, administratorima sustava i korisnicima unutar OSRH prikupljeni su podaci o iskustvima, izazovima i potrebama u vezi upravljanja pravima pristupa podacima.
- **Analiza dokumenata** – Sustavni pregled relevantnih pisanih materijala kako bi se stekao dublji uvid u politike, procedure, smjernice i postojeće dokumente koji se odnose na upravljanje korisničkim računima.
- **Tehnička analiza sustava** – Evaluacija tehničkih rješenja, infrastrukture, sigurnosnih mehanizama te performansi sustava koji podržava upravljanje pravima pristupa podacima.
- **Radionice** – Organizirane radionice sa svim relevantnim dionicima unutar OSRH s ciljem dobivanja stručnog mišljenja i prijedloga.
- **SWOT analiza** – Analiza snaga, slabosti, prilika i prijetnji u vezi s trenutačnim sustavom upravljanja korisničkim računima. Cilj SWOT analize bio je identifikacija ključnih točki koje treba poboljšati.

8.4 Analiza podataka

U ovom poglavlju dana je analiza prikupljenih podataka temeljem metoda navedenih u prethodnom poglavlju. Analiza će biti provedena iz nekoliko perspektiva kako bi se dobila cjelovita slika stanja upravljanja korisničkim računima potrebna za studiju slučaja.

Analiza rezultata intervjua – Rezultati analize intervjua usmjereni su prema dobivanju uvida u stavove i iskustva sudionika istražujući ključne teme, stavove te prijedloge za unaprjeđenje sustava. Kroz odgovore sudionika uočeni su ponavljajući obrasci mišljenja. Kroz intervjue identificirani su operativni izazovi kao i tehnološke potrebe i očekivanja korisnika što je značajno doprinijelo u dobivanju cjelovite slike korisničkih potreba.

Nadalje prepoznati su izazovi u prilagodbi specifičnim zahtjevima organizacije kao i činjenica da su sudionici predstavili odgovore i preporuke kako odgovoriti na prepoznate izazove.

Analiza dokumenata – Analiza dokumenata značajno je doprinijela u procesu oblikovanja otvorenog okvira za upravljanje korisničkim računima. Proučavanje postojećih internih dokumenata omogućilo nam je bolje razumijevanje trenutačnih praksi u organizaciji. U slučajevima gdje su dokumenti bili nepotpuni ili nedostajali, proaktivno su stvorene nove smjernice posebno orijentirane na standardizaciju procesa definiranja korisničkih prava i uloga, odobrenja korisničkih računa i revizije korisničkih prava. Ova inicijativa bila je od velike važnosti za popunjavanje praznina u sustavu upravljanja korisničkim računima. Cilj procesa analize dokumenata bio je osiguravanje da dokumentacija bude precizna i primjenjiva čime se postigla veća operativna učinkovitost i sigurnost u upravljanju korisničkim računima.

Tehnička analiza sustava – U tehničkoj analizi sustava kao ključni element prepoznat je Oracle DBMS što značajno utječe na procjenu cjelokupne arhitekture sustava za upravljanje korisničkim računima. Oracle DBMS omogućava centralizirano pohranjivanje i upravljanje korisničkim podacima, ulogama i privilegijama. Ključni aspekti koji su istaknuti u analizi Oracle DBMS su:

- **Podaci o korisnicima i ulogama** – Oracle DBMS omogućuje definiranje i pohranjivanje informacija o korisnicima uključujući njihove uloge i privilegija unutar baze podataka. To pruža čvrst temelj za kontrolu pristupa podacima na razini baze podataka.
- **RBAC model** – Oracle DBMS podržava RBAC model koji je ključan za strukturiranje i kontrolu pristupa na temelju uloga. Ovo olakšava definiranje i dodjelu prava korisnicima putem njihovih uloga.

- **Sigurnosne značajke** – Oracle DBMS nudi napredne sigurnosne značajke kao što su enkripcija podataka koristeći AES, TDES i SHA-1 algoritme te praćenje i nadzor korisnika Ovi elementi pridonose ukupnom očuvanju integriteta i povjerljivosti podataka [19].
- **Učinkovitost i skalabilnost** – Kroz tehničku analizu obuhvaćeno je i mjerenje performansi Oracle DBMS uključujući procjenu brzine upita, odziva sustava i sposobnosti skaliranja. Podaci dobiveni mjerenjem performansi izravno utječu na odluku da li sustav može zadovoljiti zahtjeve organizacije bez obzira na njezinu veličinu i kompleksnost.

SWOT analiza

Analiza podataka temeljem SWOT analize (tablica 3) pruža uvid u snažne strane, slabosti, prilike i prijetnje s kojima se organizacija susreće. SWOT analiza pruža dublji uvid u njihovu trenutačnu poziciju pomažući im prepoznati resurse koje mogu iskoristiti, izazove koje treba riješiti te prilike koje mogu odgovoriti. U kontekstu upravljanja korisničkim računima, predmetna analiza pomaže pri prepoznavanju ključnih aspekata koji utječu na učinkovitost, sigurnost i funkcionalnost sustava.

Analiza istražuje snage i slabosti postojećeg sustava za upravljanje korisničkim računima kao i prilike i prijetnje koje mogu utjecati na daljnje unapređenje. Razumijevanje ovih čimbenika ključno je za donošenje ispravnih odluka i oblikovanje strategija koje će omogućiti organizaciji pri maksimiziranju potencijala i umanjenju rizika.

Snage	Slabosti
- **Jasna struktura upravljanja pristupom:** Postojeći RBAC model pruža čvrstu strukturu za dodjelu i upravljanje pravima pristupa temeljenim na ulogama, što pojednostavljuje administraciju sustava. - **Smanjenje rizika zloupotrebe:** Precizna dodjela ovlasti putem uloga smanjuje rizik od zloupotrebe pristupa podacima. - **Fleksibilnost i prilagodljivost:** Model omogućuje prilagodbu uloga prema organizacijskim promjenama ili novim poslovnim zahtjevima.	- **Poteškoće u preciznom podešavanju pristupa:** RBAC može pružiti ograničenu fleksibilnost u preciznom podešavanju pristupa pojedinačnih korisnika, što može biti izazov u situacijama gdje je potrebna detaljna kontrola. - **Kompleksnost upravljanja velikim brojem uloga:** U organizacijama s velikim brojem uloga upravljanje može postati složeno i zahtjevno. - **Pitanje pristranosti uloga:** Postoji rizik od pristranosti pri dodjeli uloga, gdje neki korisnici mogu imati više ovlasti nego što im je stvarno potrebno.
Prilike	**Prijetnje**
- **Integracija s naprednim tehnologijama:** RBAC model može iskoristiti prednosti integracije s naprednim tehnologijama poput biometrije ili analize ponašanja za dodatno jačanje sigurnosti. - **Automatizacija procesa dodjele uloga:** Automatizacija procesa dodjele uloga može povećati učinkovitost i smanjiti moguće ljudske pogreške. - **Prilagodba modela različitim industrijskim standardima:** Prilagodba RBAC modela prema različitim industrijskim standardima može poboljšati interoperabilnost i usklađenost s regulativama.	- **Nedostatak jasne standardizacije:** RBAC implementacija može stvoriti izazove u kompatibilnosti između različitih sustava. - **Napredne tehnike napada:** Evolucija naprednih tehnika napada može izazvati sigurnosne prijetnje RBAC modelu, posebno ako nije stalno ažuriran i nadograđen. - **Ovisnost o ulogama:** Ako se nepravilno dodijele uloge ili ne postoji sustav za njihovo redovito ažuriranje, može doći do ozbiljnih rizika i praznina u sigurnosti.

Tablica 3: SWOT analiza organizacije (Izvor: autorov doprinos)

8.5 Ispitivanje rješenja

U ovom poglavlju predstavljeno je ispitivanje otvorenog okvira za upravljanje korisničkim računima prilagođeno prepoznatim organizacijskim potrebama OSRH. Ova faza predstavlja srž analize gdje se razvijeni otvoreni okvir testira kako bi se procijenila njegova funkcionalnost, performanse i usklađenost sa stvarnim organizacijskim potrebama. U sklopu studije slučaja, rješenje za upravljanje korisničkim računima u OSRH kroz otvoreni okvir temelji se na nizu komponenti i pristupa.

RBAC model

Implementiran je model kontrole pristupa podacima temeljen na ulogama (RBAC). Ovaj model pruža jasnu strukturu uloga i njihovih ovlasti čime se olakšava dodjela pristupa korisnicima prema njihovim zadacima i odgovornostima.

Administratorsko sučelje

Administratori imaju središnje administratorsko sučelje koji omogućuje pregled i upravljanje svim korisničkim računima. Mogućnosti uključuju stvaranje novih korisničkih računa, dodjelu uloga i reviziju pristupa.

Definicija uloga i pravila

Administratori imaju mogućnost definiranja različitih uloga u skladu s organizacijskim potrebama. Svaka uloga ima jasno definirane ovlasti i pravo pristupa prema specifičnostima zadatka.

Integracija s Oracle DBMS

Okvir se temelji na Oracle DBMS što omogućuje učinkovito upravljanje bazom podataka i kontrolu pristupa podacima. Administracija korisničkih računa uključuje upravljanje pravima pristupa podacima unutar baze podataka.

Sigurnosne politike

Sigurnosne politike predstavljaju važan element upravljanja sigurnošću u okviru sustava za upravljanje korisničkim računima. Cilj sigurnosnih politika je osigurati integritet, povjerljivost i dostupnost sustava čime se smanjuje rizik od neovlaštenih pristupa i povećava razina zaštite osjetljivih podataka.

8.6 Prikaz rješenja

Proces kontrole pristupa podacima (slika 4) može se jasno prikazati kroz business process model (BPM) dijagram gdje svaki korak predstavlja određenu aktivnost, a poveznice između njih označavaju tok procesa. Kroz ovakav model lakše je razumjeti i poboljšati proces kontrole pristupa podacima.

Koraci uključeni u model procesa su sljedeći:

1. Korisnik inicira proces pokušajem spajanja na neki od postojećih sustava ili spajanjem na bazu podataka koristeći neki od softvera treće strane za pristup bazi podataka.

2. Korisnik je u oba slučaja dužan unijeti korisničko ime i zaporku.

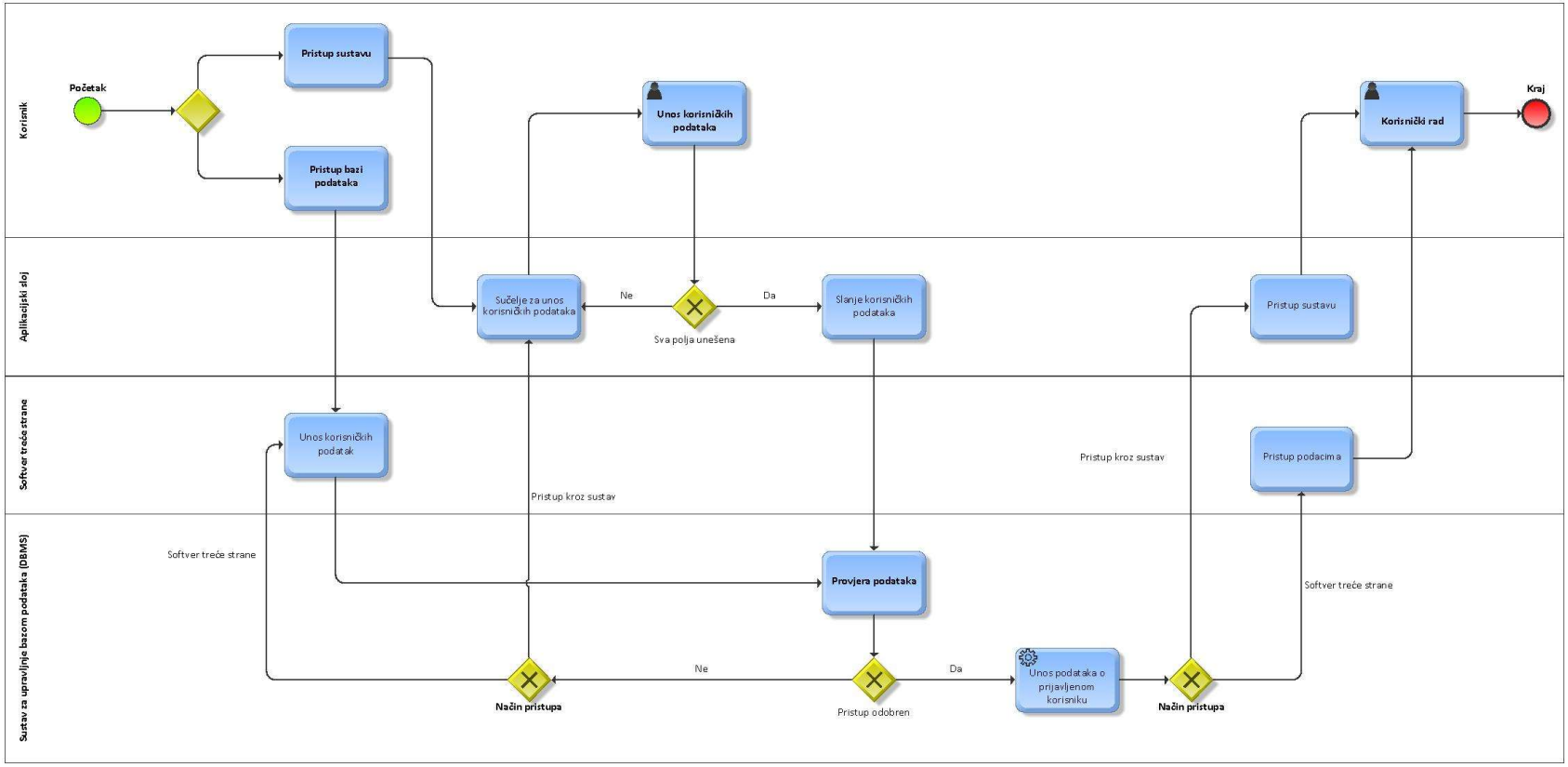
3. Mehanizam unutar Oracle DBMS sustava provjerava korisničko ime i zaporku te jedinstveni identifikator klijenta odnosno sučelja s kojim se korisnik pokušava prijaviti.

4. Ovisno o rezultatu provjere korisničkih podataka mehanizam odobrava ili ne odobrava prijava u sustav.

5. Ako je pristup odobren, okidač na bazi podataka uz osnovne podatke koji se zapisuju implicitno (DBMS automatski upisuje osnovne podatke i prijavi), zapisuje dodatne podatke definirane sigurnosnim politikama.

6. Nakon odobrenja pristupa korisnik ima pravo rada u sustavu i/ili s podacima preko softvera treće strane.

7. Ako pristup nije odobren, korisnik dobiva poruku od sustava i vraća se na početni zaslon za unos korisničkog imena i zaporke.



Slika 4: Proces kontrole pristupa podacima (Izvor: autorov doprinos)

8.7 Prednosti i ograničenja

Implementacijom otvorenog okvira za upravljanje korisničkim računima organizacija se susreće s nizom pozitivnih ishoda, ali isto tako i s određenim izazovima. Kroz analizu prednosti i ograničenja utvrđenih kroz studiju slučaja ovo poglavlje pruža pregled konkretnih dobiti i potencijalnih prepreka koje je potrebno savladati kako bi se osiguralo učinkovito upravljanje korisničkim računima.

Prednosti

- Precizna dodjela prava – Studija slučaja potvrđuje da otvoreni okvir omogućava preciznu dodjelu pristupnih prava korisnicima temeljem njihovih uloga smanjujući rizik od prekomjernih ovlasti.
- Implementacijom otvorenog okvira organizacijama je omogućen jasan uvid u strukturu resursa putem definiranih korisničkih uloga.
- Jednostavnije upravljanje korisničkim računima – Administracija korisničkih računa postaje jednostavnija jer se dodjela i upravljanje pristupnih prava obavlja kroz dodjelu uloga i korisničko sučelje što olakšava rad administratora.
- Smanjeni rizik od neovlaštenog pristupa – Primjenom otvorenog okvira za upravljanje korisničkim računima smanjuje se rizik od neovlaštenog pristupa ograničavajući pristup samo onim resursima koji su nužni za obavljanje zadaća.
- Povećana razina sigurnosti – Razina sigurnosti je povećana jer korisnici nemaju nepotrebne ovlasti.
- Prilagodljivost – Mogućnost prilagodbe korisničkih uloga i korisničkih prava omogućava organizacijama brzu prilagodbu prema novonastalim zahtjevima čime se osigurava agilnost sustava.

Ograničenja

- Složenost inicijalne implementacije – Inicijalna implementacija otvorenog okvira zahtijeva određeno vrijeme i resurse zbog potrebe za jasnim definiranjem svih dionika procesa te uloga i prava.
- Teškoće u dinamičnom okruženju – U okruženju gdje su promjene stalne, upravljanje ulogama može biti izazovno, posebice ako nema jasnih smjernica za upravljanje promjenama.
- Ovisnost o edukaciji korisnika – Učinkovitost okvira direktno je ovisna o činjenici koliko dobro svi dionici razumiju svoje uloge i odgovornosti što može zahtijevati dodatne edukacijske napore.

9. Testiranje okvira

Proces testiranja i validacije osigurava da sustav zadovoljava postavljene zahtjeve i da pruža očekivane funkcionalnosti te da je siguran i pouzdan. U ovom poglavlju predstavljena je strategija testiranja, vrste testiranja te načini validacije s ciljem osiguravanja optimalnog funkcioniranja razvijenog okvira.

Strategija testiranja predstavlja plan koji se koristi za provođenje testiranja kako bi se osigurala kvaliteta sustava. Ova strategija uključuje planiranje, organizaciju, izvođenje i analizu testiranja kako bi se prepoznale greške, osigurala funkcionalnost i zadovoljili korisnički zahtjevi.

Ciljevi strategije testiranja otvorenog okvira bili su:

- Rano otkrivanje grešaka
- Osiguravanje kvalitete sustava
- Optimizacija resursa

9.1 Funkcionalno testiranje

Ova vrsta testiranja usmjerena je na provjeru ispravnosti funkcionalnosti definiranih unutar okvira. Ova vrsta testiranja usmjerena je na provođenje testova koji procjenjuju je li sustav u skladu s funkcionalnim zahtjevima i specifikacijama.

Funkcionalno testiranje bilo je usmjereno na sljedeće aspekte:

- **Autentifikacija i autorizacija:** Testiranje je obuhvaćalo ispravnost procesa autentifikacije odnosno provjeru korisničkih pristupnih podataka. Uz navedeno testiran je i proces autorizacije kroz provjeru korisničkih privilegija.
- **Upravljanje korisničkim računima:** Funkcionalnosti poput kreiranja, uređivanja i brisanja korisničkih računa i dodjeljivanja uloga testirane su kako bi se osigurala njihova točnost i djelotvornost.
- **Upravljanje korisničkim ulogama:** Testirana je ispravnost dodjele i upravljanja korisničkim ulogama. Ovo uključuje provjeru da li korisnici s određenim ulogama imaju pravo pristupa samo određenim resursima.

- **Sigurnosne politike:** Testirana je primjena sigurnosnih politika uključujući složenost lozinki, istek lozinki, zaključavanje korisničkih računa nakon neuspješne prijave te druge sigurnosne mehanizme.
- **Integracija:** Cilj testiranja integracije bio je usmjeren na provjeru i komunikaciju s internim sigurnosnim mehanizmima Oracle DBMS.
- **Praćenje aktivnosti korisnika:** Testirana je ispravnost funkcionalnosti povezanih s evidencijom događaja i praćenjem aktivnosti korisnika za potrebe revizije i sigurnosne analize.
- **Prilagodljivost:** Testirana je sposobnost okvira za prilagodbu promjenama u zahtjevima uključujući mogućnost dodavanja novih funkcionalnosti.

10. Analiza rezultata

U ovom poglavlju predstavljena je analiza rezultata funkcionalnog testiranja kao i analiza podataka dobivenih iz ostalih izvora. Poglavlje je strukturirano kako bi pružilo jasan uvid u rezultate funkcionalnog testiranja i analizu podataka iz različitih izvora. Rezultati testiranja temelj su za donošenje zaključaka i preporuka.

10.1 Rezultati funkcionalnog testiranja

Funkcionalno testiranje pruža detaljan uvid u ispravnost i preciznost funkcionalnosti otvorenog okvira za upravljanje korisničkim računima. Predstavljena analiza rezultata opisuje aspekte funkcionalnog testiranja i pruža uvid u performanse sustava.

1. **Autentifikacija i autorizacija** – Testovi autentifikacije pokazali su točnost u verifikaciji identiteta korisnika. Sustav je prepoznao korisničke podatka dok su testovi autorizacije potvrdili ispravno primjenjivanje RBAC modela. Različite korisničke uloge jasno su definirale i osigurale potrebnu razinu prava pristupa resursima.
2. **Upravljanje korisnicima** – Funkcionalnost upravljanja korisnicima kao što su dodavanje, brisanje i promjena korisničkih podataka prošla je testiranje bez uočenih problema.
3. **Iznimke** – U testiranju robusnosti sustava primijenjen je scenarij iznimki. Različite situacije kao što je neuspjela autentifikacija ili promjena uloga iskorištene su u svrhu provjere sposobnosti sustava da se nosi s nepredviđenim situacijama. Rezultati su potvrdili da sustav uspješno upravlja iznimkama osiguravajući stabilnost.
4. **Usklađenost sa specifikacijama** – Rezultati funkcionalnog testiranja upućuju kako je sustav usklađen sa specifikacijama definiranim u zahtjevima sustava. Sustav posjeduje očekivane funkcionalnosti i ispunjava postavljene ciljeve čime je potvrđena uspješnost implementacije.
5. **Povezanost s RBAC modelom** – Rezultati funkcionalnog testiranja potvrdili su preciznost pri dodjeli prava pristupa prema korisničkim ulogama osiguravajući da svaki korisnik posjeduje odgovarajući pristup resursima sukladno svojim ovlastima.

10.2 Analiza podataka iz ostalih izvora

Prikupljeni podaci iz različitih izvora dodatno pridonose analizi rezultata. U ovom slučaju ankete su omogućile prikupljanje korisničkih iskustava i mišljenja, radionice su pružile direktnu povratnu informaciju, a tehnička analiza pomogla je pri prepoznavanju mogućih tehničkih izazova i prednosti predloženog okvira.

Prikazani rezultati zajedno čine temelj za dublje razumijevanje kako predloženi okvir utječe na procese i pruža učinkovito upravljanje korisničkim računima. Provođenjem temeljite analize moguće je prepoznati prostor za potencijalna poboljšanja i/ili prilagodbe kako bi okvir bio bolje prilagođen specifičnim potrebama organizacije.

11. Rasprava o učinkovitosti i primjenjivosti predloženog okvira

Rasprava o rezultatima istraživanja i učinkovitosti predloženog okvira nužna je za razumijevanje dubljeg konteksta i donošenja zaključaka. U ovom poglavlju predstavljeni su ključni aspekti učinkovitosti, primjenjivosti i doprinosima u području kontrole pristupa podacima.

11.1 Učinkovitost predloženog okvira

Analiza rezultata testiranja upućuje na visoku učinkovitost okvira u upravljanju korisničkim računima i pravima pristupa podacima. Mogućnost brzog odgovora pri dodjeljivanju uloga, autentifikaciju i autorizaciju korisnika doprinosi visokoj učinkovitosti. Nadalje, uspješna komunikacija aplikacijskog sloja i sloja baze podataka pokazala se stabilnom što upućuje na pouzdanost sustava.

11.2 Primjenjivost u stvarnom okruženju

Stvarna primjenjivost okvira evaluirana je kroz analizu rezultata dobivenih iz stvarnog korištenja u simuliranoj organizaciji. Povratne informacije iz radionica i anketa pridonose razumijevanju integracije okvira s postojećim operativnim procesima. Prepoznate prednosti i izazovi ukazuju na sposobnost okvira pri mogućnosti zadovoljenja specifičnih potreba organizacije.

11.3 Doprinosi u području kontrole prava pristupa podacima

Predloženi okvir značajno doprinosi u području kontrole pristupa podacima. Kroz temeljitu analizu, prepoznati su modeli koji su poslužili kao temelj za organizacije sličnih potreba. Proširenje sustava temeljenog na ulogama (RBAC) pokazala se kao učinkovita metoda upravljanja pravima pristupa pružajući organizacijama alat za preciznu kontrolu korisničkih računa.

11.4 Učinkovita kontrola prava pristupa

Proširenje modela temeljenog na ulogama (RBAC) unutar okvira omogućava organizacijama preciznu kontrolu nad pravima pristupa podacima. Kroz standardizaciju dodjele uloga, osigurava se da korisnici imaju samo ona prava koja su nužna za obavljanje njihovih specifičnih poslovnih zadataka. Predloženi pristup smanjuje rizik od zlouporabe i neovlaštenog pristupa osjetljivim podacima.

11.5 Fleksibilnost i prilagodljivost sustava

Jedna od ključnih prednosti predloženog okvira jest njegova sposobnost prilagodbe različitim organizacijskim potrebama. Kroz temeljitu analizu uloga i prava, okvir omogućuje organizacijama definiranje vlastitih pravila pristupa podacima. Ova prilagodljivost ključna je za organizacije koje se suočavaju s dinamičnim okruženjem i promjenjivim zahtjevima.

11.6 Transparentnost i praćenje prava pristupa

Implementacija sustava za praćenje prava pristupa omogućuje organizacijama da održavaju transparentnost u korištenju podataka. Pomoću detaljnog praćenja aktivnosti korisnika, administratori mogu pratiti tko, kada i kako pristupa određenim informacijama. Ova transparentnost pridonosi ukupnoj sigurnosti sustava i olakšava reviziju pristupa u skladu s regulatornim zahtjevima.

11.7 Doprinosi poboljšanoj sigurnosti sustava

Kroz implementaciju pristupa temeljenog na ulogama, okvir znatno poboljšava sigurnost sustava. Smanjenjem broja korisnika s visokim privilegijama na sustavu i preciznom kontrolom pristupa, organizacija smanjuje rizik od sigurnosnih prijetnji i zloupotrebe. Osim toga, sustavno praćenje aktivnosti korisnika pomaže u ranom prepoznavanju potencijalnih sigurnosnih incidenata.

11.8 Kontinuirano unapređenje kroz reviziju i prilagodbe

Važno je napomenuti da predloženi okvir ne završava implementacijom, već podrazumijeva kontinuirano praćenje, reviziju i prilagodbe. Aktivnosti revizije doprinose kontinuiranom unapređenju sustava kako bi se održala visoka razina učinkovitosti i zadovoljile promjenjive potrebe organizacije.

12. Zaključak

U radu je predstavljen razvoj otvorenog okvira za upravljanje korisničkim računima s fokusom na Oracle DBMS. Motivacija za razvoj otvorenog okvira proizlazila je iz prepoznatih izazova i ograničenja u postojećem modelu kontrole pristupa podacima temeljenog na ulogama u relacijskoj bazi podataka.

Rezultati analize postojećeg stanja ukazivali su na potrebu za cjelovitim i naprednijim rješenjem u odnosu na generički model unutar samog Oracle DBMS-a. Otvoreni okvir za upravljanje korisničkim računima, osim programskog dijela, uključuje i standardizaciju procesa razrade korisničkih uloga, administraciju korisničkih računa kao i proces revizije korisničkih računa.

Cilj rada bio je definirati, implementirati i testirati predmetni okvir koji omogućava preciznu kontrolu nad korisničkim pristupom i ovlastima. Sustavni pristup istraživanju očituje se kroz analize postojećih modela, razradu teorijskih osnova te implementaciju otvorenog okvira.
Rezultati funkcionalnog testiranja potvrdili su stabilnost i funkcionalnost okvira pružajući osnove za daljnji razvoj. Objedinjavanje podataka iz različitih izvora dodatno je obogatila perspektivu čime je omogućeno razumijevanje stvarnih potreba korisnika i organizacije.

Studija slučaja predstavlja konkretan prikaz implementacije razvijenog okvira pružajući dublje razumijevanje samog dizajna i arhitekture. Kroz analizu rezultata testiranja otvorenog okvira zaključeno je kako okvir doprinosi unapređenju kontrole pristupa podacima unutar relacijske baze podataka. U okviru studije slučaja razvijeni okvir uspješno je implementiran uzimajući u obzir stvarne potrebe organizacije kao i sigurnosne standarde. Kroz implementaciju okvira stvorena je prilika za testiranje i procjenu učinkovitosti okvira u stvarnom okruženju. Proces implementacije obuhvatio je prilagodbu okvira specifičnostima organizacije što je rezultiralo učinkovitim sustavom za kontrolu pristupa podacima i upravljanje korisničkim računima.

Daljnji koraci trebaju biti usmjereni prema kontinuiranom poboljšanju okvira, uzimajući u obzir povratne informacije korisnika, izazove u dinamičnom okruženju i evoluciju tehnologije. Cilj je stvoriti okvir koji će zadovoljiti rastuće zahtjeve organizacija za učinkovitom i sigurnom kontrolom korisničkih računa u Oracle DBMS.

Popis literature

[1] „Što je to informacijska sigurnost? | Ured Vijeća za nacionalnu sigurnost“. Pristupljeno: 31. listopad 2023. [Na internetu]. Dostupno na: https://www.uvns.hr/hr/sto-je-to-informacijska-sigurnost

[2] „Informacijska sigurnost - Consilium“. Pristupljeno: 31. listopad 2023. [Na internetu]. Dostupno na: https://www.consilium.europa.eu/hr/general-secretariat/corporate-policies/classified-information/information-assurance/

[3] „Zakon o informacijskoj sigurnosti“. Pristupljeno: 31. listopad 2023. [Na internetu]. Dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2007_07_79_2484.html

[4] W. C. Barker, „Guideline for identifying an information system as a national security system“, 2003, doi: 10.6028/NIST.SP.800-59.

[5] „What is Data Access? | Glossary | HPE ASIA_PAC“. Pristupljeno: 31. listopad 2023. [Na internetu]. Dostupno na: https://www.hpe.com/asia_pac/en/what-is/data-access.html

[6] T. Pavić i L. Jelenković, „Autentifikacija i autorizacija korisnika na jednom mjestu“.

[7] C. M. Gutierrez i W. Jeffrey, „FIPS PUB 200 Minimum Security Requirements for Federal Information and Information Systems“, 2006.

[8] E. Barker i W. C. Barker, „Recommendation for key management“:, Gaithersburg, MD, svi. 2019. doi: 10.6028/NIST.SP.800-57pt2r1.

[9] M. Scholl, K. Stine, K. Lin, i D. Steinberg, „Security architecture design process for health information exchanges (HIEs)“, 2010, doi: 10.6028/NIST.IR.7497.

[10] E. Barker, „Guideline for using cryptographic standards in the federal government“:, ožu. 2020, doi: 10.6028/NIST.SP.800-175BR1.

[11] „Cyber security trends 2023 | Allianz Commercial“. Pristupljeno: 01. prosinac 2023. [Na internetu]. Dostupno na: https://commercial.allianz.com/news-and-insights/reports/cyber-security-trends-2023.html

[12] B. W. Lampson, „Dynamic protection structures“, u *Proceedings of the November 18-20, 1969, fall joint computer conference on - AFIPS ’69 (Fall)*, New York, New York, USA: ACM Press, 1969, str. 27. doi: 10.1145/1478559.1478563.

[13] L. D. Elliott Bell i J. LaPadula, *Secure Computer Systems: A Mathematical Model*. Bedford: Defense Technical Information Center, 1973.

[14] K. Biba, „Integrity Considerations for Secure Computer Sytems“, Hanscom AFB, tra. 1977.

[15] D. of Defense, „Trusted Computer System Evaluation Criteria ["Orange Book"]“, 1985.

[16] Carnet CERT & LS&S, „Modeli kontrole pristupa“, velj. 2008. Pristupljeno: 07. prosinac 2023. [Na internetu]. Dostupno na: www.lss.hr

[17] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, i C. E. Youman, „Computer role-based access control models“, *Computer (Long Beach Calif)*, sv. 29, izd. 2, str. 38–47, velj. 1996, doi: 10.1109/2.485845.

[18] V. C. Hu *i ostali*, „NIST Special Publication 800-162 Guide to Attribute Based Access Control (ABAC) Definition and Considerations“, doi: 10.6028/NIST.SP.800-162.

[19] „Encryption and Redaction in Oracle Database 12c with Oracle Advanced Security“, 2017.

[20] M. Penelova, „Access Control Models“, *Cybernetics and Information Technologies*, sv. 21, izd. 4, str. 77–104, pros. 2021, doi: 10.2478/cait-2021-0044.

[21] M. Calvo i M. Beltrán, „A Model For risk-Based adaptive security controls“, *Comput Secur*, sv. 115, tra. 2022, doi: 10.1016/j.cose.2022.102612.

[22] W. Huijie, „A Security Framework for Database Auditing System“, u *Proceedings - 2017 10th International Symposium on Computational Intelligence and Design, ISCID 2017*, Institute of Electrical and Electronics Engineers Inc., srp. 2017, str. 350–353. doi: 10.1109/ISCID.2017.64.

[21] M. Calvo and M. Beltrán, “A Model For risk-Based adaptive security controls,” Comput Secur, vol. 115, 2022, doi: 10.1016/j.cose.2022.102612.

[22] F. Jaidi, F. Ayachi, and A. Bouhoula, “Advanced analysis of the integrity of access control policies: The specific case of databases,” International Arab Journal of Information Technology, vol. 17, no.5, pp. 808–815, 2020, doi: 10.34028/iajit/17/5/14.

[23] A. Suganthy and V. Prasanna Venkatesan, “An Introspective Study on Dynamic Role-Centric RBAC Models; An Introspective Study on Dynamic Role-Centric RBAC Models,” 2019.

[24] M. Toapanta, J. Nazareno, R. Tingo, F. Mendoza, A. Orizaga, and E. Mafla, “Analysis of the Appropriate Security Models to Apply in a Distributed Architecture,” in IOP Conference Series: Materials Science and Engineering, Institute of Physics Publishing, Nov. 2018. doi: 10.1088/1757-899X/423/1/012165.

[25] S. Nafisah Roslan, I. A. Rahmi Hamid, and P. Shamala, “E-Store Management Using Bell-LaPadula Access Control Security Model.”

[26] I. Indu, P. M. R. Anand, and V. Bhaskar, “Identity and access management in cloud environment: Mechanisms and challenges,” Engineering Science and Technology, an International Journal, vol. 21, no. 4. Elsevier B.V., pp. 574–588, 2018. doi: 10.1016/j.jestch.2018.05.010.

[27] Voitovych O., Kupershtein L., Lukichov V., and Mikityuk I., “Multilayer Access for Database Protection,” 2018.

[28] C. Bakir and M. Guclu, “Multi-Level Security Model Developed to Provide Data Privacy in Distributed Database Systems,” Tehnicki Vjesnik, vol. 29, no. 2, pp. 369–378, 2022, doi: 10.17559/TV-20200516084319.

[29] M. Fareed and A. A. Yassin, “Privacy-preserving multi-factor authentication and role-based access control scheme for the E-healthcare system,” Bulletin of Electrical Engineering and Informatics, vol. 11, no. 4, pp. 2131–2141, 2022, doi: 10.11591/eei.v11i4.3658.

[30] W. Huijie, “A Security Framework for Database Auditing System,” in Proceedings - 2017 10th International Symposium on Computational Intelligence and Design, ISCID 2017, Institute of Electrical and Electronics Engineers Inc., 2017, pp. 350–353. doi: 10.1109/ISCID.2017.64.

[31] L. Shan, H. Zhou, D. Hong, Q. Dong, Y. Wang, and S. Song, “Application of access control model for confidential data,” in Procedia Computer Science, Elsevier B.V., 2021, pp. 3865–3874. doi: 10.1016/j.procs.2021.09.161.74

[32] C. Bakir and V. Hakkoymaz, “Classifying database users for intrusion prediction and detection in data security,” Tehnicki Vjesnik, vol. 27, no. 6, pp. 1857–1862, 2020, doi: 10.17559/TV-20190710100638.

[33] Z. Yang and K. Levchenko, “Securing Web Applications with Predicate Access Control,” pp. 541–554, 2017, doi: 10.1007/978-3-319-61176-1_30ï.

[34] H. Alsobhi and R. Alshareef, “SQL Injection Countermeasures Methods,” in 2020 International Conference on Computing and Information Technology, ICCIT 2020, Institute of Electrical and Electronics Engineers Inc., 2020. doi: 10.1109/ICCIT-144147971.2020.9213748.

[35] M. Muntean and L. Dijmarescu, “Sustainable implementation of access control,” Sustainability (Switzerland), vol. 10, no. 6, 2018, doi: 10.3390/su10061808.

Popis slika

Popis tablica

ŽIVOTOPIS PRISTUPNIKA/PRISTUPNICE:	
Obrazovanje (kronološki od novijeg prema starijem datumu):	- Diplomski studij, smjer Poslovna informatika, Ekonomski fakultet u Osijeku, Sveučilište J.J. Strossmayera u Osijeku - Razlikovna godina, smjer Poslovna informatika, Ekonomski fakultet u Osijeku, Sveučilište J.J. Strossmayera u Osijeku - Stručni studij Primjena informacijske tehnologije u poslovanju, Fakultet organizacije i informatike, Sveučilište u Zagrebu - Sredna strukovna škola „Braća Radić“, Đakovo - Osnovna škola „Vladimir Nazor, Đakovo
Radno iskustvo (kronološki od novijeg prema starijem datumu):	2008 – danas, Ministarstvo obrane RH
Popis radova pristupnika/pristupnice (ako ih je bilo)	/