UNIVERZITET CRNE GORE

Prirodno-matematički fakultet Podgorica

Vijeću Prirodno-matematičkog fakulteta

IZVJEŠTAJ KOMISIJE O PODOBNOSTI TEME MAGISTARSKOG RADA KANDIDATKINJE DRAGICE KALEZIĆ

Vijeće Prirodno-matematičkog fakulteta na sjednici održanoj 15.02.2022. imenovalo je mentora i Komisiju za ocjenu podobnosti teme za izradu magistarskog rada pod nazivom "Primjena enkripcije zasnovane na atributima kod prenosa i čuvanja podataka u cloud sistemima", kandidatkinje Dragice Kalezić, u sastavu:

dr Vladimir Božović, redovni profesor – mentor;

dr Aleksandar Popović, vanredni profesor – član i

dr Milenko Mosurović, redovni profesor – član.

Nakon uvida u podneseni materijal, a u vezi sa članom 24 Pravila studiranja na postdiplomskim studijama, podnosimo sljedeći

IZVJEŠTAJ

Dragica Kalezić, specijalista matematike i računarskih nauka, prijavila je temu magistarskog rada pod nazivom "Primjena enkripcije zasnovane na atributima kod prenosa i čuvanja podataka u cloud sistemima". Tema spada u oblast matematike i računarskih nauka za koju je matičan Prirodno-matematički fakultet. Dokumenta podnesena za prijavu teme sadrže: biografiju kandidatkinje, naziv i kratku razradu teme, kao i kratko obrazloženje predmeta istraživanja i strukture rada.

Podaci o kandidatkinji

Dragica Kalezić je rođena 08. 12. 1990. godine u Podgorici. Završila je osnovnu školu "Vuk Karadžić" u Podgorici sa odličnim uspjehom, a zatim srednju elektrotehničku školu "Vaso Aligrudić" kao đak generacije i dobitnik diplome Luča. Završila je specijalističke

studije odsjek Matematika i računarske nauke Prirodno-matematičkog fakulteta Univerziteta Crne Gore 2016. godine. Nakon završenih specijalističkih studija, nastavila je sa praktičnim usavršavanjem u Čikomu, gdje je i danas zaposlena kao implementator softverskih rješenja. U septembru 2016. godine upisala je magistarske studije odsjek za Matematiku i računarske nauke Prirodno-matematičkog fakulteta. U periodu od septembra 2016. do oktobra 2018. položila je sve ispite predviđene programom studija.

Aktuelnost teme

Enkripcija zasnovana na atributima je relativno nov pristup u okviru koncepta kriptografije javnog ključa. Kod tradicionalne kriptografije javnim ključem poruka se kriptuje za odgovarajućeg primaoca pomoću njegovog javnog ključa. Enkripcija zasnovana na atributima ima široku praktičnu primjenu u slučajevima kada korisnici žele da primijene "finu" kontrolu pristupa podacima.

Ovo bi u konkretnom slučaju značilo da u jednoj kompaniji možemo imati finu kontrolu pristupa, recimo, EDMS aplikaciji po pojedinim ulogama u sistemu u zavisnosti od definisanih uloga zaposlenih.

Na taj način administratori aplikacije definišu uloge ostalih korisnika u sistemu, dodaju novu strukturu organizacije po organizacionim cjelinama, definišu radne tokove dokumentacije i pripadajuće životne cikluse, kao i njihova stanja prema funkcionalnim zahtjevima korisnika, grupišu korisnike u sistemu prema ulogama koje imaju, itd. Korisnici sistema imaju uvid u odgovarajuće module i funkcionalnosti aplikacije prema ulogama koje im je dodijelio administrator. Obrađivači dokumenata - referenti - podgrupa grupe korisnici koja ima mogućnost manipulacije dokumentima kao što je dodavanje novih dokumenata u već kreirane predmete (koje su zaveli korisnici koji imaju ulogu pisarnice ukoliko samom referentu nije omogućeno kreiranje predmeta kroz aplikaciju), slanje istih nadređenim na odobravanje i elektronsko potpisivanje i na kraju, kada je proces obrade dokumentacije završen, slanje dokumenta pisarnici na otpremanje stranci. Rukovodioci - podgrupa grupe korisnici koja vrši dodjelu predmeta u rad svojim referentima, odobravanje dokumentacije i elektronsko potpisivanje iste, po potrebi kreiranje svoje dokumentacije, itd.

Takođe, kod aplikacija u kojima se elektronski čuvaju medicinski podaci definišu se uloge na osnovu kojih određeni korisnici mogu pristupati odgovarajućim podacima u zavisnosti od svoje uloge u medicinskoj ustanovi (dr. biohemije će imati pristup samo analizama koje je on obradio, ali ne i analizama koje su odradile njegove kolege, dijagnozama određenog pacijenta će imati pristup samo njegov izabrani specijalista, itd.).

Prethodna dva primjera pripadaju RBAC (eng. Role-Based Access Control) modelu, koji za sada ima primat iako u velikim kompanijama nije praktičan kao rješenje zbog kreiranja velikog broja uloga koje je kasnije teško održavati.

Sa druge strane, kod ABAC (eng. Attribute-Based Access Control) modela, administratori mogu definisati, poboljšavati i uvoditi mnogo drugih varijabli, osiguravajući na taj način visok stepen kontrole, ali ukoliko jednom dođe do pogrešne administracije jako je teško ili u nekim slučajevima nemoguće izmijeniti definisane varijable.

Primjer ABAC modela predstavlja "data lake" sistem podataka. Naime, kompanije čuvaju sve vrste podataka u klasterima podataka i na taj način ih čine dostupnim različitim stranama kojima su ti podaci potrebni, koji se, između ostalog, koriste i za poslovnu analitiku.

ABE omogućava da se klaster podataka učini dostupnim zaposlenima kojima je potreban pristup, istovremeno štiteći osjetljive informacije (npr. podatke o platama i informacije o klijentima) na način što imamo kontrolu pristupa podacima na nivou sloja podataka (za razliku od prethodno opisanog modela gdje smo imali kontrolu pristupa na nivou uloga).

Prema projekcijama stručnjaka, očekivalo se da će do 2020. godine oko 70% kompanija širom svijeta korisititi kontrolu pristupa zasnovanu na atributima ABAC kao dominantni mehanizam u zaštiti kritičnih resursa. Uporedna prognoza data je u odnosu na stanje iz 2014. godine gdje je manje od 5% svjetskih kompanija koristilo ABAC mehanizam, kada se i počelo sa njegovom komercijalnom primjenom. Međutim, još uvijek ABAC pristup nije preuzeo primat od RBAC rješenja. Kao jedan od glavnih razloga sporog uvođenja ABAC standarda navodi se nepostojanje dobre dokumentacije sa studijama slučaja o tome koji su benefiti prelaska na ABAC rješenja u kompanijama. Nadalje, same organizacije se i uobičajeno opiru promjenama u postojećoj infrastrukturi, koje su uslovljene i promjenama regulativa, kojma je opet potrebno dodatno vrijeme za usvajanje. Za rezultat imamo da nije dovoljno da praktična i inovativna rješenja kontrole pristupa zadovoljavaju samo tehničke preduslove, već da ona imaju za cilj rješavanje problema iz realnog okruženja sa što manje promjena u operativnim procedurama institucija kod kojih će biti implementirana.

Koncept kontrole pristupa baziran na atributima (ABAC) postoji već dugi niz godina i on predstavlja tačku u prostoru logičke kontrole pristupa koja uključuje polise za kontrolu pristupa, kontrolu pristupa baziranu na rolama i ABAC metodu za pružanje pristupa na bazi procjene atributa. Tradicionalno, kontrola pristupa bazira se na identitetu korisnika koji traži izvršavanje određene operacije na objektu, poput prava upisa podataka u datoteku, bilo direktno, bilo putem unaprijed definisanih vrsta atributa, kao što su role ili grupe koje su dodijeljene tom korisniku. U praksi je primijećeno da je ovaj pristup

kontrole pristupa često glomazan za upravljanje, s obzirom na potrebu povezivanja korisnika sa odgovarajućim rolama ili grupama. Takođe je primijećeno da kvalifikatori identiteta, grupa i rola podnosioca zahtjeva često nisu dovoljni za izražavanje polise kontrole pristupa u stvarnom svijetu. Alternativa je odobravanje ili odbijanje korisničkih zahtjeva na bazi proizvoljnih atributa korisnika i proizvoljnih atributa objekta, te uslova okruženja koji mogu biti globalno priznati i relevantniji za dotična pravila, što predstavlja osnovu ABAC pristupa.

Danas, skladištenje podataka u cloud sistemima dobija sve više na značaju budući da korisnicima nudi resurse kvalitetnih performansi bez dodatnih ulaganja u skupu opremu. Međutim, sa druge strane, skladištenje podataka na cloud serverima korisnike dovodi do problema sa privatnošću i kontrolom pristupa istim. Tradicionalne tehnike kriptovanja koje nude simetrična i asimetrična kriptografija nisu pogodne za obezbjeđivanje kontrole pristupa usljed nedostatka fleksibilnosti i granuslisane kontrole pristupa. Jedna od istaknutih kriptografskih tehnika čiji su glavni ciljevi obezbjeđivanje privatnosti i granulirana kontrola pristupa kod skladištenja podataka u cloud sistemu jeste enkripcija zasnovana na atributima (ABE).

Cilj, struktura i metodologija rada

Cilj ovog rada je da pokaže svrsishodnost upotrebe ABAC modela kroz konkretnu implementaciju ABE kod autorizacije korisnika na sistem za dijeljenje podataka i regulisanje pristupa odgovarajućim grupama datoteka, koristeći komponente otvorenog koda na virtuelnim mašinama u cloud sistemu (AWS u konkretnoj implementaciji).

S obzirom da ovaj rad tretira pitanje primjene ABE enkripcije kod prenosa i čuvanja podataka u cloud sistemima, na početku je dat pregled postojećih ABE rješenja, sa posebnim osvrtom na njihovu konstrukciju (koristeći matematički aparat), evaluaciju performansi i odgovarajući sigurnosni model za svaki od njih ponaosob. U nastavku, u cilju demonstracije ABE mehanizma za autorizaciju, korišćena je OpenABE kriptografska biblioteka otvorenog koda, gdje je, koristeći CP-ABE i KP-ABE enkripciju testirana autorizacija korisnika sa atributima baziranim na LDAP (eng, Lightweight Directory Access Protocol) protokolu. Korisnički podaci su skladišteni po direkturijumima web servera i shodno prethodno definisanim pristupnim polisama, određeni tip kornisnika čiji atributi odgovaraju listi atributa iz pristupne polise, mogu pristupiti odgovarajućim direktorijumima sa podacima. Autenitakcija na web server definisana je klasičnom upotrebom korisničkih imena i lozinki. Obje komponte, Web i LDAP server instalirane su na dvije EC2 (eng. Elastic Cloud Computing) instance sa Amazon Linux 2 operativnim sistemom u AWS cloud-u kroz odgovarajuće alate otvorenog koda. Kao web server korišćen je Apache web server, dok je za LDAP server korišćeno OpenLDAP rješenje. Takođe, u drugom dijelu demonstracije, testirane su mogućnosti dekripcije podataka kriptovanih uz pomoć ABE, u slučajevima kada korisnički atributi sa

LDAP servera odgovaraju atributima korišćenim prilikom enkripcije dokumenata. U toku implementacije koristila se kombinacija različitih tipova atributa, počevši od tekstualnih, preko brojčanih, do datumskih, kako bi se što vjerodostojnije simulirali korisnički slučajevi iz realne prakse. Na kraju, izvršena je i evaluacija efikasnosti OpenABE kriptografske biblioteke u vidu svojevrsnog benchmark testa u odnosu na različiti broj atributa i iteracija, kao i u odnosu na ponuđene tipove enkripcije koju ova bilblioteka otvorenog koda podržava.

Objedinjavanjem prikaza ABE kriptografskih šema je na jednom mjestu dat sveobuhvatni rezime aktuelnih postignuća iz domena enkripcije bazirane na atributima. Pregledom primjera iz prakse, dat je presjek postojeće primjene ABE enkripcije kod IoT (eng. Internet of Things) uređaja, cloud computing sistema, mrežama za autonomnu vožnju i blockchain transakcija. U sopstvenoj implementaciji OpenABE kriptografske biblioteke otovrenog koda, potvrđena je zaštićenost kontrole pristupa i integriteta podataka u odnosu na predloženi dizajn pristupnih polisa. Istovjetni rezultati su postignuti koristeći sva tri tipa ponuđenih kriptografskih opcija CP-ABE, KP-ABE i PKE (eng. Public Key Encryption), kao i koristeći različite kombinacije atributa koji mogu biti tekstualnog, brojčanog ili datumskog tipa. Kao jedan od glavnih doprinosa ovog rada, data je mogućnost da se predloženi sistem inkorporira kod web i desktop aplikacija čija se autentikacija bazira na LDAP protokolu, koji je dominantni mehanizam autentikacije i autorizacije u korporativnom svijetu.

Sama inkorporacija OpenABE biblioteke sa OpenLDAP i Web serverima, daće smjernice za korišćenje ABE enkripcije u postojećim aplikacijama otvorenog koda za dijeljenje dokumenata između registrovanih korisnika. Na kraju, sa sprovedenom procjenom efikasnosti OpenABE kriptografske biblioteke (kompletiranjem benchmark testova), potvrđena je svrsishodnost ideje o uključenju ovog alata kod rješenja za zaštitu dokumenata u cloud sistemima.

Rad se sastoji od sljedećih cjelina: Uvod, Osnove enkripcije bazirane na atributima, Detaljni pregled različitih vrsta enkripcije bazirane na atributima, Praktične primjene enkripcije bazirane na atributima (ABE), Prijedlog ABE rješenja za zaštitu podataka zasnovanog na OpenABE biblioteci otvorenog koda, Implementacija predloženog rješenja u AWS cloud-u sa prikazom performansi i efikasnosti zaštite podataka i Zaključak.

Zaključak

Na osnovu prethodno izloženog smatramo da predložena tema magistarskog rada kandidatkinje Dragice Kalezić ispunjava sve uslove predviđene Pravilima studiranja na postdiplomskim studijama, propisanim od strane Senata Univerziteta Crne Gore.

Komisija predlaže Vijeću Prirodno-matematičkog fakulteta da kandidatkinji Dragici Kalezić odobri izradu magistarskog rada pod nazivom "Primjena enkripcije zasnovane na atributima kod prenosa i čuvanja podataka u cloud sistemima".

U Podgorici, 6. 3. 2022.

KOMISIJA

dr Vladimir Božović, redovni profesor PMF-a – mentor;

dr Aleksandar Popović, vanredni profesor PMF-a – član i

dr Milenko Mosurović, redovni profesor PMF-a – član.