Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 007:004.056
DOI: https://doi.org/10.24867/20BE10Ilic

IMPLEMENTACIJA INFORMACIONE BEZBEDNOSTI AKVIZICIONO-UPRAVLJAČKIH SISTEMA NA *CLOUD*-U

IMPLEMENTATION OF THE INFORMATION SECURITY OF A SCADA SYSTEM ON THE CLOUD

Nemanja Ilić, *Fakultet tehničkih nauka, Novi Sad*

Oblast – PRIMENJENO SOFTVERSKO INŽENJERSTVO

Kratak sadržaj – *U ovom radu je detaljno opisan podsistem za autentifikaciju i autorizaciju korisnika kako u tradicionalnom, tako i u Cloud okruženju. Za ove potrebe, razvijene su dve aplikacije koje simuliraju procese akviziciono-upravljačkih sistema i detaljno su opisani koraci koje je potrebno preduzeti kako bi se migriralo sa tradicionalnog okruženja na Cloud okruženje. Potreba za prelaskom sa tradicionalnog okruženja na Cloud okruženje se javlja iz činjenice da Cloud okruženje pruža brojne prednosti po pitanju performansi* [1]*, ali i zbog lakoće implementacije sigurnosnih aspekata u već postojeća rešenja što je i demonstrirano u ovom radu.*

Ključne reči: *Informaciona bezbednost, AUS, Cloud, autentifikacija, autorizacija*

Abstract – *This paper describes the user authentication and authorization subsystem in detail in the traditional as well as in the Cloud environment. For these demonstration purposes, two applications that simulate the processes of a SCADA system have been developed and steps that need to be taken have been described in great detail in order to migrate from the traditional to the Cloud environment. The need for moving to the Cloud environment from the traditional one arises from the fact that the Cloud environment offers numerous advantages in terms of performance* [1]*, but also because of the ease of implementation of the security aspects into existing solutions which is demonstrated in this paper.*

Keywords: *Information security, SCADA, Cloud computing, authentication, authorization*

1. UVOD

Objekti kritične infrastrukture predstavljaju objekte koji su od visokog značaja za normalno funkcionisanje jedne države. U ovakve objekte se nabrajaju telekomunikacioni objekti, objekti za proizvodnju i prenos električne energije, objekti za skladištenje, transport i preradu nafte, gasa i drugih derivata, objekti za vodosnabdevanje, saobraćajna infrastruktura (putevi i signalizacija), objekti vitalnih državnih institucija (bolnice, generalštab, televizije, itd.).

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Srđan Vukmirović, red. prof.

Kritične infrastrukture kao što je elektrodistribucija su uvek u potencijalnoj opasnosti od zlonamernih softverskih napada.

Neadekvatnom zaštitom elektrodistribucione infrastrukture omogućeni su napadi kao što su Black Energy [2] i napad na kompaniju Telvent [3].

Iz ova dva napada moguće je uočiti da su pouzdana identifikacija, autentifikacija i autorizacija prvi i ključni korak pri izbegavanju zloupotrebe softverskih rešenja, što je od posebno visoke važnosti u industrijskim sistemima i objektima kritične infrastrukture.

2. TEORIJSKE OSNOVE

Informacija predstavlja određeno znanje koje je moguće preneti ili primiti kao podatak, a vezano je za određenu činjenicu ili okolnost. Informacioni sistem predstavlja skup komponenti koje se nekada nazivaju i resursi, a one su: hardver, softver, podaci, komunikaciona mreža, ljudski resursi i procedure. Svi ovi resursi omogućavaju informacionom sistemu da vrše prikupljanje, obradu, prenos i skladištenje informacija [4].

U današnje vreme, *informaciona bezbednost* [5] se uglavnom zasniva na uspešnoj implementaciji tzv. CIA trijade (eng. *Confidentiality-Integrity-Availability*), kao i na osiguranju neporicivosti i autentičnosti podataka. Ovo se postiže implementacijom bezbednosnih mehanizama koji trebaju da budu unapred određeni, konstantno nadgledani i u skladu sa tim poboljšavani.

Cilj informacione bezbednosti je da se u najvećoj meri smanje ili u koliko je moguće, eliminišu u potpunosti bezbednosni rizici kako bi se smanjila mogućnost za potencijalni napad, ali i da se obezbede mehanizmi za detekciju i oporavak od eventualnih napada.

Akviziciono-upravljački sistem, odnosno SCADA je sistem za prikupljanje mernih vrednosti uređaja na terenu, ali isto tako i za slanje upravljačkih zahteva uređajima kojima se može upravljati. Dve glavne osobine koje svaki SCADA sistem mora prvenstveno da ispuni jesu dugovečnost i stabilnost u radu. Na žalost, usled potrebe da ova dva zahteva budu ispunjena, ovi sistemi kao posledicu imaju sporo prihvatanje novih tehnologija i nadogradnje njihovog sistema, ali i primene novih bezbednosnih mehanizama jer uvek postoji mogućnost da svaka izmena učini sistem nestabilnim i nepouzdanim. Iz tog razloga, nadogradnja se vrši tek nakon detaljnih testiranja što u većini slučajeva zahteva dosta vremena.

2.1. Cloud računarstvo

Cloud računarstvo predstavlja isporuku računarskih servisa kao što su računari, skladište, mreže i softver putem interneta. Po načinu fizičke realizacije, *Cloud* rešenja je moguće podeliti ga na tri tipa: Javni (*eng. public*), privatni (*eng. private*) i hibridni (*eng. hybrid*) *Cloud*.

Javnim *Cloud*-om upravljaju takozvani *Cloud* provajderi. *Cloud* provajderi su treća lica koja pružaju računarske resurse poput servera i skladišta putem interneta i sav hardver, softver i propratna infrastruktura je u njihovom vlasništvu. Sam klijent datim servisima pristupa, koristeći svoj nalog, putem web pretraživača. Jedan primer ovakvog tipa javnog *Cloud*-a je Microsoft Azure.

Nasuprot javnom *Cloud*-u je privatni *Cloud* kod kojeg se svi resursi *Cloud* računarstva koriste isključivo od strane jedne kompanije ili organizacije. Glavna stvar koja razgraničava privatni *Cloud* od javnog *Cloud*-a je činjenica da se u privatnom *Cloud*-u servisi i infrastruktura održavaju na privatnoj mreži.

Između privatnog i javnog *Cloud*-a se nalazi hibridni *Cloud* koji kombinuje prednosti javnog i privatnog *Cloud*-a tako što omogućuje kompanijama da privatne podatke drže na privatnoj infrastrukturi i mreži, ali i da imaju pristup svoj računarskoj snazi i skalabilnosti koje omogućava javni *Cloud*. Ovo je omogućeno razmenom poruka između javnog i privatnog *Cloud*-a što omogućava aplikacijama da sarađuju kao kompaktna celina.

3. AKTUELNO STANJE U OBLASTI

Imajući u vidu da je oblast istraživanja ovog master rada u preseku tri različite oblasti – *Cloud* računarstvo, informaciona bezbednost i upravljanje akviziciono upravljačkim sistemima, konkretno sistemima upravljanja elektro distributivnih sistema, potrebno je uzeti u obzir da već postoji veliki broj naučnih radova i istraživanja koji se detaljno bave delovima ovih oblasti.

3.1. Prednosti *Cloud* računarstva

Ideja o mogućnosti skaliranja softverskog rešenja na naizgled neograničen broj resursa zarad poboljšanja performansi aplikacije i po potrebi smanjenje broja resursa zarad smanjenja troškova u trenutcima kada više nisu potrebni predstavlja jedno od glavnih motivacija za razvoj *Cloud* aplikacija kada se govori o javnom *Cloud*-u [6].

Pouzdanost i visoka dostupnost su takođe veoma primamljivi argumenti za prelazak na *Cloud* računarstvo jer o ova dva faktora brinu sami pružaoci usluge *Cloud* računarstva. Moderni pružaoci usluga *Cloud* računarstva dostupnost i pouzdanost rešavaju činjenicom da imaju centre podataka na nekoliko različitih fizičkih lokacija. Ukoliko bi došlo do prekida rada nekog od centra podataka, mehanizmi replikacije podataka i oporavka od otkaza omogućavaju minimalan zastoj rada aplikacije i konstantan integritet podataka. [6].

3.2. Primene *Cloud* računarstva u elektroenergetici

Veliki broj radova je razmatrao ideju o povezivanju tehnologija *Cloud* računarstva sa elementima upravljanja elektroenergetskom, odnosno elektrodistributivnom mrežom. Kao što je obrazloženo u radu [1], primena praktičnog rešenja u produkciji nailazi na izazove usled bezbednosnih, a prvenstveno zakonskih ograničenja usled kojih je u nekim zemljama zabranjeno čuvanje poverljivih informacija i.e. informacija o korisnicima van geografskih granica država u kojima se usluga pruža [7]. Postoji indikacija da će ovaj nedostatak biti prevaziđen u slučaju saradnji nekih od zemalja u skorijoj budućnosti [8] [9], međutim, izazov predstavlja činjenica da su regulacije specifične za svaku zemlju sveta i podložne određenim izmenama tako da je pitanje regulacije zakona o deljenju poverljivih podataka sa drugim zemljama aktuelna tema kod svih softverskih proizvoda koji se razvijaju za *Cloud* okruženje.

3.3. Bezbednosni aspekti *Cloud* računarstva

U radu [10] dat je detaljan pregled velikog broja potencijalnih bezbednosnih pretnji za *Cloud* rešenja, vektore napada, kao i potencijalne preventivne mere koje je moguće preduzeti kako bi se suzbio rizik od napada, dok je u radu [11] dat prikaz izazova implementacije bezbednosnih aspekata *Cloud* računarstva kod kritičnih infrastruktura i donosi zaključak da je neophodno razvijanje pouzdanog sistema za pristup servisima, kao i razvijanje pouzdanog modela kontrole pristupa.

4. KORIŠĆENE TEHNOLOGIJE

Kerberos [12] predstavlja protokol za autentifikaciju i autorizaciju klijent-server aplikacija razvijen od strane MIT-a, a sada se koristi u Microsoft rešenjima, prvenstveno u Windows-u. On omogućava single sign-on čime se omogućava da se korisnik samo jednom prijavi, a potom, u skladu sa svojim pravima, ima pristup svim resursima na mreži.

Ukoliko bi neka aplikacija želela da iskoristi podatke sa nekog drugog web servisa i pri tom se predstavila kao određeni korisnik kako bi uradila nešto na tom servisu umesto korisnika, aplikacija bi tražila od korisnika da im daju svoje kredencijale kako bi se ulogovali kao oni i odradili posao koji imaju. Ovo predstavlja problem delegirane autorizacije. Ovaj problem je rešen uvođenjem OAuth i kasnije OAuth 2.0 protokola, specijalno osmišljenih za tu svrhu.

Kako je postajao zastupljeniji i kako su se potreba za novim slučajevima upotrebe pojavljivala, OAuth 2.0 protokol je počeo da se koristi za šta nije bio namenjen, između ostalog i za autentifikaciju, a za to nije postojala nikakva standardizacija protokola. Iz ove potrebe, smišljen je *OpenID Connect* protokol koji predstavlja ekstenziju OAuth 2.0 protokola sa standardizovanom autentifikacijom.

5. IMPLEMENTACIJA PREDLOŽENOG REŠENJA

Kako bi se demonstrirao proces prelaska sa *on premise* rešenja na *Cloud* bazirano rešenje inicijalna ideja je bila razviti WCF aplikaciju koja simulira procese akviziciono upravljačkog sistema (AUS) kod koje je autentifikacija i autorizacija implementirana putem Active Directory-a, odnosno korišćenjem Kerberos protokola. Nakon uspešne implementacije, planirano je istu aplikaciju prilagoditi tako da koristi OAuth i OpenID Connect umesto Kerberos

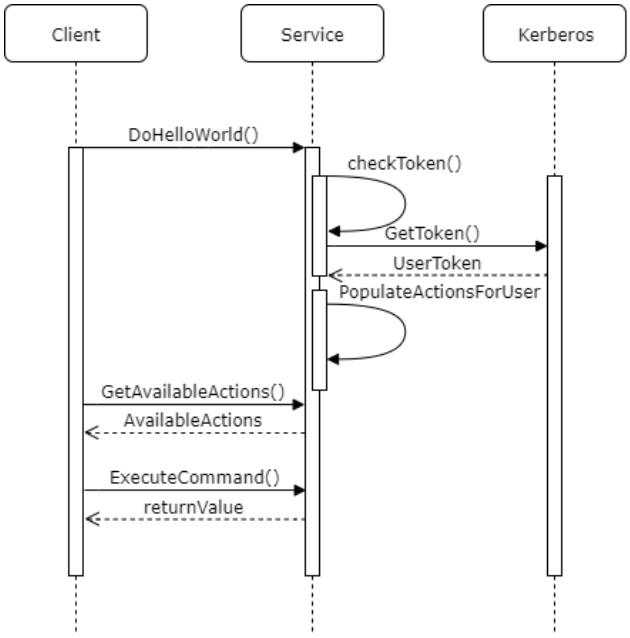
protokola. Na žalost, ovaj pristup nije imao trivijalno rešenje, te je razvijena još jedna, ASP.NET Core aplikacija, kako bi se uspešno implementirao OAuth i OpenID Connect protokol radi autentifikacije i autorizacije.

5.1. WCF aplikacija

Kako bi WCF aplikacija bila u mogućnosti da iskoristi pogodnosti koje pruža Active Directory, a to se prvenstveno odnosi na autentifikaciju, neophodno je da implementira IIdentity interfejs i njega je neophodno pozvati pri prvoj komunikaciji aplikacije sa servisom. Ukoliko se koristi odgovarajući komunikacioni protokol, o implementaciji ovog interfejsa vodi računa sama tehnologija.

Nakon toga, moguće je koristiti klasu ServiceSecurityContext.Current.PrimaryIdentity u kojoj se nalaze svi neophodni parametri potrebni za uspešnu autentifikaciju.

Autentifikaciju je neophodno proveriti pri prvoj komunikaciji klijenta sa servisom. U demonstrativnoj aplikaciji, to se vrši u metodi DoHelloWorld() koju poziva klijent. To je ujedno i jedina metoda koju neautentifikovani klijent može da pozove, a da mu se vrati neki odgovor. Grafički prikaz toka komunikacije ilustruje Slika 1. Ukoliko bi se pozvala bilo koja od druge dve otvoreno dostupne metode klijenta, koje se vide na dijagramu klasa, dobio bi prazan odgovor jer klijent nije autentifikovan.



Slika 1: *Dijagram sekvenci* NSZUR-a

U zavisnosti od toga koja prava korisnik ima, klijentu će biti vraćene različite funkcije koje može i sme da izvrši čime se ostvaruje implementacija RBAC-a.

5.2. ASP.NET Core aplikacija

Nakon implementacije Kerberos i on premise AD autentifikacije, naredan logičan korak je implementacija Azure AD i OpenID Connect autentifikacije. Azure AD [13] predstavlja Azure-ovu SaaS implementaciju Active Directory-a koja se koristi pri *Cloud* aplikacijama. Intenzivnim istraživanjem, ustanovljeno je da WCF ne podržava mogućnost implementacije korišćenja Azure AD umesto on premisse Active Directory-a [14].

Ovo znači da bi deo aplikacije koji predstavlja servis, morao biti napisan kao web aplikacija, odnosno web servis. ASP.NET Core je izabran kao najpogodniji kandidat za korišćenu tehnologiju iz razloga što je neophodno koristiti distribuirano rešenje, a Web aplikacije su po definiciji distribuirane i stoga se izbor sveo na tu tehnologiju.

Prelazak na novu tehnologiju i to konkretno prelazak sa WCF na ASP.NET Core znači da se sama aplikacija fundamentalno menja. Najveća promena je ta što se više između servisa i klijenta ne šalju SOAP poruke već RESTful poruke. Zbog jednostavnosti implementacije, ovo je kao posledicu donelo to da se za razmenu poruka više ne koristi TCP protokol već HTTPS.

Autentifikacija se u ASP.NET Core realizuje anotacijama nad metodama kontrolera ili Razor Pages *code behind*-a.

Kod MVC (eng. *Model View Controller*) pristupa, autentifikacija se realizuje anotacijama iznad metoda nad kojim postoji potreba da se primeni. Anotacije od interesa za autentifikaciju su: [Authorize] i [AllowAnonymous]. *Authorize* označava da metodu anotiranu ovom anotacijom može isključivo da poziva korisnik koji je autorizovan tj. onaj koji se uspešno predstavio sistemu. Metode anotirane *AllowAnonymous* može da poziva bilo koji korisnik, bilo da je on autentifikovan ili ne i svakoj metodi je ovo podrazumevano ponašanje.

Pri korišćenju *Razor Pages* tehnologije za prikaz sadržaja, gubi se MVC metodologija i više nije moguće primeniti anotacije na kontroler. U ovom slučaju se anotacije primenjuju na *OnGet* i *OnPost* metode klase koja predstavlja model te stranice.

Trebalo bi primetiti da je glavna razlika između dva prethodno navedena pristupa u tome što jedan kontroler može da opslužuje mnoštvo stranica dok jedan model u *Razor Pages* odgovara samo jednoj stranici. Stoga je mnogo lakše obezbediti servis ukoliko se realizuje kao MVC jer jedna anotacija na početku klase obezbeđuje čitav kontroler, a samim tim i sve stranice koje se oslanjaju na taj kontroler dok je kod *Razor Pages* pristupa moguće da se zaboravi anotacija kod nekog od modela čime se ostavlja ta putanja i akcija nezaštićena.

Aplikacija pisana za demonstraciju rešenja je implementirana MVC pristupom.

5.3. Grupe

Često pri korišćenju aplikacije, nije dovoljan samo podatak da li je korisnik autentifikovan ili ne, već je važno znati i koja prava konkretan korisnik ima jer je moguće da aplikacija jednim korisnicima prikazuje jedan interfejs, a drugim korisnicima drugi. Ovo je moguće implementirati korišćenjem Azure AD grupa. Da bi se ovo implementiralo, neophodno je naravno da AD ima definisane grupe i korisnike koje pripadaju određenim grupama.

Grupe treba da budu tipa „Security Group“. Kako bi se grupa mogla koristiti u aplikaciji za autorizaciju, neophodno je najpre registrovati grupu u aplikaciji nakon čega je moguće koristiti je u anotacijama za autorizaciju uz pomoć anotacije [Authorize("NazivGrupe")].

Manipulacija prikaza u odnosu na grupu nije toliko očigledna za implementirati i zahteva da se napravi „helper“ klasa koja bi iz podataka o korisniku koji su stigli sa tokenom (OpenID Connect), ustanovila kojoj grupi trenutni korisnik pripada.

6. ZAKLJUČAK

U radu je predstavljen samo inicijalni pristup problemu autentifikacije i autorizacije, odnosno dokaz o mogućnosti implementacije i zbog toga uvek ima mogućnosti da se unapredi i treba da služi samo kao početna tačka, a ne kao finalni proizvod.

U trenutnoj implementaciji koristeći Azure Active Directory, za implementaciju RBAC-a su korišćene Azure Active Directory grupe koje su fabrički podržane za ovu ulogu na servisu, odnosnu na back end-u. Poteškoće nastaju kada se javi potreba da se različit sadržaj prikazuje određenim korisnicima u zavisnosti od toga kojoj grupi pripadaju. Ovaj izazov se rešava korišćenjem helper klase koja povezuje OBJECT ID od tražene grupe sa njenim imenom

Elegantnije rešenje za pristup ovom izazovu je korišćenje Microsoft Azure Active Directory role.

Konkretna metoda koja se za to koristi jeste Microsoft.AspNetCore.Identity.RoleManager koja ima već gotove metode za manipulaciju sa rolama.

Treba napomenuti da bi korišćenje rola za RBAC bilo poželjno samo za manipulaciju prikaza dok bi servise ipak trebalo obezbediti koristeći Azure Active Directory grupe jer je to preporučen način. Kao rešenje se nameće korišćenje kombinacije rola i grupa za najelegantniju implementaciju RBAC-a.

Iz ovoga se zaključuje da bi u najvećem broju slučajeva role i grupe bile identične, odnosno isti korisnici bi bili dodeljeni istim grupama i istim rolama. Takođe treba da se napomene da je ovim pristupom omogućena još fleksibilnija implementacija rešenja jer se omogućava da određeni korisnici pripadaju istoj grupi i da imaju ista prava pristupa ali da im u suštini nije potrebno prikazati neke delove NSZUR-a što se rolama upravo i omogućava jer dva korisnika mogu da pripadaju istoj grupi, a različitim rolama.

7. LITERATURA

[1] N. Popović, „Napredni distributivni menadžment sistem zasnovan na Cloud infrastrukturi,“ Fakultet tehničkih nauka, Novi Sad, 2018.

[2] O. Ashman and I. Damsky, "ThreatSTOP Report: BlackEnergy," THREATSTOPBME, 2016.

[3] F. Y. Rashid, "Telvent Hit by Sophisticated Cyber-Attack, SCADA Admin Tool Compromised," SecurityWeek, 26 September 2012. [Online]. Available: https://www.securityweek.com/telvent-hit-sophisticated-cyber-attack-scada-admin-tool-compromised. [Accessed 11 May 2022].

[4] K. Straub, "Information Security: Managing Risk with Defense in Depth," SANS Institute, 2003.

[5] M. E. Whitman and H. J. Mattord, Principles of Information Security, 4th ed., Boston: Course Technology, 2012.

[6] E. Bauer and R. Adams, Reliability and Availability of Cloud Computing, Hoboken, New Jersey: IEEE Press and John Wiley & Sons, Inc., 2012.

[7] J. Thornton, "matomo," 17 July 2020. [Online]. Available: https://matomo.org/blog/2020/07/storing-data-on-us-cloud-servers-dont-comply-with-gdpr/. [Accessed 15 May 2022].

[8] European Commission, "EU-US data transfers: How personal data transferred between the EU and US is protected.," European Commision, [Online]. Available: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en. [Accessed 15 May 2022].

[9] European Commission, "European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework," 25 March 2022. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087. [Accessed 15 May 2022].

[10] A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," *Journal of Network and Computer Applications*, vol. 79, pp. 88-115, 2017.

[11] Y. A. Younis, M. Merabti i K. Kifayat, „Secure Cloud Computing for Critical Infrastructure: A Survey,“ *The 14th Annual PostGraduate Symposium on The Convergence of Telecommunications, Networking and Broadcasting (PGNet 2013), Liverpool, UK*, pp. 1-6, 2012.

[12] J. G. Steiner, C. Neuman and J. I. Schiller, "Kerberos: An Authentication Service for Open Network Systems".

[13] Microsoft, "What is Azure Active Directory?," [Online]. Available: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis. [Accessed September 2019].

[14] "Azure Active Directory and WCF authentication," 14 November 2014. [Online]. Available: https://stackoverflow.com/questions/26930018/azure-active-directory-and-wcf-authentication. [Accessed April 2019].

Kratka biografija:

Nemanja Ilić rođen je u Novom Sadu 1993. god. Godine 2012. je završio Gimnaziju Jovan Jovanović Zmaj u Novom Sadu. Diplomirao je 2016. god. Na Fakultetu tehničkih nauka, odsek Elektrotehnika i računarstvo, smer Primenjene računarske nauke i informatika.