Različiti aspekti zaštite pristupa digitalizovanoj kulturnoj baštini

Narcis Behlilović [*], Pamela Begović [*], Saša Mrdović [*]
[*] Elektrotehnički fakultet u Sarajevu
E-mail: narcis.behlilovic@etf.unsa.ba; pamela.begovic@etf.unsa.ba; sasa.mrdovic@etf.unsa.ba

Abstract - *U ovom radu predstavljeni su različiti aspekti zaštite pristupa elementima digitalizovane kulturne baštine. U cilju identifikacije različitih scenarija za pohranu i prezentaciju digitalizovanih sadržaja, u radu je prezentovan sam koncept digitalizacije kulturne baštine, kroz prikaz elemenata baštine, opis važnosti postupka digitalizaije, te tehnološke korake procesa digitalizacije. U složenim informacionih sistemima, kakav je i sam sistem sa digitalizovanim sadržajima, od velike je važnosti jasno utvrditi scenarije za pohranu, prezentaciju i zaštitu sadržaja. U tom kontekstu, predložena su tri različita scenarija organizacije i prezentacije sadržaja, te za svaki od njih predstavljen koncept zaštite. U radu je detaljno razrađen koncept zaštite pristupa i integriteta podataka, za svaki od predloženih scenarija, u nadi da će predložena rješenja biti od koristi kulturno-historijskim institucijama, u neizbježnom procesu digitalizacije.*

Keywords - *digitalizacije kulturne baštine, pohrana sadržaja, prezentacija sadržaja, zaštita pristupa, zaštita integriteta podataka*

1. UVOD

Prateći intenzivne procese digitalizacije kulturne baštine u svijetu, a naročito u Evropi, može se uočiti da je u mnogim zemljama svijeta proces digitalizacije dijela kulturne baštine prepoznat kao važan cilj u ostvarivanju kulturne politike i kulturnog razvitka zemlje. Naime, izgradnja informacionog društva i usluga, naročito u području gospodarstva i javnih službi, u novije je vrijeme predmet mnogih zakonodavnih, normativnih i strategijskih inicijativa i dokumenata, pa je nesumnjivo da se s njima postepeno stvara novo okruženje i za kulturne djelatnosti.

Kada se govori o problematici digitalizacije kulturne baštine, ideja projekta je da se kulturni sadržaji, koji čine važan dio nacionalnog identiteta postepeno digitalizuju i posredstvom digitalnih biblioteka stave na uvid i upotrebu građanima, učenicima i studentima, kulturnim radnicima, umjetnicima i naučnicima, omogućavajući na taj način velikom broju zainteresiranih pristup i pretraživanje sadržaja kulturne baštine sa udaljenih lokacija te distribuciju i promociju kulturnih sadržaja u inostranstvo. U tom kontekstu potrebno je pokrenuti projekte digitalizacije najznačajnijih sadržaja kulturnog i nacionalnog blaga, te na temelju digitalizovanog materijala započeti sa stvaranjem digitalnih biblioteka.

Ovaj rad bavi se problematikom digitalizacije kulturne baštine, u prvom redu arhivske, bibliotečke i muzejske građe, naručito potencirajući problematiku njene zaštite. Organizovan je u dvije cjeline. Prva cjelina daje kratak uvid u elemente kulturne baštine, te koncept digitalizacije iste. Cilj ove cjeline je da ukratko identificira elemente kulturne baštine, ukaže na važnost i razloge za proces digitalizacije baštine, te približi i ukratko rezimira postupak digitalizacije arhivske, muzejske i bibliotečke građe, bez detaljne obrade svakog od nabrojanih segmenata postupka.

Druga cjelina rada se bavi pitanjem zaštite i sigurnosti sadržaja digitalizovane baštine. Naime, nakon digitalizacije, građa postaje datoteka na računaru, koju je potrebno zaštititi, kako od neovlaštenog pristupa, tako i od narušavanja njenog integriteta. Pri tome, pitanje zaštite sadržaja digitalizovane baštine tretira se slično pitanju zaštite bilo kojeg tipa datoteka u informacionim sistemima, zanemarujući u tom kontekstu sam sadržaj datoteke. Sam proces pohrane i prezentacije digitalizovane građe može biti organizovan na više načina, te se zaštita u različito organizovanim informacionim sistemima i različito tretira. U radu je predloženo nekoliko organizacija informacionog sistema sa pohranjenim digitalizovanim sadržajima, te predloženi i objašnjeni mehanizmi zaštite pristupa i integriteta podataka, za identificirane scenarije organizacije.

2. KONCEPT PROJEKTA DIGITALIZACIJE KULTURNE BAŠTINE

U posljednje dvije decenije se u potpunosti izmjenio koncept komuniciranja, informisanja, prenosa podataka i njihove pohrane. Računar i nove računarski bazirane tehnologije nametnule su se kao sastavni dio gotovo svakog segmenta u privatnom i poslovnom okruženju, što je odvelo ljudsku komunikaciju i potrebe u digitalni svijet. Ipak, nisu svi izvori po svojoj prirodi digitalni. Postoje brojni sadržaji, u vidu knjiga, časopisa, objekata itd. koji izvorno nisu u digitalnom obliku. U skladu sa nastalim trendovima, i te sadržaje postaje nužno prevesti u digitalni oblik.

U tom kontekstu javlja se potreba i za izmjenama u klasičnom pristupu kulturnoj baštini. Kulturna baština, u opštem slučaju obuhvata širok spektar materijalnog i nematerijalnog stvaralaštva, koji je u svojoj suštini jedan od temelja nacionalnih korijena i identiteta, te se sastoji od arhitektonskog naslijeđa, historijskih spomenika, pokretnih kulturnih dobara, u koja spadaju: marke, filmovi i filmski materijali, vrijedni predmeti stariji od 100 godina, rijetke zbirke i primjerci flore i faune, dijelovi spomenika, slike i crteži, etnološki materijal i dr. [1]. Dio tog stvaralaštva, koji je od interesa kada se govori o procesu izmjene klasičnog pristupa, i to po pitanju arhiviranja i distribucije sadržaja, predstavljaju knjige, uglavnom izrazite historijske vrijednosti, razne prepiske, časopisi i dokumenti od historijskog značaja za zemlju itd., koje je, u skladu sa dolazećim trendovima, potrebno digitalizirati. Pored toga, procesom je moguće obuhvatiti i fotografije arhitektonskog naslijeđa, spomenika i predmeta, odnosno elemenata koji nisu u papirnoj formi, a predstavljaju važne elemente baštine, koje je na neki način moguće prezentovati javnosti putem uobičajenih oblika digitalnog oglašavanja. Međutim, ovaj segment digitalizacije nije primarni predmet analize u ovom radu, čiji je fokus prvenstveno na zaštiti arhivske i bibliotečke građe.

Digitalizacija kulturne baštine, u opštem slučaju, predstavlja prenošenje arhivske, književne i muzejske građe u digitalni zapis prepoznatljiv računaru, u kojoj učestvuju relevantne institucije, kao što su državni arhiv, nacionalne i gradske biblioteke, muzeji, univerziteti itd. Digitalizacijom baštine omogućava se pristup jedinicama građe koje predstavljaju vrijedne i jedinstvene primjerke ne samo kulturne, nego i historijske i naučne baštine. Digitalizacija arhivske, bibliotečke i muzejske građe provodi se radi zaštite izvornika, povećanja dostupnosti i mogućnosti korištenja građe, radi stvaranja nove ponude, odnosno usluga korisnicima ili pak radi upotpunjavanja postojećega fonda. Svaki od navedenih ciljeva digitalizacije postavlja određene zahtjeve koje treba imati u vidu pri planiranju i izvođenju projekata digitalizacije. Vrlo je važno da projekti digitalizacije uoče te zahtjeve, procijene njihovu razmjernu težinu za pojedini projekt i jasno definišu čime, kako i u kojoj mjeri će njihov krajnji proizvod odgovoriti na pojedini zahtjev [2].

2.1. Razlozi za digitalizaciju kulturne baštine

Digitalizacija radi zaštite izvornika ima dva osnovna oblika. Umjesto samih izvornika na korištenje se mogu davati digitalne kopije, čime se izvornici čuvaju od mogućih oštećenja tokom korištenja, prenošenja, prevoza ili drugih postupaka. Pored toga, digitalne kopije se mogu koristiti i kao sigurnosne kopije koje u slučaju gubitka ili znatnijeg oštećenja izvornika mogu barem djelomično nadoknaditi tako nastao gubitak. U tu svrhu su se donedavno najčešće koristili mikrofilmovi, no posljednjih je godina uočljiv porast korištenja digitalizacije i u ovu svrhu. Taj je trend potpomognut razvojem tehnologije, koja pruža sve bolje mogućnosti za trajniju pohranu i zaštitu digitalnih sadržaja, padom troškova digitalizacije i čuvanja digitalnih sadržaja.

Da bi digitalizacija radi zaštite postigla svoju svrhu, nužno je da proizvedeni digitalni objekti dobro i kvalitetno predstavljaju izvornik, da ga mogu u dovoljnoj mjeri nadomjestiti te da su na primjeren način dostupni za korištenje. Ako su digitalne kopije takve da ne predstavljaju dobro u izvornik, ako nisu dostupne, ako je njihovo korištenje otežano ili nudi manjkave mogućnosti, ne može se reći da su primjereno postignuti ciljevi digitalizacije radi zaštite.

Ustanove koje građu digitaliziraju radi zaštite trebaju znati, odnosno jasno utvrditi koja obilježja moraju imati digitalne preslike i sustavi u kojima se nalaze i kako osigurati da obilježja budu prisutna, prepoznatljiva i očuvana. Pojedinačne digitalne kopije u pravilu čine dio određene digitalne zbirke i nalaze se u određenom informacionom sistemu koji omogućava upravljanje zbirkom i njenu dostupnost. Zato je važno da budu prepoznata relevantna tražena obilježja i digitalnih objekata i zbirki kojima pripadaju i informacionog sistema u kojem se nalaze [2].

Drugi česti razlog za digitalizaciju građe je poboljšanje njezine dostupnosti. Objavljivanjem digitalizovanog sadržaja putem Interneta, građa postaje dostupna na daljinu, bez obzira na to gdje se korisnik nalazi, i u vrijeme koje odgovara korisniku.

Dobro osmišljen sistem za pristup digitalnim sadržajima uklanja ili u velikoj mjeri smanjuje potrebu za posredovanjem osoblja ustanove između korisnika i građe koju koristi. Također pojednostavljuje korištenje same građe i manje opterećuje ustanove.

Uspješnost digitalizacije u cilju poboljšanja dostupnosti znatno zavisi od obrađenosti, načinu organizacije i opisu digitalnih zbirki te o karakteristikama i mogućnostima informacionog sistema koji osigurava dostupnost. U ovoj se funkciji digitalizacije najjasnije vidi međuzavisnost postupka same digitalizacije u užem smislu, obrade digitalnih zbirki i samih informacionih sistema i aplikacija koji se koriste za obradu, pristup i dohvat digitalnih sadržaja [2].

Digitalizacijom i drugim oblicima izrade digitalnoga sadržaja mogu se ponuditi ne samo novi sadržaji, nego i nove usluge koje ne bi bile moguće ili bi bile teško izvedive izvan elektronskog okruženja.

Neke od takvih usluga usmjerene su prema klasičnim korisnicima, npr. objedinjene informacione službe, sistema koji podržavaju distribuisano pretraživanje ili pristup građi različitih

vlasnika u toku iste korisničke sesije, oblikovanje i održavanje tematskih portala, mogućnosti postavljanja online izložbi i ostalih iz građe izvedenih ili popratnih sadržaja i sl.

Određeni oblici nove ponude na temelju digitalizovane građe mogući su i prema tzv. stručnoj javnosti, odnosno drugim ustanovama, organizacijama i pojedincima iz iste ili srodnih djelatnosti. Digitalizovani sadržaji i pripadajući metapodaci koje je izradila jedna ustanova mogu biti korisni i drugim ustanovama, kako za oblikovanje i upotpunjavanje njihove ponude, tako i za sam proces obrade njihovih sadržaja. Pojedini se projekti i usluge, npr., uspostava „virtualnih zbirki“, u cjelini zasnivaju na izvorno vanjskim sadržajima pribavljenim digitalizacijom građe drugih vlasnika.

Jedan od proizvoda sistematskog bavljenja digitalizacijom je i razvoj infrastrukture, resursa, znanja i iskustva, koji također mogu poslužiti uvođenju određenih specijalizovanih usluga [2].

2.2. Tehnološki koraci digitalizacije i pohrane kulturne baštine

Digitalizacija sadržaja kulturne baštine može se definisati kao proces snimanja, pohranjivanja i obrade sadržaja, korištenjem digitalne kamere, skenera i računara, sa pripadnim software-ima za obradu slike i optičko prepoznavanje znakova (OCR-Optical Character Recognition). Pri tome, tip korištenog skenera, tehnologija obrade, kodiranja i spašavanja digitalne kopije, zavisi ne samo od vrste građe nego i od njene starosti, literarne, umjetnicke i komercijalne vrijednosti.

Nakon samog procesa digitalizacije sadržaji postaju dostupni u digitalnoj formi, te se postavlja pitanje organizacije sadržaja u LAN/WAN baziranim mrežama. Digitalizovani sadržaji mogu se dati na korištenje samo u lokalnim mrežama, članovima koji pripadaju toj mreži ili se dijelovi odnosno cjelokupni sadržaj može staviti na raspolaganje svim zainteresovanim potencijalnim korisnicima, putem Interneta. U tom kontekstu, veliku pažnju treba posvetiti zaštiti digitalizovanih sadržaja baštine.

3. TEORETSKE POSTAVKE ZAŠTITE DIGITALIZOVANIH SADRŽAJA

Digitalizirana kulturna baština, posmatrana kao informacija zapisana u digitalnom obliku, podliježe istim pravilima i tehnikama osiguravanja kao i ostale informacije u digitalnoj formi. Sa druge strane sadržaj onoga što je digitalizirano nameće neke nove dileme o načinima distribucije i zaštite. S obzirom na resurse koji su potrebni za ovu vrstu digitalizacije jasna je želja vlasnika prava na digitalni sadržaj da imaju čvrstu kontrolu nad onim što korisnici ovog sadržaja mogu učiniti sa istim. Digitalni zapisi imaju prednost lakog kopiranja i izmjena što u ovom kontekstu predstavlja poteškoću, slično kao što je to slučaj sa drugim multimedijalnim sadržajima koji su zaštićeni autorskim pravima.

U nastavku će biti data oba aspekta zaštite, onaj koji se odnosi generalno na zaštitu digitalnih informacija, te onaj koji se odnosi na osobitosti zaštite digitalizirane kulturne baštine.

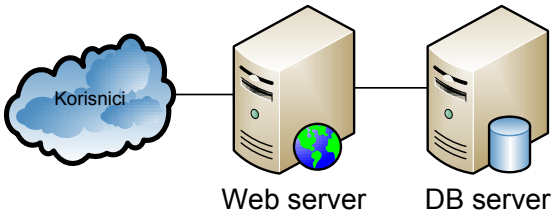
3.1. Zaštita digitalnih informacija

Sigurnost informacija u digitalnom svijetu zasniva se na očuvanju povjerljivosti, integriteta i dostupnosti [3]. Povjerljivost znači da su informacije dostupne samo onima kojima treba da su dostupne. Integritet osigurava promjenu informacija samo od strane ovlaštenih subjekata i to samo na ovlašten način. Dostupnost osigurava da su informacije uvijek dostupne ovlaštenim subjektima. Uobičajeno se sigurnost informacionih sistema realizuje kroz tri procesa: dokazivanje identiteta, ovlaštenja i evidentiranje. Da bi pristupili informacijama subjekti dokazuju svoj identitet, na osnovu koga dobivaju odgovarajuća ovlaštenja, prava pristupa, pri čemu se sve akcije subjekata evidentiraju.

Još jedan važan element zaštite informacija je strategija takozvane dubinske odbrane. Ova strategija nalaže slojevitu implementaciju odbrambenih mehanizama koja se ne oslanja na samo jedan nivo zaštite već na odgovarajuću zaštitu Jedan mogući pristup realizaciji zaštite digitalizirane kulturne baštine zasnovan na navedenom dat je u nastavku.

3.2. Pristup digitaliziranoj kulturnoj baštini

U duhu savremene tendencije pohranjivanja digitalnih sadržaja u baze podataka, te njihove Web bazirane prezentacije, može se dati opšti model pristupa digitalnoj baštini kao na slici 1.



Slika 1. Opšti model pristupa digitalnoj kulturnoj baštini

U opštem slučaju digitalizirana kulturna baština pohranjuje se u bazu podataka na serveru, a pristup korisnicima omogućava se putem Web servera. Konceptualno to su dvije usluge, dva servera, dok u konkretnoj implementaciji obje usluge mogu biti pružane sa jednog računara. Također, korisnici mogu pristupati Web serveru lokalno ili preko Interneta što će kasnije biti detaljnije obrađeno.

3.3. Zaštita na nivou baze podataka

Koristeći strategiju dubinske odbrane, osiguravanje informacija kreće od baze podataka. Na nivou baze podataka, nezavisno od konačnog načina prezentacije sadržaja korisnicima, implementiraju se mehanizmi sigurnosti.

Za identifikaciju korisnika koriste se mehanizmi baze podataka. To može biti jednostavni mehanizam poput korisničkog imena i lozinke ili složeniji mehanizmi poput digitalnih certifikata.

Sadržaj baze se dijeli u grupe, gdje jednu grupu predstavljaju sadržaji koji treba da budu dostupni svima, a drugu grupu ili više njih sadržaji kojima treba obezbijediti kontrolisan pristup. Sa druge strane, korisnici baze podataka također se dijele u grupe. Četiri osnovne grupe mogu biti slijedeće:

- Administratori - dodjeljuju prava ostalim korisnicima, te održavaju softver baze podataka;
- Operatori - unose nove i ažuriraju postojeće sadržaje;
- Identificirani korisnici - imaju prava pregleda sadržaja prema utvrđenom identitetu;
- Neidentificirani korisnici - imaju pravo pregleda sadržaja dostupnog svima.

Uobičajena realizacija prava pristupa je putem adminstratorski konfigurabilne matrice pristupa [4]. Matrica pristupa definiše kakvo pravo pristupa određenoj grupi dokumenata ima određena grupa korisnika. Svaki korisnik pripada jednoj ili više grupa, što je konfigurabilno. Takođe svaki sadržaj pripada jednoj ili više grupa, što je takođe konfigurabilno. Prava pristupa mogu biti jednostavnog oblika da se može ili ne može pristupiti sadržaju, ili preciznije definisana da utvrđuju nivo prava pristupa, recimo pristup zaključanim ili otključanim verzijama. Inicijalna konfiguracija bi imala dvije grupe korisnika, one identificirane i neidentificirane, i dvije grupe dokumenata javno dostupne i dostupne samo identificiranim korisnicima. Matrica pristupa bi omogućavala korisnicima u grupi identificiranih pristup i jednoj i drugoj grupi dokumenata, a onima u grupi neidentificiranih samo pristup dokumentima u grupi javnih. Administrator može kreirati nove grupa korisnika i dodavati korisnika u grupe ili ih brisati iz grupa. Moguće je kreiranje novih grupa sadržaja te dodavanje sadržaja u grupe i njihovo uklanjanje. Na ovaj način omogućeno je fleksibilno upravljanje pravima pristupa sadržajima u potpunosti prilagodljivo modelu pružanja usluga koji izabere organizacija koja pruža korisnicima digitaliziranu kulturnu baštinu.

Koristeći ugrađene mehanizme evidentiranja, dostupne u svim bazama podataka, sve akcije korisnika se bilježe radi utvrđivanja pojedinačne odgovornosti u slučaju potrebe, kao i moguće rekonstrukcije neovlašteno izmijenjenih ili obrisanih podataka.

Implementacijom navedenih mehanizama utvrđivanja identiteta, davanja prava pristupa i evidentiranja omogućava se ostvarivanje povjerljivosti, jer će digitalizirana kulturna baština biti dostupna onima koji su ovlašteni da joj pristupe i to na način kako su ovlašteni.

Za očuvanju integriteta uz navedene mehanizme, koji omogućavaju kontrolu izmjena, moguće je dodati uobičajeni mehanizam za provjeru integriteta, *hash* sadržaja. *Hash*-evi svih sadržaja mogu se čuvati u posebnim tabelama dostupnim samo administratoru, te redovno provjeravati i porediti sa *hash*-evima sadržaja koji su u bazi. Takođe je neophodno ažurirati ove *hash*-eve prilikom svakog ovlaštenog ažuriranja sadržaja. Na ovaj način moguće je otkriti sve neovlaštene promjene sadržaja.

Za očuvanje dostupnosti uz navedene mehanizme neophodno je obezbijediti redovno pravljenje rezervnih kopija. Rezervne kopije potrebno je praviti na eksterni uređaj (traka, eksterni hard disk, ...) i pohranjivati taj uređaj na drugu lokaciju. Na ovaj način se obezbjeđuje dostupnost sadržaja putem povrata iz ovih kopija čak i u slučajevima kada je narušena sigurnost baze podataka.

Posebno pitanje je zaštita programa koji pruža uslugu baze podataka. Neophodno je poduzeti korake da se ovaj program konfiguriše prema uputama proizvođača i najboljoj praksi, te redovno ažurira sa sigurnosnim popravkama [5]. Ovim se dodatno osigurava i sigurnost podataka pohranjenih u bazi.

Na ovaj način obezbjeđuje se sigurnost digitalnih sadržaja u bazi podataka nezavisno i bez oslanjanja na druge nivoe zaštite. Istovremeno nudi se rješenje koje je modularno i skalabilno i ne ograničava nadgradnju i uslovljava način pristupa bazi podataka.

3.4. Zaštita na nivou Web servera

Zaštita na nivou Web servera provodi se nezavisno od drugih oblika zaštite digitalizovanih oblika kulturne baštine. Slično kao i kod baze podataka potrebno je zaštiti program Web servera i koristiti kontrolu pristupa koju Web server omogućava da se zaštite podaci koje server daje korisnicima.

Zaštita softvera Web servera provodi se adekvatnom konfiguracijom preporučenom od strane proizvođača i poštovanjem ustaljene najbolje prakse. Web server koji funkcioniše po specifikaciji može implementirati svoje sigurnosne kontrole za koje je projektovan.

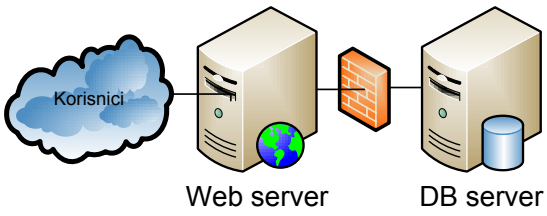
Zaštita sadržaja koje Web server pruža provodi se kontrolama. Pristup sadržajima se kontroliše dokazivanjem identiteta te dobivanje ovlaštenja za pristup na osnovu utvrđenog identiteta. Sve akcije korisnika koji pristupaju serveru se evidentiraju radi

osiguravanja individualne odgovornosti i oporavka u slučaju potrebe.

Kako se u predloženoj konfiguraciji podaci ne nalaze na Web serveru već u bazi podataka, Web server ne kontroliše pristup podacima već Web stranicama ili aplikaciji koje prikazuju podatke ili omogućavaju njihovo ažuriranje. Korisnici i stranice kojim se pristupa mogu biti podijeljene u slične ili čak iste grupe kao što je učinjeno za bazu podataka. Na osnovu pripadnosti određenoj grupi korisnik dobiva pravo pristupa grupi stranica. Ove stranice mu omogućavaju pristup bazi u skladu sa njegovim ovlaštenjima.

Korisnikovi podaci za pristup, korisničko ime i lozinka ili druga vrsta identifikacija, se na odgovarajući način proslijeđuju sa Web servera prema bazi podataka. Korisnik ove podatke unosi samo jednom i nije svjestan ovog koraka, ali je on bitan jer osigurava da direktan pristup bazi koji bi zaobišao zaštitu Web servera i dalje nije moguć bez identifikacije korisnika i provjere ovlaštenja.

Ovaj prenos korisničkih podataka između Web servera i baze podataka koristi vezu između ove dvije komponente sistema. Istom vezom se prenose i svi ostali podaci, kao što su upiti ili ažuriranja ka bazi i odgovori baze. Očigledno je da je i ovu vezu neophodno osigurati. Potrebno je obezbijediti da podaci koji putuju ne mogu biti pročitani ili izmijenjeni, kao i da doputuju na drugu stranu. U ovakvim konfiguracijama uobičajeno je da Web server ima dvije IP adrese od kojih se po jednoj omogućava pristup korisnicima dok se druga koristi za povezivanje sa bazom podataka Zaštitu podataka od čitanja i izmjene moguće je postići šifriranjem podataka koristeći SSL ili IPsec protokole. U praksi se ovi serveri uglavnom nalaze unutar jedne organizacije ili čak u istoj server sobi i povezani su kablom direktno, ili preko swtich-a. U ovim slučajevima dovoljan nivo zaštite je uglavnom već postojeća kontrola pristupa lokalnoj mreži i fizička kontrola pristupa kablovima i server sobi. Dodatni nivo zaštite može se postići korištenjem *firewall*-a koji može biti instaliran između Web servera i servera baze podataka ili kao proces na svakom od servera koji vrši kontrolu saobraćaja i omogućava da pristup po ovoj vezi serveru baze podataka ima samo Web server i obratno (Slika 2).



Slika 2. Prošireni model pristupa digitalnoj kulturnoj baštini

Administrator projekta može u tom slučaju vršiti izmjene samo direktno na serveru, koji bi bilo poželjno i fizički izolovati, u neki dobro čuvani prostor (dalje od mjesta na kojima se okupljaju korisnici), te dodatno zaštititi lozinkom, na nivou mašine. Ukoliko se u sistemu nalazi više administratora koji dodaju sadržaj u bazu, tada se i njihovim računarima (IP adresama), može dozvoliti pristup na server, na nivou firewall-a.

3.5. Osobitosti zaštite digitalizirane kulturne baštine

Kako je ranije rečeno očuvanje kulturne baštine ima neke aspekte pored onih vezani za do sada obrađenu standardnu sigurnost elektronskih informacija. Digitalni zapisi imaju prednost lakog kopiranja i izmjena što u ovom kontekstu predstavlja poteškoću, slično kao što je to slučaj sa drugim multimedijalnim sadržajima koji su zaštićeni autorskim pravima. Digitalizirana kulturna baština treba biti očuvana u svom neizmijenjenom obliku radi očuvanja autentičnosti i ograničavanja neovlaštenog kopiranja ili mijenjanja.

Digitalni vodeni žigovi su se pokazali kao efikasna tehnika za zaštitu prava intelektualnog vlasništva na različite vrste multimedijalnih digitalnih zapisa. Ovom tehnikom se u multimedijalnu datoteku umeću određeni nizovi bita, digitalni kodovi, koji sadrže informacije o intelektualnom vlasništvu sadržaja datoteke. Informacije mogu biti o autoru, porijeklu, pravima pristupa ili slično. Ovi digitalni kodovi su na odgovarajući način raspoređeni u datoteci tako da ih se ne može prepoznati i njima manipulirati. Oni trebaju biti sasvim neprimjetni prilikom normalnog korištenja multimedijalne datoteke. Ne smiju se primjetiti na slikama, čuti na zvučnim zapisima, a ni čuti ni vidjeti na video zapisima. U ovome se razlikuju od običnih vodenih žigova na papiru koji treba da budu neupadljivi, ali primjetni. Sa druge strane digitalni vodeni žigovi trebaju biti robusni, u smislu da se ne izgube kroz normalne transformacije multimedijalnih datoteka kao što su promjene načina zapisa kojima se gubi nešto od kvaliteta početnog zapisa (primjer je pretvaranje audio zapisa sa CD-a u mp3 format ili pretvaranje bitmapirane slike u jpg format). Zadovoljavanje svih navednih uslova nije ni malo jednostavno, ali postoje različite tehnologije koje to postižu u dovoljno dobroj mjeri. Za upisivanje i očitanje vodenog žiga neophodan je poseban program koji je zavisi od izabrane tehnologije [6].

Primjena ove tehnologije za zaštitu digitalizirane kulturne baštine je postala uobičajena u posljednje vrijeme [7], [8] i [9].

Ubacivanje vodenih žigova u digitalne datoteke ili druge vrste digitalnih zapisa koji se čuvaju u bazi podataka može u velikoj mjeri povećati njihovu sigurnost nezavisno od drugih, ranije pomenutih, mjera zaštite. Njihovim korištenjem moguće je očuvati informacije bitne za zaštitu intelektualnog

vlasništva koje je za ovakve sadržaje od velikog značaja. Korištenje ovih žigova unosi dodatni korak u proces digitalizacije, ali korak koji je vjerovatno vrijedan napora.

4. SCENARIJI IZVEDBE

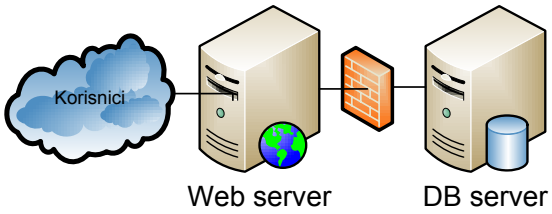
Na osnovu prethodnog osnovnog modela koji pokriva neophodne elemente zaštite digitalizirane kulturne baštine, biće predložena tri scenarija praktične izvedbe. Scenariji su poredani od najlakšeg za implementaciju sa ograničenim skupom korisnika do najzahtjevnijeg sa javnim pristupom. Svaka organizacija može izabrati onaj koji joj odgovara shodno tehničkim i materijalnim mogućnostima i ciljanoj skupini korisnika.

4.1. Scenario 1

Ovaj scenario je najmanje zahtjevan sa aspekta sigurnosti. Naime, podrazumijeva potpuno izolovan sistem (LAN mrežu, koja ne izlazi na Internet), i ograničen na zgradom biblioteke, odnosno čitaonice u muzeju, arhivu... Pitanje kontrole pristupa ovdje dijelom riješeno fizičkom kontrolom pristupa. Pretpostavka je da svi u čitaonici imaju regulisano pravo pristupa, kroz plaćanje članarina i slične vidove pretplate. Dakle, može se pretpostaviti da svi koji pristupe računarima iz LAN mreže, imaju to pravo. U tom kontekstu, kontrola pristupa koristi postojeće mehanizme kontrole pristupa Web serveru, koji reguliše pristup odgovarajućim stranicama i sadržajima u bazi podataka.

Moguće je dodati mogućnost da sistem sam provjerava važenje članarine korisnika u datom trenutku. U tom kontekstu, može se pri prijavljivanju na lokalnu web stranicu korisnicima postaviti upit za lozinkom, koju korisnici dobijaju prilikom učlanjivanja ili obnavljanja članarine, sa ograničenim rokom trajanja. U tom slučaju, pored korisničkog imena, lozinke i permisija, u bazi korisnika, svakom korisniku mora biti pridružen i datum isteka njegove članarine. Sistem onda provjerava unesene parametre, ispituje i trajanje članarine, te na osnovu svega pomenutog, korisniku daje određena prava. Ukoliko se na sistem želi prijaviti osoba koja ima prava izmjene sadržaja, ona unosom svog korisničkog imena i lozike, dobija pravo editovanja i dodavanja.

Iako pitanje kontrole pristupa nije kritično, čak i u ovom slučaju, sa najelementarnijim sigurnosnim zahtjevima, potrebno je sistem obezbijediti radi zaštite podatka. Naime, čak i članovi čitaonice, sa regulisanim pravima pristupa, mogu biti zlonamjerni napadači na integritet sadržaja, te je na neki način potrebno spriječiti i korisnike čitaonice da pristupe sadržajima na server baze podataka. Ova mogućnost spriječena je ranije izloženom slojevitom zaštitom koja se zasniva na nezavisnoj provjeri identiteta i prava pristup svakom elementu sistema.



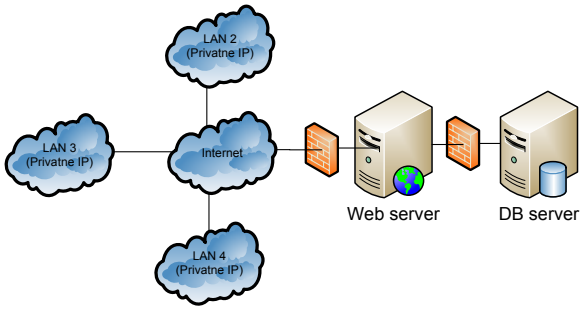
Slika 3. Scenario 1

Primjer organizacije sistema sa digitalizovanim sadržajima kulturne baštine prema scenariju 1, postoji na Nacionalnoj sveučilišnoj knjižnici u Zagrebu. Prostor biblioteke je pokriven bežičnom mrežom, a sastoji se od servera sa digitalizovanim sadržajima i laptop računara. Signal je dovoljno jak da prekriva samo područje biblioteke, te samo korisnici unutar zgrade, sa posuđenim ili vlastitim laptop računarima mogu pristupiti mreži. Regulacijom svojih prava pristupa sadržajima biblioteke, korisnici dobijaju korisničko ime i lozinku, pomoću kojih mogu pristupati sadržajima na serveru [10].

4.2. Scenario 2

Ovaj scenario predstavlja proširenje prethodno opisanog koncepta, omogućavajući i odabranim korisnicima izvan LAN mreže u biblioteci, arhivu ili muzeju, pristup digitalizovanim sadržajima na serveru. Ti korisnici, kao što je navedeno, mogu biti određeni fakulteti, druge biblioteke, arhivi i sl., kojima bi ovakav koncept jednostavnog pristupa historijskim i drugim dokumentima i sadržajima, u velikoj mjeri pomogao u učenju i radu. Pri tome, ovaj scenario ne dozvoljava pristup podacima izvan odabranih institucija. U tom kontekstu, ovaj scenario ima značajne zahtjeve, ne samo za očuvanje kvalitete sadržaja, nego i po pitanju kontrole pristupa, i treba, pored sigurnosnih zahtjeva iz scenarija 1, da obezbijedi i dodatne elemente sigurnosti.

Gledano sa tehničkog aspekta realizacije mrežnog sistema, ovaj scenario treba da poveže udaljene LAN mreže, pri čemu se u LAN 1 mreži nalazi server baze podataka sa digitalizovanim sadržajima, a u ostalim LAN 2, LAN 3... mrežama, samo klijentski računari za pristup sadržajima u bazi. Pri tome se, za povezivanje pomenutih LAN-ova koristi Internet. Kao što je rečeno u opisu scenarija, postoje i druga, sigurnija rješenja, koja su ekonomski neisplativa za analiziranu aplikaciju, te se neće ni razmatrati u radu (Slika 4).



Slika 4. Scenario 2

Međutim, Internet je javna mreže, koja po svojoj prirodi nije sigurna, te je podatke koji se njome prenose potrebno zaštititi. U tom kontekstu, treba obezbijediti kontrolu pristupa, jer nije poželjno da sadržaje mogu čak ni čitati korisnici izvan odabranih LAN mreža, i zaštititi integritet podataka koji se prezentuju.

Korištenjem predstavljenog koncepta univerzalnog za sva pretpostavljena rješenja, štiti se i sam pristup podacima, koji se dozvoljava samo korisnicima iz LAN mreža, koji posjeduju znanje lozinke za prijavljivanje na sistem (pohranjene na serveru baze podataka, zajedno sa ovlaštenjima). Na taj način se onemogućava pristup sadržajima neželjenim korisnicima, koji se nalaze u prostorijama, odnosno za računarima iz LAN mreža, u institucijama kojima je dozvoljen pristup sadržajima.

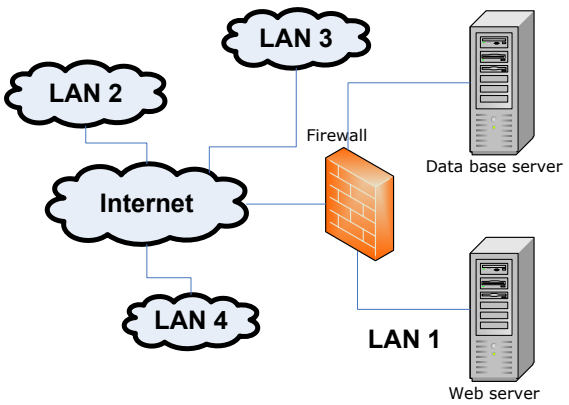
Ukoliko se prezentacije digitalizovanih sadržaja kulturne baštine sa servera baze podataka stave na raspolaganje korisnicima na fakultetima, u drugim arhivama i sl., za pretpostaviti je da neće svi računari iz tih mreža trebati pristup sadržajima baštine.

Na primjeru fakulteta, može se pretpostaviti da će fakultetska čitaonica trebati pristup sadržajima u cilju istraživanja, dok se ostalim računarima u mreži ne treba dozvoliti pristup (opšte službe, lokalne laboratorije...). U tom kontekstu, interesne prostorije na fakultetu, odnosno pomenuta čitaonica, treba se organizovati kao LAN mreža, sa privatnim adresnim planom, za sve računare u toj prostoriji/ama, neovisno od adresnog plana ostalih računara na fakultetu. Za izlaz na Internet, korištenjem NAT-iranja, za tu LAN mrežu potrebna je samo jedna javna IP adresa, preko koje svi računari u LAN-u, mogu pristupiti javnoj mreži. Pri tome treba naglasiti da LAN mreža kojoj se dozvoljava pristup digitalizovanoj baštini mora predstavljati potpuno neovisnu mrežu od ostatka lokalne mreže fakulteta na kojem se nalazi, te da se pripadna javna IP adresa ne bi smjela koristiti ni u koje druge svrhe, štiteći na taj način baštinu od neželjenog pristupa, iz same zgrade fakulteta, a izvan čitaonice.

Ovako organizovane LAN mreže potrebno je još povezati na LAN 1 (sa serverom baze podataka), putem Interneta. Problem koji se javlja prilikom korištenja infrastrukture Interneta, za povezivanje udaljenih LAN, jeste mogućnost narušavanja integriteta podataka, te neovlaštenog pristupa podacima. Jedan od načina zaštite ovakvog sistema je korištenjem firewall-a između web servera i routera, preko kojeg LAN 1 izlazi na Internet. Na pomenutom firewall-u konfiguriše se lista IP adresa, kojima se dozvoljava pristup LAN 1 mreži. To su javne IP adrese, preko kojim čitaonice na fakultetima itd. izlaze na Internet. Dakle, na firewall-u se, korištenjem pravila "Podrazumjevano zabrani", onemogućuju svi sa Interneta da pristupe LAN 1 mreži, osim odabranih LAN mreža, preko fiksnih IP adresa.

Kao što možete vidjeti na slici 4, predstavljeno tehničko rješenje je nešto malo kompleksnija mrežna arhitektura prezentacije web aplikacije, no vrlo često se koristi. Sa ovakvom arhitekturom, baza podataka je kompletno izolovana i zaštićena od direktnih udara sa Interneta. Kako bi neko sa Interneta došao do baze podataka, mora proći vrlo kompleksan put i zaobići razne sigurnosne mjere. Veza između web aplikacije i baze podataka je uspostavljena preko privatnih IP adresa koje nisu "routabilne" tj. ne koriste se na Internetu, što još dodatno otežava pristup. Sve to znači da, da bi neko došao do baze podataka, treba prvo zauzeti web server (preko firewall-a), te zatim probati zauzeti server baze podataka kojeg štiti još jedan dodatni firewall. Ovakva zona izolacije web servera, koji je postavljen iza routera, njegovih pristupnih listi i firewall-a, a ipak dostupan sa Interneta, naziva se demilitarizirana zona (DMZ) [11].

DMZ se može realizovati kao što je prikazano na slici 4 (slojevita DMZ implementacije [11]) ili korištenjem firewall implementacije sa višestrukim interfejsom. U tom slučaju, koristi se samo jedan firewall, ali sa dodanim interfejsima i postavljenim DMZ sistemom. To znači da se koriste 3 interfejsa na firewall-u: na jedan interfejs se spaja Internet (eksterna mreža), zatim na drugi interfejs LAN 1 mreža (mreža koja se štiti) i na treći DMZ mreža (web server). Ovo omogućava istom firewall-u, da upravlja saobraćajem između Interneta i DMZ zone, a također i da štiti internu mrežu (Slika 5).



Slika 5. Scenario 2 sa DMZ

Ovakva metoda omogućava korištenje seta hardvera i softvera povoljnije cijene koji se treba koristi kako bi se osigurala mreža. Također, može se zaključiti da se na ovakav način centralizira set pravila koji se koriste u kompletnoj mreži, te se time olakšava upravljanje i otkrivanje problema u njoj. Ova metoda implementacije se puno češće koristi nego prethodno rješenje sa dva firewall-a.

Ovdje nije razmatrana dodatna mogućnost osiguravanja sigurnosti koju bi korištenje virtuelnih privatnih mreža (VPN) donijelo. VPN bi bilo vrlo pogodno rješenje za scenario 2, ali objašnjenje ovakve implementacije izlazi iz okvira ovog rada. Ovu činjenicu je potrebno imati u vidu prilikom praktične implementacije i razmotriti korištenje VPN-a ako postoje mogućnosti.

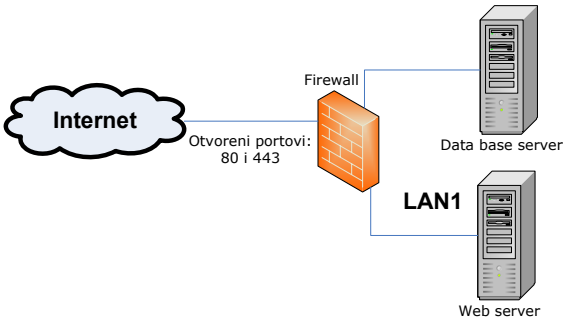
Na kraju još treba napomenuti da, kako se u ovom rješenju udaljeni računari povezuju na LAN 1 mrežu i Web odnosno server baze podataka, korištenjem Interneta kao transportne mreže, lozinke koje se prenose kroz mrežu nikada se ne bi smjele slati u čistom tekstualnom obliku.

4.3. Scenario 3

Ovaj scenario podrazumijeva prezentaciju sadržaja na Internet, sa mogućnošću pristupa od strane svih korisnika. Zaštita pristupa ima iste elemente kao i ranije s tim što su podaci dostupni većem broju potencijalnih korisnika. Iz ovih razloga zaštita integriteta je ovdje od velikog značaja, jer svi koji žele imaju mogućnost pregleda sadržaja sa servera baze podataka.

Zaštita podataka se i u ovom slučaju može obezbijediti korištenjem DMZ zone, uz razliku što se na firewall-u (njegovom portu) koji izlazi na Internet, ne ograničava pristup IP adresama, kao u scenariju 2, nego portovima. Uz dozvoljavanje ulaska u LAN 1 samo preko porta 80 (HTTP) i 443 (HTTPS), praktično se omogućava samo pristup web serveru, štiteći na taj način podatke u bazi. Implementacijom DMZ zone, napadač da bi došao do podataka u bazi ili do lozinki, mora proći dva firewall-a, što znatno otežava upad u sistem i štiti integritet sadržaja digitalizovane kulturne baštine.

Predstavljeni koncept slojevite zaštite i u ovom slučaju se koristi, zahtijevajući od korisnika sa Interneta da se registruju sa svojim imenom i lozinkom, u slučaju da žele pregledati sadržaje, ili se može potpuno izbjeći za korisnike i sadržaje koji treba da budu javno dostupni svim zainteresovanim.



Slika 6. Scenario 3

Na kraju još treba dodati da predstavljeni scenariji u praksi ne moraju biti izolovani. Na primjer, u bazi se mogu nalaziti neki manje značajni digitalizovani sadržaji, za opštu upotrebu, te neki vrijedni dokumenti, kojima mogu pristupati samo odabrani korisnici. To onda podrazumijeva kombinaciju scenarija. Najbitnija karakteristika svih ponuđenih rješenja je da su skalabilna, te omogućavaju nadogradnju u slučaju pojave novih zahtjeva, kroz njegovu implementaciju.

5. ZAKLJUČAK

Digitalna obrada kulturne baštine ne samo da je projekat od velike važnosti za očuvanje, popularizaciju, dostupnost građe, nego je i neizbježan proces u nastojanjima da se BiH približi svjetskim, a naročito evropskim standardima. U tom smislu, brojne institucije se već prepoznale važnost ovog projekta, i donekle otpočele proces digitalizacije svojih izvornika. Međutim, sve urađeno predstavlja samo mali dio onoga što bi, prema evropskim standardima, trebalo biti obuhvaćeno procesom digitalizacije. U tom kontekstu, cilj ovog rada je da pruži smjernice kulturno-historijskim institucijama u procesu digitalizacije, posebno u dijelu koji se odnosi na organizaciju i prezentaciju digitalizovanih sadržaja, sa fokusom na moguće koncepte zaštite istih.

REFERENCES

[1] Hrvatski gospodarski "žilogriz" i kulturna "stoljetna suša", (tekst preuzet sa stranice: http://www.rb-donjahercegovina.ba)

[2] Nacionalni program digitalizacije arhivske, knjižnične i muzejske građe, Ministarstvo kulture Republike Hrvatske, Zagreb, listopad 2006.

[3] M. Bishop, Introduction to Computer Security, Addison-Wesley Professional, 2004.

[4] B.W. Lampson, “Protection,” ACM SIGOPS Operating Systems Review, vol. 8, 1974, pp. 18-24.

[5] "Database Security Best Practices: Implementing the Missing Piece", Embarcadero Technologies, 2006.
[6] I. Cox et al., Digital Watermarking and Steganography, Second Edition (The Morgan Kaufmann Series in Multimedia Information and Systems), Morgan Kaufmann, 2007.
[7] Y. Zhao, P. Campisi, and D. Kundur, "Dual domain watermarking for authentication and compression of cultural heritage images," Image Processing, IEEE Transactions on, vol. 13, 2004, pp. 430-448.
[8] A. Del Mastio et al., "Virtual Restoration and Protection of Cultural Heritage Images", Digital Signal Processing, 2007 15th International Conference on, 2007, pp. 471-474.
[9] A. Dunning and B. Justrell, "Cultural Heritage Online: The Challenge of Accessibility and Preservation", Ariadne, 2007.
[10] "Digitalni arhiv" (tekst preuzet sa stranice: http://www.nsk.hr/DigitalLib.aspx?id=80).
[11] C. Hare and K. Siyan, Internet Firewalls and Network Security, New Riders Pub, 1996.