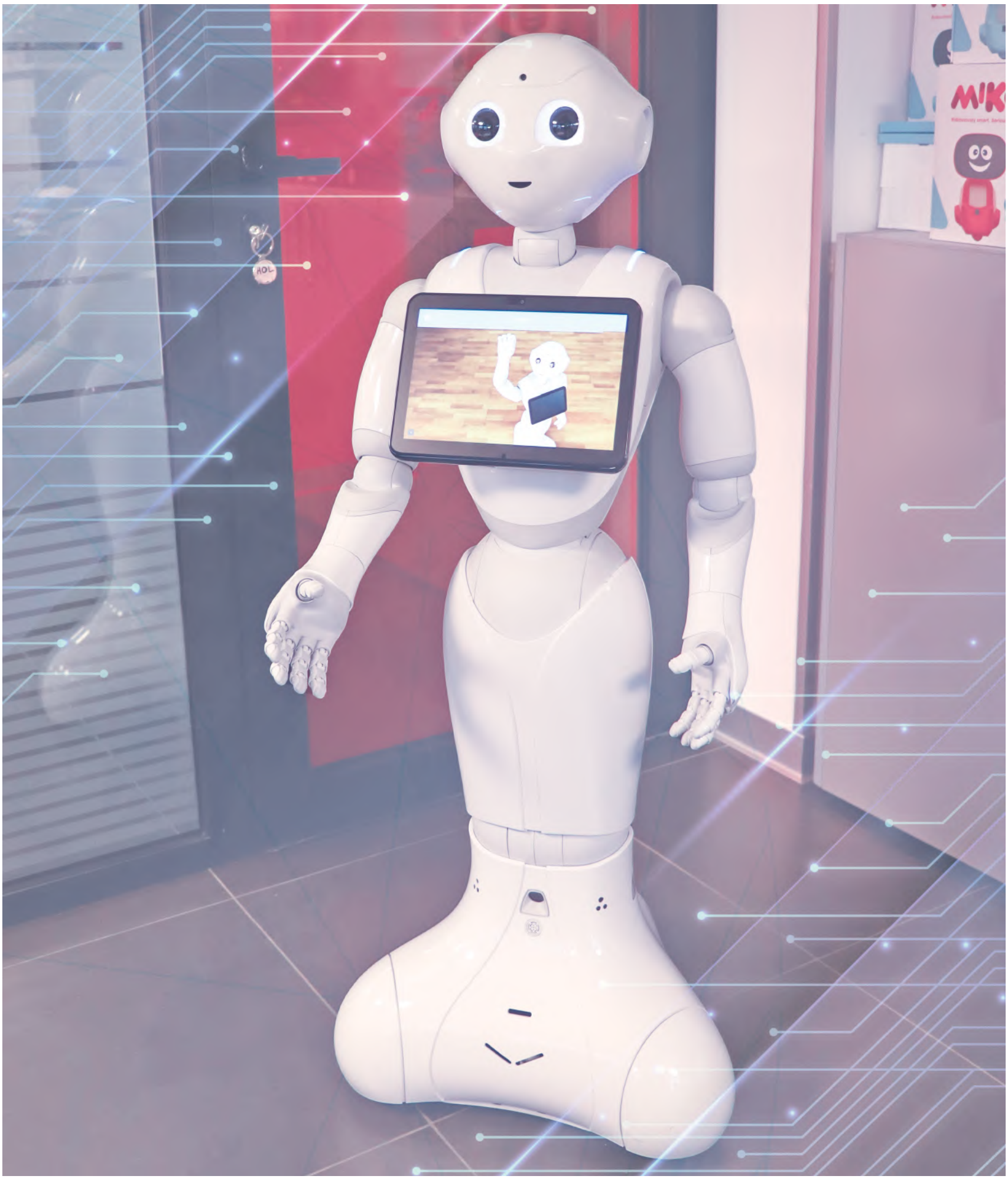
NAUČNI ČASOPIS ZA SAVREMENO OBRAZOVANJE I PRIMENU INFORMACIONIH TEHNOLOGIJA

EdTech JOURNAL

edtechjournal.org

UDK: 371.3
004.9:37
ISSN 2812 - 8753 (Štampano izd.)
ISSN 2812 - 8761 (Online)
VOL. 2 BR. 2
OKTOBAR 2022
BEOGRAD

SCIENTIFIC JOURNAL FOR CONTEMPORARY EDUCATION AND APPLICATION OF INFORMATION TECHNOLOGIES



EdTech JOURNAL

IMPRESSUM

Izdavač/Publisher

Institut za moderno obrazovanje
Masarikova 5, Beograd
11000 Beograd
+381 (0)11/40-11-260
office@institut.edu.rs

Kontakt podaci uredništva/ Editorial contact information

EdTech Journal
Masarikova 5, Beograd
11000 Beograd
Telefon: + 381 (0)11/40-11-260; Mobilni telefon: + 381 60/55-22-581
Imejl-adresa: EdTech@institut.edu.rs;
Veb-sajt: http://www.edtechjournal.org/; http://www.edtech-journal.org/

IMPRESSUM

Jezička redakcija/ Language editing

Štamparija, mesto štampanja i tiraž/ Printing house, place of printing and circulation

Jovšić Printing Centar
Patrijarha Dimitrija 53, 11090 Beograd
tiraž: 100 kom.

Naziv i internet adresa (URL) baze podataka u kojoj su članci dostupni u vidu punog teksta/Name and Internet address (URL) of the database where the articles are available in full text
Časopis je open access i ne naplaćuje kotizaciju za obradu radova, niti za njihovo objavljivanje. Svi objavljeni naučni radovi su vidljivi u celini na sajtu časopisa/ The journal is open access and does not charge a registration fee either for processing or publishing papers. In addition, all published scientific papers are visible in their entirety on the journal's website.

Open Access PKP website EdTech Journal

Svi tekstovi su dostupni u celini na/ Full text available at: http://www.edtechjournal.org/; http://www.edtech-journal.org/
Naučni radovi se upućuju na najmanje dve recenzije, a stručni na najmanje jednu recenziju. Sve recenzije su double-blind. Časopis izlazi jednom godišnje u 2021. godini i šestomesečno, u aprilu i oktobru od 2022. godine / Scientific articles are submitted for at least two reviews, and professional articles for at least one review. All reviews are double-blind. The journal is published once a year in 2021 and every six months, in April and October since 2022.

Sadržaj

TABLE OF CONTENTS

Table of Contents

„Education must evolve to meet the needs of ever-evolving societies. People's potential can be realised throughout their lives, from infancy to old age, if they are given the best possible opportunities to acquire the necessary knowledge, skills, attitudes, and values."

Valentin Kuleto

Uvodna reč

Poštovani profesori, nastavnici, saradnici, istraživači i stručnjaci,

Da bismo bolje pripremili učenike za njihov budući posao, oblast IT-ja moramo da integrišemo u celoživotno učenje tako da dopunjuje onlajn i hibridno učenje i da ide u korak sa njegovim brzim rastom i razvojem. Rešenja u vezi sa virtuelnom i proširenom stvarnošću će igrati sve važniju ulogu kako se u budućnosti budemo kretali ka učenju na daljinu i sve više kombinovanom modelu obrazovanja i rada. Pored toga, oblast IT-ja omogućava bezbedno i stalno vežbanje snalaženja u teškim situacijama i rad na ključnim i neophodnim veštinama.

Naučnici iz brojnih oblasti postaju sve više zaintrigirani potencijalom virtuelne i proširene stvarnosti u obrazovanju. Virtuelna stvarnost postaje sve češća u inženjerstvu, računarstvu, astronomiji i mnogim drugim oblastima.

Takođe, svedoci smo rasta upotrebe robota u obrazovanju. Različiti tipovi robota se mogu naći u učionicama širom sveta, ali oni sa najvećim potencijalom mogu se naći samo u školama koje su spremne za budućnost. S druge strane, mnogi edukatori dovode u pitanje korisnost robota u obrazovanju. Oni su mišljenja da će roboti možda moći da odgovore na pitanja brže od nastavnika, ali ti odgovori možda neće biti tačni. Međutim, ovo je laž koju šire oni koji su protiv tehnološkog napretka. Roboti će moći brže i efikasnije da obavljaju zadatke i odgovore na pitanja učenika nego što to rade ljudi. Veštačka inteligencija robota takođe može izvršiti individualne procene na osnovu mišljenja i povratnih informacija učenika.

Moguće je da bi roboti čak mogli da prilagode celokupno iskustvo u učionici na osnovu karakteristika pojedinca. Dok roboti to mogu da urade automatski, nastavnici i dalje moraju da provode vreme istražujući i stvarajući najbolje moguće okruženje i atmosferu u učionici. Roboti mogu da procene jače i slabije strane učenika i pruže povratne informacije kako bi im pomogli da napreduju.

Mnogim školama nedostaje dovoljno nastavnog kadra zbog generalnog manjka nastavnika u svetu. Sve dok društveni roboti ne postanu priuštiviji, neke institucije će možda moći da priušte da plate edukatore uprkos tome što nisu u mogućnosti da ih plaćaju po tržišnoj ceni. U bliskoj budućnosti roboti će biti od velikog značaja u svim učionicama, ocenjivaće učenike i vodiće ih ka uspehu. Sa razvojem veštačke inteligencije, roboti će napredovati na više nivoe funkcionalnosti. Pored očigledne koristi od trenutnog pristupa bilo kom izvoru ili korpusu znanja, postoji i mnogo drugih prednosti u pedagogiji.

Postoji mnogo vrsta robota koji mogu pomoći ljudima da nauče nove stvari i unaprede svoje veštine. Roboti mogu pomoći edukatorima u nastavi u različitim disciplinama, uključujući istoriju i geografiju. Roboti se često koriste u učionici za upoznavanje učenika sa računarskim programiranjem i drugim STEM predmetima. Zbog svojih brojnih prednosti, roboti će uskoro igrati značajnu ulogu u učionicama širom sveta, kako u razvijenim zemljama tako i u zemljama u razvoju. Danas je humanoidni robot u učionici neobičan prizor koji se može videti samo u učionicama koje su spremne za budućnost. Dobrodošli ste da posetite naše učionice u Savremenoj osnovnoj školi, gde će vas dočekati naš asistent u nastavi Pepper.

Glavni urednik prof. dr Valentin Kuleto

> "Education must evolve to meet the needs of ever-evolving societies. People's potential can be realised throughout their lives, from infancy to old age, if they are given the best possible opportunities to acquire the necessary knowledge, skills, attitudes, and values.."
>
> Valentin Kuleto

Introductory

Distinguished professors, teachers, associates, scientific researchers, and professionals,

To better prepare students for the future workforce, IT is being integrated into lifelong learning in a way that complements the rapid growth in online and hybrid learning. Virtual and augmented reality solutions will play an increasingly important role as we move toward more blended and remote education and work environments in the future. In addition, IT makes it possible to safely and repeatedly practise difficult situations and high-risk skills.

Scientists from numerous fields are becoming increasingly intrigued by the educational potential of virtual and augmented reality. Virtual reality is becoming more common in engineering, computer science, and astronomy, among other fields.

Also, we are witnessing the growth of the use of robots in education. Different types can be found in classrooms worldwide, but those with the most tremendous potential can be found only in future-ready schools. On the other hand, many educators question the usefulness of robot workers. They may be able to respond to questions more quickly than a teacher, but they may not be as accurate. However, this is a falsehood spread by those against technological progress. Robots will be able to complete tasks and respond to student questions more quickly and effectively than humans. The robot's artificial intelligence will also make several individualised assessments based on the students' opinions.

It's possible that robots could even customise the entire classroom experience based on the individual's characteristics. While robots can do this automatically, teachers still need to spend time investigating and creating the best possible classroom setting. Robots can assess a student's strengths and weaknesses and provide feedback to help them improve.

Many classrooms lack sufficient teachers due to a worldwide shortage. Until socially connected robots become more affordable, some institutions may be able to afford instructors despite being unable to pay market rates. In the near future, robots will be great for all classrooms grading students and guiding them to success. With the development of AI, robots will progress to higher levels of functionality. Besides the apparent benefit of instantaneous access to any resource or body of knowledge, there are plenty of other pedagogical benefits.

There are many types of robots that can help humans learn new information and improve existing skills. Robots can help instructors with lessons in various disciplines, including history and geography. Robots are frequently used in the classroom to introduce students to computer programming and other STEM subjects. Because of their many advantages, robots will soon play an integral role in classrooms all over the world, both in developed and developing nations. But nowadays, a humanoid robot in the classroom is an unusual sight only seen in future-ready classrooms. You are welcome to visit ours in Primary School Savremena, where our T.A. Pepper will greet you.

Editor-in-chief prof. dr Valentin Kuleto

Naučni članci / Scientific articles

Vrsta rada: Originalni naučni rad
Primljen: 23. 12. 2021.
Prihvaćen: 21. 01. 2022.
UDC: 004.9:37.018
004.424

Projektovanje i implementacija veb-aplikacije „Podrška u obrazovanju" korišćenjem Spring i Hibernate frameworka

Vladimir Bošković [1] , Svetlana Jevremović[1]

[1] ITS – Information Technology School, Zemun, Beograd, Srbija
* vladimir2417@its.edu.rs, svetlana.jevremovic@its.edu.rs

Sažetak: U ovom radu prikazani su projektovanje i implementacija veb-aplikacije „Podrška u obrazovanju" korišćenjem Spring i Hibernate frameworka. Cilj rada bio je da istraži mogućnosti projektovanja i implementacije ove veb-aplikacije, koja bi korisnicima omogućila laku pretragu i odabir obrazovnih ustanova, a ustanovama bi omogućila da lako komuniciraju sa korisnicima koji su zainteresovani za njih. Ovakva aplikacija bi omogućila korisnicima da se informišu, isplaniraju i na vreme obezbede svoje mesto u obrazovnoj ustanovi uz mogućnost određenih beneficija. Obrazovnim ustanovama bi se olakšalo poslovanje kroz efikasnu i jednostavnu evidenciju pretplaćenih korisnika, pregled zahteva za obilazak obrazovnih ustanova i slanje promotivnih poruka korisnicima. Tema je izabrana zbog nedostatka sličnih veb-aplikacija na našem tržištu. Kao metoda razvoja ove veb-aplikacije korišćena je Larmanova metoda kroz sve faze razvoja.

Ključne reči: veb-aplikacija; Spring; Hibernate; Larmanova metoda

1. Uvod

Veb-aplikacija „Podrška u obrazovanju" bazirana je na aktuelnim Java veb-tehnologijama, kao što su Spring i Hibernate. Dakle, za izradu ove aplikacije korišćen je Spring framework, uključujući Servlete, Maven, Hibernate i Thymeleaf sa serverske strane. Sa klijentske strane korišćeni su HTML, CSS, JS, i biblioteke JQuery i Bootstrap. Kao razvojno okruženje korišćen je IntelliJ IDEA Ultimate, dok su za bazu podataka korišćeni Servleti.
U prvom delu rada prikazan je Spring framework, sa posebnim naglaskom na koncepte Spring MVC modula, koji je korišćen za razvoj aplikacije „Podrška u obrazovanju". Drugi deo rada posvećen je problematici objektno-relacionog preslikavanja i perzistenciji podataka korišćenjem Hibernate ORM (object–relational mapping) alata. Centralni deo rada posvećen je izradi aplikacije „Podrška u obrazovanju".

U razvoju aplikacije korišćena je Larmanova metoda razvoja softvera kroz faze: specifikacije, analize, projektovanja, implementacije i testiranja [10]. Larmanova metoda je bazirana na iterativnom i inkrementalnom modelu životnog ciklusa softvera, predstavljena je slučajevima korišćenja i koristi objektno orijentisanu metodu projektovanja gde se koriste UML (Unified Modeling Language) dijagrami. Okrenuta je programerima, jer je prednost data fazama analize i projektovanja, a jedinstvena je po pravljenju ugovora za sistemske operacije [8].

2. Primenjene tehnologije

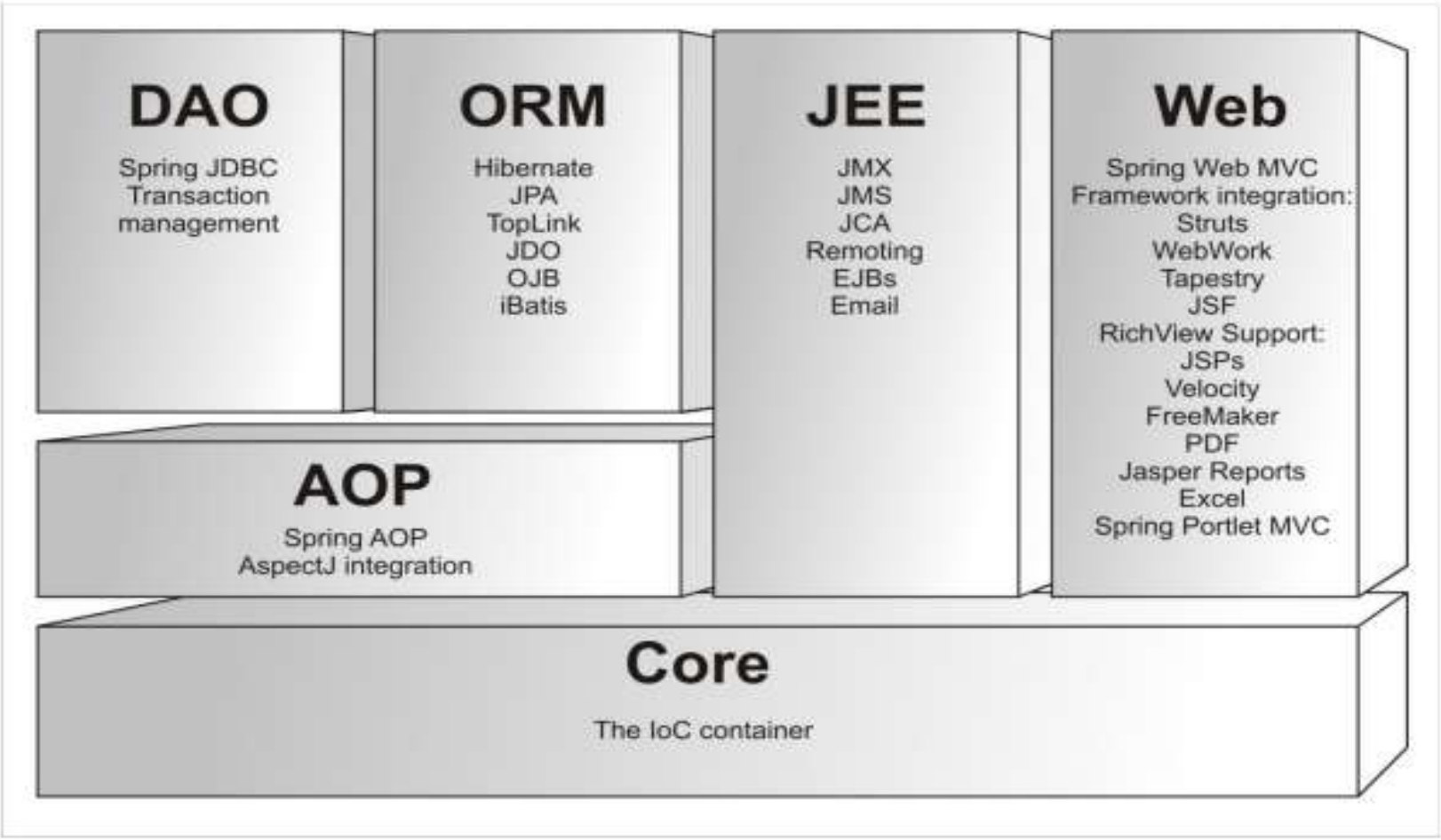
Pre analize dokumentacije o projektovanju i implementaciji veb-aplikacije „Podrška u obrazovanju" analizirane su tehnologije korišćene u toku faza razvoja aplikacije. Najviše pažnje posvećeno je osobinama i rešenjima koja Spring framework nudi u kontekstu razvoja veb-aplikacija.

2.1. Spring framework

Jedna od najbitnijih karakteristika Spring frameworka jeste njegova modularnost, koja omogućava da se prilikom projektovanja aplikacije ne koristi celokupan framework, već samo oni moduli koji su potrebni u specifičnoj situaciji. Modularan pristup omogućava da se pomoću Spring frameworka razviju Java aplikacije različitog nivoa složenosti. U zavisnosi od zahteva aplikacije, moguće je koristiti bilo koji Spring modul nezavisno od drugih modula. Na primer, može da se koristi samo Springov osnovni (core) kontejner za upravljanje slojem poslovne logike aplikacije, dok se drugi delovi aplikacije mogu realizovati korišćenjem neke druge tehnologije. Pored modularnosti, Spring omogućava i integraciju sa velikim brojem tehnologija.

Arhitektura Spring frameworka obuhvata sledećih šest modula i prikazana je na slici 1 [5]:

- Core (osnovni, jezgro);
- AOP (aspect-oriented programming);
- DAO (Data Access Objects);
- ORM (object–relational mapping);
- JEE (Java Enterprise Edition);
- Web.



Slika 1. Moduli Spring frameworka [5]

Core modul je centralni modul Spring frameworka. U okviru Core modula realizovan je Inversion of Control (IoC), odnosno dependency injection (DI) mehanizam. Realizacija DI mehanizma u Core modulu ostvaruje se preko interfejsa BeanFactory, tj. preko implementacija ovog interfejsa. AOP modul obezbeđuje podršku za aspektno orijentisano programiranje, koje omogućava da se na jednostavan način razdvoje komponente sistema, implementirajući funkcionalnosti koje su logički odvojene. DAO modul obezbeđuje JDBC (Java Database Connectivity) sloj koji uklanja potrebu za klasičnim pristupanjem bazama podataka korišćenjem JDBC upravljačkih programa. Naime, korišćenje JDBC-a podrazumeva pisanje koda za pribavljanje konekcije, formiranje naredbi (statement), obradu rezultata i zatvaranje konekcije, dok se korišćenjem Spring JDBC frameworka celokupan posao apstrahuje i pojednostavljuje. ORM modul obezbeđuje sloj za integraciju Spring frameworka sa popularnim ORM alatima.

Pored Hibernate frameworka, čija je integracija sa Spring frameworkom i korišćena u ovom radu, Spring pruža mogućnost integracije sa sledećim ORM alatima: iBatis SQL Maps, JDO, Apache OJB, Oracle TopLink. ORM modul, pored integracije sa navedenim ORM alatima, pruža i mogućnost korišćenja deklarativnog upravljanja transakcijama. JEE modul omogućava integraciju Spring frameworka i EJB (Enterprise Java Bean) komponenti, kao i integraciju sa JMS (Java Message Service) komponentama, što omogućava asinhrono kreiranje, slanje i primanje poruka. Web modul sadrži kompletnu implementaciju MVC4 okvira koji se koristi za razvoj veb-aplikacija. Spring Web MVC implementacija obezbeđuje potpuno razdvajanje poslovne logike aplikacije od njenog prezentacionog sloja, omogućavajući uz to i korišćenje svih IoC osobina okvira prilikom razvoja veb-aplikacije.

2.1.1. Dependency injection

Spring IoC kontejner zasniva se na dependency injection (DI) mehanizmu. Sam naziv (u slobodnom prevodu: ubrizgavanje zavisnosti) dosta govori o odnosu između aplikacije i kontejnera, kao i o načinu na koji se razrešavaju zavisnosti između komponenti aplikacije. Aplikacija može da se posmatra kroz skup komponenti koje na određeni način sarađuju, zavise jedna od druge u toku izvršenja aplikacije. Kod Java aplikacija, ove komponente su pojavljivanja Java klasa, odnosno objekti. Poslovni objekti aplikacije kojom upravlja Spring IoC kontejner nisu zaduženi za pribavljanje resursa i kreiranje drugih objekata sa kojima sarađuju i od kojih zavise. Umesto njih, kreiranje i konfigurisanje njihovih zavisnosti vrši kontejner, što omogućava da se prilikom projektovanja poslovnih klasa pažnja fokusira na poslovnu logiku koju metode klase treba da izvrše.

Postoje tri osnovne varijante DI mehanizma koje podržava Spring kontejner:

» setter injection;
» constructor injection;
» method injection.

2.1.2. Spring kontejner

Dependency injection mehanizam predstavlja suštinu Spring frameworka, a sama implementacija ovog mehanizma realizovana je kroz dva interfejsa koji su srž Spring IoC kontejnera:

» org.springframework.beans.factory.BeanFactory
» org.springframework.context.ApplicationContext

BeanFactory je osnovni interfejs Spring kontejnera koji omogućava konfigurisanje i povezivanje beanova koristeći DI mehanizme. Kada se interfejs BeanFactory kreira, Spring framework vrši validaciju konfiguracije beanova. Svaki singleton bean se kreira prilikom pokretanja frameworka, dok se ostali beanovi kreiraju na zahtev korisnika. Pored toga, interfejs BeanFactory obezbeđuje i neke mehanizme za upravljanje životnim ciklusom beanova, pri čemu se to odnosi samo na singleton beanove, jer kod prototype beanova kontejner nakon kreiranja beana gubi kontrolu nad njim.

ApplicationContext interfejs nasleđuje BeanFactory interfejs. Njegove implementacije takođe omogućavaju kreiranje i upravljanje životnim ciklusom beanova, ali pored toga nude podršku za integraciju sa Springovim AOP modulom, upravljanje resursima za poruke (message resource support), kao i propagaciju događaja (application events propagation). Pored toga, obezbeđuje i posebne kontekste aplikacionog sloja kao što je interfejs WebApplicationContext, koji se koristi u veb-aplikacijama.

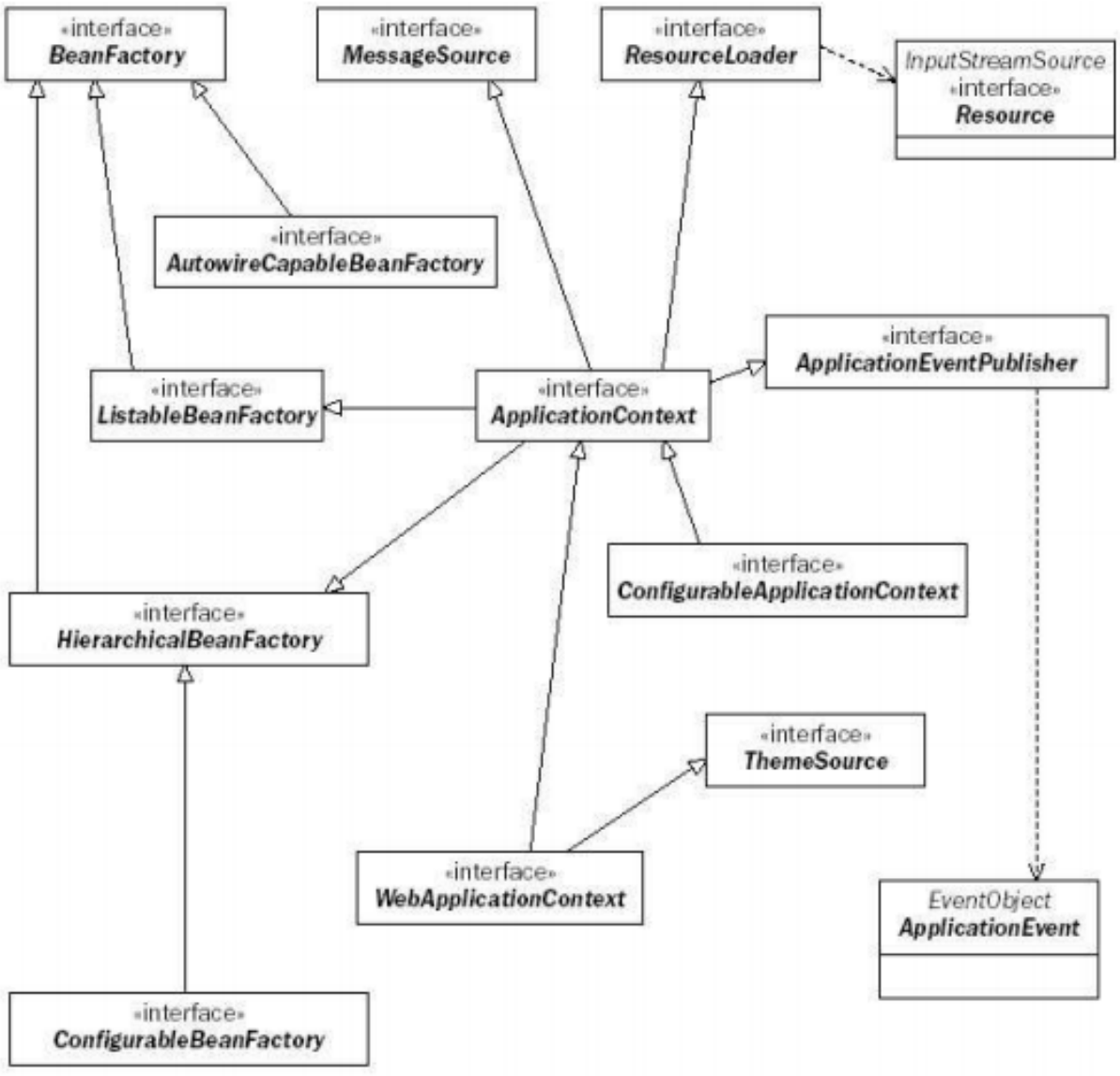
Dakle, interfejs BeanFactory obezbeđuje konfigurisanje frameworka, kao i njegove osnovne funkcionalnosti, dok interfejs ApplicationContext dodaje frameworku nove, složenije funkcionalnosti, pri čemu interfejs ApplicationContext predstavlja kompletan nadskup interfejsa BeanFactory, odnosno omogućava sve što i BeanFactory interfejs. Odnos ova dva interfejsa prikazan je na slici 2.

2.1.3. Rad sa Java Bean komponentama

Bean je softverska komponenta sa mogućnošću ponovnog korišćenja, kojom se može vizuelno manipulisati u odgovarajućem alatu [4]. U kontekstu aplikacija koje se baziraju na Spring frameworku, termin bean se koristi za sve objekte koje kreira Spring kontejner i kojima kontejner upravlja [5]. Prilikom definisanja beanova, konfiguraciona datoteka se sastoji od jednog (korenog) beans elementa i jednog ili više bean elemenata. Validacija ove XML datoteke vrši se u odnosu na XML DTD datoteku spring-beans.dtd, koja u potpunosti opisuje sve validne atribute i elemente koje konfiguraciona datoteka može da sadrži.

Ono što se u najvećem broju slučajeva prvo definiše jeste identifikator beana. Bitno je naglasiti da nije neophodno definisati identifikator, jer se u tom slučaju definisani bean tretira kao anoniman bean. Ime beana može da se definiše korišćenjem name ili id atributa bean elementa.

Preporuka je da se prilikom definisanja imena beana koristi id atribut, jer je on XML IDREF tipa, tako da u slučaju da ga drugi beanovi referenciraju, XML parser može odrediti da li je referenca validna. IDREF tip poseduje ograničenja zbog kojih nije pogodan za korišćenje u određenim situacijama.



Slika 2. Odnos BeanFactory i ApplicationContext interfejsa [5]

Najčešće primenjivan mehanizam kreiranja beanova jeste pomoću konstruktora beana. Prilikom definisanja beana, u okviru class atributa navodi se ime klase beana. U trenutku kada kontejneru zatreba novo pojavljivanje ovog beana, kontejner će interno izvršiti operaciju koja je ekvivalent pozivu new operatora u Java kodu.

Kreiranje beana moguće je izvršiti i pomoću statičkog factory metoda. U tom slučaju potrebno je definisati klasu čija je uloga da učauri proces kreiranja beana unutar statičke metode. Zatim se, koristeći class atribut, definiše ovaj bean, a factory-method atributom se specificira koja metoda beana je zadužena za kreiranje beana.

Sledeći pristup u kreiranju beanova je korišćenje nestatičke (instance factory) metode. U tom slučaju za kreiranje beana se koristi metoda nekog drugog beana koji je kontejner već kreirao.

2.1.4. Koncepti Spring Web MVC frameworka

MVC uzor predstavlja uzor arhitekture i sastoji se od tri ključne komponenete: Model (Model), Pogled (View) i Kontroler (Controller) [6]. Model je komponenta koja sadrži strukturu poslovnog sistema i njene operacije, odnosno, sadrži podatke i operacije za obradu podataka. View komponenta obezbeđuje korisnički interfejs preko koga korisnik komunicira sa sistemom. Takođe, on šalje korisniku izveštaje koji se dobijaju iz modela. Controller je komponenta koja je zadužena da upravlja izvršavanjem sistemskih operacija. Ona prihvata zahtev od klijenta i nakon toga poziva operaciju koja je definisana u modelu i kontroliše njeno izvršavanje.

Arhitektura Spring Web MVC frameworka podrazumeva postojanje kontroler servleta, kao centralne ulazne tačke za sve dolazeće zahteve. Ova komponenta u Spring MVC frameworku realizovana je preko klase DispatcherServlet. Sloj poslovne logike aplikacije realizovan je preko kontroler komponente. U prezentacionom delu, Spring MVC podržava različite tehnologije prikaza. Kao najznačajnija karakteristika prezentacionog sloja ističe se mogućnost ostvarenja potpune nezavisnosti između poslovne logike i konkretne prezentacione tehnologije.

Centralna komponenta Spring Web MVC frameworka jeste klasa DispatcherServlet, koja predstavlja glavnu ulaznu tačku za svaki dolazeći zahtev koji je adresiran na Spring Web MVC aplikaciju. Ova klasa je u potpunosti integrisana u Spring IoC kontejner, što omogućava korišćenje svih osobina koje poseduje Spring framework.

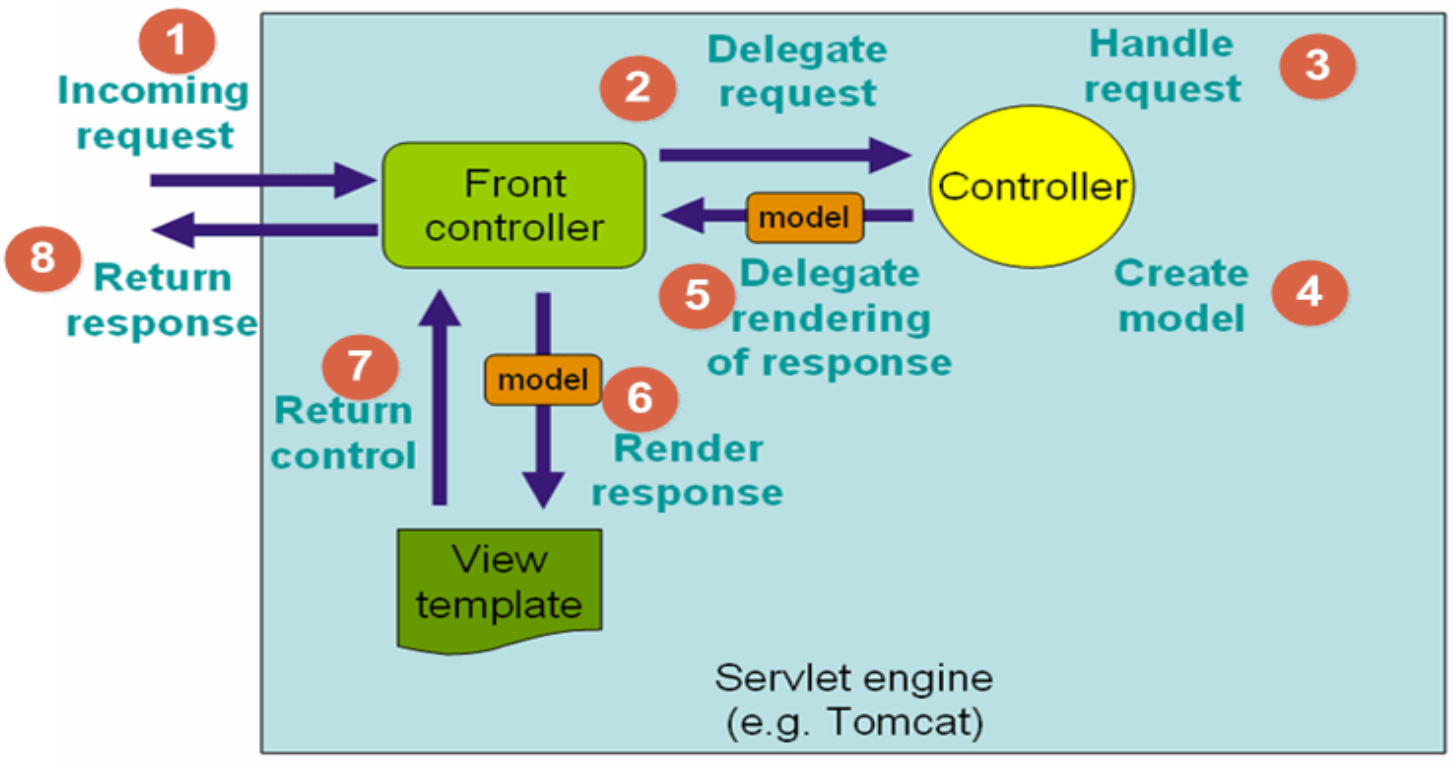
Slika 3 prikazuje konceptualni model obrade zahteva korišćenjem DispatcherServlet klase kao centralnog kontrolera. Kao što se sa slike vidi, centralni kontroler je ulazna tačka za svaki dolazeći zahtev (request). Centralni kontroler po prijemu zahteva delegira zahtev odgovarajućem kontroleru koji je zadužen za obradu zahteva. Kontroler kreira model i obrađuje zahtev, zatim predaje centralnom kontoleru model i logičko ime pogleda. Model sadrži atribute koje pogled treba da prikaže klijentu. Na osnovu logičkog imena pogleda vrši se preslikavanje ka konkretnoj realizaciji pogleda kako bi se izvršila priprema (render) prikaza koji će biti vraćen klijentu kao odgovor (response).

Klasa DispatcherServlet je, zapravo, servlet (izvedena iz klase javax.servlet.http.HttpServlet). Jedini je servlet koji je potrebno deklarisati i konfigurisati u opisivaču rasporeda (deployment descriptor) veb-aplikacije. Pored deklaracije servleta, u opisivaču rasporeda neophodno je definisaiti preslikavanja zahteva ka centralnom kontroleru (klasi DispatcherServlet).

2.2. Hibernate framework

Perzistencija podataka predstavlja jedan od fundamentalnih koncepata u razvoju softverskih sistema. Uopšteno, podaci su perzistentni ukoliko nadžive program koji ih je kreirao. Postoji nekoliko definicija koje se odnose na perzistenciju podataka u kontekstu objektno orijentisanog razvoja softvera [6].

» Objekat je perzistentan ukoliko se može materijalizovati i dematerijalizovati.
» Objekat je perzistentan ukoliko nastavi da postoji i nakon prestanka rada programa koji ga je stvorio (G. Booch).
» Materijalizacija predstavlja proces transformacije slogova baze podataka u objekte programa.
» Dematerijalizacija predstavlja proces transformacije objekta iz programa u slogove baze podataka.
» Perzistentni okvir je skup interfejsa i klasa koji omogućava perzistentnost objektima različitih klasa.



Slika 3. Konceptualni model toka obrade podataka [9]

Najrasprostranjeniji oblik čuvanja podataka u današnjim aplikacijama jeste korišćenje relacionih baza podataka, tako da se kod perzistencije podataka u Java aplikacijama najčešće podrazumeva čuvanje Java objekata u relacionoj bazi podataka. Relacione baze podataka postale su svojevrsni standard u domenu perzistencije podataka.

U objektno orijentisanim aplikacijama perzistencija treba da omogući čuvanje objekata u relacionoj bazi podataka. Pri tome se ne misli samo na čuvanje pojedinačnih objekata, već cele mreže uzajamno povezanih objekata koja reprezentuje određeni objektni model. Pored objekata koji se trajno čuvaju, u objektno orijentisanim aplikacijama postoji i veliki broj tzv. transijentnih objekata. Transijentni objekti su objekti čije je trajanje ograničeno trajanjem aplikacije koja ih je kreirala. Najčešće u ovakvim aplikacijama postoji podsistem koji treba da obezbedi materijalizaciju i dematerijalizaciju perzistentnih objekata, tj. njihovu transformaciju u oblik pogodan za čuvanje u relacionim bazama podataka – relacioni model.

Dakle, perzistentnost u objektno orijentisanim aplikacijama koje koriste relacionu bazu podataka možemo posmatrati kao proces transformacije objektnog modela u relacioni model i obratno.

2.2.1. Asocijacije

Problem asocijacija odnosi se na transformacije veza koje se uspostavljaju između objekata u objektnom modelu i veza koje se ostvaruju između relacija u relacionom modelu. U relacionom modelu veze se ostvaruju korišćenjem spoljnih ključeva, tj. spoljni ključ u referentnoj tabeli predstavlja primarni ključ u referenciranoj tabeli. U objektnom modelu postoji nekoliko vrsta asocijacija: 1-1 (one-to-one), * - * (many-to-many), 1 - * (one-to-many). Ove asocijacije je u relacionom modelu potrebno obezbediti korišćenjem spoljnih ključeva [7].

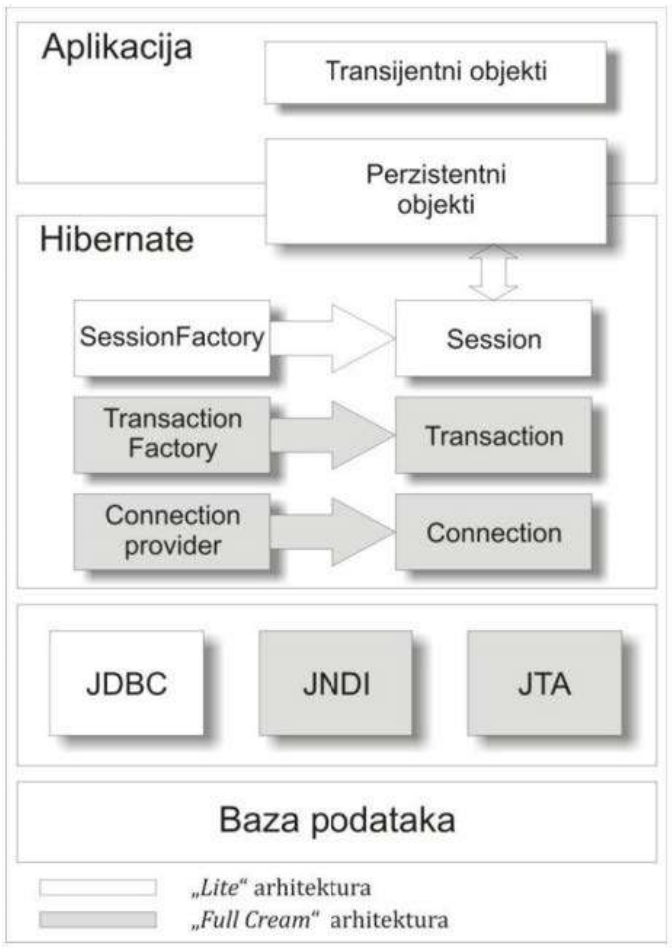
Najčešće se transformacija vrši na taj način što se oba objekta predstavljaju jednom relacijom. Na taj način podaci jednog objekta proširuju se podacima drugog objekta i postaju jedinstvena relacija. Atributi relacije postaju atributi i jednog i drugog objekta.

Many-to-many transformacija se vrši na taj način što se pored relacija koje se prave za svaki od tipova objekata pravi i dodatna agregirajuća relacija koju čine primarni ključevi relacija koje stupaju u vezu. Kada jedan objekat pravi vezu sa više objekata nekog tipa, tada se transformacija vrši tako što se naprave posebne relacije za svaki od tipova objekata, a zatim se primarni ključ objekta koji pravi vezu pamti kod svih objekata sa kojima je on u vezi, tj. primarni ključ relacije na strani one predstavlja se kao spoljni ključ relacije na strani many.

2.2.2. Arhitektura Hibernate frameworka

Hibernate framework je veoma fleksibilan alat koji omogućava nekoliko različitih pristupa prilikom odabira servisa koje okvir pruža, a koji će se koristiti u razvoju aplikacije. Tri ključna servisa (komponente) Hibernate okvira su: upravljanje konekcijama (connection management), upravljanje transakcijama (transaction management) i objektno–relaciono preslikavanje (object–relational mapping).

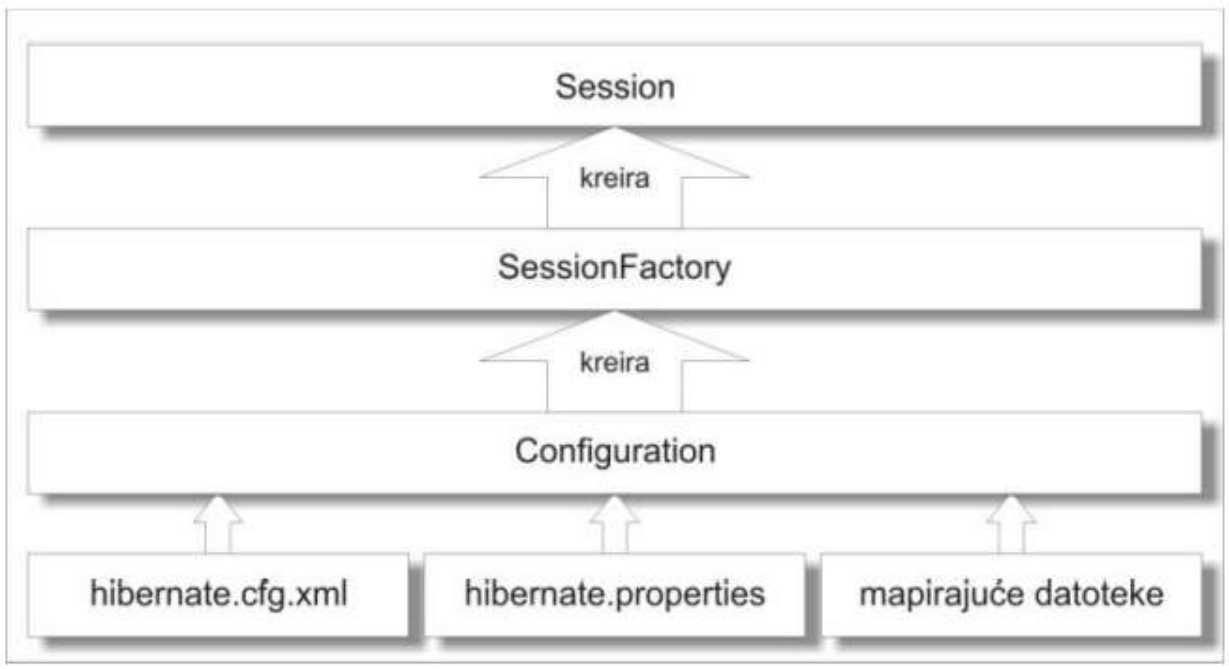
Slika 4 prikazuje dve osnovne arhitekture: „Lite“ i „Full cream“ arhitekturu. Ovo je klasifikacija u zavisnosti od toga koje komponenete okvira se koriste u razvoju aplikacije. „Lite“ arhitektura podrazumeva korišćenje samo komponente za objektno–relaciono preslikavanje, a upravljanje transakcijama i obezbeđivanje JDBC konekcija je prepušteno aplikaciji. „Full Cream“ arhitektura podrazumeva korišćenje sve tri komponente.



Slika 4. Arhitektura Hibernate frameworka

2.2.3. Konfigurisanje Hibernate frameworka

Hibernate, kao perzistentni framework, može da komunicira sa velikim brojem različitih SUBP-a i može da se izvršava u različitim okruženjima. Ovakva prilagodljivost Hibernatea različitim SUBP-ovima i okruženjima u kojima se izvršava zahteva različite načine konfigurisanja frameworka. Bez obzira na okruženje i bazu podataka sa kojom aplikacija komunicira, konfigurisanje frameworka može se logički podeliti u dve celine. U prvom delu obezbeđuju se konfiguracioni podaci koji su neophodni frameworku da bi pristupio bazi podataka, a drugi deo čine konfiguracioni podaci kojima se obezbeđuje preslikavanje između perzistentnih klasa aplikacije i odgovarajućih tabela u relacionoj bazi podataka. Centralna klasa, pomoću koje se vrši konfigurisanje i pokretanje Hibernate frameworka, jeste klasa org.hibernate.cfg.Configuration. Prilikom kreiranja, ovoj klasi je potrebno obezbediti konfiguracione podatke, na osnovu kojih Configuration objekat kreira jedno pojavljivanje (singleton) klase



Slika 5. Konfigurisanje Hibernate frameworka

Jedno pojavljivanje SessionFactory klase u suštini predstavlja potpuno konfigurisan Hibernate framework, koji omogućava komunikaciju sa jednom bazom podataka. Pored toga što Configuration objekat kreira jedinstveno (singleton) pojavljivanje SessionFactory klase, stanje ovog objekta nije moguće menjati nakon kreiranja. Klasa SessionFactory je zadužena za kreiranje objekata klase Session prilikom svake interakcije sa bazom podataka.

3. Projektovanje i implementacija veb-aplikacije „Podrška u obrazovanju“

Detaljna priprema dokumentacije usledila je nakon istraživanja adekvatnih tehnologija. Prvo će biti prikazan verbalni opis modela na osnovu kojeg će biti utvrđeni slučajevi korišćenja aktora sistema.

3.1. Specifikacija zahteva

Potrebno je projektovati i implementirati veb-aplikaciju koja bi krajnjim korisnicima pružila pomoć pri odabiru obrazovnih ustanova. Slika 6 prikazuje da postoje tri vrste učesnika: korisnik, administrator i ustanova.

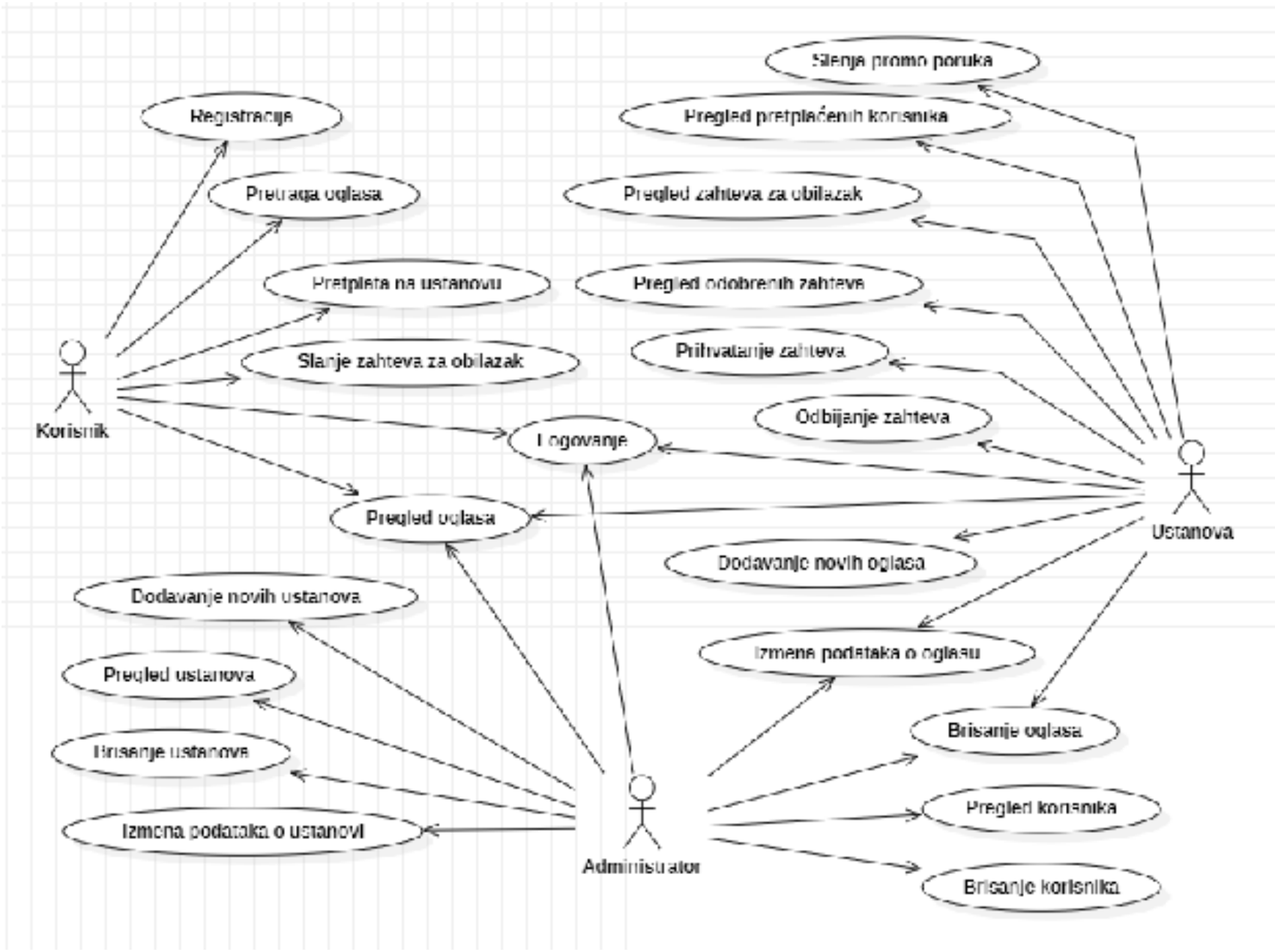
Korisniku sistem treba da omogući registrovanje na sajt, ukoliko već nije registrovan. Nakon registracije, korisniku stiže na mejl poruka dobrodošlice i sada ima mogućnost logovanja na sajt. Nakon logovanja, imao bi mogućnost da pretražuje oglase na osnovu više kriterijuma, koji se biraju na početnoj strani, a zatim se ispisuju svi oglasi za željene parametre. Ukoliko je korisnik zainteresovan za neki od oglasa, klikom na oglas, može videti detalje oglasa, kao i detalje same ustanove. Dodatna mogućnost je besplatna pretplata na određenu ustanovu gde korisnik potvrđuje da želi da prima promotivne mejlove od ustanove. Prilikom svake pretplate korisnik ostvaruje poene. Nakon što skupi određeni broj poena, korisniku se dodeljuje elektronski poklon-vaučer. Poklon-vaučer mu daje mogućnost da ostvari popust na školarinu za određene ustanove. Ako želi da sazna više o obrazovnoj ustanovi, može zakazati obilazak ustanove čija je realizacija moguća nakon potvrde zaposlenog u ustanovi. Ukoliko ustanova ne potvrdi zahtev u roku od 24 sata pred obilazak, zahtev se automatski briše.

Administratoru sistema aplikacija treba da omogući dodavanje novih ustanova, kao i izmenu podataka o ustanovi i brisanje ustanova. Prilikom dodavanja nove ustanove automatski bi se poslao mejl ustanovi sa parametrima za logovanje. Takođe, administrator bi imao mogućnost izmene i brisanja oglasa i korisnika.

Ustanova dobija parametre za logovanje od administratora aplikacije putem mejla. Nakon logovanja, ustanova može da postavlja, menja ili briše oglase. Takođe, ako se korisnik pretplati na ustanovu nakon što je ušao na njen oglas, onda ustanova, kada se uloguje, može videti koji korisnici su se pretplatili i poslati im promo-poruku. Ukoliko je neko od korisnika zahtevao obilazak ustanove, te zahteve ustanova može prihvatiti ili odbiti. Ako ustanova prihvati zahtev, korisniku će se poslati mejl sa obaveštenjem da je zahtev prihvaćen; u suprotnom, dobiće mejl da je zahtev odbijen.

3.1.1. Slučajevi korišćenja

Na osnovu verbalnog modela uočeni su sledeći slučajevi korišćenja: Logovanje, Registracija, Pretraga oglasa, Pregled oglasa, Pretplata na ustanovu, Slanje zahteva za obilazak, Dodavanje novih ustanova, Pregled ustanova, Izmena podataka o ustanovi, Brisanje ustanova, Dodavanje novih oglasa, Izmena podataka o oglasu, Brisanje oglasa, Pregled korisnika, Brisanje korisnika, Pregled pretplaćenih korisnika, Slanje promotivnih poruka, Pregled zahteva za obilazak, Pregled odobrenih zahteva za obilazak, Prihvatanje zahteva za obilazak, Odbijanje zahteva za obilazak (slika 6).



Slika 6. Use-case dijagram svih slučajeva korišćenja

Zbog ograničenog obima rada, u nastavku sledi primer jednog opisa slučaja korišćenja (SK4).

SK4: Pregled oglasa

Naziv: Pregled oglasa

Aktori: Korisnik, Administrator, Ustanova

Učesnici: Korisnik, Administrator, Ustanova i sistem

Preduslovi: Sistem je aktivan, korisnik ulogovan i prikazana je stranica sa oglasima

Osnovni scenario:

1. Korisnik poziva sistem da prikaže detalje oglasa (APSO)
2. Sistem pronalazi detalje oglasa (SO)
3. Sistem prikazuje korisniku detalje oglasa (IA)

Alternativni scenario:

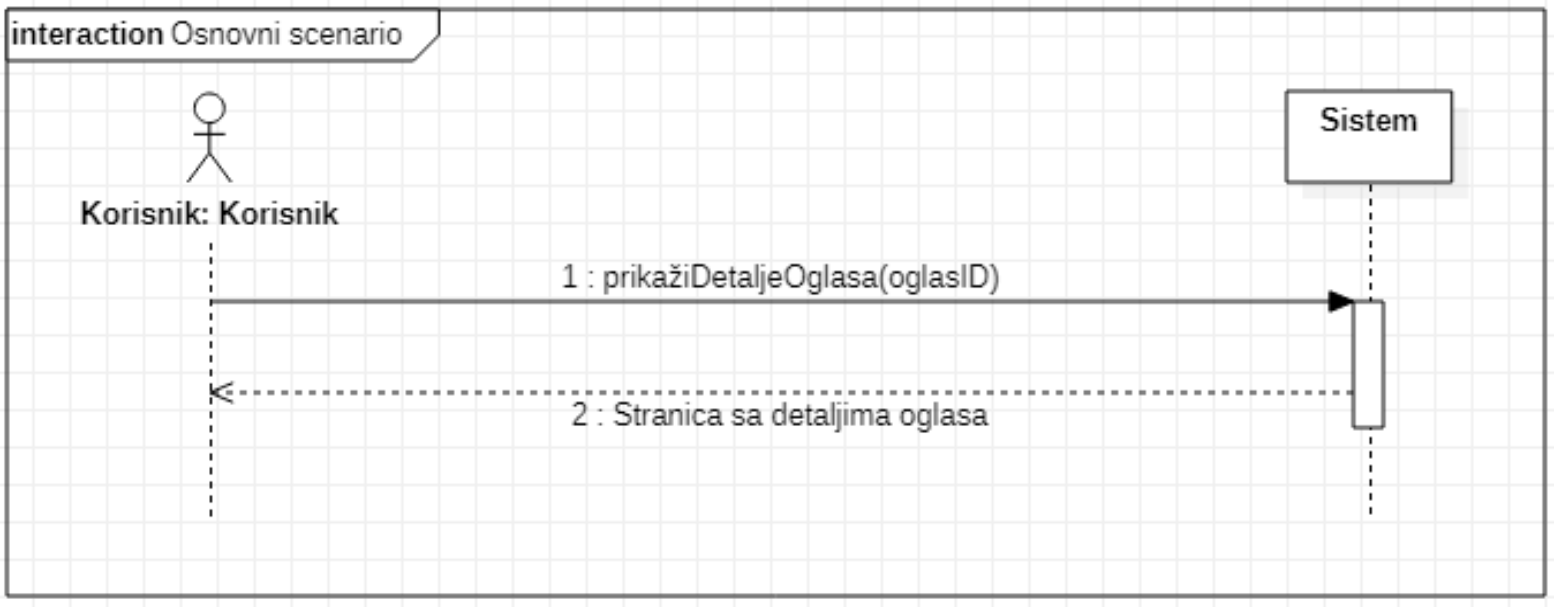
2.1. Sistem ne može da uspostavi vezu sa bazom podataka, prikazuje odgovarajuću poruku (IA)

3.2. Analiza

U fazi analize opisuje se logička struktura i ponašanje softverskog sistema. Struktura softverskog sistema se opisuje pomoću konceptualnog i relacionog modela. Ponašanje sistema se opisuje pomoću dijagrama sekvenci (DSSK), koji se prave za svaki slučaj korišćenja i pomoću ugovora o sistemskim operacijama dobijenih na osnovu prethodnih dijagrama. Sledi primer jednog sistemskog dijagrama sekvenci.

DSSK4: Pregled oglasa

Osnovni scenario:
1. Korisnik poziva sistem da prikaže detalje oglasa (APSO)
2. Sistem prikazuje korisniku detalje oglasa (IA)



Slika 7. DSSK4 – Pregled oglasa

Uvedena je sistemska operacija:
1. prikažiDetaljeOglasa(oglasID)

Za svaku od uočenih sistemskih operacija prave se ugovori, koji opisuju šta operacija radi, a ne i kako, pri čemu se jedan ugovor vezuje za jednu sistemsku operaciju [8]. Sledi primer jednog ugovora (UG18).

Ugovor UG18: prikaziZahteveZaObilazak

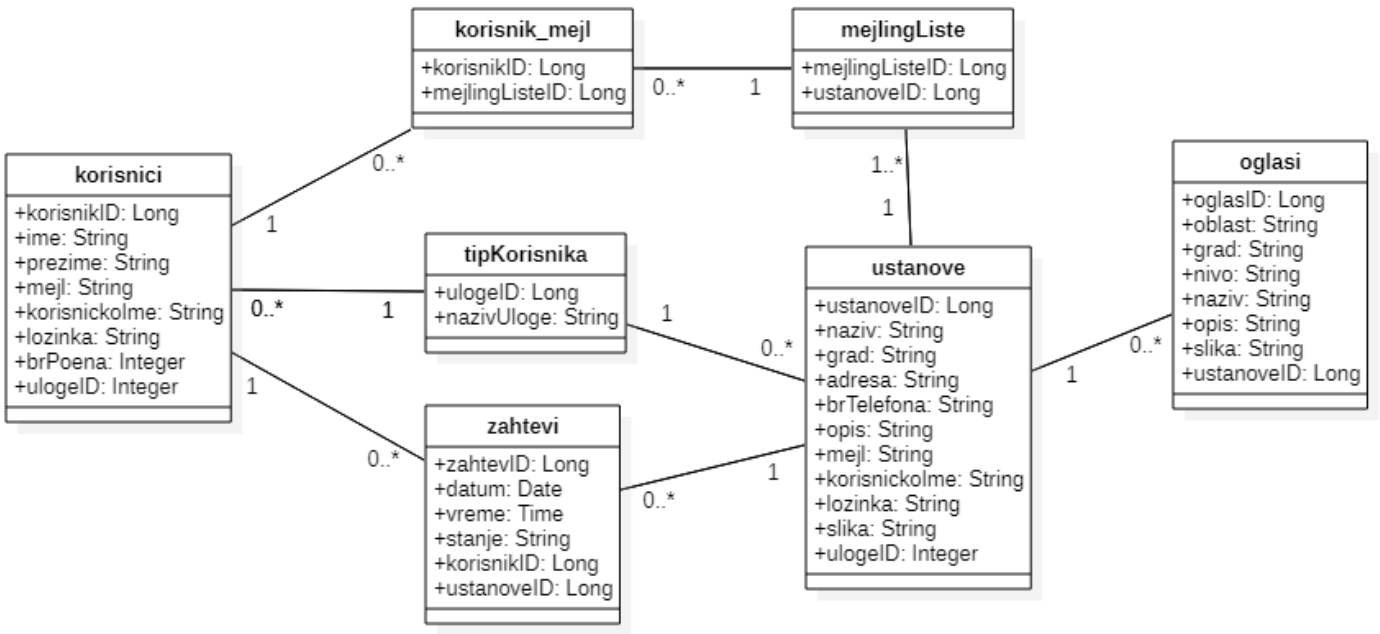
Operacija: prikaziZahteveZaObilazak(ustanoveID)

Veza sa SK: SK18

Preduslovi: Zahtevi za obilazak postoje u bazi podataka

Postuslovi: Prikazana je lista zahteva za obilazak

Nakon definisanja svih ugovora kreira se konceptualni model na osnovu podataka iz funkcionalnog zahteva i slučajeva korišćenja (slika 8).



Slika 8. Konceptualni model

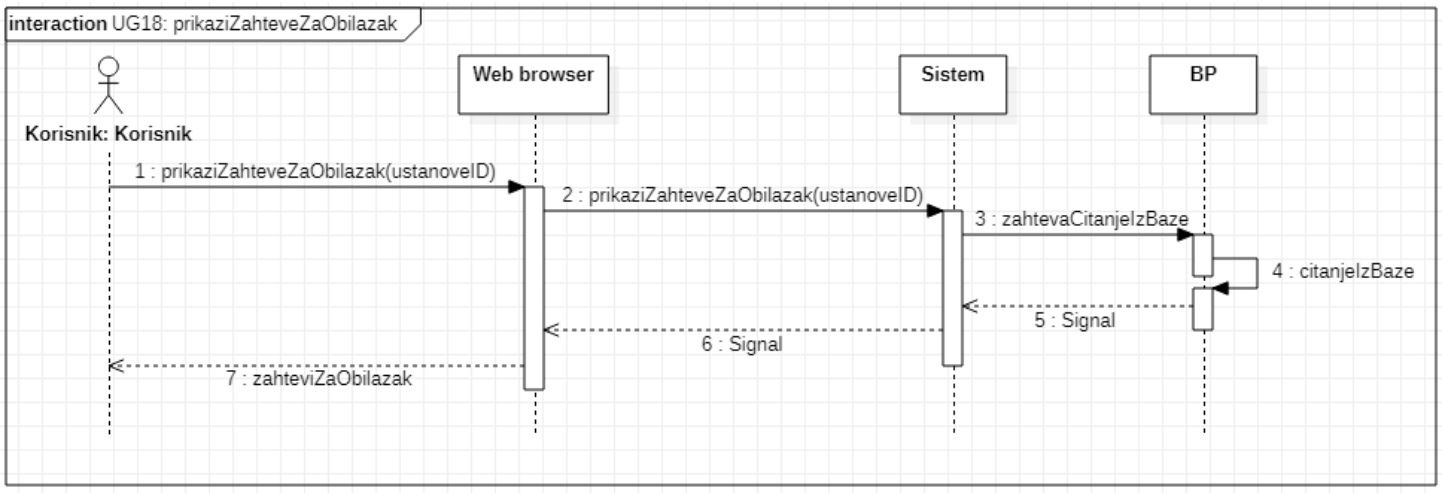
Na osnovu konceptualnog, pravi se i relacioni model, koji predstavlja dalju osnovu za projektovanje baze podataka.
tipKorisnika(ulogeID, nazivUloge)
korisnici(korisnikID, ime, prezime, mejl, korisnickoIme, lozinka, brPoena, ulogeID)
korisnici(ulogeID) references tipKorisnika(ulogeID)
ustanove(ustanoveID, naziv, grad, adresa, brTelefona, opis, mejl, korisnickoIme, lozinka, slika, ulogeID)
ustanove(ulogeID) references tipKorisnika(ulogeID)
oglasi(oglasID, oblast, grad, nivo, naziv, opis, slika, ustanoveID)
oglasi(ustanoveID) references ustanove(ustanoveID)
mejlingListe(mejlingListeID, ustanoveID)
mejlingListe(ustanoveID) references ustanove(ustanoveID)
korisnik_mejl(korisnikID, mejlingListeID)
korisnik_mejl(korisnikID) references korisnici(korisnikID)
korisnik_mejl(mejlingListeID) references mejlingListe(mejlingListeID)
zahtevi(zahtevID, datum, vreme, stanje, korisnikID, ustanoveID)
zahtevi(korisnikID) references korisnici(korisnikID)
zahtevi(ustanoveID) references ustanove(ustanoveID)

3.3. Projektovanje

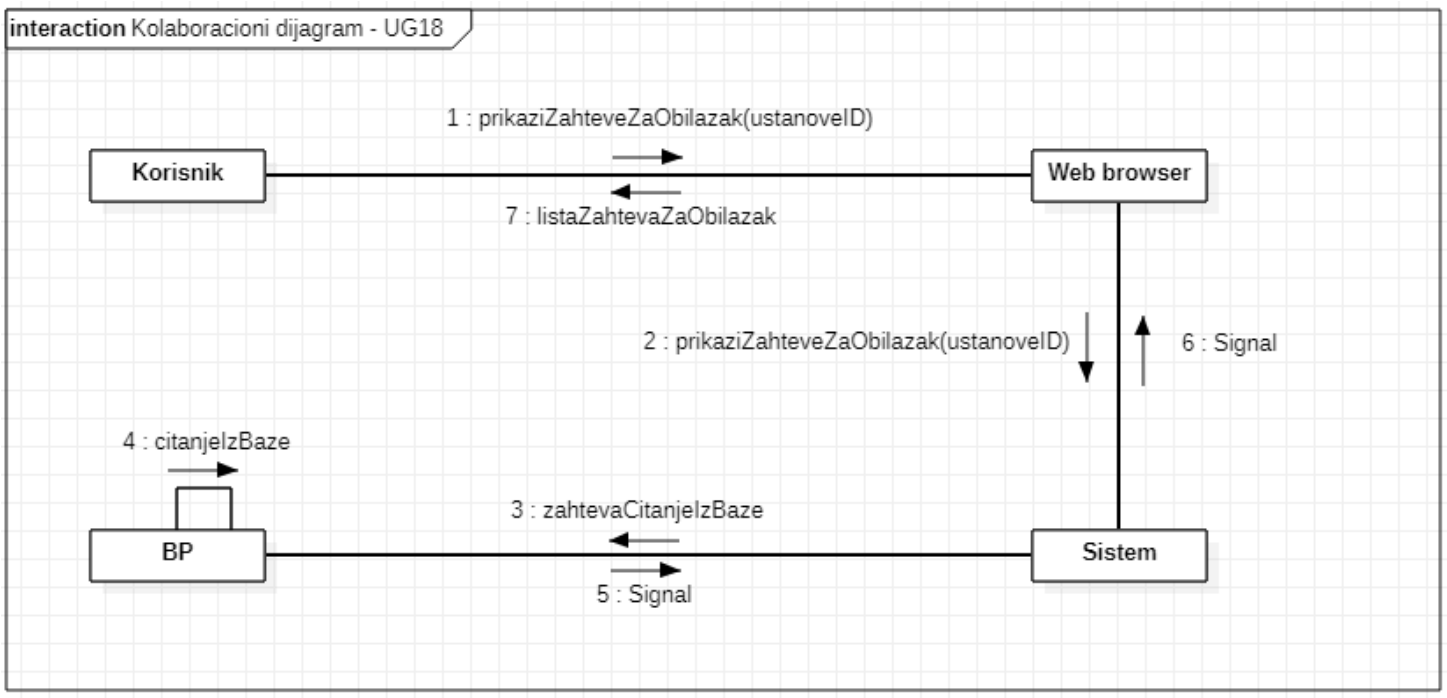
Faza projektovanja opisuje fizičku strukturu i ponašanje softverskog sistema, odnosno arhitekturu sistema. Kao takva obuhvata projektovanje aplikacione logike i projektovanje logičke strukture i ponašanja softverskog sistema.

3.3.1. Projektovanje aplikacione strukture

Ugovor UG18: prikaziZahteveZaObilazak (slika 9 i slika 10)
Operacija: prikaziZahteveZaObilazak(ustanoveID)
Preduslovi: Zahtevi za obilazak postoje u bazi podataka
Postuslovi: Prikazana je lista zahteva za obilazak



Slika 9. Dijagram sekvenci UG18 – PrikaziZahteveZaObilazak



Slika 10. Kolaboracioni dijagram UG18 – PrikaziZahteveZaObilazak

3.3.2 Projektovanje korisničkog interfejsa

Sledi primer definisanja jednog dela korisničkog interfejsa za aplikaciju „Podrška u obrazovanju".

SK4: Pregled oglasa

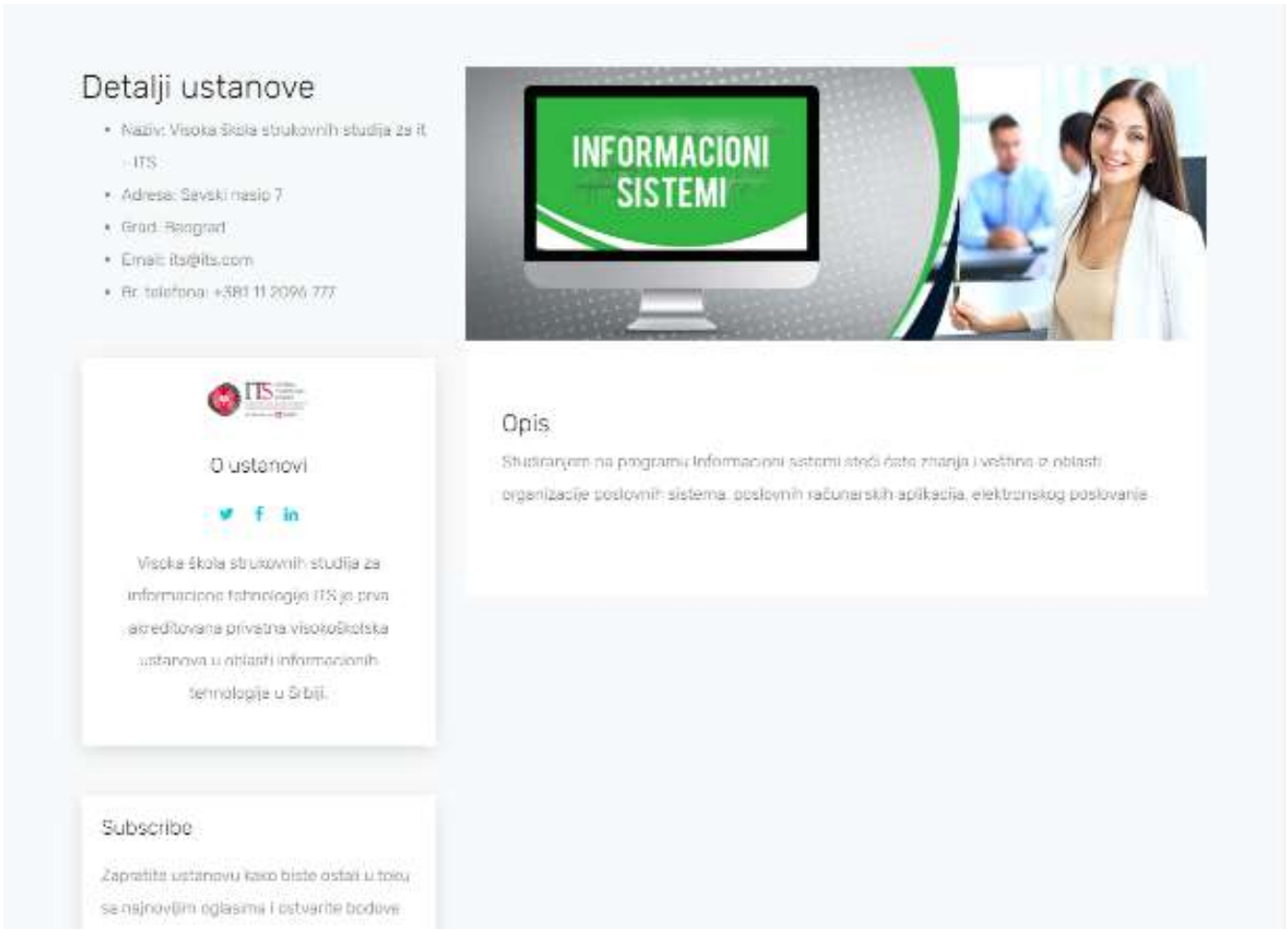
Preduslovi: Sistem je aktivan, korisnik je ulogovan i prikazana je stranica sa oglasima (slika 11).

Slika 11. Projektovanje korisničkog interfejsa – SK4

Osnovni scenario:

1. Korisnik poziva sistem da prikaže detalje oglasa klikom na
   Opis akcije: Korisnik klikom na oglas pozivva sistem da prikaže detalje o
2. Sistem pronalazi detalje oglasa
3. Sistem prikazuje korisniku detalje oglasa (slika 12)

Kliknite na oglas za
više detalja.



Slika 12. Projektovanje korisničkog interfejsa – SK4

Alternativni scenario:
Sistem ne može da uspostavi vezu sa bazom podataka i prikazuje odgovarajuću poruku (slika 13)

Slika 13. Projektovanje korisničkog interfejsa – SK4

3.4. Implementacija i testiranje

U fazi implementacije vrši se kodiranje sistema primenom određenih tehnologija. Za izradu ove veb-aplikacije korišćene su sledeće tehnologije: Spring framework, uključujući Servlete, Maven, Hibernate i Thymeleaf sa serverske strane. Sa klijentske strane korišćeni su HTML, CSS, JS, i biblioteke JQuery i Bootstrap. U fazi testiranja, tokom razvoja aplikacije „Podrška u obrazovanju", vršeno je testiranje funkcionalnosti same aplikacije, pri čemu su unošeni razni podaci radi utvrđivanja i otklanjanja eventualnih nedostataka.

4. Zaključak

U radu je kreirana veb-aplikacija koja olakšava pronalaženje željenih institucija radi daljeg školovanja zainteresovanih korisnika i time doprinosi samom razvoju obrazovanja u našoj zemlji. Aplikacija svakako može doprineti daljem razvoju nečije karijere. Za izradu aplikacije odabrana je Spring tehnologija, jer ona doprinosi bržem, lakšem i sigurnijem programiranju veb-aplikacija. U daljem radu ispitivale bi se mogućnosti da se veb-aplikacija „Podrška u obrazovanju" obogati novim funkcionalnostima.

Reference

1. Vlajić, S., Savić, D., Stanojević, V., Antović, I., Milić, M. Projektovanje softvera – Napredne Java tehnologije. Beograd: Zlatni Presek, 2008.
2. Jevremović, S. Java programiranje veb aplikacija. Beograd: ITS, 2016.
3. Spring Framework – Reference Documentation, Spring Framework, 2020. Available at: www.springframework.org
4. JavaBeans Documentation, Oracle, 2020. Available at: http://java.sun.com/javase/technologies/desktop/javabeans/docs/spec.html
5. Smeets, B., Ladd, S. Building Spring 2 Enterprise Applications. US: Apress, 2007.
6. Vlajić, S. Projektovanje programa. Beograd: FON, 2004.
7. Hibernate – Reference Documentation, Hibernate, 2020. Available at: http://www.hibernate.org/
8. Anđelić, S. WPF i ASP.NET Framework - projektovanje i implementacija softvera. Beograd: ITS, 2016.
9. Spring Web MVC Framework Flow, 2015. Available at: https://www.onlinetutorialspoint.com/spring/spring-web-mvc-framework.html
10. Vlajić, S. Projektovanje softvera, skripta. Beograd: FON, 2009.

Type of the Paper: Original scientific paper
Received: 23. 12. 2021.
Accepted: 21.1. 2022.
DOI: https://doi.org/10.18485/edtech.2022.2.2.1
UDC:

Designing and implementing the "Education Support" web application using Spring and Hibernate frameworks

Vladimir Bošković [1], **Svetlana Jevremović** [1]

[1] ITS – Information Technology School, Zemun, Belgrade, Serbia
* vladimir2417@its.edu.rs, svetlana.jevremovic@its.edu.rs

Summary: In this paper, we present the process of developing and implementing the web application "Education Support" using Spring and Hibernate frameworks. The objective of the paper is to explore the modes of designing and implementing this web application that aims to provide an accessible way of searching and selecting between various educational institutions, as well as to provide an easy way for educational institutions to communicate with their potential clients. This application aims to enable users to collect information, plan ahead and secure their enrolment with special benefits. Educational institutions would benefit from this app business-wise, thanks to having an efficient and user-friendly list of their subscribers, along with a list of the requests to schedule an informative visit to their institution, with the option to send promotional messages to users. We chose this subject as we noted that no such web application is available on our market. We have applied Larman's methodology in each development phase of this web application.

Keywords: web-application; Spring; Hibernate; Larman's methodology

1. Introduction

The "Education Support" web application is based on the current Java web technologies Spring and Hibernate. Therefore, to design this application, for the server side, we used the Spring framework, including Servlets, Maven, Hibernate and Thymeleaf. For the client side, we used HTML, CSS, JS, and libraries JQuery and Bootstrap. We used IntelliJ IDEA Ultimate as our development environment and Servlets for the database.

The first part of the paper presents the Spring framework, with a special emphasis on Spring MVC module concepts, which we used for the development of the application "Education Support". The second part of the paper is dedicated to the subject of object-relational mapping and data persistence through using the Hibernate ORM (object-relational mapping) tool. The central part of the paper is dedicated to the development of the web application "Education Support".

While developing this application, we used Larman's software development methodology during the planning, analysis, design, implementation and testing [10]. Larman's methodology is based on an iterative and incremental model of software lifecycle; it consists of Use cases and utilises object-oriented development methodology with UML (Unified Modelling Language) diagrams. This methodology is software-developer-oriented, since its focus is on the analysis and design, and it is unique for its operation contracts [8].

2. Technologies applied

Before we analyse the design and implementation documentation for the web application "Education Support", we will analyse the technologies we used during the phases of the web application development. We focused on the characteristics and solutions provided in the Spring framework, in the context of web application development.

2.1. The Spring framework

One of the most important characteristics of the Spring framework lies in its modularity which allows programmers to use only the modules that are required in a specific situation instead of the entire framework. Thanks to the modular approach, Spring can be used to develop Java applications of various levels of complexity. Depending on the application requirements, one can use any Spring module, independently from the rest of the modules. For instance, we can use the Spring core container to manage the business logic of the application and create other parts of the application by using some other technology. In addition to its modularity, Spring also allows integration with various other technologies.

The Spring framework architecture consists of the following six modules and can be seen in Figure 1 [5]:

» Core;
» AOP (aspect-oriented programming);
» DAO (Data Access Objects);
» ORM (object-relational mapping);
» JEE (Java Enterrrise Edition);
» Web.

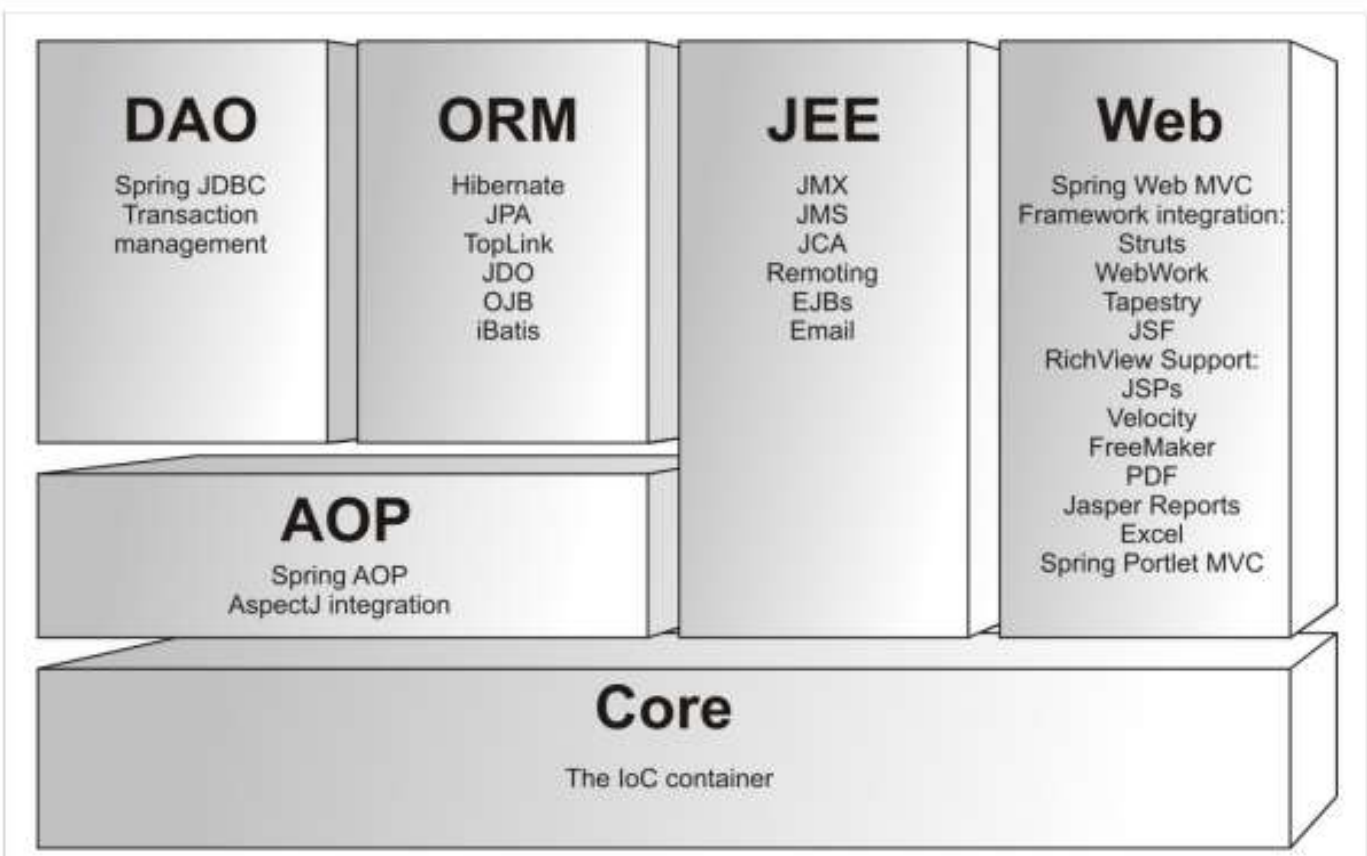


Figure 1. Spring framework modules [5]

Core module is the central module of the Spring framework. The Inversion of Control (IoC) mechanism, i.e. dependency injection (DI) mechanism, is realised in the Core module. The realisation of the DI mechanism in the Core module takes place via the BeanFactory interface, i.e. through the implementation of this interface. The AOP module supports aspect-oriented programming that allows the developer to easily separate the components of the system by implementing logically separated functionalities. The DAO module provides the JDBC (Java Database Connectivity) layer that removes the need for traditional database access by using JDBC management software. The use of JDBC implies writing the code for opening a connection, creating statements, processing results and for closing a connection; however, with the Spring JDBC framework, the entire job is abstracted and simplified. The ORM module provides a layer for integrating the Spring framework with popular ORM tools. In addition to the Hibernate framework, whose integration with the Spring framework we used in this paper, Spring also allows integration with the following ORM tools: iBatis SQL Maps, JDO, Apache OJB, Oracle TopLink. In addition to the integration with these ORM tools, the ORM module enables the use of declarative transaction management. The JEE module enables the integration of the Spring framework and EJB (Enterprise JavaBeans) components, as well as the integration with JMS (Java Message Service) components, which enables asynchronous creation, along with sending and receiving of messages. The Web module contains a complete implementation of the MVC4 framework used for web application development. Spring Web MVC implementation provides a complete separation of the application business logic from its presentation layer, at the same time enabling the use of all IoC characteristics of the framework during web application development.

2.1.1. Dependency injection

Spring IoC container is based on the dependency injection (DI) mechanism. The very name tells a lot about the relationship between the application and the container, and the way in which dependencies between application components are resolved. The application can be seen as a set of components that cooperate and depend on each other during the execution. With Java applications, these components are Java class instances, i.e. objects. Business objects of an application run by Spring IoC container are not in charge of collecting resources and creating other objects they work with and depend on; instead, the container creates and configures their dependencies, which allows us to place more focus on the business logic that needs to be executed by the class methods while creating business classes.

There are three basic types of the DI mechanism supported by the Spring container:

» setter injection;
» constructor injection;
» method injection.
»

2.1.2. Spring container

Dependency injection mechanism is the essence of the Spring framework. The implementation of this mechanism is realised through two interfaces constituting the core of the Spring IoC container:

» org.springframework.beans.factory.BeanFactory
» org.springframework.context.ApplicationContext
»

BeanFactory is the main Spring container interface that enables configuring and connecting beans by using DI mechanisms. When the BeanFactory interface is created, Spring framework conducts bean configuration validation. A singleton bean is created when the framework is launched, and other beans are created upon the user's request. In addition to this, the BeanFactory interface provides a mechanism for bean lifecycle management, but this only applies to singleton beans, since when it comes to prototype beans, the container loses control over them once they have been created.

ApplicationContext interface inherits the BeanFactory interface. Its implementation also enables bean creation and bean lifecycle management. However, it also provides support for integration with the Spring AOP module, message resource support, as well as application events propagation. In addition to this, it also provides specific application layer contexts such as the WebApplicationContext interface used in web applications.

Therefore, the BeanFactory interface enables framework configuration, as well as basic functionalities of such configuration, while the ApplicationContex interface adds new and more complex functionalities. The ApplicationContext interface constitutes a comprehensive superset of the BeanFactory interface, i.e. it enables everything that BeanFactory does. The relationship between these two interfaces is illustrated in Figure 2.

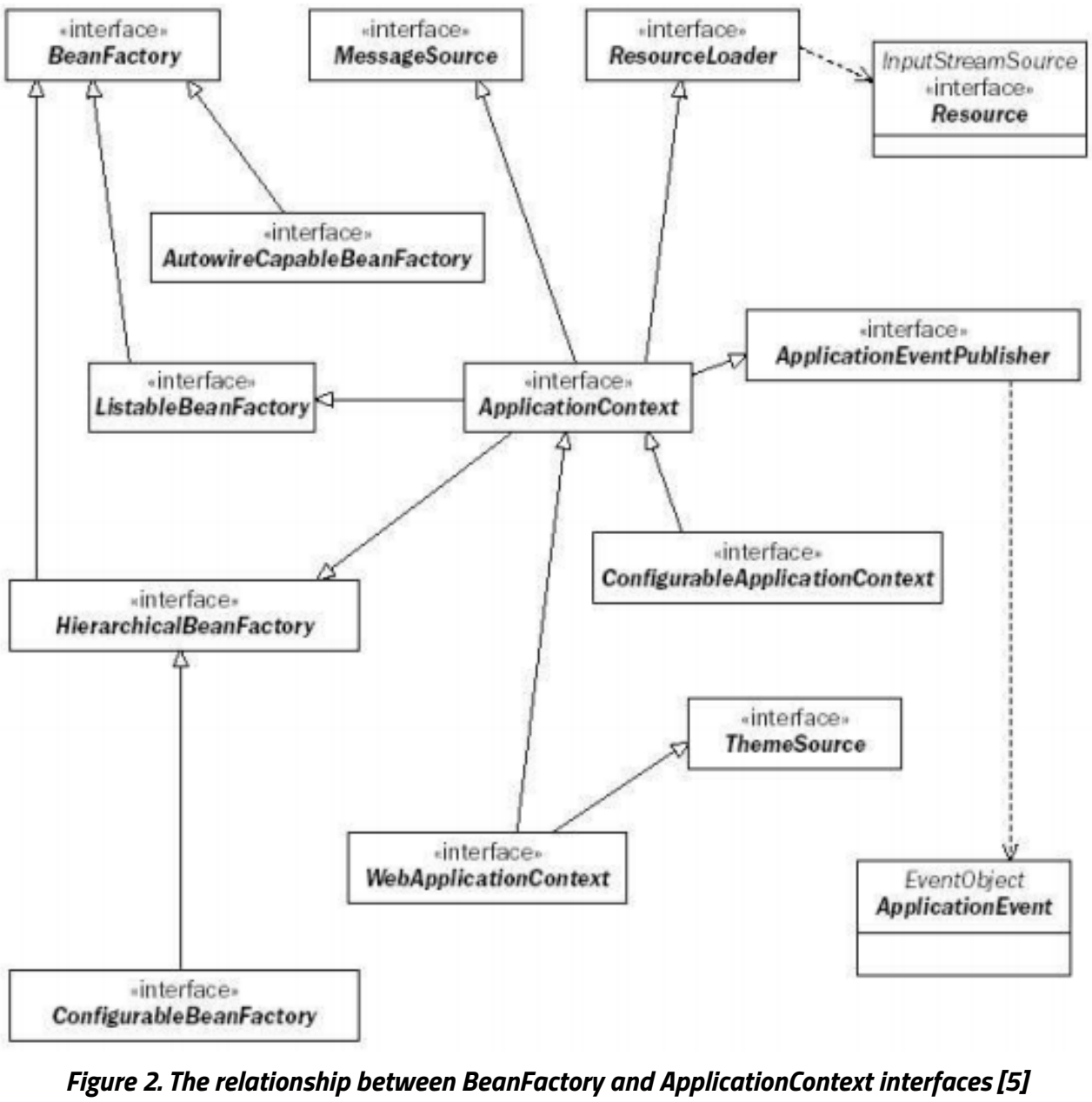


Figure 2. The relationship between BeanFactory and ApplicationContext interfaces [5]

2.1.3. Working with JavaBean components

Bean is a software component that can be reused and visually manipulated by using an appropriate tool [4]. In the context of apps based on the Spring framework, the term bean refers to any object created and managed by the Spring container [5]. When defining beans, the configuration file consists of one (root) bean element and one or two bean elements. Validation of this XML file is conducted in relation to the XML DTD file spring-beans.dtd, which describes in detail all the valid attributes and elements that the configuration file might contain.

In most cases, the bean identifier is the first element defined. It is important to have in mind that it is not necessary to define the identifier, in which case, the bean will be treated as an anonymous bean. A Bean name can be defined by using the bean element's name or id attribute. Using the id attribute while naming beans is recommended because this attribute is of the XML IDREF type. Therefore, in case other beans reference it, the XML parser will be able to decide whether the reference is valid or not. The IDREF type comes with certain limitations that make it inapplicable in some situations.

Beans are usually created with the bean constructor. When defining a bean, the name of the bean class is stated in the class attribute. When the container requires a new instance of this bean, it will internally execute an operation equivalent to using the new operator in Java code.

A bean can also be created by using the static factory method. In that case, one needs to define a class whose role will be to encapsulate the process of bean creation within a static method. Then, using the class attribute, the bean is defined, and then the factor-method attribute is used to specify the bean method in charge of creating the bean.

The next approach to creating beans is using the non-static (instance factory) method. In this case, a method from another bean already created by the container is used.

2.1.4. Spring Web MVC framework concepts

MVC framework is an architectural pattern; it consists of three key components: Model, View and Controller [6]. The Model is a component that contains the business system structure, along with its operation, i.e. it contains data and data processing operations. The View component provides a user interface via which the user communicates with the system. It also sends reports to the user. These reports are obtained from the Model. The Controller is the component in charge of managing the execution of system operations. It accepts client requests, calls an operation defined in the model and controls its execution.

The architecture of the Spring Web MVC framework implies the existence of controller servlets as central input points for all incoming requests. In the Spring MVC framework, this component is realised via DispatcherServlet class. The application business logic layer is realised via the controller component. In the presentation layer, Spring MVC supports various presentation technologies. The most prominent characteristic of the presentation layer is the possibility of realising full independence between the business logic and the concrete presentation technology.

The central component of the Spring Web MVC framework is the class DispatcherServlet, which constitutes the main entry point for any incoming request addressed at a Spring Web MVC application. This class is fully integrated into the Spring IoC container, which ensures that all properties of the Spring framework can be utilised.

Figure 3 shows the conceptual model of request processing using DispatcherServlet class as the central controller. As can be seen in the picture, the central controller is the entry point for any incoming request. Upon the reception of the request, the central controller delegates the request to the appropriate controller in charge of request processing. The controller creates a model and processes the request, and then it passes the model and the logical name of the view to the central controller. The model contains the attributes which the view is supposed to show to the client. Based on the logical name of the view, the view that will be returned to the client as a response is rendered through mapping to a concrete realisation of the view.

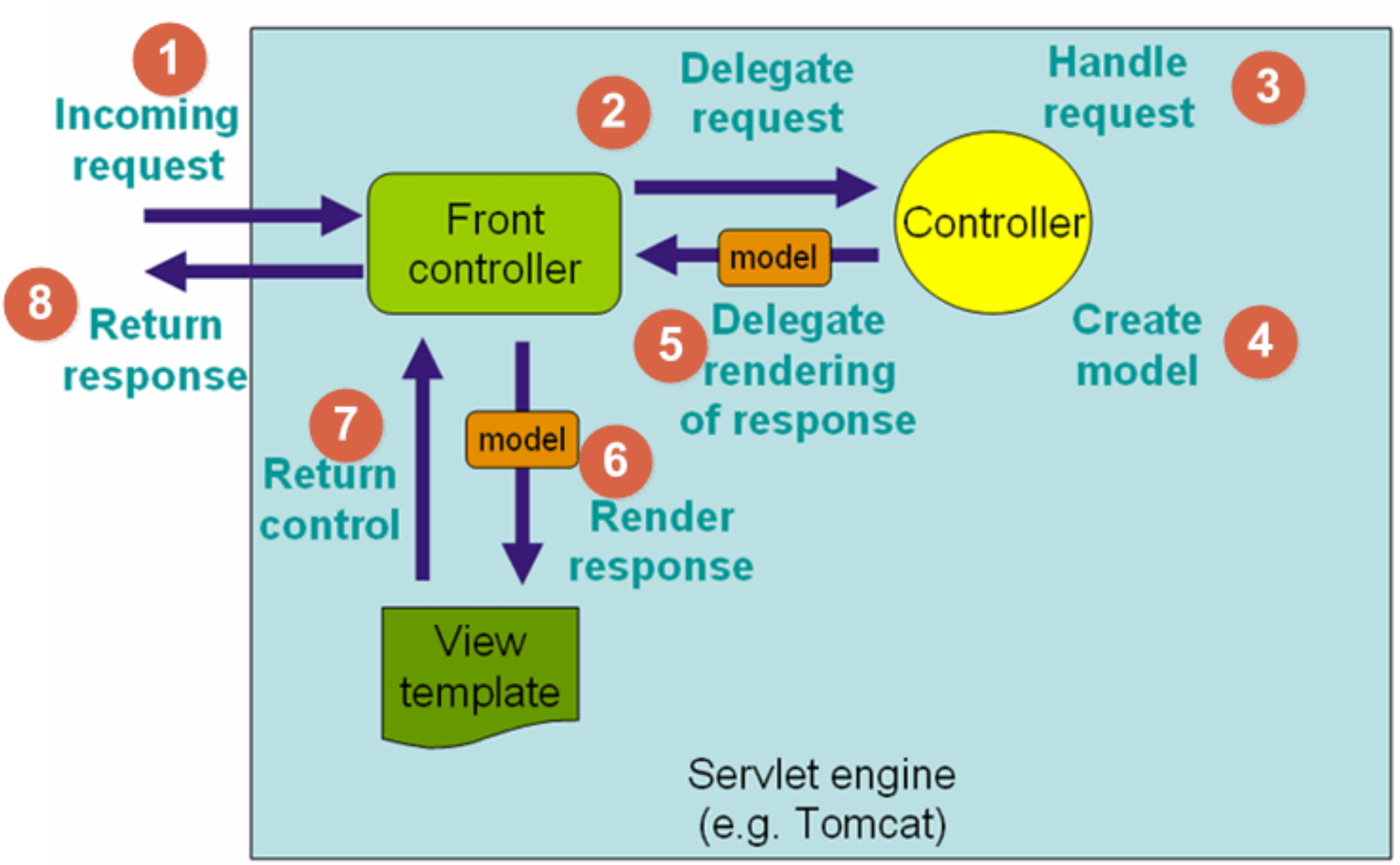


Figure 3. Conceptual model of data processing flow [9]

Class DispatcherServlet is, in fact, a servlet (derived from class javax.servlet.http.HttpServlet). It is the only servlet that needs to be declared and configured in a web application's deployment descriptor. In addition to servlet declaration, the deployment descriptor should contain the definition of request mapping to the central controller (class DispatcherServlet).

2.2. Hibernate framework

Data persistence is one of the fundamental concepts of software system development. Generally, data are said to be persistent if they outlive the programme that created them. There are several definitions that concern data persistence in the context of object-oriented software development [6].

»
» An object is persistent if it can be materialised and dematerialised.
» An object is persistent if it continues to exist after the programme that created it stops working (G. Booch).
» Materialisation is the process of transforming database syllables into objects of the programme.
» Dematerialisation is the process of transforming object s from the programme into database syllables.
» A persistent framework is a set of interfaces and classes that provides persistence to objects of different classes.

The most popular form of data storage in today's apps is using relational databases, and data persistence in Java applications usually implies storing Java objects in a relational database. Relational databases have become a standard of sorts in the realm of data persistence.

In object-oriented applications, persistence ought to provide storing of objects in a relational database. This does not refer merely to storing individual objects, but to storing an entire network of interconnected objects that represents an object model. In addition to permanently stored objects, object-oriented apps also contain a large number of the so-called transient objects. Transient objects are objects whose duration is limited by the duration of the app that created them. Such apps usually contain a subsystem in charge of materialising and dematerialising persistent objects, i.e., their transformation into a form conducive to storage in relational databases – relational model. Therefore, persistence in object-oriented apps that use a relational database can be viewed as a process of transforming the object model into a relational one and vice versa.

2.2.1. Associations

The problem of associations concerns the transformation of the relationships established between objects in the object model and the relationships created among the relations in the relational model. In the relational model, these connections are realised using external keys: an external key in a referencing table represents a primary key in a referenced table. In the object model, there are several types of associations: 1-1 (one-to-one), * - * (many-to-many), 1 - * (one-to-many). In the relational model, these associations need to be provided using external keys [7].

Transformation is usually performed by representing two objects by a single relation. In this way, one object's data is expanded by another object's data, and they become a unique relation. The attributes of the relationship become attributes of both objects.

Many-to-many transformation is performed by creating, in addition to the relationships created for each object type, an additional, aggregated relationship comprising the primary keys of the relations in question. When an object is creating a relationship with several objects of a certain type, the transformation is performed by creating separate relationships for each of these object types, and the primary key of the object that creates the relationship is memorised for all objects it is connected to, i.e., the primary key of the relation on the one side is represented as the external key of the relation on the many side.

2.2.2. Hibernate framework architecture

The Hibernate framework is a very flexible tool that provides a choice between several different approaches when it comes to choosing the framework's service that will be used in the development of an application. The three major services (components) of the Hibernate framework are connection management, transaction management, and object-relational mapping.

Figure 4 shows the two basic architectures: Lite and Full Cream. This classification is based on the components of the framework that are used in app development. Lite architecture uses only the components for object-relational mapping, while transaction management and the provision of JDBC connections are left to the app. Full Cream architecture uses all three components.

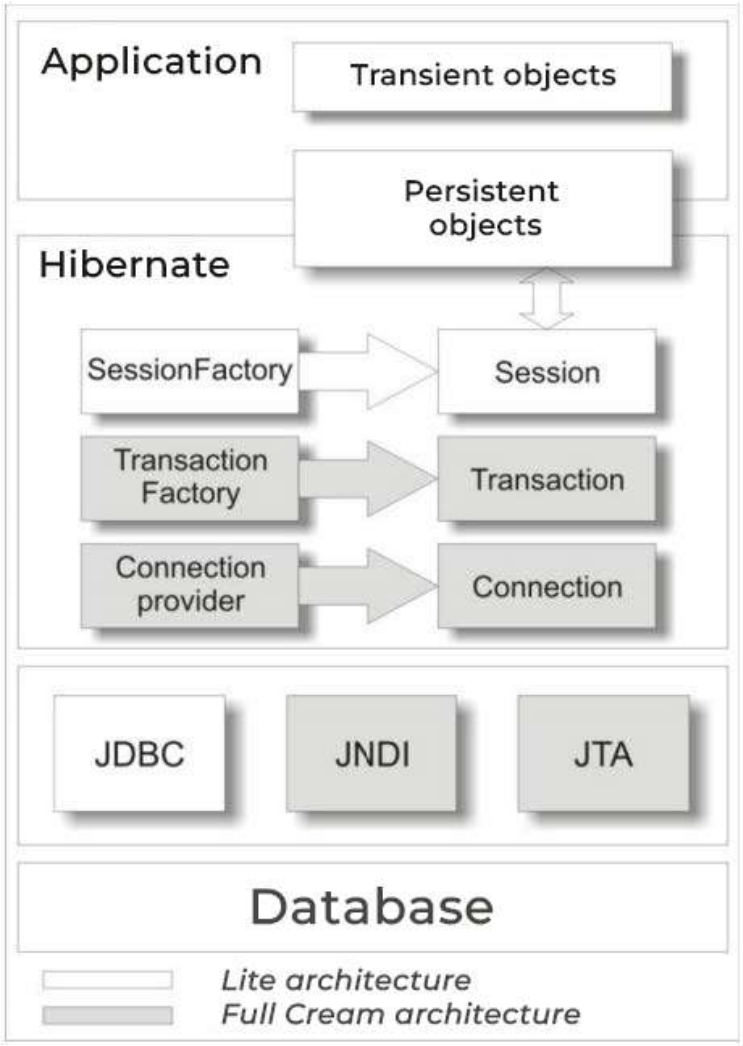


Figure 4. Hibernate framework architecture

2.2.3. Configuring the Hibernate framework

As a persistent framework, Hibernate is able to communicate with numerous different SUBPs and can be executed in various environments. Hibernate's adaptability to different SUBPs and environments in which it is executed requires different modes of framework configuration. Regardless of the environment and the database which the application communicates with, framework configuration can be logically divided into two parts. In the first part, there is the configuration data that the framework needs in order to access the database, and the second part consists of configuration data that enables mapping between the application's persistent classes and the relevant tables in the relational database. The central class used for configuring and starting the Hibernate framework is the class org.hibernate.cfg.Configuration. On creation, this class has to be provided with configuration data based on which the Configuration object will create a singleton of the SessionFactory class (Figure 5).

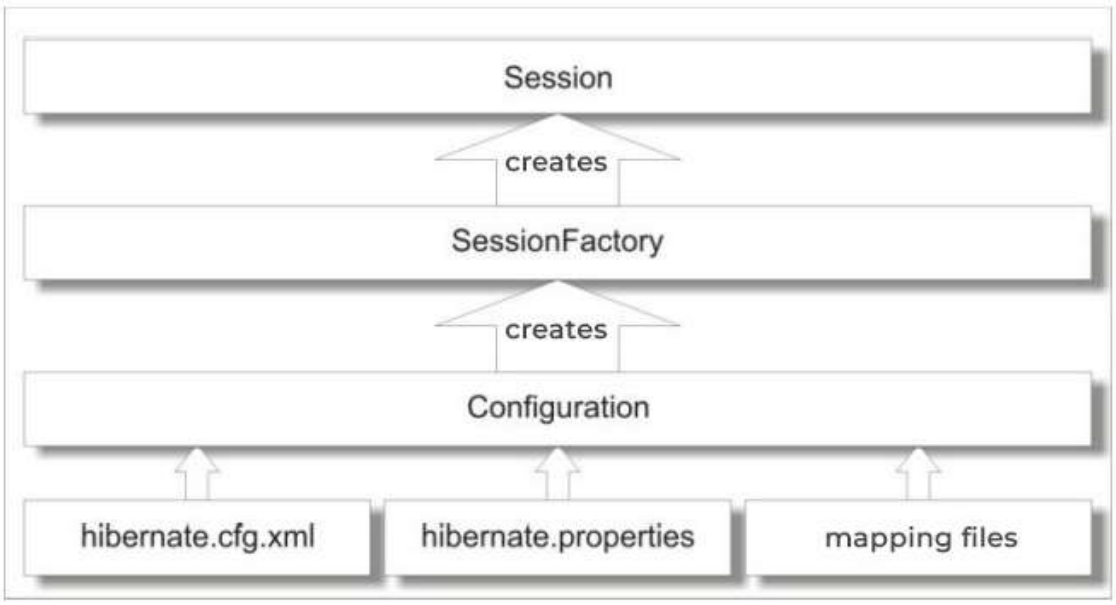


Figure 5. Configuring the Hibernate framework

A singleton of the SessionFactory class essentially constitutes a completely configured Hibernate framework that provides communication with a single database. In addition to the Configuration object creating a singleton of the SessionFactory class, the state of this object becomes unchangeable after the creation. The SessionFactory class is in charge of creating objects of the Session class during each interaction with the database.

3. Designing and implementing the web application "Education Support"

The research of the suitable technologies was followed by detailed documentation. First, we will present a verbal description of the model, and we will use it to define the system actors' Use cases.

3.1. Request specification

A web application which would help its users find and select a suitable educational institution needs to be designed and implemented. Figure 6 shows three types of actors: user, administrator and institution.

The system has to enable the user to register on the website if the user is not already registered. After registering, the user will receive a welcome message with the option to log in to the website. After logging in, the user would be able to search through the advertisements and assign several search criteria on the homepage, and then they would see a list of all the advertisements that match the parameters the user has given. If the users are interested in an ad, when they click on it, they can view the ad in detail, as well as learn some details about the institution. An additional possibility is a free subscription to a certain institution, where the users confirm that they would like to receive promotional emails from the institution. With each subscription, the user collects points. After accumulating a certain number of points, the user receives an electronic voucher as a present. This voucher allows them to receive a discount on the scholarship fee for certain institutions. If they would like to learn more about an institution, they can schedule a visit to the institution, with the realisation dependent upon the confirmation by an employee of the institution. If the institution does not confirm the request 24 hours before the tour, the request is automatically deleted.

The app should allow the system administrator to add new institutions, change information about an institution and remove institutions. On adding a new institution, an email would automatically be sent, containing login parameters. The administrator would also be able to change and delete ads and users.

The institution receives login parameters from the app administrator via email. After login, the institution can publish, change and delete ads. Also, if a user subscribes to an institution before opening its ad, the institution, once logged in, can see which users have logged in, and send them a promo message. If a user has requested a tour of the institution, the institution can accept or reject the request. If the institution accepts a request, the user will receive an email informing them that the request has been accepted; otherwise, they will receive an email notifying them that the request has been denied.

3.1.1. Use cases

Based on the verbal model, the following Use cases have been identified: Login, Registration, Add search, Add view, Subscription to an institution, Sending a visit request, Adding new institutions, Institutions overview, Changing institution info, Deleting institutions, Adding new ads, Changing ad information, Deleting ads, Users overview, Deleting users, Subscribed users overview, Sending promotional messages, Visit requests overview, Approved visit requests overview, Accepting visit requests, Denying visit requests (Figure 6).

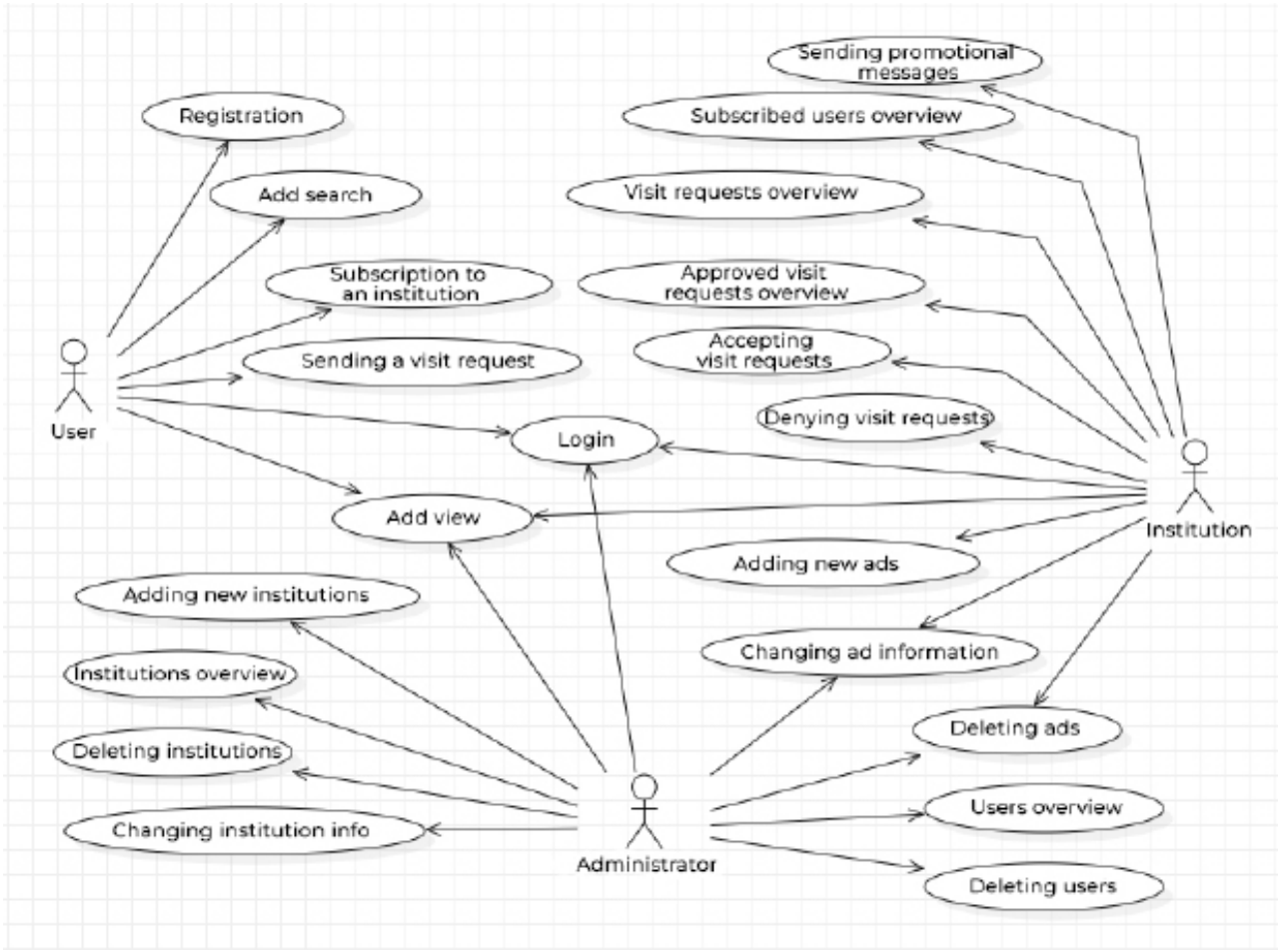


Figure 6. Use case diagram of all Use cases

Due to the limited scope of the paper, we are providing a description of one Use case as an example (UC4).

UC4: Ad view

Name: Ad view

Actors: User, Administrator, Institution

Participants: User, Administrator, Institution and system

Prerequisites: The system is active, the user is logged in and the page with ads is displayed

Basic scenario:

1. The user asks the system to show detailed ad info (APSO).
2. The system finds the request details (SO).
3. The system shows the requested details to the user (IA).

Alternative scenario:

2.1. The system cannot connect to a database and displays an appropriate message (IA).

3.2. Analysis

In the analysis phase, we describe the logical structure and the behaviour of the software system. We describe the structure of the software system using a conceptual and relational model. We describe the behaviour of the system using sequence diagrams (UCSD) made for each Use case and using the system operation contracts received on the basis of the previous diagrams. Now follows an example of a system sequence diagram.

UCSD4: Ad view

Basic scenario:

1. The user requests that the system display advertisement details (APSO).
2. The system displays advertisement details to the user (IA).

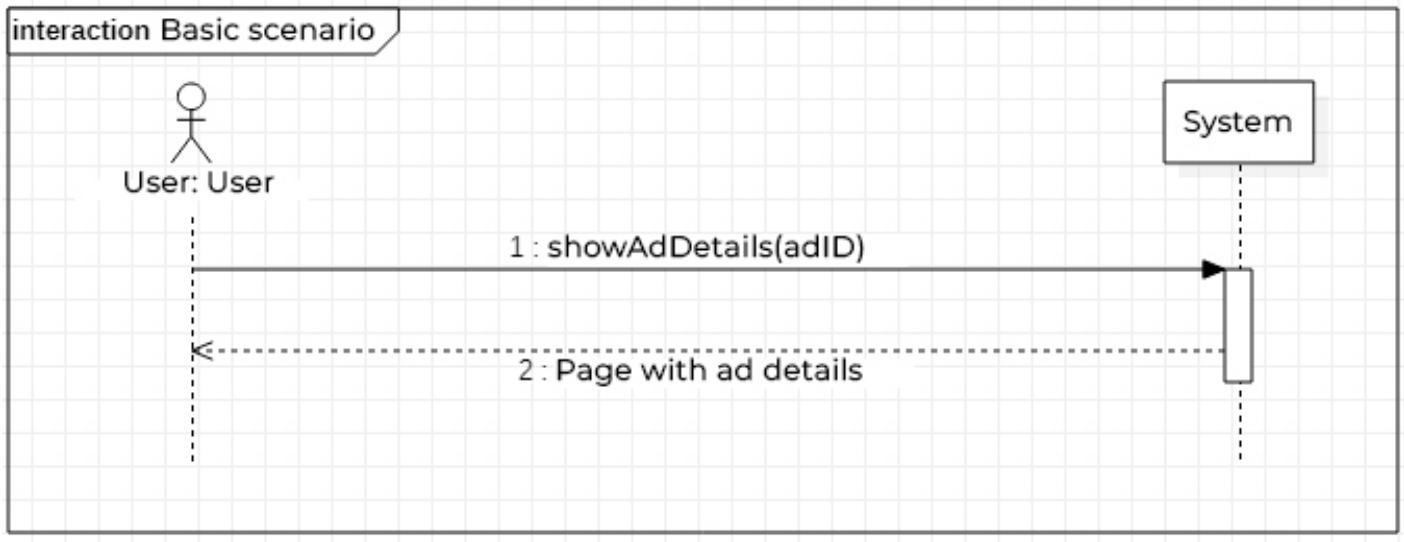


Figure 7. UCSD4 – Viewing an ad

We introduced a system operation:

1. showAdDetails(adID)

For each detected system operation, a contract is made that describes what the operation does, but not how it does it, and one contract is connected with one system operation [8]. Now follows an example of a contract (UC18).

Contract UG18: showVisitRequests
Operation: showVisitRequests(institutionsID)
Connection to UC: UC18
Preconditions: Requests for visits exist in the database
Postcondition: The list of requests for visits is displayed

After defining all the contracts, a conceptual model was created on the basis of the data from the functional requirements and Use cases (Figure 8).

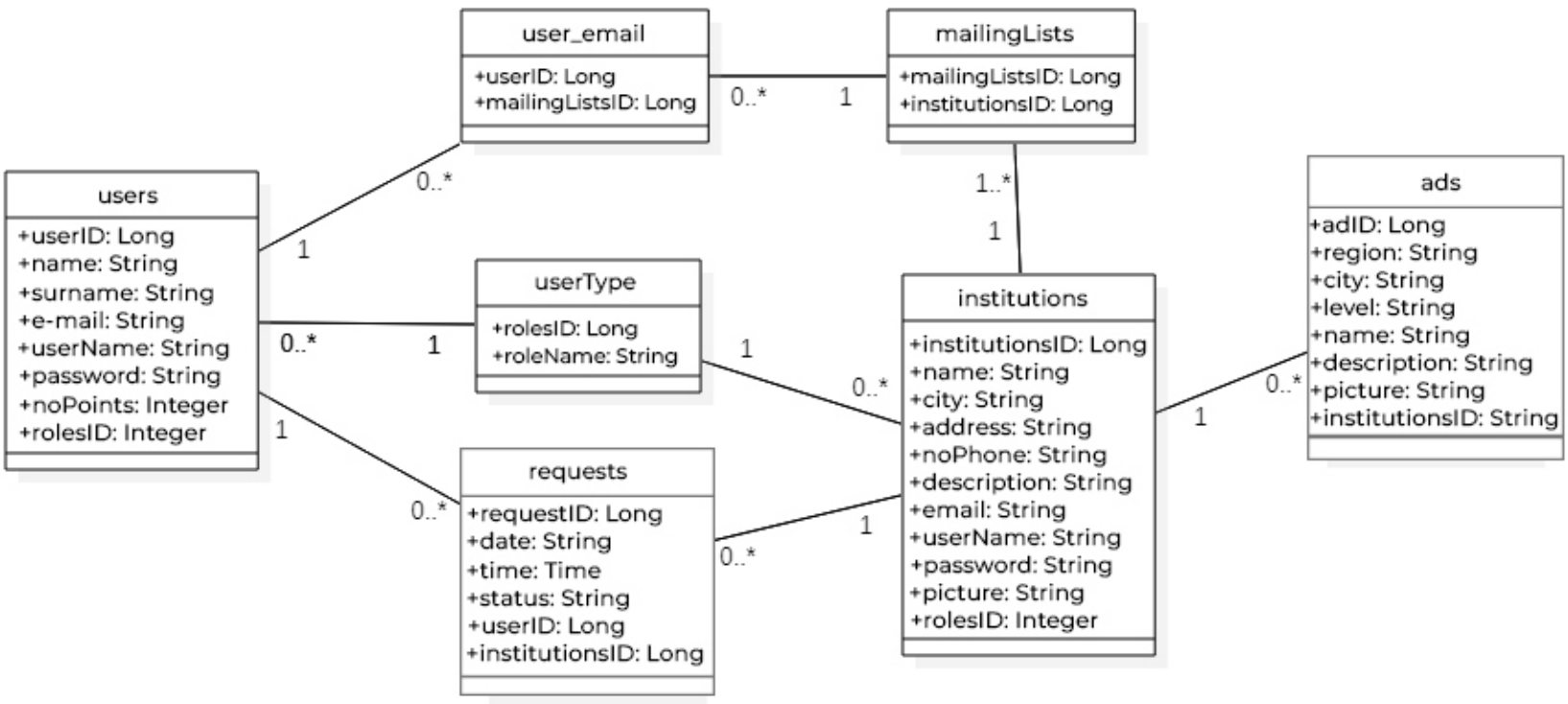


Figure 8. Conceptual model

The relational model is created on the basis of the conceptual model. It constitutes the basis for database design.
userType(rolesID, roleName)
users(userID, name, surname, e-mail, userName, password, noPoints, rolesID)
users(rolesID) references userType(rolesID)
institutions(institutionsID, name, city, address, noPhone, description, email, userName, password, picture, rolesID)
institutions(rolesID) references userType(rolesID)
ads(adID, region, city, level, name, description, picture, institutionsID)
ads(institutionsID) references institutions(institutionsID)

mailingLists(mailingListsID, institutionsID)
mailingLists(institutionsID) references institutions(institutionsID)
user_email(userID, mailingListsID)
user_email(userID) references users(userID)
user_email(mailingListsID) references mailingLists(mailingListsID)
requests(requestID, date, time, status, userID, institutionsID)
requests(userID) references users(userID)
requests(institutionsID) references institutions(institutionsID)

3.3. Design

The phase of design describes the physical structure and the behaviour of the software system, i.e. its architecture. As such, it includes the design of application logic and the design of logical structure and behaviour of the software system.

3.3.1. Application structure design

Contract UG18: showVisitRequests (Figure 9 and Figure 10)
Operation: showVisitRequests(institutionsID)
Precondition: Requests for visits exist in the database
Postcondition: The list of requests for visits is displayed

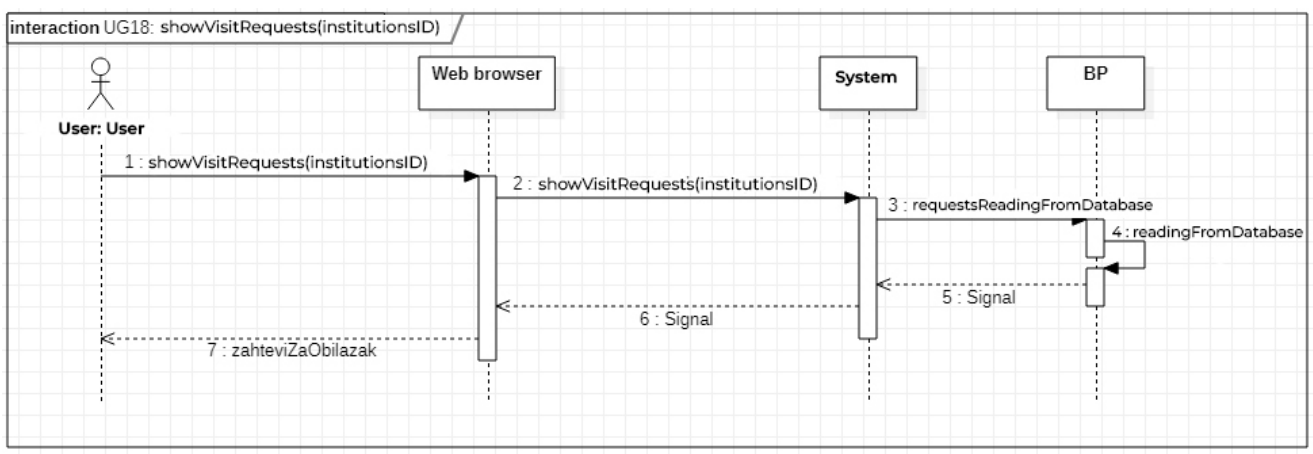


Figure 9. Sequence diagram UG18 – showVisitRequests

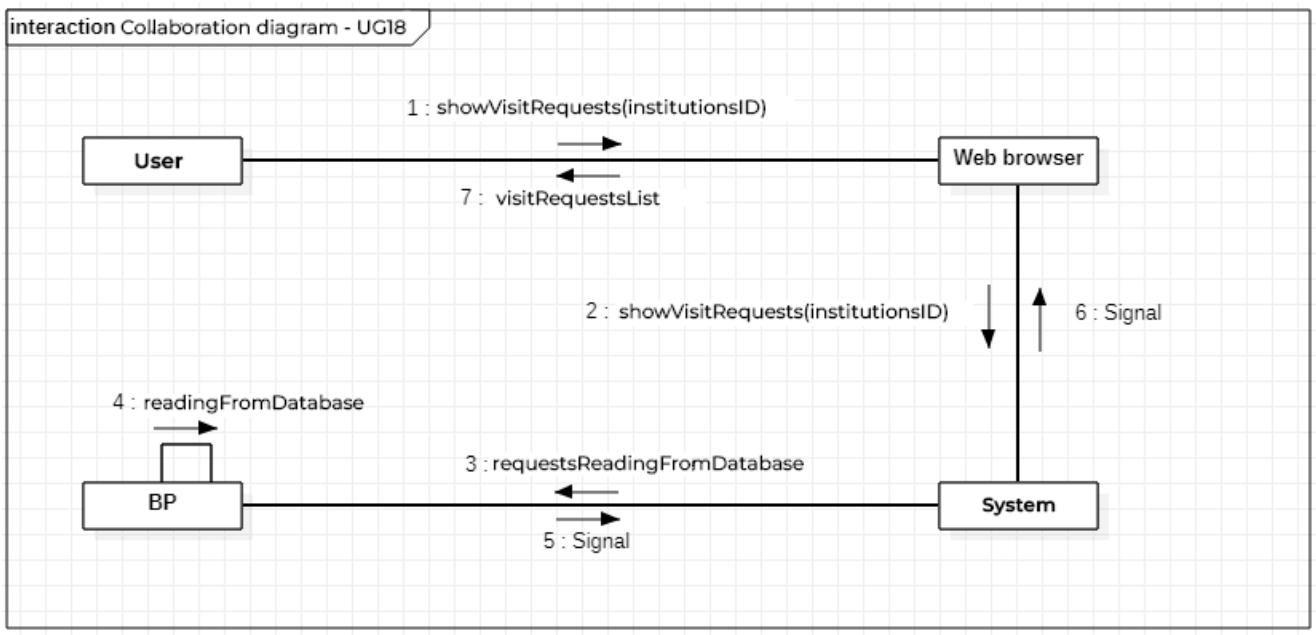


Figure 10. Collaboration diagram UG18 – showVisitRequests

3.3.2 Creating the user interface

What follows is an example of defining a portion of the user interface for the "Education Support" app.
UC4: Ad view
Prerequisites: The system is active, the user is logged in and the page with ads is displayed (Figure 11)

Figure 11. Creating the user interface – UC4

Basic scenario:

1. The user asks the system to display detailed ad information b
   Action description: By clicking on an advertisement, the user asks the system to display detailed information.
2. The system locates ad information
3. The system shows detailed information to the user (Figure 12)

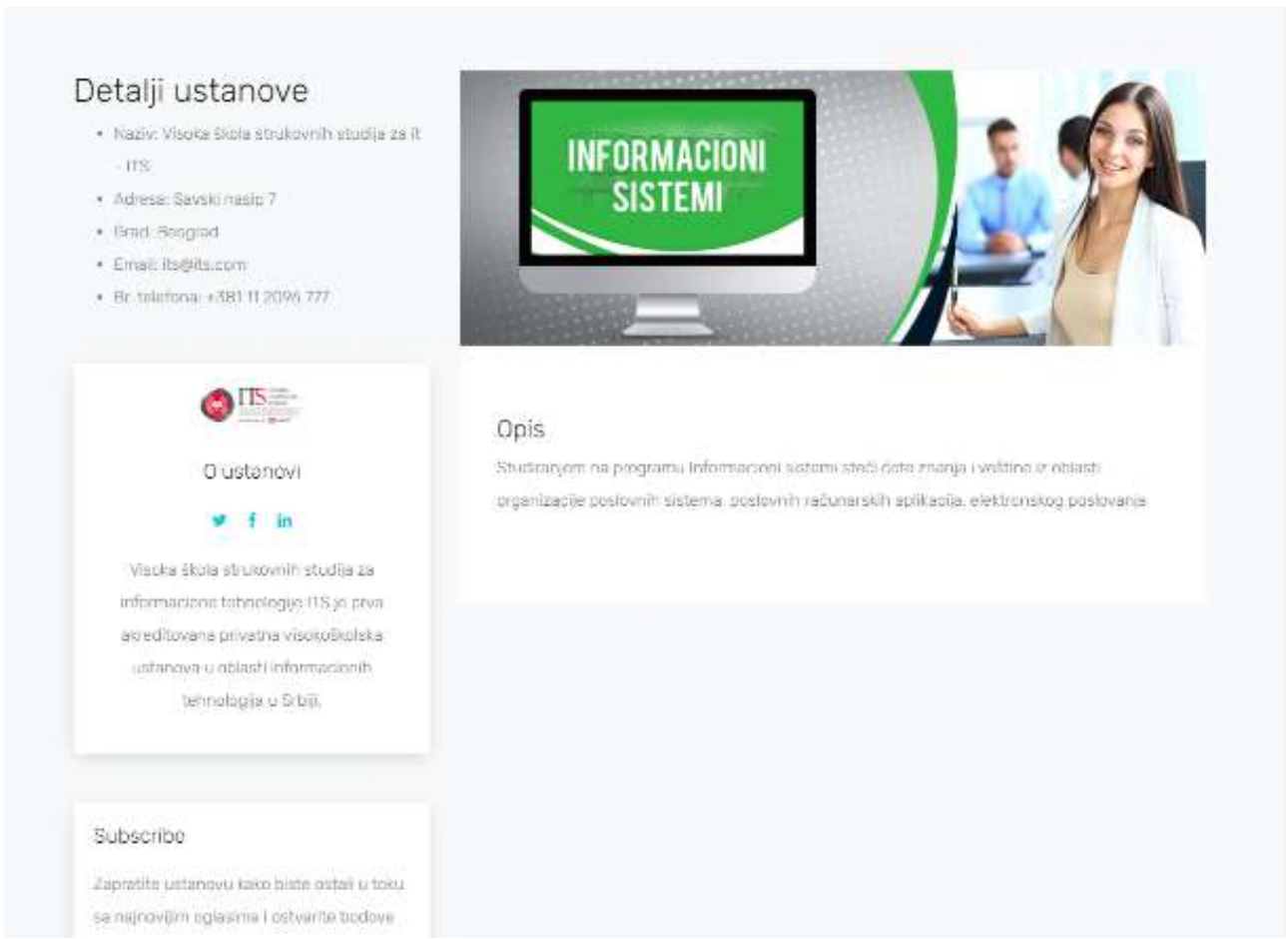


Figure 12. Creating the user interface – UC4

Alternative scenario:

The system cannot connect to a database and displays a corresponding message (Figure 13)

Figure 13. Creating the user interface – UC4

3.4. Implementation and testing

In the implementation phase, the system is coded by utilising certain technologies. The following technologies were utilised for the development of this web application: Spring framework, including Servlets, Maven, Hibernate and Thymeleaf on the server side. On the client side, HTML, CSS, JS, and JQuery and Bootstrap libraries were used. In the testing phase of the "Education Support" web app development, the functionalities of the application itself were tested, including entering various data in order to determine and ameliorate possible irregularities.

4. Conclusion

In this research, a web application was created to facilitate the locating of the desired institutions for further education of the interested users, and thereby contribute to the development of education in our country in general. The application can certainly be helpful in further career development. The technology of choice for the application was Spring, as it is conducive to faster, easier and more secure web application development. Further research would concentrate on the possibilities of enriching the "Education Support" web app with new functionalities.

References

1. Vlajić S, Savić D, Stanojević V, Antović I, Milić M. Projektovanje softvera – Napredne Java tehnologije. Beograd: Zlatni Presek, 2008.
2. Jevremović S. Java programiranje veb aplikacija. Beograd: ITS, 2016.
3. Spring Framework – Reference Documentation, Spring Framework, 2020. Available at: www.springframework.org
4. JavaBeans Documentation, Oracle, 2020. Available at: http://java.sun.com/javase/technologies/desktop/javabeans/docs/spec.html
5. Smeets B, Ladd S. Building Spring 2 Enterprise Applications. US: Apress, 2007.
6. Vlajić S. Projektovanje programa. Beograd: FON, 2004.
7. Hibernate – Reference Documentation, Hibernate, 2020. Available at: http://www.hibernate.org/
8. Anđelić S. WPF i ASP.NET Framework - projektovanje i implementacija softvera. Beograd: ITS, 2016.
9. Spring Web MVC Framework Flow, 2015. Available at: https://www.onlinetutorialspoint.com/spring/spring-web-mvc-framework.html
10. Vlajić S. Projektovanje softvera, skripta. Beograd: FON, 200

Vrsta rada: Originalni naučni rad
Primljen: 14. 2. 2022.
Prihvaćen: 6. 11. 2022.
UDK:

Zaštita i upravljanje bezbednosnim rizicima, predlog kriptoloških mera i rešenja za preduzeće „Vesimpex"

Ivan Jovanović [1], Milosav Majstorović [1] i Hana Stefanović[1] *

[1] Visoka škola strukovnih studija za informacione tehnologije ITS, Beograd, Srbija; ivan59218@its.edu.rs; milosav.majstorovic@its.edu.rs
* hana.stefanovic@its.edu.rs; +381 (0)63/84-97-189

Sažetak: Predmet istraživanja ovog rada je pravljenje asocijativne mreže pojmova u okviru upravljanja bezbednosti i primena kriptografije kroz sekundarno istraživanje, kao i uočavanje značaja bezbednosti u konkretnoj organizaciji kroz primarno istraživanje. Cilj je da se na osnovu analize preduzeća formuliše predlog bezbednosnih i kriptoloških mera kako bi se unapredio bezbednosni sistem preduzeća. Cilj osnovnih principa informatičke bezbednosti malih i srednjih preduzeća, kao i primene odgovarajućih kriptografskih algoritama zasnovanih na principu jednokratne šifre (OTP – one-time pad) i vizuelne kriptografije (VC – Visual Cryptography), predstavlja kreiranje završnog rešenja za odabrano preduzeće. Rad pored teorijske osnove sadrži i informacije o samom preduzeću sakupljene posmatranjem i beleženjem i analizom sadržaja, kao i proces kreiranja bezbednosnog rešenja inkorporiran u projektnu povelju i samo rešenje.

Ključne reči: mala i srednja preduzeća; bezbednosna rešenja; konkurentska prednost; jednokratna šifra (OTP – one-time pad); vizuelna kriptografija (VC – Visual Cryptography)

1. Uvod

Informatičko doba i digitalizacija doprinose značajnom poboljšanju svih oblika poslovanja, ali su takođe i informacije lako dostupne, što ugrožava bezbednost samog poslovnog sistema [1]. U veoma oštroj konkurentskoj trci na tržištu zaštita informacija postala je neophodna [2], jer postoje različiti upadi, bez obzira na to da li su internog, eksternog ili slučajnog tipa, a sve češće nastaju usled zloupotrebe novih tehnologija [3][4]. Zahvaljujući pouzdanim bezbednosnim sistemima, znatno se smanjuje rizik od curenja informacija [5] koje može da bude fatalno za preduzeće.

„Vesimpex" je malo preduzeće koje se bavi prodajom i ugradnjom elektroopreme, kao i kreiranjem samostalnih rešenja u oblasti elektrodistribucije [6]. Preduzeće sarađuje sa mnogim uspešnim kompanijama u različitim granama industrije, pa pitanje bezbednosti i pouzdanosti informacija sve više dobija na značaju. U takvom okruženju pojačana bezbednost može preduzeću dati prednost u odnosu na konkurenciju, koja je često nelojalna [7]. Kako bi se obezbedila zaštita od raznih napada, potrebno je analizirati postojeće stanje i nivo stručnosti zaposlenih i na osnovu toga dati predlog o formiranju bezbednosnog sistema za posmatrano malo preduzeće.

Predmet istraživanja rada je multidisciplinaran i ulazi u discipline ekonomike preduzeća, upravljanja projektima, bezbednosti i kriptografije. Glavni motiv je formiranje konkretnog rešenja na praktičnom primeru kroz analiziranje bezbednosnih karakteristika preduzeća. Svrha istraživanja je pronalaženje adekvatnih načina za realizaciju formulisanih ciljeva kako bi se omogućila realizacija bezbednosnih kriterijuma.

Glavni cilj ovog primenjenog istraživanja je rešenje specifičnog bezbednosnog problema kroz kreiranje bezbednosnog rešenja i obezbeđenje konkurentske prednosti za preduzeće „Vesimpex" [6]. Pomoćni ciljevi su proučavanje postojećih i uvođenje novih mera kriptološke zaštite radi povećanja bezbednosti poslovanja.

S obzirom na to da je savremeno poslovanje, koje se pre svega zasniva na upotrebi računarskih sistema i razmeni podataka u elektronskom obliku, izloženo različitim rizicima koji mogu imati nesagledive posledice, neophodno je analizirati i sprečiti sve učestalije napade na računarske mreže, pokušaje neovlašćenog pristupa podacima, prisluškivanja, kao i zlonamerne izmene podataka [8]. U tom smislu, neophodno je primeniti nove načine komunikacije koje napredak tehnologije omogućava. Problem sigurnosti nameće potrebu za uvođenjem novih mehanizama koji treba da preuzmu ulogu klasičnih rešenja sa ciljem efikasne identifikacije, kontrole pristupa i verifikacije. Odgovor na većinu ovakvih izazova nudi primena kriptografskih rešenja [9], mada postoje i problemi na koje kriptografija ne može adekvatno da odgovori.

Kriptografija izučava različite tehnike transformacije podataka koji se prenose na takav način da značenje podataka bude dostupno samo ovlašćenim stranama u komunikaciji. Istovremeno, transformacija treba da bude takva da neovlašćene strane u komunikaciji koje dođu u posed transformisane poruke ne mogu da dođu do polaznih podataka.

Postoji veliki broj kriptografskih algoritama, klasičnih i modernih, a takođe i onih koji koriste isti ključ za šifrovanje i dešifrovanje, kao i nesimetričnih, koji koriste različite ključeve u procesu šifrovanja i dešifrovanja. Za svaku od kriptografskih šifara, bez obzira na to da li se koristi simetričan ili nesimetričan kriptografski algoritam, ključno je pitanje sigurnosti šifre [10] [11].

Pod bezuslovno sigurnom šifrom se smatra ona šifra koja ima osobinu da se ne može doći do otvorenog teksta iz šifrata bez poznavanja ključa, čak ni potpunom pretragom ključeva. Sigurno je da se potpunom pretragom (ne ograničavajući vreme pretrage i raspoložive resurse) može doći do ključa, ali napadaču nije od interesa da to bude urađeno nakon nekoliko desetina ili stotina godina. Međutim, ukoliko bi napadač posedovao najbolju moguću opremu i resurse, bezuslovno sigurna šifra treba da omogući da on ne dođe u posed otvorenog teksta ni pri idealizovanim uslovima. Osnovna ideja bezuslovno sigurne šifre je da se potpunom pretragom potencijalnih ključeva, koji svakako generišu veliki broj poruka, učini da napadač nema načina da odredi koja je od njih prava. Napadač će potpunom pretragom dobiti veliki broj besmislenih poruka, koje će odbaciti, ali će svakako dobiti i određeni broj smislenih, a ako su sve te poruke podjednako verovatne, onda napadač nema načina da odredi koja je od njih prava.

Primer bezuslovno sigurne šifre je one-time pad – OTR šifra [12], koja je primenjena u ovom radu. Simulacioni modeli koji prikazuju osnovne principe OTP algoritma realizovani su u softverskom alatu CrypTool [13], sa posebnim osvrtom na slučaj ponovljene upotrebe ključa koji je predviđen za jednokratnu upotrebu. Priložen je i jedan primer procesiranja elektronske finansijske transakcije primenom OTP-a, uz deljenje tajnih informacija primenom tehnike virtuelne kriptografije [14][15].

2. Materijali i metode

Tokom izrade korišćeni su brojne naučne i stručne metode, tehnike i alati, a plan istraživanja obuhvata:

- definisanje predmeta istraživanja (kroz formulaciju problema istraživanja);
- definisanje ciljeva istraživanja;
- pregled relevantne literature i njen izbor za istraživanje;
- određenje teorijskog okvira istraživanja (u skladu sa zastupljenim disciplinama i izborom relevantne literature);
- situaciona analiza;
- ispitivanja ciljne grupe kroz anketno istraživanje;
- statistička analiza podataka anketnog istraživanja;
- osmišljavanje i izrada bezbednosnog rešenja.

Glavna hipoteza istraživanja:
H1: Nivo informatičke bezbednosti u preduzeću „Vesimpex" nije optimalan, te ga je, s obzirom na elemente okruženja i željeni rast i razvoj kao organizacioni cilj, potrebno unaprediti novim bezbednosnim rešenjem.
H2: Ako bi se adekvatno unapredila informatička bezbednost preduzeća, to bi mu obezbedilo konkurentsku prednost.

Ishodi istraživanja, odnosno očekivani rezultati istraživanja su: analiza odabranih bibliotečkih i drugih referentnih izvora, dokazivanje postavljenih hipoteza i rešavanje centralnog problema istraživanja kroz odabrani model. Sa stanovišta stručne opravdanosti, rešenje koje je predloženo dodatno bi unapredilo poslovanje i bezbednost posmatranog preduzeća, poboljšalo sigurnost poslovanja, kao i sigurnost uključenih partnera (dobavljača, klijenata). Društvena opravdanost istraživanja leži u podizanju svesti o značaju bezbednosti informacija i u optimizaciji nivoa bezbednosti podataka domaćih preduzeća.

3. Rezultati

Rezultati prezentovani u ovom poglavlju predstavljaju konkretno rešenje za bezbednosni sistem preduzeća, koji, iako je na prihvatljivom nivou, ima dosta prostora za unapređenje. Glavne nadgradnje predložene su na polju vršenja transakcija i skladištenja poverljivih informacija, kao što su lozinke zaposlenih.

Nakon što je obezbeđen siguran kanal i način prenosa poverljivih informacija, dat je predlog da se poverljivim podacima, kao što su lozinke zaposlenih, pre određivanja heš vrednosti doda slučajna salt vrednost, kako bi se postigla dodatna zaštita u slučaju napada.

3.1. Deljenje tajnih informacija prilikom vršenja transakcija

U slučaju vršenja elektronskih finansijskih transakcija primenjena je tehnika proširivanja piksela originalne digitalne slike, čiji je sadržaj jednokratni PIN kod. Procesi šifrovanja i dešifrovanja su relativno jednostavni i imaju visoku sigurnost, jer se predložena tehnika vizuelne kriptografije oslanja na one-time pad algoritam.

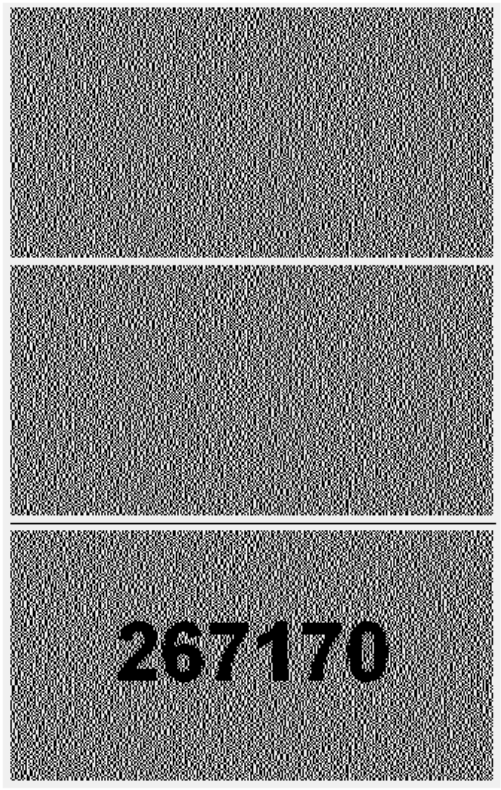
Vizuelna kriptografija predstavlja kriptološku tehniku koja omogućava skrivanje informacija, odnosno tajnih poruka, na takav način da one mogu biti dešifrovane na mestu prijema bez upotrebe računara ili bilo kakvih drugih izračunavanja [12]. U postupku dešifrovanja koristi se samo ljudski vizuelno-perceptivni sistem. Ova tehnika predložena je prvi put na EUROCRYPT konferenciji (Noni Naor i Adi Šamir). Procesi šifrovanja i dešifrovanja su relativno jednostavni i imaju visoku sigurnost, a imaju primenu u deljenju različitih vrsta informacija, naročito u finansijskim transakcijama preko interneta, kao i prilikom provere glasačkih listića, obveznica i sl.

Algoritam deljenja originalne slike na slojeve (share images) realizovan je u Visual Studio C# programskom okruženju. Oba sloja su iste rezolucije i njihovim preklapanjem očitava se tajna poruka [16]. Izabrana je jednostavna varijanta proširivanja piksela koja se vrši slučajnim generisanjem na jednom sloju, dok drugi sloj sa komplementarnim pikselima nakon vizuelnog XOR-ovanja sa prvim (primenom operacije ekskluzivno ILI – XOR) daje informaciju (tajnu poruku) nakon preklapanja.

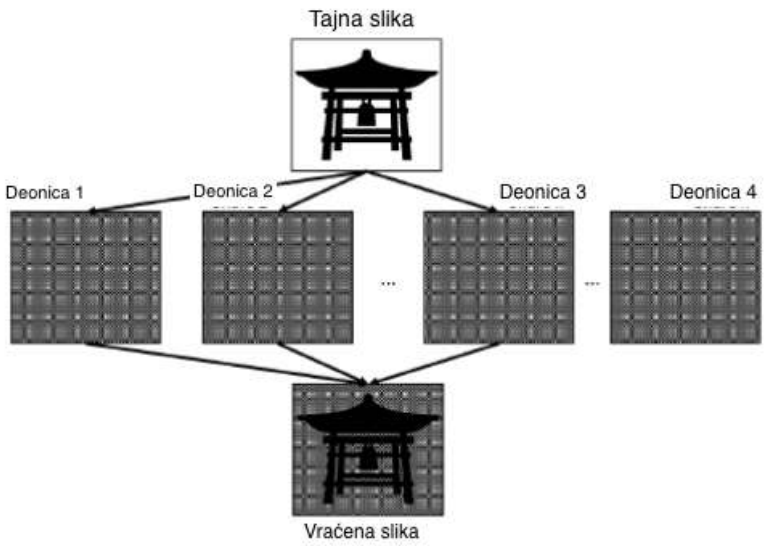
S obzirom na to da su vrednosti kojima su predstavljeni pikseli na prvom sloju slučajno generisane, ova tehnika se može posmatrati kao jedna varijanta one-time pad šifrovanja, koj ima dobre sigurnosne karakteristike.

Transparentne slike (sloj 1 i sloj 2) prikazane su na slici 1, pri čemu prvi sloj sadrži slučajno generisane proširene vrednosti piksela i ta slika predstavlja ključ. Svaki piksel predstavljen je blokom u kojem uvek postoji isti broj belih i crnih piksela. Ukoliko se vrši jednostavniji model ekspanzije piksela, piksel će biti prezentovan jednim belim i jednim crnim pikselom, a ukoliko se koristi složeniji model ekspanzije, piksel će biti predstavljen sa četiri nova piksela, od kojih su dva bela i dva crna. Piksel u sloju 1 ima određeno stanje, a piksel u sloju 2 može imati isto ili suprotno stanje. Ako su stanja u sloju 1 i sloju 2 ista, preklapanjem se dobija polovina belih i polovina crnih piksela, što će ljudsko oko detektovati kao neku nijansu sivog, a ako su stanja u sloju 1 i sloju 2 suprotna, preklapanjem se dobijaju crni pikseli, što će ljudsko oko detektovati kao crno. Preklapanjem ■□ sa istim takvim blokom u sloju 2 dobija se svetli piksel (nijansa sivog), dok se preklapanjem ■□ sa □■ dobija crni piksel. Slično je i u slučaju proširenja blokom od četiri piksela za svaki originalni piksel: preklapanjem ■■ sa istim takvim takvim blokom u sloju 2 dobija se nijansa sivog, a preklapanjem ■■ sa ■■ dobija se crni blok. Sloj 1 sadrži piksele čije su vrednosti određene na slučajan način, što je identično postupku generisanja ključa za one-time pad šifru, dok sloj 2 sadrži fiksne blokove koji su nosioci informacije u fazi preklapanja. Rezultat preklapanja slojeva prikazan je na slici 1, ispod sloja 1 i 2.

Postoje i složenije šeme u vizuelnoj kriptografiji, dok neke od njih ne uključuju model proširivanja piksela, u smislu predstavljanja originalnog piksela grupom subpiksela, ili uključuju dodatne tehnike poboljšanja kontrasta dekodovane slike [17] [18]. Primer upotrebe većeg broja generisanih slojeva na osnovu kojih se dobija dekodovana slika prikazan je na slici 2.



Slika 1. Dobijanje dekodovane slike na osnovu slojeva 1 i 2



Slika 2. Dobijanje dekodovane slike na osnovu četiri sloja (deonice)

3.2. Prikaz osnovnih principa one-time pad algoritma

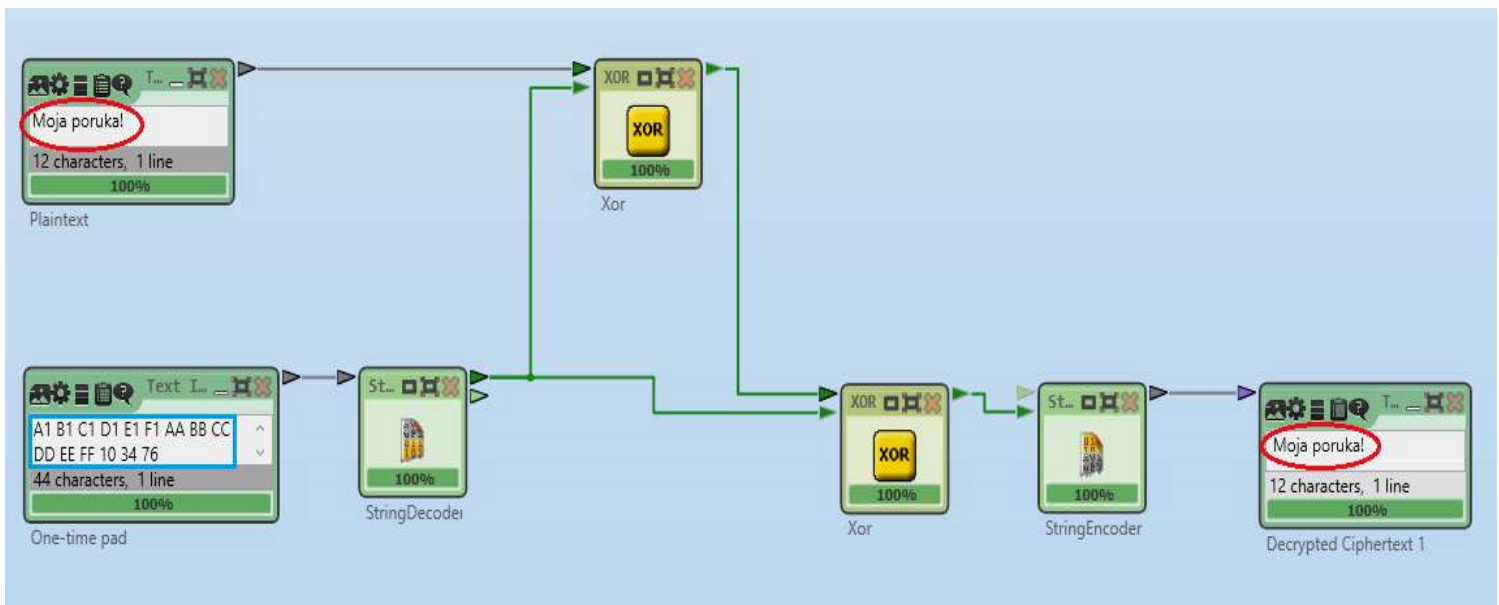
Pre postupka šifrovanja potrebno je poruku predstaviti binarnim nizom na osnovu definisanog koda. Nakon toga je neophodan drugi binarni niz, koji je iste dužine kao i sama poruka, koji će predstavljati ključ. Taj niz treba da ima osobine slučajnog niza. Postupak šifrovanja podrazumeva da se svaki bit otvorenog teksta p_i sabira po modulu 2 (operacija XOR) sa po jednim bitom ključa k_i da bi se dobio odgovarajući bit šifrata c_i [8][19]:

$$c_i = p_i \oplus k_i \quad (1)$$

U postupku dešifrovanja svaki bit šifrata sabira se po modulu 2 sa istim bitom ključa koji je korišćen pri šifrovanju, što, s obzirom na osobine XOR operacije, daje originalni tekst:

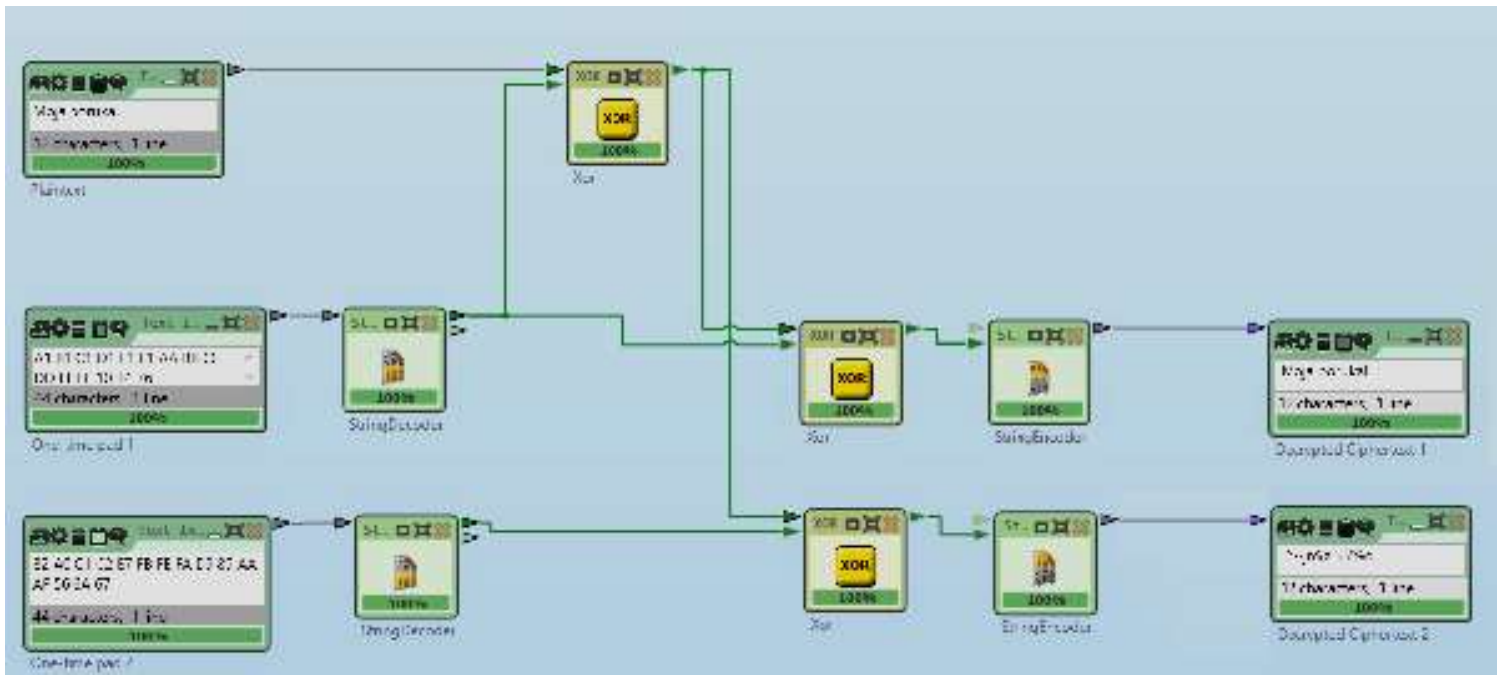
$$p_i = c_i \oplus k_i \quad (2)$$

Simulacioni model, kreiran u softverskom alatu CrypTool, koji prikazuje postupak šifrovanja i dešifrovanja otvorenog teksta (sadržaja „Moja poruka!") primenom OTP-a, prikazan je na slici 3. Ključ koji je korišćen zapisan je u heksadecimalnom formatu u donjem levom uglu, dok je dešifrovana poruka prikazana u donjem desnom uglu.



Slika 3. Simulacioni model koji prikazuje postupak šifrovanja i dešifrovanja otvorenog teksta (sadržaja „Moja poruka!") primenom OTP-a

Pretragom potencijalnih ključeva napadač generiše veliki broj poruka, od kojih će neke biti besmislene, kao što je prikazano na slici 4. Napadač će ovakve poruke odbaciti, ali će sigurno generisati i određeni broj smislenih poruka. Ako su sve te poruke podjednako verovatne, onda napadač nema načina da odredi koja je od njih prava.



Slika 4. Simulacioni model koji prikazuje postupak pretrage potencijalnih ključeva

Sigurnost OTP algoritma zasniva se na slučajnosti ključa. Za pojam slučajnosti ne postoji egzaktna definicija, ali su sa kriptografske strane neophodne dve osnovne karakteristike binarnog slučajnog ključa:

» nepredvidljivost: bez obzira na broj bita ključa koji su poznati, verovatnoća da se pogodi sledeći bit ne sme biti veća od ½. Šansa da sledeći bit bude 1 ili 0 tačno je jednaka ½;
» balansiranost: broj jedinica i nula mora biti približno jednak, u nizu dovoljno velike dužine.

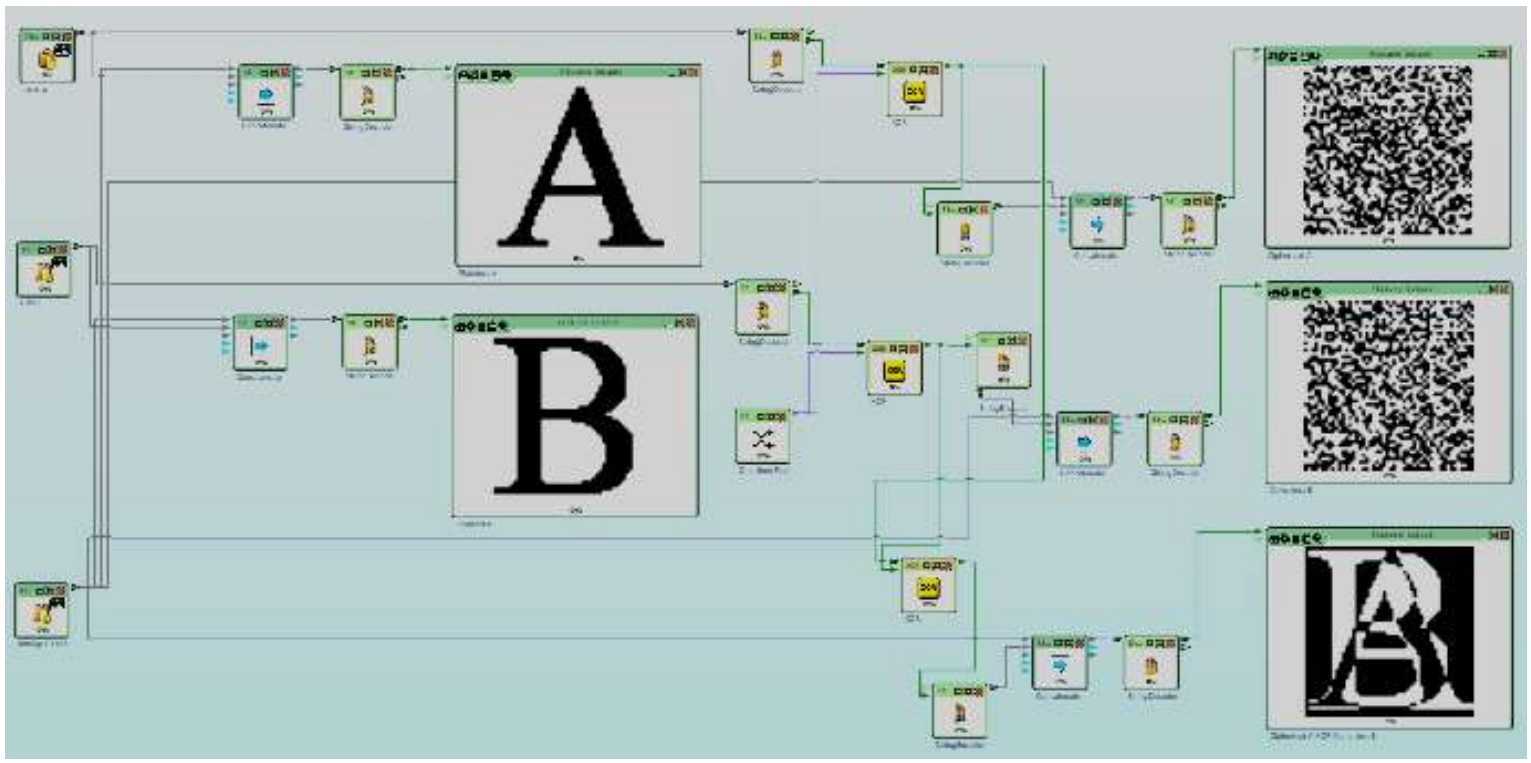
3.3. Slabosti algoritma usled višestruke upotrebe istog ključa

Ako je ključ slučajni binarni niz, onda je verovatnoća da bilo koji bit ključa ima vrednost logičke jedinice jednaka verovatnoći da taj bit ima vrednost logičke nule i iznosi ½. Za razliku od toga, otvoreni tekst ima određene statističke osobine i verovatnoća pojave logičkih jedinica i nula nije jednaka.

Simulacioni model koji ilustruje primenu istog OTP ključa u postupku šifrovanja dve različite poruke prikazan je na slici 5. Kao otvoreni tekst izabrana je digitalna slika da bi se i vizuelno prikazale posledice višestruke primene istog OTP ključa. Ukoliko se izvrši XOR operacija nad šifratima CA i CB, dobija se rezultat:

$$C_A \oplus C_B = (A \oplus K) \oplus (B \oplus K) = (A \oplus B) \oplus (K \oplus K) = (A \oplus B) \oplus 0 = A \oplus B \quad (3)$$

Posledica ove osobine je da inventivni napadač, nakon vršenja XOR operacije nad šifratima, iako napadaču nije poznat ključ K, otkriva dosta o originalnim porukama, što je razlog zbog kojeg višestruka upotreba istog OTP ključa nije preporučljiva. Rezultat prikazan u donjem desnom uglu na slici 5 dosta otkriva o originalnim slikama, što je posledica navedenih osobina XOR operacije [20].

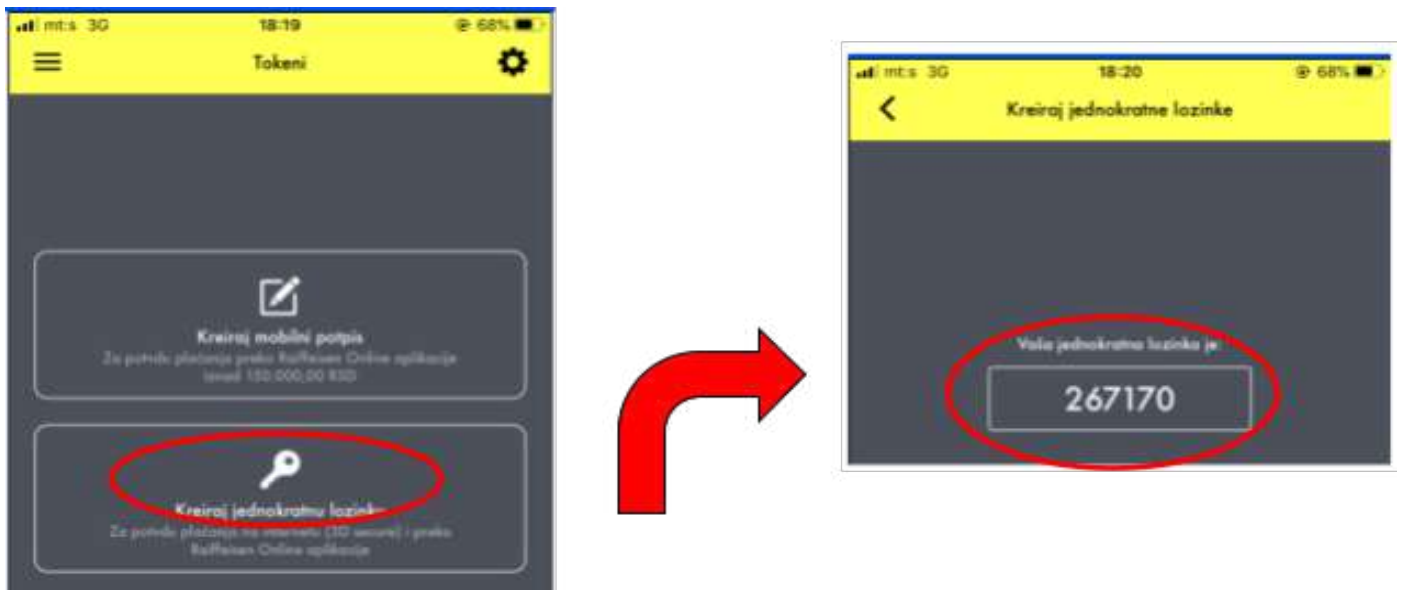


Slika 5. Simulacioni model koji ilustruje višestruku primenu istog OTP ključa

3.4. Primer vršenja elektronskih finansijskih transakcija primenom OTP algoritma

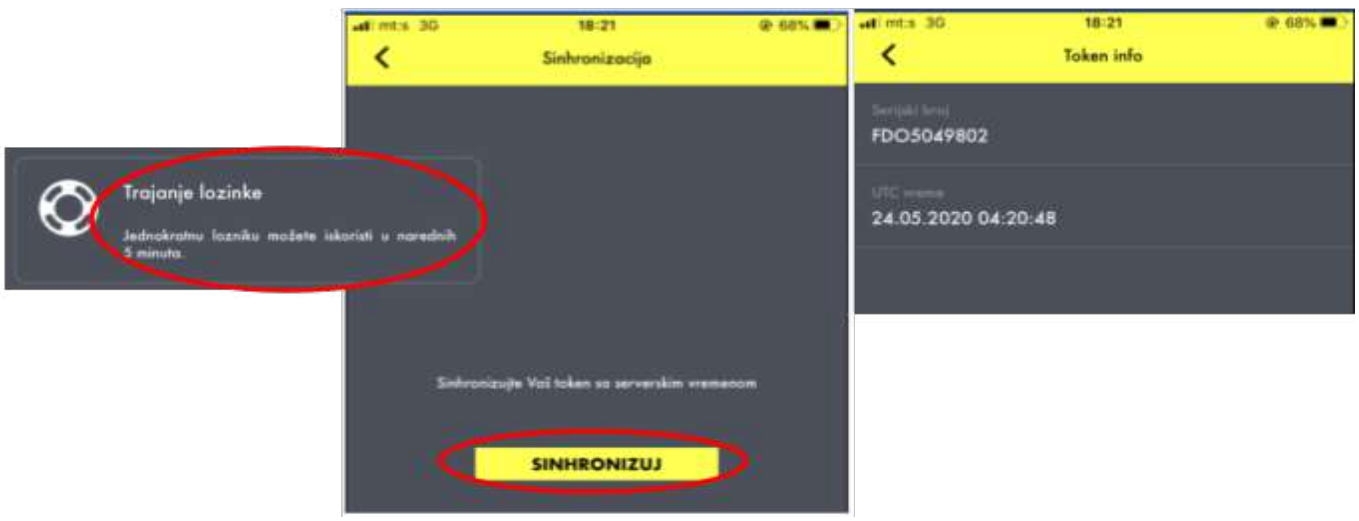
Za prijavu na e-banking aplikacije, koje se vrlo često koriste u poslovnim i privatnim finansijskim transakcijama, potreban je samo serijski broj tokena ili m-tokena. Korisnik nikom ne otkiva svoj PIN za token ili m-token, dok je podrazumevana preporuka da se PIN ne drži uz token ili m-token.

Banka od korisnika ne traži jednokratnu lozinku ni podatak za potpisivanje transakcije [21]. Kreiranje zahteva za generisanje jednokratne lozinke prikazano je u levom delu na slici 6, dok je generisana lozinka poslata na mobilni uređaj korisnika prikazana u desnom delu.



Slika 6. Kreiranje zahteva za generisanje jednokratne lozinke i slanje lozinke na mobilni uređaj korisnika

Podatak o vremenskom važenju lozinke takođe se prosleđuje korisniku, kao što je prikazano na slici 7, uključujući i neke dodatne informacije o tokenu. Trajanje lozinke, prosleđeno korisniku nakon izvršene sinhronizacije sa serverskim vremenom, prikazano je u levom delu na slici 7 i iznosi 5 minuta. Dodatne informacije o tokenu (Token info) koje prikazuju serijski broj i UTC vreme nalaze se u desnom delu na slici 7.



Slika 7. Prikaz podatka o vremenskom važenju lozinke

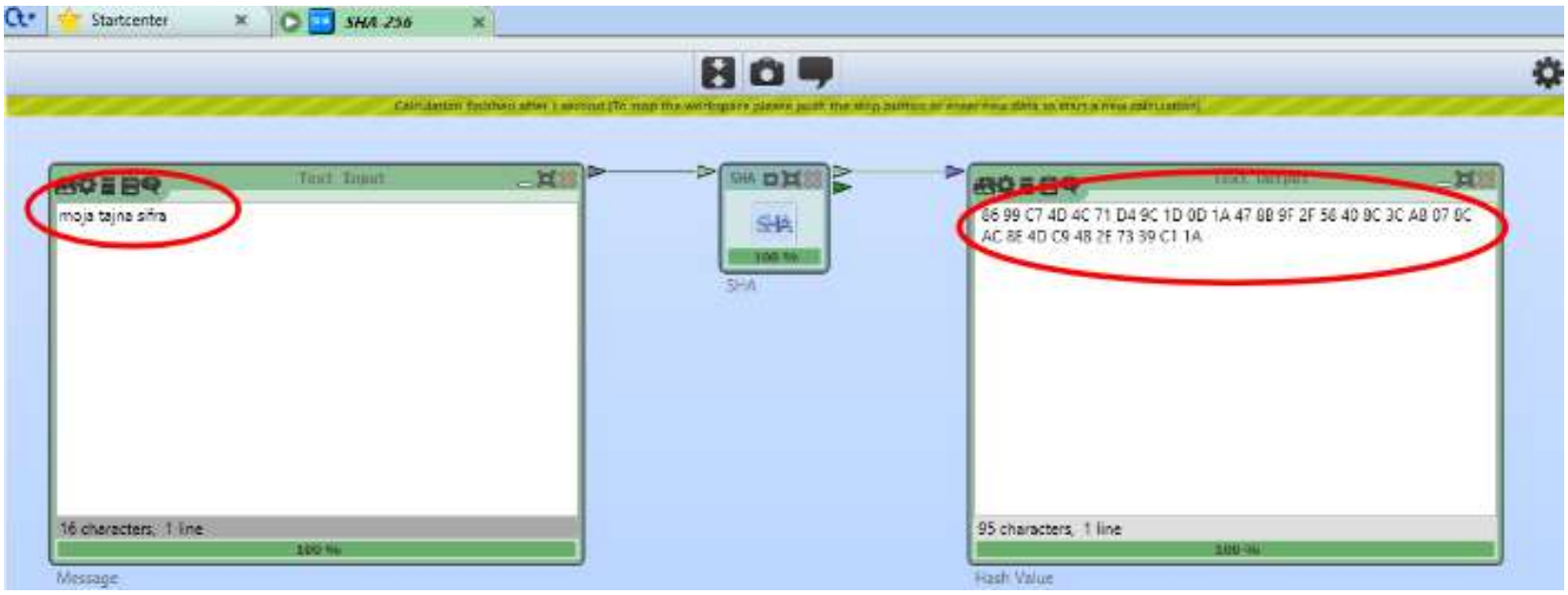
3.4. Predlog čuvanja lozinki zaposlenih primenom heš funkcija i dodavanjem slučajne salt vrednosti

Nakon što je obezbeđen siguran kanal i način prenosa poverljivih informacija, neophodno je čuvati lozinke na način koji sprečava da ih napadač dobije čak i ako je aplikacija ili baza podataka ugrožena. Većina modernih jezika i frejmvorka pruža ugrađenu funkcionalnost za bezbedno čuvanje lozinki.

Heširanje i šifrovanje predstavljaju načine za čuvanje osetljivih podataka. Međutim, u gotovo svim okolnostima lozinke je poželjno čuvati u obliku heš vrednosti, a ne kao šifrovane podatke [22]. Heš funkcija je jednosmerna funkcija, što podrazumeva da je praktično nemoguće na osnovu heš vrednosti dobiti originalnu informaciju. Ukoliko bi napadač došao u posed heš vrednosti lozinke, ne bi mogao da na osnovu toga dođe do originalnog podatka, odnosno sadržaja lozinke. U starijim heš algoritmima, kao što je MD5, pronađene su kolizije, i preporuka je primenjivati algoritme novijih generacija (novije generacija SHA).

Kriptografska heš funkcija je jednosmerna funkcija koja za ulazni podatak (poruka, fajl...) proizvoljne konačne dužine kao izlaznu vrednost daje niz fiksne dužine. Osim kompresije kao odlike, heš funkcija mora biti i efikasna, jednosmerna i otporna na kolizije.

Primena SHA algoritma prilikom određivanja heš vrednosti lozinke (sadržaja „moja tajna šifra") prikazana je na slici 8, dok je model koji uključuje dodavanje slučajne salt vrednosti prikazan na slici 9. Modeli prikazani na slici 8 i slici 9 kreirani su u CrypTool softverskom alatu.



Slika 8. Prikaz heš vrednosti lozinke zaposlenog, primenom SHA algoritma

Slika 9. Prikaz heš vrednosti lozinke zaposlenog, primenom SHA algoritma nakon dodavanja salt vrednosti

4. Diskusija

Poboljšanja bezbednosti poslovanja preduzeća „Vesimpex" predložena su u vršenju procesa elektronskih finansijskih transakcija i u postupku skladištenja poverljivih informacija, kao što su lozinke zaposlenih.

Tokom vršenja transakcije primenjena je tehnika proširivanja piksela radi deljenja tokena prilikom generisanja jednokratne lozinke. Procesi šifrovanja i dešifrovanja su relativno jednostavni i imaju visoku sigurnost, jer se oslanjaju na one-time pad tehniku.

Predlog čuvanja pristupnih lozinki zaposlenih uključuje dodavanje slučajne salt vrednosti pre heširanja. Salt vrednosti predstavljaju jedinstvene nasumično generisane nizove koji se dodaju svakoj lozinki i jedinstveni su za svakog korisnika.

Svrha opisanog procesa je da u slučaju upada poverljiva informacija potencijalnom hakeru bude potpuno nerazumljiva i samim tim neupotrebljiva. Na taj način se veći deo odgovornosti za rizik curenja podataka prenosi sa ljudskog faktora na sam bezbednosni sistem, što značajno poboljšava sigurnost poslovanja preduzeća.

Reference

1. Crovini C. Risk management in small and medium enterprises. Routledge; 2019.
2. Hughes P, Ferrett E. Introduction to Health and Safety at Work. 6th ed. New York: Routledge; 2016.
3. Hughes P, Ferrett E. Business Intelligence and Analytics in Small and Medium Enterprises. Melo PN, Machado C, editors. Boca Raton, FL : CRC Press/ Taylor & Francis Group, 2020. | Series: Manufacturing design and technology series: CRC Press; 2018.
4. Ranković M, Ilić M. Upravljanje projektima. Beograd: ITS – Beograd; 2018.
5. Seo JH. Information Security and Cryptology – ICISC 2019: 22nd International Conference, Seoul, South Korea, December 4–6, 2019, Revised Selected Papers. In: Seo JH, editor. Cham: Springer International Publishing; 2020 [cited 2022 Feb 14]. Available from: https://link.springer.com/conference/icisc
6. https://www.vesimpex.rs/ [Internet]. [cited 2022 Feb 14]. Available from: https://www.vesimpex.rs/
7. Ilić M. Osnove ekonomije, finansija i računovodstva. Beograd: ITS-Beograd; 2017.
8. Kumar V, Sharma A, Ntroduction I, August IJ-. A Survey on Various Most Common Encryption Techniques. Int J Adv Res Comput Sci Softw Eng [Internet]. 2014 [cited 2022 Feb 14];3:307–12. Available from: https://www.ijettcs.org/Volume3Issue4/IJETTCS-2014-08-25-137.pdf
9. Menez J., van Oorschot P., Vanstone S. A Handbook of Applied Cryptography. 5th edition. CRC press Series on Discrete Mathematics and Its Applications; 2001.
10. Klima RE, Sigmon NP. Cryptology Classical and Modern. 2nd ed. Chapman and Hall/CRC; 2019.
11. Stallings W. Cryptography and Network Security: Principles and Practice. 3rd ed. Prentice Hall; 2002.
12. Manucom EMM, Gerardo BD, Medina RP. Analysis of Key Randomness in Improved One-Time Pad Cryptography. 2019 IEEE 13th Int Conf Anti-counterfeiting, Secur Identif [Internet]. IEEE; 2019. p. 11–6. Available from: https://ieeexplore.ieee.org/document/8925173/
13. https://www.cryptool.org/en/ [Internet]. Available from: https://www.cryptool.org/en/
14. Ateniese G, Blundo C, Santis A De, Stinson DR. Extended capabilities for visual cryptography. Theor Comput Sci [Internet]. 2001;250:143–61. Available from: https://linkinghub.elsevier.com/retrieve/pii/S0304397599001279
15. Ibrahim DR, Teh J Sen, Abdullah R. An overview of visual cryptography techniques. Multimed Tools Appl [Internet]. 2021;80:31927–52. Available from: https://link.springer.com/10.1007/s11042-021-11229-9
16. Gnanaguruparan M, Kak S. Recursive Hiding of Secrets in Visual Cryptography. Cryptologia [Internet]. 2002;26:68–76. Available from: http://www.tandfonline.com/doi/abs/10.1080/0161-110291890768
17. Askari N, Heys HM, Moloney CR. An extended visual cryptography scheme without pixel expansion for halftone images. 2013 26th IEEE Can Conf Electr Comput Eng [Internet]. IEEE; 2013. p. 1–6. Available from: https://ieeexplore.ieee.org/document/6567726
18. Gonzalez RC, Woods RE. Digital Image Processing Third Edition. 3rd ed. New York: Upper Saddle River, NJ: Prentice Hall; 2008.
19. Dent AW, Mitchell CJ. User's guide to cryptography and standards [Internet]. Boston: Artech House; 2005. Available from: https://pure.royalholloway.ac.uk/portal/en/publications/users-guide-to-cryptography-and-standards(2bda27a3-da21-4407-b057-66c80213c16b).html
20. Stefanovic H, Savic A, Veselinovic R, Bjelobaba G. An application of visual cryptography scheme with digital watermarking in sharing secret information from car number plate digital images. Int J Eng Invent [Internet]. 2021;10:1–11. Available from: www.ijeijournal.com
21. https://www.raiffeisenbank.rs/token/ [Internet]. Available from: https://www.raiffeisenbank.rs/token/
22. Islam MS. Using ECG signal as an entropy source for efficient generation of long random bit sequences. J King Saud Univ - Comput Inf Sci [Internet]. 2022; Available from: https://linkinghub.elsevier.com/retrieve/pii/S1319157822000015

Type of the Paper: Original scientific paper
Received: 14. 02. 2022
Accepted: 6. 11. 2022.
DOI: https://doi.org/10.18485/edtech.2022.2.2.2
UDK:

Protection and security risk management, a proposal of cryptologic measures and solutions for Vesimpex company

Ivan Jovanović [1], Milosav Majstorović [1] and Hana Stefanović [1*]

[1] Information Technology School – ITS, Belgrade, Serbia; ivan59218@its.edu.rs; milosav.majstorovic@its.edu.rs
[*] hana.stefanovic@its.edu.rs; +381 (0)63/84-97-189

Summary: The subject of this paper comprises the creation of an associative concept network in the realm of security management, and the application of cryptography through secondary research, along with perceiving the importance of security in a concrete organisation through primary research. The objective is to formulate, based on the analysis of a specific company, a proposal regarding security and cryptology measures to advance the security system of a company. The basic principles of information security of small and medium-sized enterprises, along with the application of adequate security algorithms based on a one-time pad (OTP) and visual cryptography (VC) are utilised for the design of a complete solution for the company in question. Alongside its theoretical foundation, the paper contains information about the company itself, collected through observation, note-taking and content analysis, as well as the process of creating the security solution incorporated into the project charter, and the solution itself.

Keywords: small and medium-sized enterprises (SMEs); security solutions; competitive advantage; one-time pad (OTP); visual cryptography (VC)

1. Introduction

The information age and digitalisation have contributed to a considerable advancement of all forms of business, but they have also rendered information easily accessible, which is a potential threat to the security of the business system itself [1]. In a very fierce competitive race on the market, the protection of information has become indispensable [2], as various types of breaches may take place – internal, external or incidental, increasingly perpetrated through the abuse of new technology [3][4]. Reliable security systems considerably lower the risk of information leaks [5] which can be fatal for a company.

Vesimpex is a small enterprise operating in the realm of electrical equipment and solutions, including original solutions in power distribution [6]. The company works with a number of successful companies in different branches of industry, and the issue of information security and reliability is exceedingly important. In such an environment, advanced security can give the company an advantage over its often disloyal competition [7]. To provide security from various attacks, one must analyse the existing state and the level of employees' expertise and, accordingly, formulate a proposal for forming a security system for the small enterprise in question.

The subject of this paper's research is multidisciplinary and has to do with the disciplines of business economics, project management, security and cryptography. The central motive is to formulate a concrete solution on a practical example, by analysing the security characteristics of the company. The purpose of this research is to find adequate ways to realise the formulated goals in order to ensure that the security criteria are realised.

The primary objective of this applied research is to provide a solution to a specific security problem and ensure a competitive advantage for the Vesimpex company [6]. The secondary objective is to study the existing and introduce new cryptologic protection measures to increase the security of the business.

As the modern way of doing business, based primarily on the utilisation of computer systems and the exchange of data in electronic form, is exposed to various risks with potentially catastrophic consequences, it is necessary to analyse and prevent the increasingly frequent attacks on computer networks, attempts at unauthorised data access, tapping, and malicious data exchange [8]. This requires the implementation of new forms of communication, made possible by the advancements in technology. The problem of security necessitates the need for the introduction of new mechanisms that should assume the role formerly played by the traditional solutions for the purposes of efficient identification, access control and verification. Most of these challenges can be resolved through the use of cryptographic solutions [9], although there are problems that cannot be adequately solved by cryptography alone.

Cryptography studies various techniques of transformation of transferred data so that the meaning of the data is accessible only to authorised parties in communication. At the same time, said transformation ought to be such that unauthorised parties in communication who come into possession of the transformed message should be unable to access the initial data.
There are a large number of traditional and modern cryptography algorithms, those that use the same key for encryption and description, as well as the asymmetric ones, which use different keys for encryption and decryption. For any cipher, those with symmetric and asymmetric algorithms alike, the crucial issue is the security of the cipher [10][11].

An unconditionally secure cipher is a cipher that ensures that, without the knowledge of the key, not even a full search of the keys can result in accessing the plaintext from the ciphertext. A comprehensive search (with no limitations regarding time and available resources) can encounter the key, but it is not in the attacker's interest to have it accomplished after several decades or even centuries. However, even assuming that the attacker has the best possible equipment and resources, an unconditionally secure password ought to ensure that the attacker does not come into possession of plaintext, not even in ideal conditions. The basic idea behind an unconditionally secure password is to ensure that a comprehensive search of potential keys, which are sure to generate a large number of messages, should not enable the attacker to determine which one is the right one. Through an exhaustive search, the attacker will get a large number of nonsensical messages, which will be discarded, along with a certain number of messages that make sense, and if the latter messages are equally probable, the attacker should have no way of determining which one is right.

A one-time pad – OTP [12], used in this paper, is an unconditionally secure cipher. Simulation models that illustrate the basic principles of OTP algorithms have been realised in CrypTool software [13], with an emphasis on the case of repeated use of a one-time key. We also include an example of processing an electronic financial transaction using OTP, where confidential information is shared using the visual cryptography technique [14][15].

2. Materials and methods

The work on this paper included the use of a number of scientific and professional methods, techniques and tools, with a research plan that included:

- Defining the subject of the research (through formulating the research problem);
- Defining the research objectives;
- An overview of relevant literature and making a selection of literature for use in the research;
- Determining the theoretical framework of the research (in accordance with the relevant disciplines and the selection of relevant literature);
- Situational analysis;
- Examining the target group through polling;
- Statistical analysis of data from the poll;
- Designing and making the security solution.

The main hypothesis of the study:

H1: The level of information security at Vesimplex is not optimal; it needs to be elevated through a new security solution, considering the elements from the environment and the desired growth and development as an organisational goal.

H2: An adequate advancement of the company's information security would ensure its competitive advantage.

The outcomes of the research, that is, the anticipated results of the research, include analysis of the selected literature and other references, proving the hypotheses and solving the central problem of the research through the selected model. From the professional relevance standpoint, the proposed solution would further advance the business and the security of the observed company, elevating the security of the business, as well as the security of the partners involved (suppliers, and clients). The social justification of this research concerns the awareness of the importance of information security and the optimisation of the level of security of the companies in the country.

3. Results

The results presented in this chapter constitute a concrete solution for the security system of the company, which, although it is already at an acceptable level, still leaves a lot of room for improvement. The major upgrades concern the realm of transactions and the storage of confidential information, such as employees' passwords.

Having provided a secure channel and method of transferring confidential information, we propose that confidential data, such as employees' passwords, should be secured by a random salt value before determining the hash value, to provide additional security in case of an attack.

3.1. Sharing confidential information during transactions

For electronic financial transactions, the technique of expanding the pixels of the original digital image containing a one-time PIN code was used. The encryption and decryption processes are fairly simple, and provide high security, as the proposed visual cryptography technique relies upon a one-time pad algorithm.

Visual cryptography is a cryptology technique that provides the hiding of information, i.e. secret messages so that they can be decrypted at reception without using a computer or performing any other type of calculation [12]. The decryption procedure uses solely human visual perception. This technique was first proposed at the EUROCRYPT conference, by Noni Naor and Adi Shamir. Its encryption and decryption systems are fairly simple and can be used for sharing different types of information, especially in financial transactions over the internet, as well as for verifying ballots, securities, etc.

The algorithm for dividing the original image into layers (share images) was realised in the Visual Studio C# programming environment. Both layers have the same resolution and their overlaying results in the unveiling of the secret message [16]. A simple pixel expansion variant was selected, achieved by random generation on one layer, whereas the second layer with complementary pixels, after visual XORing with the first one (using the exclusive or operation – XOR) provides information (secret message) upon overlaying. Since the values representing pixels on the first layer are randomly generated, this technique can be viewed as a variant of one-time pad encryption, with good security properties.

Transparent images (layer 1 and layer 2) are shown in Fig. 1, with the first layer containing randomly generated expanded values of pixels, and this image constitutes the key. Each pixel is represented by a block which always contains the same number of white and black pixels. If the simpler pixel expansion model is used, a pixel will always be represented by one white pixel and one black pixel, and if the more complex expansion model is used, a pixel will be represented by four new pixels – two white ones and two black ones. A pixel in layer 1 has a certain state, whereas a pixel in layer 2 can have the same state or the opposite state. If the states in layers 1 and layer 2 are the same, the overlaying results in one-half of white and one-half of black pixels, which the human eye will register as a shade of grey, and if the states in layer 1 and layer 2 are opposite, the overlaying yields black pixels, which will be detected by the human eye as the colour black. Overlaying ■□ with an identical block in layer 2 results in a bright pixel (shade of grey), while overlapping ■□ with □■ results in a black pixel. The case with expansion by a four-pixel block for each original pixel is similar: overlaying ■■ with the same block in layer 2 results in a shade of grey, while overlaying ■■ with ■■ results in a black block. Layer 1 contains pixels whose values are determined randomly, which is identical to the procedure for generating a key for a one-time pad cipher, while layer 2 contains fixed blocks that carry information in the overlay phase. The result of overlaying layers is shown in Fig. 1, after layers 1 and 2.

There are also more complex schemes in visual cryptography, and some do not involve the pixel expansion model, in the sense of representing the original pixel by a group of subpixels, while some involve additional techniques for improving the contrast in the decoded image [17][18]. Fig. 2 shows an example of using several generated layers based on which the decoded image is formed.

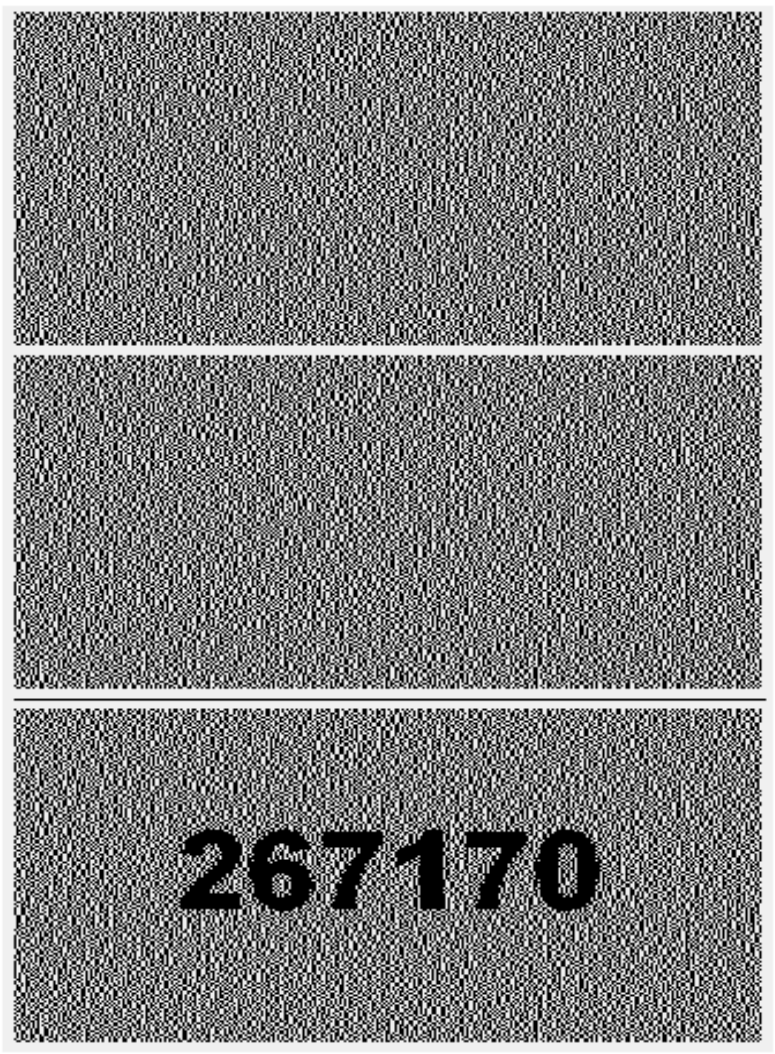


Figure 1. Acquiring the decoded image based on layers 1 and 2

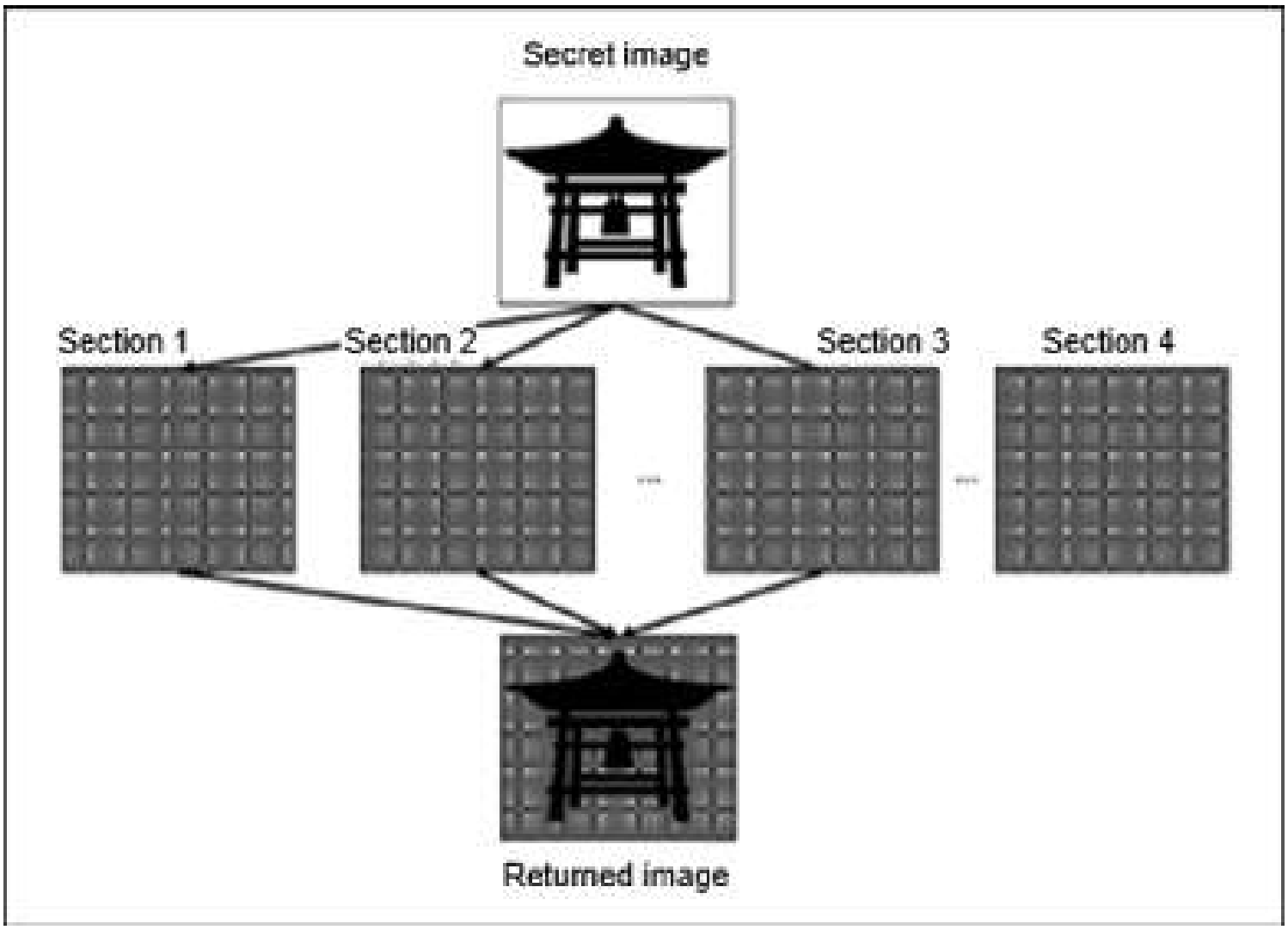


Figure 2. Acquiring the decoded image based on four layers (sections)

3.2. The basic principles of a one-time pad algorithm

Prior to the encoding procedure, the message needs to be represented by a binary sequence based on the defined code. This should be followed by another binary sequence, of the same length as the message itself, which will represent the key. This sequence would have the properties of a random sequence. During the encryption procedure, each bit of the plaintext p_i is added, using modulo 2 (XOR operation), with one bit of the key k_i, to get the relevant bit of the ciphertext c_i [8][19]:

$$c_i = p_i \oplus k_i \tag{1}$$

In the decoding procedure, each bit of the ciphertext is added, using modulo 2, with the same bit of the key which was used for encryption, which, according to the properties of the XOR operation, yields the original text:

$$p_i = c_i \oplus k_i \tag{2}$$

The simulation model, created in CrypTool software, which shows the process of encryption and decryption of the plaintext ("My message!") using OTP, is shown in Fig. 3. The key which was used is written in hexadecimal format in the lower left corner, while the decoded message is shown in the lower right corner.

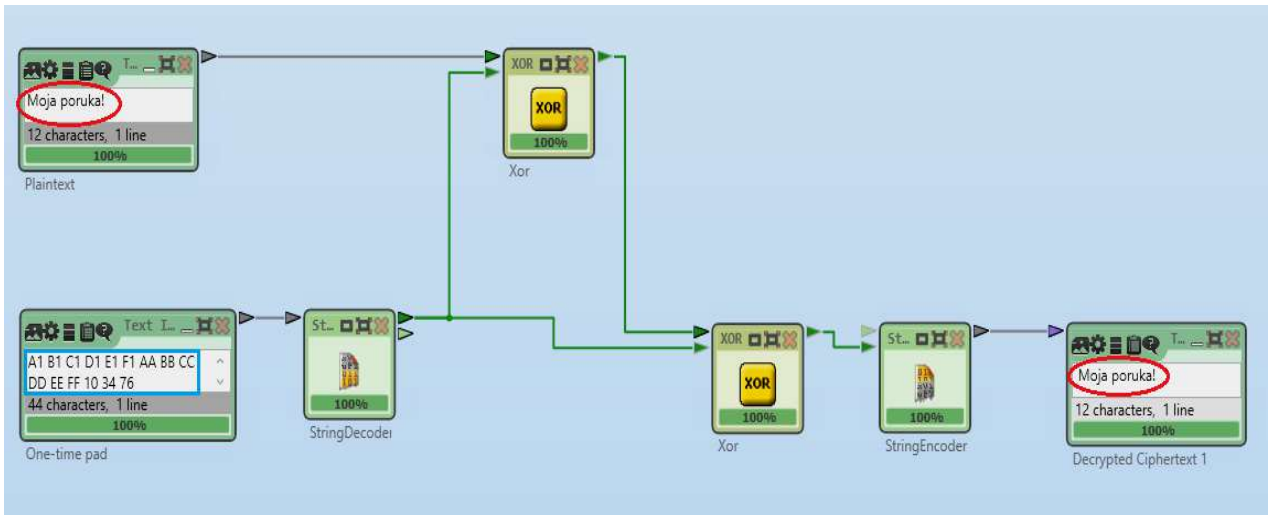


Figure 3. Simulation model illustrating the encryption and decryption procedure for plaintext ("My message!") using OTP

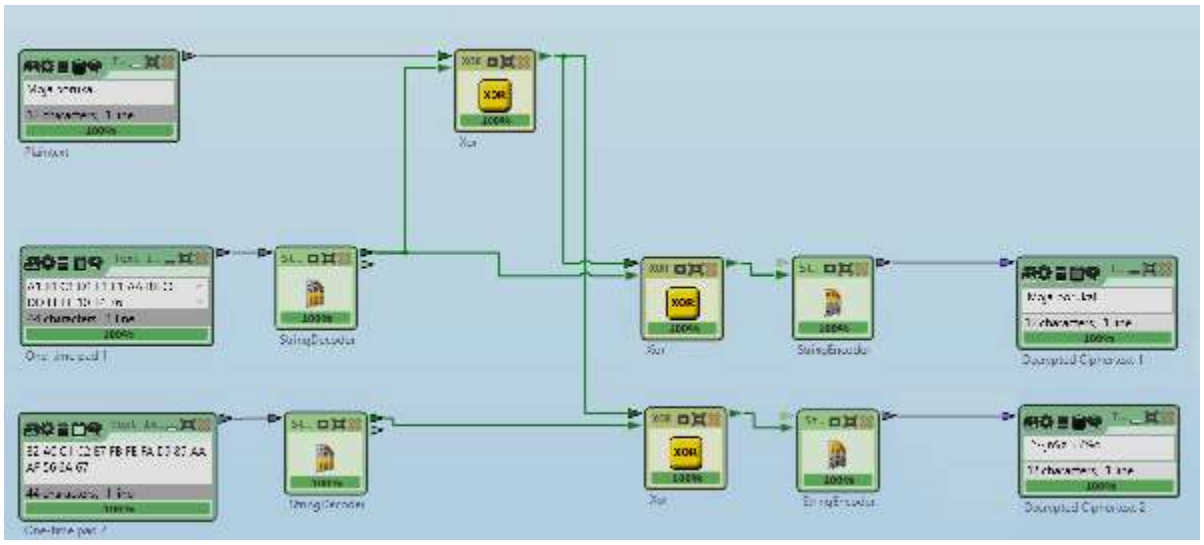


Figure 4. Simulation model showing the procedure of a search for potential keys

Searching the potential keys, the attacker generates a large number of messages, some of which will be nonsensical, as shown in Fig. 4. The attacker will discard such messages, but he will surely also generate a certain number of sensible ones. If all these messages are equally probable, the attacker has no way of ascertaining which one of them is real.

The security of an OTP algorithm is based on the randomness of the key. There is no exact definition for randomness, but from the cryptography standpoint, there are two basic characteristics of a binary random key:

» Unpredictability: Regardless of the number of known bytes of the key, the probability of guessing the next bite must not exceed ½. The chance of the next bit being 1 or 0 is exactly ½.

» Balance: The number of 1s and 0s must be approximately the same, in a sufficiently long sequence.

3.3. Weaknesses of the algorithm due to multiple uses of the same key

If the key is a random binary sequence, the probability of any bit of the key having the value of logic one is the same as the probability of that bit having the value of logic zero: it is ½. However, plaintext has certain statistical properties and the probability of the occurrence of logic ones and zeroes is not the same.

The simulation model that illustrates the use of the same OTP key in the process of encoding two different messages is shown in Fig. 5. To illustrate plaintext, we chose a digital image, to provide a visual representation of multiple uses of the same OTP key. XORing ciphertext CA and CB yields:

$$C_A \oplus C_B = (A \oplus K) \oplus (B \oplus K) = (A \oplus B) \oplus (K \oplus K) = (A \oplus B) \oplus 0 = A \oplus B \tag{3}$$

The consequence of these properties is that an inventive attacker, after XORing the ciphertext, although unfamiliar with the key K, actually discovers a lot about the original messages, which is the reason why multiple uses of the same OTP key is not recommended. The result shown in the lower right corner of Fig. 5 reveals a lot about the original images, which is a consequence of the aforementioned properties of XOR operation [20].

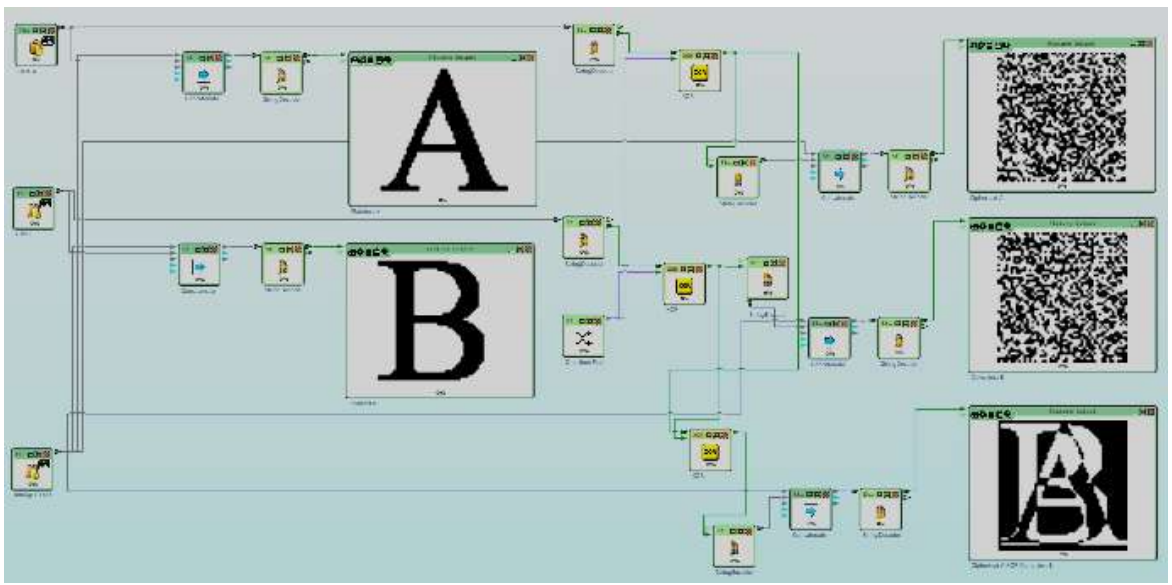


Figure 5. Simulation model illustrating multiple uses of the same OTP key

3.4. An example of an electronic financial transaction using the OTP algorithm

Usually, all it takes to log in to e-banking applications, which are widely used in corporate and private financial transactions, is the serial number of the token or m-token. The user does not reveal the PIN for the token or m-token, and of course, it is recommended that the PIN should be kept separately from the token or m-token.

The bank does not require a one-time password or transaction signing data [21]. The process of creating a request for a one-time password is shown in the upper left part of Fig. 6, while the generated password sent to the user's mobile device is shown on the right.

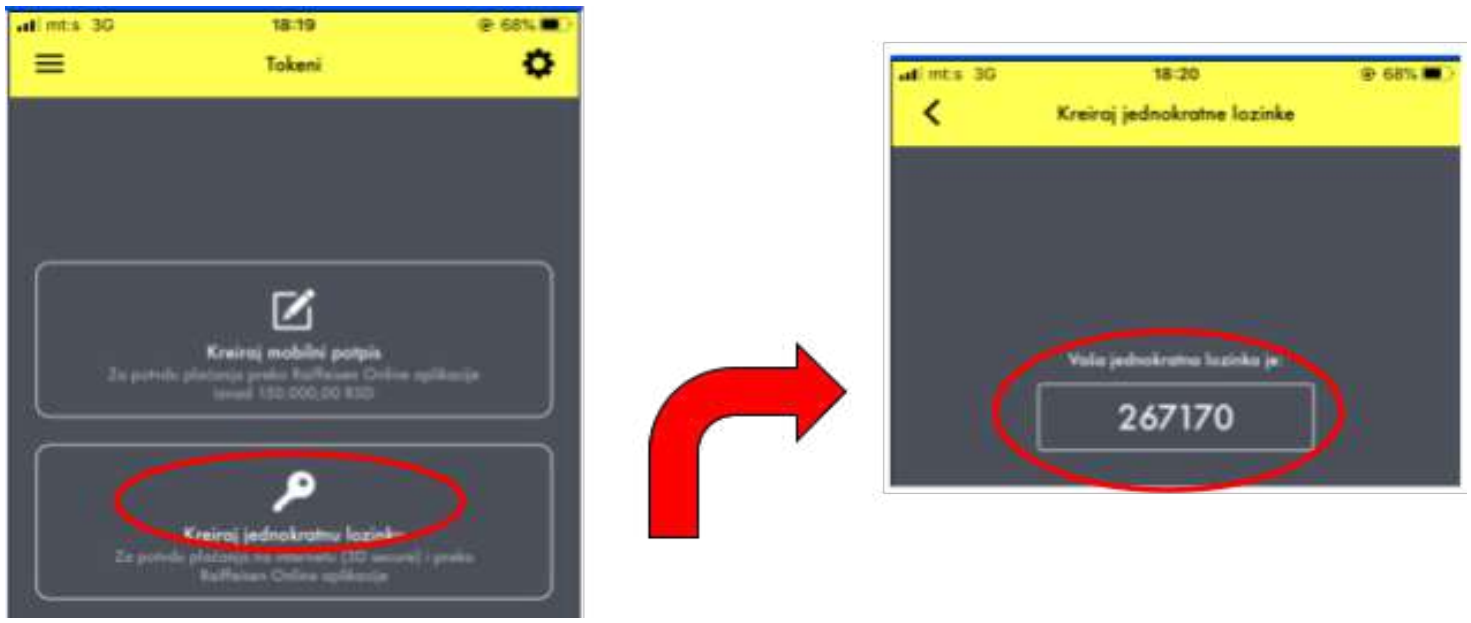


Figure 6. Creating a request for generating a one-time password and sending the password to the user's mobile device

The information about the validity period of the password is also sent to the user, as shown in Fig. 7, along with some additional information about the token. The duration of the password, sent to the user after synchronising with server time, is shown on the left in Fig. 7; it is 5 minutes. Additional information about the token (Token info) showing the serial number and the UTC time is shown on the right in Fig. 7.

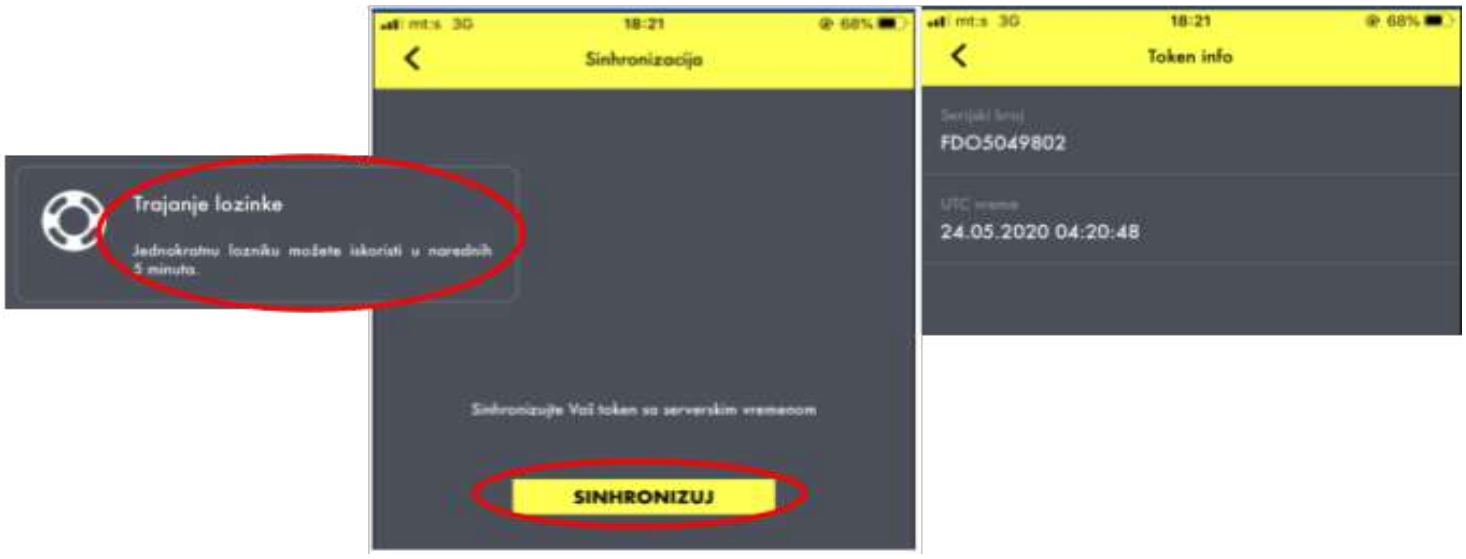


Figure 7. Information about the validity period of the password

3.4. Proposal for storing employees' passwords using hash functions and adding a random salt value

After providing a secure channel and mode of transmission of confidential information, passwords must be kept in a way that prevents the attacker from obtaining them even if the application or the database is compromised. Most modern languages and frameworks provide built-in functionality for the secure storing of passwords.

Hashing and encryption are two different ways of storing sensitive data. In almost any circumstance, it is preferable that passwords should be stored as hash values, not as encrypted data [22]. The hash function is a one-way function, which means that it is practically impossible to obtain the original information based on the hash value.

If the attacker came into possession of a password's hash value, he would be unable to acquire the original data, i.e. the content of the password. Older hash algorithms, such as MD5, have been found to be vulnerable to collisions, and the use of newer generation algorithms (later generation SHA) is recommended.

A cryptographic hash function is a one-way function which, for input data (message, file…) of any final length, returns the same length "hash". Besides providing compression, a hash function must be efficient, one-way and collision-proof.

The application of the SHA algorithm when determining the hash value of the password (content "my secret password") is shown in Fig. 8, while the model that includes the addition of a random salt value is shown in Fig. 9. The models shown in Fig. 8 and Fig. 9 were created in CrypTool software.

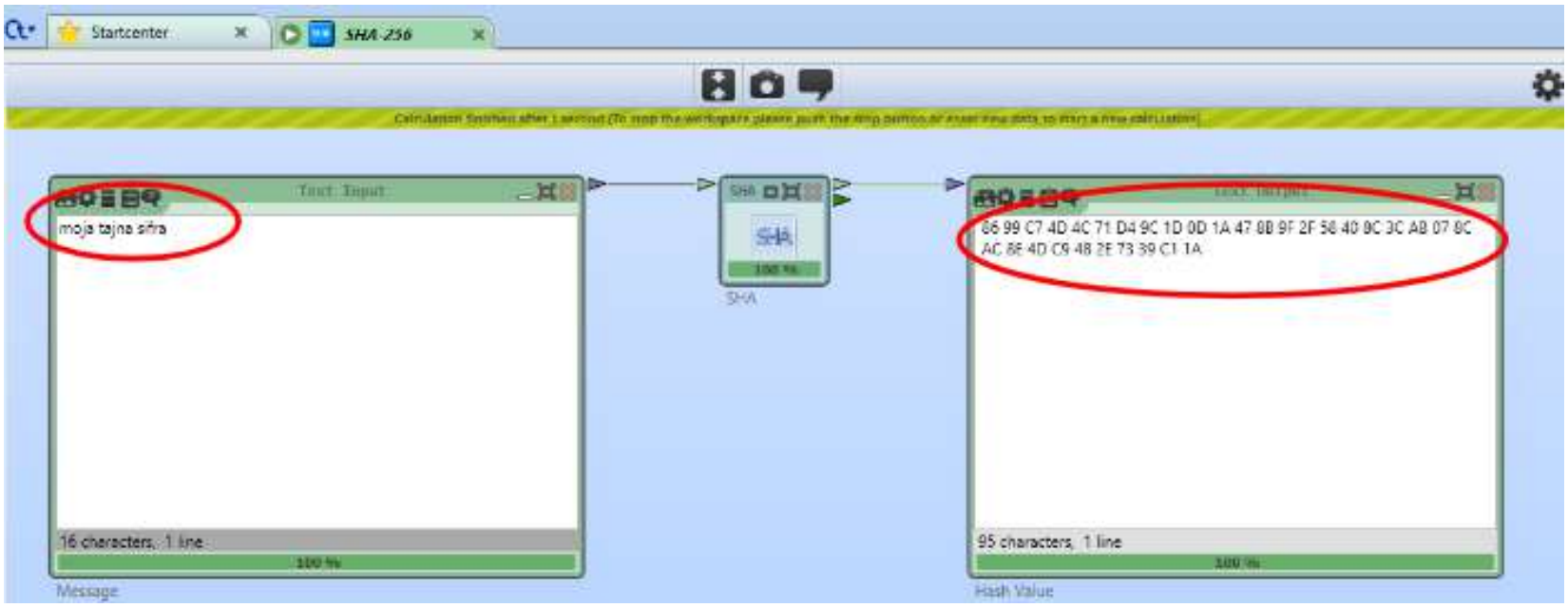


Figure 8. Illustration of a hash value of an employee's password, using SHA algorithm

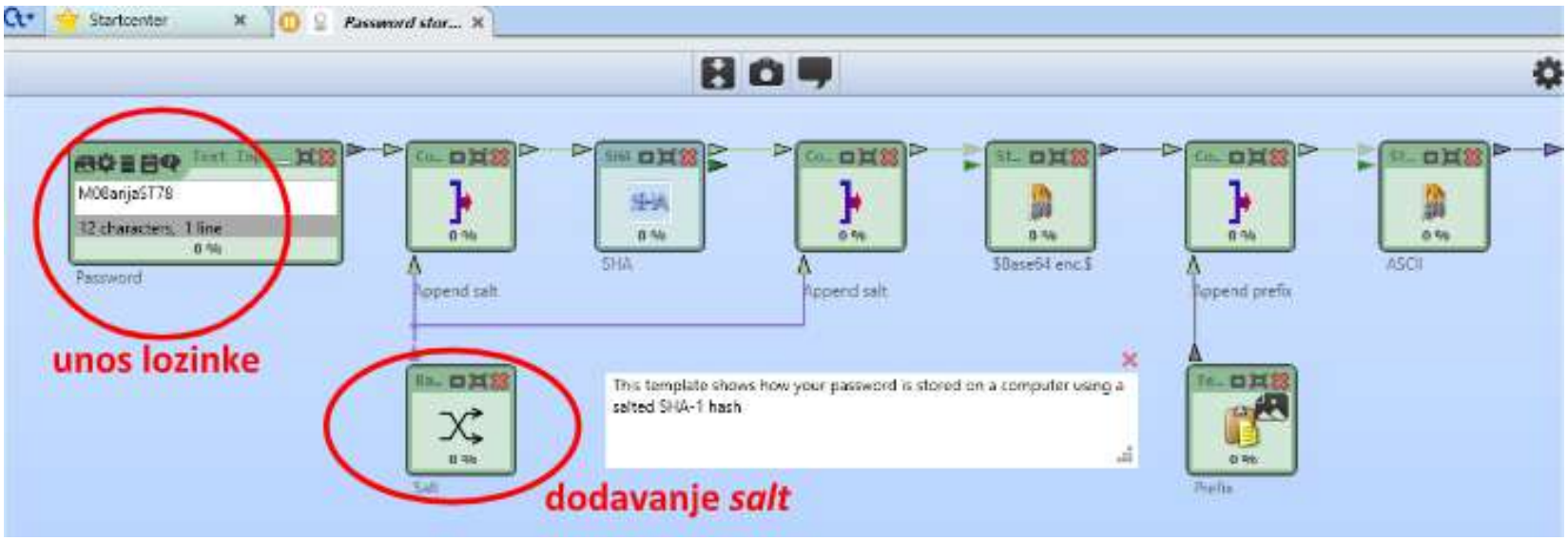


Figure 9. Illustration of a hash value of an employee's password, using the SHA algorithm after adding a salt value

4. Discussion

Improvements in the security of the business of Vesimpex have been proposed for the process of financial transactions and the procedure of storing confidential information, such as employees' passwords.

The transaction implemented the pixel expansion technique for the purpose of assigning tokens when generating a one-time password. The encryption and decryption processes are fairly simple and provide a high level of security because they rely upon the one-time pad technique.

The proposal for storing the login passwords of employees includes adding random salt values before hashing. Salt values are unique randomly generated sequences added to each password, unique for each user.

The purpose of the process described here is to ensure that the potential hacker should find the confidential information entirely incomprehensible and therefore completely useless. This way, most of the responsibility for a data leak risk is conveyed from the human factor to the security system itself, which considerably enhances the security of the company's business.

References

1. Crovini C. Risk management in small and medium enterprises. Routledge; 2019.
2. Hughes P, Ferrett E. Introduction to Health and Safety at Work. 6th ed. New York: Routledge; 2016.
3. Hughes P, Ferrett E. Business Intelligence and Analytics in Small and Medium Enterprises. Melo PN, Machado C, editors. Boca Raton, FL : CRC Press/Taylor & Francis Group, 2020. | Series: Manufacturing design and technology series: CRC Press; 2018.
4. Ranković M, Ilić M. Upravljanje projektima. Beograd: ITS – Beograd; 2018.
5. Seo JH. Information Security and Cryptology – ICISC 2019: 22nd International Conference, Seoul, South Korea, December 4–6, 2019, Revised Selected Papers. In: Seo JH, editor. Cham: Springer International Publishing; 2020 [cited 2022 Feb 14]. Available from: https://link.springer.com/conference/icisc
6. https://www.vesimpex.rs/ [Internet]. [cited 2022 Feb 14]. Available from: https://www.vesimpex.rs/
7. Ilić M. Osnove ekonomije, finansija i računovodstva. Beograd: ITS-Beograd; 2017.
8. Kumar V, Sharma A, Introduction, August IJ-. A Survey on Various Most Common Encryption Techniques. Int J Adv Res Comput Sci Softw Eng [Internet]. 2014 [cited 2022 Feb 14];3:307–12. Available from: https://www.ijettcs.org/Volume3Issue4/IJETTCS-2014-08-25-137.pdf
9. Menez J., van Oorschot P., Vanstone S. A Handbook of Applied Cryptography. 5th edition. CRC Press Series on Discrete Mathematics and Its Applications; 2001.
10. Klima RE, Sigmon NP. Cryptology Classical and Modern. 2nd ed. Chapman and Hall/CRC; 2019.
11. Stallings W. Cryptography and Network Security: Principles and Practice. 3rd ed. Prentice Hall; 2002.
12. Manucom EMM, Gerardo BD, Medina RP. Analysis of Key Randomness in Improved One-Time Pad Cryptography. 2019 IEEE 13th Int Conf Anti-counterfeiting, Secure Identify [Internet]. IEEE; 2019. p. 11–6. Available from: https://ieeexplore.ieee.org/document/8925173/
13. https://www.cryptool.org/en/ [Internet]. Available from: https://www.cryptool.org/en/
14. Ateniese G, Blundo C, Santis A De, Stinson DR. Extended capabilities for visual cryptography. Theor Comput Sci [Internet]. 2001;250:143–61. Available from: https://linkinghub.elsevier.com/retrieve/pii/S0304397599001279
15. Ibrahim DR, Teh J Sen, Abdullah R. An overview of visual cryptography techniques. Multimed Tools Appl [Internet]. 2021;80:31927–52. Available from: https://link.springer.com/10.1007/s11042-021-11229-9
16. Gnanaguruparan M, Kak S. Recursive Hiding of Secrets in Visual Cryptography. Cryptologia [Internet]. 2002;26:68–76. Available from: http://www.tandfonline.com/doi/abs/10.1080/0161-110291890768
17. Askari N, Heys HM, Moloney CR. An extended visual cryptography scheme without pixel expansion for halftone images. 2013 26th IEEE Can Conf Electr Comput Eng [Internet]. IEEE; 2013. p. 1–6. Available from: https://ieeexplore.ieee.org/document/6567726
18. Gonzalez RC, Woods RE. Digital Image Processing Third Edition. 3rd ed. New York: Upper Saddle River, NJ: Prentice Hall; 2008.
19. Dent AW, Mitchell CJ. User's guide to cryptography and standards [Internet]. Boston: Artech House; 2005. Available from: https://pure.royalholloway.ac.uk/portal/en/publications/users-guide-to-cryptography-and-standards(2bda27a3-da21-4407-b057-66c80213c16b).html
20. Stefanovic H, Savic A, Veselinovic R, Bjelobaba G. An application of visual cryptography scheme with digital watermarking in sharing secret information from car number plate digital images. Int J Eng Invent [Internet]. 2021;10:1–11. Available from: www.ijeijournal.com
21. https://www.raiffeisenbank.rs/token/ [Internet]. Available from: https://www.raiffeisenbank.rs/token/
22. Islam MS. Using ECG signal as an entropy source for efficient generation of long random bit sequences. J King Saud Univ - Comput Inf Sci [Internet]. 2022; Available from: https://linkinghub.elsevier.com/retrieve/pii/S131915782200015

Vrsta rada: Originalni naučni rad
Primljen: 30. 4. 2022.
Prihvaćen: 10.10. 2022.
UDK:

Iskustva i preporuke u radu sa kriptovalutama u oblaku (cloudu)

Simo Jaković[1], Dragana Petrović [1*]

1. Visoka škola strukovnih studija za informacione tehnologije – ITS, Beograd, Srbija; simo@jakovic.com
*dragana.petrovic@its.edu.rs

Sažetak: Kriptovalute stiču neverovatnu popularnost poslednjih godina. Broj kriptovaluta je narastao od jedne valute do nekoliko hiljada, a vrtoglavo se povećao u periodu od 2021. do 2022. godine kada se broj kriptovaluta udvostručio i sada ih ima preko 12.000. Dosta kriptovaluta koje su se pojavile ima ulogu samo u pravljenju novca svojim tvorcima. Pojava kriptovaluta je dovela do promena u načinu na koji ljudi čuvaju novac, investiraju i plaćaju proizvode i usluge. Broj firmi koje podržavaju plaćanje kriptovalutama je sve veći, iako postoji otpor nekih država prema ovakvom načinu plaćanja. U radu je prikazano kako se kriptovalute mogu koristiti, na koje načine se mogu čuvati i koji načini čuvanja su trenutno mogući u oblaku. Ukratko je prikazan i opis tehnologije kojom su napravljene kriptovalute. Drugi deo treba da se osvrne na isplativost kriptovaluta i to da li je stvarno isplativo ulagati u ovaj vid „digitalnog zlata", ali i da prikaže najbolje opcije za rudarenje kriptovaluta.

Ključne reči: biznis, oblak, kriptovalute, kripto, valuta, finansije, novac, internet

1. Uvod

Kriptovalute su se pojavile zbog nezadovoljstva ljudi načinom na koji banke upravljaju novcem i želje da države ne kontrolišu valute. Računarstvo u oblaku je omogućilo razvoj i široku primenu kriptovaluta u svetu.

U radu će biti obrađen nastanak i razvoj kriptovaluta, kao i Blockchain tehnologije, biće navedeni primeri nekoliko glavnih kriptovaluta i prikazani delovi algoritama za kreiranje kriptovaluta. Zatim, deo rada prikazaće upotrebu digitalnih novčanika i kako se valute čuvaju u oblaku.

Blockchain metodologija predstavlja novu tehnologiju koja se realizuje putem lanaca blokova, pri čemu svaki blok sadrži u sebi određenu vrstu podataka. Tehnika pomoću koje se ovi blokovi vezuju u lanac blokova se naziva kriptografija i ona omogućava njihovu nepromenljivost. U slučaju da se promeni jedan blok, to utiče na to da se promeni sadržaj svih ostalih blokova. Ova metodologija se zasniva na postulatima nepromenljivosti, decentralizovanosti i transparentnosti. Nepromenljivost znači da podaci koji se jednom zabeleže na jednom bloku nikada više ne mogu da se menjaju. Decentralizovanost predstavlja skladištenje podataka kod svakog člana mreže, a ne na jednom mestu, što im omogućava da ih razmenjuju međusobno bez posrednika. Transparentnost transakcija govori u prilog tome da je vidljiva svaka realizovana transakcija između članova mreže.

U okviru ove analize korišćena je literatura iz oblasti Blockchain metodologije koja proučava tipove kriptovaluta, Blockchain aplikacije, digitalne novčanike, budućnost kriptovaluta i rudarenje kriptovaluta. Autori Banafa i Mugajar su objasnili ulogu i značaj Blockchain tehnologije u savremenom modernom svetu, a takođe su korišćeni i internet izvori kao što su Wikipedia (stranica Bitcoin) i Ripple (payment protocol). Korišćeni su podaci sa veb-stranica koje pružaju informacije o uvođenju kriptovaluta, razvoju Blockchain tehnologija i budućnosti samih kriptovaluta. Na sajtovima kao što su Wikipedia (stranica Bitcoin), Bitcoin Price i Best Cloud Mining Sites su objašnjene vrste kriptovaluta (Bitcoin, Ethereum i Ripple). Za potrebe analize čuvanja i rudarenja u oblaku su korišćene sledeće internet strane: blockchain.com-scaling and saving with cloud Spanner, learn.bybit.com/crypto/what is cloud mining i best-cloud-mining-sites-trusted.html. Autor Morkunas i saradnici su objasnili kako Blockchain tehnologija utiče na poslovanje kompanija i zaključili su da će ova tehnologija imati strateški značaj u inoviranju poslovnih modela samih kompanija.

2. Istorija kriptovaluta

Kriptovalute su se pojavile 2009. godine. Prva kriptovaluta je Bitcoin. Ova valuta je i dan-danas najpopularnija kriptovaluta u upotrebi. Ne zna se tačno ko je napravio Bitcoin, ali se spekuliše da je to bila grupa ili pojedinac pod imenom Satoši Nakamoto. Kriptovalute su rešavale probleme starih bankarskih sistema i ljudi su bili veoma uzbuđeni oko ove ideje.

Ideja o kriptovalutama datira još iz 1998, kada se shvatilo koliko banke upravljaju tokovima novca. Ljudi su želeli da se pomoću digitalnih tehnologija napravi neka vrsta „digitalnog zlata" kako bi se zaštitili od inflacije.

Bitcoin je napravljen upotrebom Blockchain technologije i postao je najpopularnija valuta među ostalim kao što su Ethereum, Dash, Litecoin i dr. Upotreba kriptovaluta je bila bezbednija jer niko nije mogao da ih kopira ili falsifikuje, čak ni sam tvorac [1].

3. Blockchain tehnologija

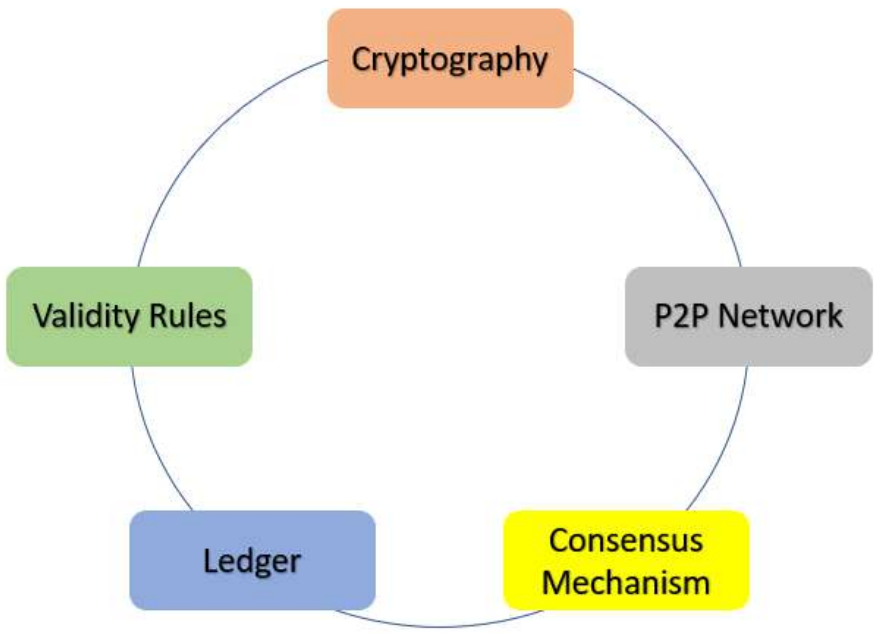
Blockchain je jednostavno softver čija je definicija: „distribuirana baza podataka koja postoji na više računara u isto vreme. Stalno raste kako mu se dodaju novi setovi snimaka ili blokova. Svaki blok sadrži vremensku oznaku ili vezu sa prethodnim blokom, tako da oni zapravo čine lanac" [2]. Postoji i druga definicija, a to je: kriptografija + ljudska logika.

3.1. Komponente Blockchaina

Blockchain je sastavljen od pet komponenti:

- kriptografija;
- P2P mreža;
- mehanizam konsenzusa;
- glavna knjiga (ledger);
- pravila važenja (validity rules).

Na slici 1 vidimo grafički prikaz komponenti Blockchaina.



Slika 1. Komponente Blockchaina [2]

Bilo koji od sledećih jezika može da se koristi za programiranje Blockchain platformi: C++ (Bitcoin), Python, JavaScript, Solidity (Smart Contract), Java and Go. Slika 2 prikazuje primer koda za kreiranje instance Blockchain bloka u programskom jeziku JavaScript.

4. Tri tipa kriptovaluta

Postoji mnogo tipova kriptovaluta. Iako su kriptovalute bazirane na sličnim principima kao i Bitcoin, svaka kriptovaluta je dizajnirana da pruži neku novu funkcionalnost. Pouzdanost je jako bitna kod kriptovaluta. Svaka kriptovaluta je dizajnirana pomoću Blockchain tehnologije i svaka valuta je šifrovana specijalnim kompjuterskim kodom [16]. Taj kod se zove kriptografija. Ovde ćemo navesti tri najpopularnije kriptovalute.

```
class Block {
        constructor(timestamp, transactions,
        previousHash = '') {
        this.previousHash = previousHash;
        this.timestamp = timestamp;
        this.transactions = transactions;
        this.hash = this.calculateHash();
        this.nonce = 0;
        }
}
```

Slika 2. Primer koda Blockchain bloka [3]

4.1. Bitcoin

Prva i najpopularnija kriptovaluta nastala je 2009. godine. Algoritam za rudarenje novčića (rešavanje matematičkih problema) zahteva više računarske snage od drugih kriptovaluta, što otežava i poskupljuje rudarenje. Ovo daje vrednost Bitcoinu i otežava stvaranje novih koji povećavaju potražnju na tržištu. Bitcoini su decentralizovani, što znači da se ne oslanjaju ni na jednu državnu centralnu banku ili upravljačko telo. Oni koriste Blockchain tehnologiju u kombinaciji sa algoritmima matematičkog softvera koji kontrolišu njegovo puštanje u opticaj, sprečavajući nagomilavanje inflatornih pritisaka usled prekomerne proizvodnje valutnih jedinica. Bitcoin nije bio samo pokretač trendova na mreži kriptovaluta izgrađenih na decentralizovanoj meri, već je postao i defakto standard za kriptovalute [4].

4.2. Ethereum

Ethereum je javni Blockchain otvorenog koda koji se može koristiti za razvoj i primenu decentralizovanih aplikacija. Vitalik Buterin je predložio Ethereum kao platformu za izvršavanje peer-to-peer pametnih ugovora – sporazuma o kodu koji se automatski izvršavaju kada se ispune određeni uslovi, a da ih ne kontroliše bilo koja banka ili centralna vlast. Značajna karakteristika ove valute je njegova podrška za „gas", zasnovana na cenama ponude, a ne potražnje, kao većina kriptovaluta: ovo osigurava da se transakcije neće zaglaviti jer nema podsticaja da se kasnije obrađuju ako su sada skupe. Ostale karakteristike uključuju skriptni jezik, tako da ljudi mogu da naprave svoje tokene, kao i kompatibilnost sa Bitcoin adresama, što znači da nije potrebna nova adresa svaki put kada pošaljete novac. Nastao je 2013. godine [5].

4.3. Ripple

Valuta koja povezuje banke, razmenu digitalnih sredstava, provajdere plaćanja i kompanije preko jedne jedinstvene infrastrukture za poravnanje kako bi pružio jedno iskustvo bez problema za slanje novca na globalnom nivou. Kompaniju su 2012. godine osnovali Kris Larsen i Džed Makejleb, koji su želeli da omoguće trenutna međunarodna plaćanja za banke bez potrebe za korespondentskom bankom. Ripple je brz i ima niske troškove transakcije (sa planovima za njihovo smanjenje). Fokusiran je na integraciju drugih provajdera u svoju mrežu kroz rebrendiranje tako da se integriše sa raličitim tehnologijama u različitim slučajevima korišćenja kao što su globalne kompanije koje gledaju na doznake, prodavci e-trgovine koji prihvataju plaćanja od potrošača u inostranstvu itd. [6].

5. Blockchain aplikacije u finansijskim uslugama

Sa unutrašnje tačke gledišta implementacije, evolucija Blockchaina u finansijskim uslugama odvijaće se u skladu sa segmentacijom glavnih oblasti aplikacija:

- proizvodi okrenuti potrošačima;
- B2B usluge;
- trgovina i tržište kapitala;
- pozadinski procesi;
- međuindustrijske posredničke usluge.

Ono što je zajedničko za svaki od gorenavedenih slučajeva je da su ove transakcije od početka do kraja na ravnopravnoj osnovi, bez centralnih posrednika. Ugovorne strane nisu morale da se poznaju ili da zahtevaju treću stranu da posreduju u transakciji. Decentralizacija i konačnost ravnopravnih transakcija su ključne inovacije Blockchaina koje se moraju sačuvati kako bi se maksimizirao potencijalni uticaj implementacije Blockchaina [17]. Identitet i reputacija drugih strana se automatski verifikuju na Blockchainu putem adresa novčanika. Postoji mnogo aplikacija u kojima će rešenje za Blockchain ili distribuiranu konsenzusnu knjigu imati smisla [2].

Najveći segmenti na koje će to uticati: obveznice, razmena, derivati, roba, hartije od vrednosti, tržišta bez recepta, upravljanje kolateralom, sindicirani krediti, magacinske priznanice i otkupno tržište.

6. Digitalni novčanici

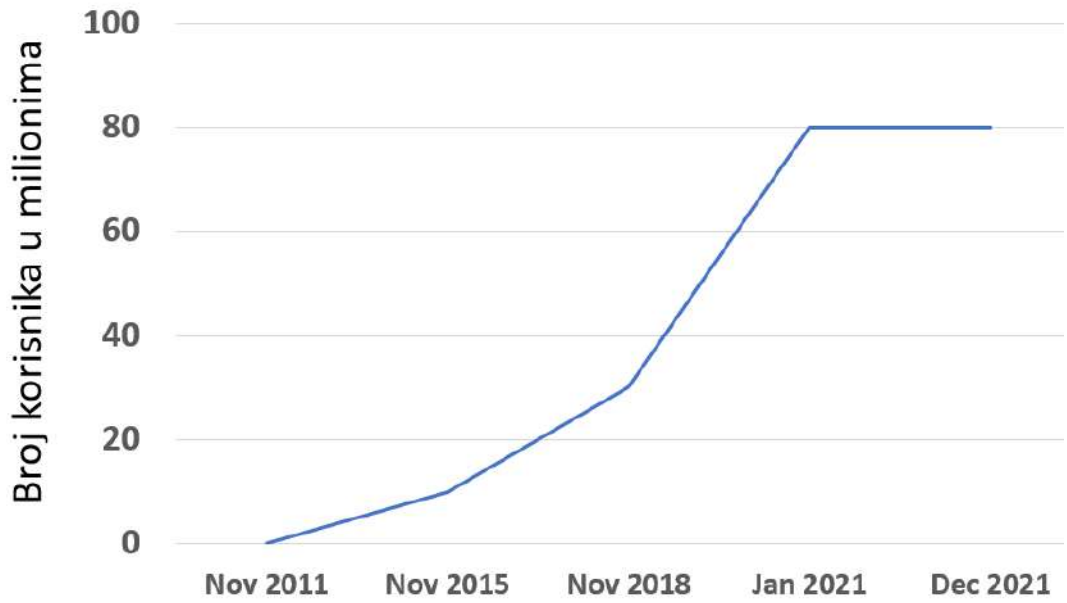
Digitalni novčanik je aplikacija ili softver zasnovan na oblaku koji bezbedno čuva podatke o plaćanju korisnika kako bi im omogućio da kupuju na mreži na različitim veb-lokacijama ili fizičkim prodavnicama bez davanja podataka o plaćanju. Da biste podesili digitalni novčanik, potrebno je da instalirate softver na svoj uređaj ili da mu pristupite preko onlajn-platforme. Funkcioniše na prilično jednostavan način. Prvo morate da instalirate softver na svoj uređaj ili da mu pristupite preko onlajn-platforme.

Zatim napravite nalog u koji dodajete svoje lične podatke, detalje o plaćanju i sve druge potrebne informacije za verifikaciju. Nakon toga, sve što vam treba je da vaša banka potvrdi vaše podatke o plaćanju i da počnete da koristite aplikaciju novčanika za plaćanje na mreži gde god želite jednim klikom ili dodirom. Kada kupujete u fizičkim prodavnicama, mobilni novčanici koriste komunikaciju bliskog polja (NFC) za dovršavanje plaćanja. Ako terminal za plaćanje trgovca ima simbol za beskontaktno plaćanje, jednostavno usmerite svoj pametni telefon blizu njega i potvrdite kupovinu skeniranjem QR koda, unosom lozinke ili dodirom na potrebno dugme [7].

Digitalni novčanici za kriptovalute funkcionišu na sličan način kao i za digitalni novac, sa jedinom razlikom što su ovi poslednji povezani sa fizičkim trezorima u kojima se čuva fizički novac, dok se novčanici kriptovalute koriste za čuvanje privatnih ključeva koji se koriste za dobijanje pristupa digitalnim novčićima snimljenim na Blockchainu u oblaku.

Privatni ključ je najvažnija stvar kada radite sa novčanicima kriptovaluta, jer bez njega korisnik neće moći da pristupi svom novcu. Za slanje ili primanje sredstava pomoću novčanika kriptovalute, osobi je potreban i javni ključ. Ovaj ključ ne dozvoljava pristup sredstvima uskladištenim u novčaniku, već se koristi kao adresa novčanika, kao što je broj kartice ili računa. Većina provajdera usluga kriptovaluta nudi funkciju dinamičkih javnih ključeva, omogućavajući njihovu promenu pre svake transakcije. Za ovu funkciju se kaže da poboljšava bezbednost novčanika, međutim, s druge strane, može čak izazvati dodatne probleme. Stvar je u tome da su transakcije snimljene na Blockchainu nepromenljive, tako da sve dok korisnik generiše novu adresu novčanika, stara postaje nevažeća. Sva sredstva koja su naknadno poslata na staru adresu su nepovratno izgubljena i za pošiljaoca i za primaoca. Iz istog razloga potrebno je biti oprezan prilikom unosa javnog ključa pre nego što se potvrdi transakcija. Ako se napravi greška, sredstva će takođe biti izgubljena [7].

Na slici 3 prikazan je rast broja korisnika digitalnih novčanika u periodu od 2011. do 2021. godine.



Slika 3. Broj digitalnih novčanika korisnika od novembra 2011. do decembra 2021. godine [8]

7. Budućnost kriptovaluta

Ekonomski analitičari predviđaju da će uslediti velika promena u kriptovalutama kako institucionalni novac ulazi na tržište. Postoji mogućnost da će kriptovalute biti plasirane na Nasdaku, što bi dodatno povećalo kredibilitet Blockchainu i njegovoj upotrebi kao alternativi konvencionalnim valutama [9]. Kripto verifikovan fond kojim se trguje na berzi definitivno bi olakšao ljudima da ulažu u Bitcoin, ali i dalje treba da postoji želja za ulaganjem u kriptovalute, što se možda neće automatski generisati sa fondom [15].

Pri ulaganju u kriptovalute trebalo bi se prema investicijama odnositi na isti način kao prema bilo kom drugom veoma špekulativnom poduhvatu. Kriptovaluta nema suštinsku vrednost osim onoga što je kupac spreman da plati za nju u određenom trenutku [18].

Kriptovalute su podložne velikim promenama cena, što povećava rizik od gubitka za investitora. U tabeli 1 možemo da vidimo cene kriptovalute Bitcoin u periodu od četiri godine. Može se primetiti da su oscilacije u promeni cene Bitcoina dosta velike za 2017. i 2018. godinu, kao i za 2020. i 2021. godinu.

Tabela 1. Cene Bitcoina u periodu od 2017. do 2021. godine [10]

Godina	*Cena (USD)*
2021	46.732,74
2020	10.764,2
2019	7.251,28
2018	3.689,56
2017	13.062,15

Analiziranjem nekoliko godina unazad primetićemo da je fluktuacija vrednosti kriptovaluta velika i to je nešto što je u kratkom periodu privuklo dosta investitora širom sveta. Iako dosta finansijskih stručnjaka predlaže kriptovalute kao stabilan vid ulaganja, umesto recimo nekretnina, akcija na berzi i dr., niko ne objašnjava i ne navodi konkretne razloge zašto bi trebalo ulagati u kriptovalute. Ono što ide u korist kriptovalutama je ROI indeks (povraćaj uloženog kapitala), koji je najveći od svih finansijskih proizvoda na tržištu. Ali ovo ne može i ne treba da bude jedini razlog za investiranje u kriptovalute. Šta ćemo sa pouzdanošću? Trenutna cena Bitcoina je oko 47.000 dolara [10], pre četiri meseca je bila oko 67.000 dolara, što nam ukazuje na veliku nestabilnost ove valute. Takođe, možemo primetiti da sve ostale valute skaču i padaju zajedno sa Bitcoinom i to nam ukazuje na povezanost ovih valuta i njihovu međuzavisnost, što opet nije dobro, jer se na taj način praktično sve valute ponašaju isto.

Ukoliko želite da rudarite, opet ćete morati da uložite veliku sumu novca u računare, da potrošite dosta električne energije pa se postavlja pitanje koliko je to isplativo. Trenutna cena struje na Balkanu je povoljna i ovo je možda jedini region povoljan za rudarenje. Takođe, sajtovi na kojima možete da trgujete uzimaju procente za svaku transakciju, pa je i to nešto o čemu morate voditi računa.

8. Čuvanje i rudarenje u oblaku

Oblak se pokazao kao pogodna platforma za čuvanje i razvoj kriptovaluta. Blockchain, korisnik Google Clouda, u početku je bio fokusiran na kreiranje alata za razumevanje i korišćenje Bitcoina, ali se kompanija od tada proširila na druge kriptovalute kao što su Ethereum, Bitcoin Cash, Stellar Lumens i Pakos Standard. Sada se milioni pojedinaca oslanjaju na Blockchain novčanik da bi obezbedili i koristili vodeće svetske kriptovalute. Nepotrebno je reći da sa veličinom i geografskim širenjem baze korisnika upravljanje ovim skupovima podataka nije lak podvig i bez oblaka teško da bi bio ostvariv [11].

Od osnivanja kompanije, Blockchain je koristio Google Cloud Platform (GCP), dodajući usluge svuda gde je tim video mogućnosti da zadovolji svoje potrebe u razvoju. Dok Blockchain održava neke od sopstvenih hardverskih i data centara, želeo je da razvije svoj pristup upravljanju infrastrukturom kako bi poboljšao bezbednost, pouzdanost i tačnost informacionih platformi [11].

Blockchainovi vodeći proizvodi, Blockchain Wallet i Blockchain Explorer, zahtevaju komplikovane proračune teško dostupnih podataka u masivnim, decentralizovanim knjigama koje podržavaju mreže kriptovaluta. Pristup tim podacima zahteva kompleksno znanje o domenu, tehničku infrastrukturu i razvojni napor, a da ne pominjemo vreme za obradu celog lanca podataka. Ovo je postao veliki poduhvat koji je zahtevao značajne interne IT resurse i režijske troškove [11].

Da bi upravljao ovim izazovima i poboljšao korisničko iskustvo na svim proizvodima i platformama, Blockchain je počeo da pokreće infrastrukturu na Compute Engine instancama. Blockchain je takođe odabrao Cloud Spanner kao svoju uslugu baze podataka po izboru, jer ovaj server baze podataka može brzo da se skalira (bez zastoja) i da obezbedi visoku dostupnost sa malim operativnim troškovima. Cloud SKL, Stackdriver i proizvodi za upravljanje identitetom takođe čine Blockchainovu infrastrukturu oblaka [11].

8.1. Rudarenje u oblaku

Rudarenje u oblaku je proces rudarenja kriptovaluta koji koristi udaljeni centar podataka sa zajedničkom procesorskom snagom. Rudarstvo u oblaku pomaže korisnicima da rudare Bitcoine ili druge kriptovalute bez potrebe da koriste sopstveni hardver. Rudarske platforme su smeštene u objektu u vlasništvu rudarske kompanije. Korisnik treba da se registruje i kupi ugovore o rudarenju da bi pokrenuo proces rudarenja u oblaku. To je proces generisanja kriptovaluta korišćenjem iznajmljene računarske snage od treće strane (provajder usluga rudarenja u oblaku). Svaki rudar zapravo učestvuje u „rudarskoj farmi" (udaljenom centru podataka posvećenom kriptorudarstvu) kupovinom određene količine „heš snage" od dobavljača usluga [14]. U zamenu, provajder će im odobriti pristup nagradama koje su proporcionalne količini heš snage rudara koju su kupili. Pošto se rudarenje obavlja preko oblaka, rudari ne moraju da brinu o održavanju računarske opreme, buci, toploti ili računima za energiju. Nakon što pronađu pouzdanog dobavljača usluga rudarenja u oblaku, rudari samo treba da odaberu vrstu ugovora za potpisivanje i željeno trajanje. Moraće da uplate unapred, bilo u Fiat valutama ili digitalnim valutama, nakon čega će im provajder postaviti sve što im je potrebno za operaciju [12].

8.2. Kako funkcioniše rudarenje u oblaku

Postoje dva tipa modela rudarenja u oblaku: host rudarenje i iznajmljivanje heš snage.

Kod host rudarenja rudari kupuju ili iznajmljuju rudarske platforme na rudarskim farmama i plaćaju njihovo postavljanje i održavanje. Ovaj model smanjuje troškove povezane s pristupom električnoj energiji. Osim toga, budući da rudari imaju veću kontrolu nad rigovima, mogu preusmeriti generisanu moć heširanja na rudarske bazene. Osim toga, rudari imaju potpunu kontrolu nad generisanim nagradama [12].

Iznajmljivanje heš snage je sistem u kome rudari uzimaju u zakup deo heš snage koju generiše rudarska farma. Oni su u suštini pretplaćeni na plan koji nudi kompanija za rudarenje u oblaku da dobiju udeo u profitu rudarske farme. Rudari ne moraju plaćati nikakve naknade za postavljanje ili održavanje, a nagrade za rudarenje se raspodeljuju u zavisnosti od udela heš moći koju svaki rudar kontroliše [12].

U tabeli 2 je prikazana ručno odabrana lista najboljih kompanija za rudarenje u oblaku sa njihovim popularnim funkcijama i vezama do veb-lokacija. Lista sadrži i softver otvorenog koda (besplatan) i komercijalni (plaćen) softver.

Tabela 2. Sajtovi za rudarenje kriptovaluta [13]

Naziv	*Godina osnivanja*	*Podržane kriptovalute*
ECOS	2017	Bitcoin, Ethereum, Ripple, Bitcoin Cash, Tether, Litecoin
ChickenFast	2015	Bitcoin, Ethereum and Bitcoin Cash
Trustcloudmining	2017	Bitcoin, Ethereum, Zen and more
BeMine	2018	Bitcoin, Ethereum, Zcash
Shamining	2018	Bitcoin
Freemining	2014	Bitcoin, Litecoin, Dogecoin, BCH, XMR i TRX

8. Zaključak

U ovom radu smo istražili kriptovalute i objasnili kako one rade u računarstvu u oblaku. Došli smo do zaključka da bez računarstva u oblaku kriptovalute ne bi ni postojale i da je on osnova za dalji razvoj kriptovaluta. Uočili smo da je tržište kriptovaluta još uvek nestabilno i da ne možemo sa sigurnošću da predvidimo ponašanje kriptovaluta i očekivanu dobit. Još uvek mnoge države ne podržavaju kriptovalute, a neke ih čak i zabranjuju (Kina) i time onemogućavaju ulazak ovih valuta u regularne tokove. Sve dok kriptovalute nemaju neku realnu vrednost, teško je govoriti o budućnosti. Takođe, imperativ je stvaranje kriptofonda koji bi olakšao trgovanje kriptovalutama.

Dalji izazov je usavršavanje računarstva u oblaku i poboljšanje bezbednosti, jer sa razvojem kriptovaluta dolazi do izmeštanja finansijskih transakcija na onlajn-platforme, sa čime dolazi i do povećanja sajbernapada na račune korisnika koji svoje podatke čuvaju na oblaku. Bezbednost internet pretraživača predstavlja jedan od osnovnih vidova zaštite prilikom vršenja transakcija kriptovalutama. Treba koristiti pretraživače koji imaju poboljšane bezbednosne funkcije.

Blockchain tehnologija predstavlja novu tehnologiju koja se sastoji iz lanca nepromenljivih blokova i ova tehnologija će tek dati svoj pečat u 21. veku. Značaj ove tehnologije je u tome što se ona može primeniti u svim sferama života (finansije, industrija, nekretnine, zdravstvo itd.). Najpoznatije kriptovalute su Bitcoin, Ethereum i Ripple. Njihova trgovina postaje sve intenzivnija i zbog toga one predstavljaju platežno sredstvo budućnosti. Međutim, treba biti oprezan prilikom korišćenja kriptovaluta, jer su ove valute zbog velikih oscilacija nestabilne i predstavljaju rizične investicije. Digitalni novčanik kriptovaluta obezbeđuje da ove valute uvek budu bezbedne, jer se one čuvaju pomoću digitalnih lozinki koje su ljudima uvek nadohvat ruke. Prilično su jednostavni za korišćenje, ali najbitnije od svega je da se sačuvaju privatni ključevi pomoću kojih se pristupa digitalnim novčićima koji su snimljeni na Blockchainu u oblaku.

Na kraju, neizvesna je budućnost kriptovaluta na svetskim finansijskim tržištima, jer njih ne reguliše centralna banka jedne države ili neka druga finansijska institucija i iz tog razloga su ove valute decentralizovane. Zbog toga su one podložne sistemskim rizicima, pa je njihova vrednost varijabilna (oscilirajuća) u kratkim vremenskim periodima. Međutim, države će nastojati da pronađu načine njihove regulacije u oblaku. Može se zaključiti da će ove valute zajedno sa Blockchain tehnologijom u budućnosti i dalje predstavljati izazov kao sredstvo plaćanja i realizacije finansijskih transakcija na svetskom tržištu, a vreme će pokazati da li će u potpunosti zameniti tradicionalne valute.

Reference

1. Frank. Cryptocurrency History. Online Wealth Chronicles. [Internet]. 2021 December 24. Available from: https://onlinewealthchronicles.com/when-why-did-cryptocurrency-start
2. Banafa A, Blockchain Technology and Applications. River Publishers; 2020
3. Mougayar W, The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. 1st Edition. Wiley; 2016
4. Bitcoin. Wikipedia. [Internet]. 2022 February 15. Available from: https://en.wikipedia.org/wiki/Bitcoin
5. Ripple (payment protocol). Wikipedia. [Internet]. 2022 March 15. Available from: https://en.wikipedia.org/wiki/Ripple_(payment_protocol)
6. Ethereum. Wikipedia. [Internet]. 2022 March 20. Available from: https://en.wikipedia.org/wiki/Ethereum
7. Jules. Digital Wallets. Easyship. [Internet]. 2021 December 27ZZZ. Available from: https://www.easyship.com/blog/digital-wallets-guide
8. Number of Bitcoin block explorer Blockchain.com wallet users worldwide from November 2011 to March 27, 2022. Statista. [Internet]. 2021 December 29. Available from: https://www.statista.com/statistics/647374/worldwide-blockchain-wallet-users
9. Daily Stock Market Overview, Data Updates, Reports & News. Nasdaq market. [Internet]. 2021 December 29. Available from: https://www.nasdaq.com
10. Bitcoin Price | BTC Price Index and Live Chart. Coindesk. [Internet]. 2022 March 28. Available from: https://www.coindesk.com/price/bitcoin/
11. Poole A, Srivastava D, Blockchain.com, scaling and saving with Cloud Spanner. Google Cloud. [Internet]. 2022 January 04. Available from: https://cloud.google.com/blog/products/databases/blockchain-scaling-and-saving-with-cloud-spanner
12. What Is Cloud Mining and How Does it Work?. Bybit Learn. [Internet]. 2022 January 10. Available from: https://learn.bybit.com/crypto/what-is-cloud-mining
13. Thompson B. 10 BEST Cloud Mining Sites (Bitcoin, Ethereum Mining). Guru99. [Internet]. 2022 January 05. Available from: https://www.guru99.com/best-cloud-mining-sites-trusted.html
14. Montecchi M, Plangger K, Etter M, It`s real, trust me! Establishing supply chain provenance using blockchain, Business Horizons, Volume 62, Issue 3, 2019, pp. 283-293.
15. Morkunas JV, Paschen J, Boon A, How blockchain tehnologies impact your business model, Business Horizons, Volume 62, Issue 3, 2019, pp. 296-306
16. Casey JM, Vigna P, The truth Machine: The Blockchain And The Future of Everything, Book Depot Inc, 2019
17. Tapscott D, Lansiti M, Lakhani RM, Tucker C, Blockchain: The Insight You Need from Harvard Business Review (HBR Insights), Kindle Edition, Boston, Massachusetts, 2019
18. Jović Z, Kunjadić G, Monetary and Technological Aspects of the Emergence and the Development of Cryptocurrencies, FINIZ -The Role of Financial and Non-Financial Reporting in Responsible Business Operation, Singidunum University International Scientific Conference, Belgrade, 2018, pp. 63-67.

Type of paper: Original scientific paper
Received: 30. 4. 2022
Accepted: 10.10. 2022.
DOI: https://doi.org/10.18485/edtech.2022.2.2.3
UDC:

Experiences and Recommendations regarding Cloud Cryptocurrencies

Simo Jaković[1], Dragana Petrović [1*]

1. Information Technology School – ITS, Belgrade, Serbia; simo@jakovic.com
*dragana.petrovic@imefedu.rs

Summary: Cryptocurrencies have been gaining incredible popularity in recent years. Their number has grown from a single cryptocurrency to several thousand, and the peak was reached in the period between 2021 and 2022 when the number of cryptocurrencies doubled to over 12,000. Many cryptocurrencies exist only to make money for their creators. The emergence of cryptocurrencies has changed the way in which people store money, invest, and pay for products and services. The number of companies that support payments in cryptocurrency is increasing, although there is still resistance from some countries to this method of payment. The paper explains how cryptocurrencies can be used, stored, and what cloud storage methods are currently available. It also provides a brief description of technologies that are used to create cryptocurrencies. The second part provides an overview of the profitability of cryptocurrencies, explains whether it is actually profitable to invest in this form of "digital gold", and presents the best options for mining cryptocurrencies.

Keywords: business, cloud, cryptocurrencies, currency, finance, money, Internet

1. Introduction

Cryptocurrencies emerged due to people's dissatisfaction with the way banks managed their money, and governments' desire to control currencies. Cloud computing has enabled the development and widespread use of cryptocurrencies around the world.

The paper will discuss the origin and development of cryptocurrencies, as well as Blockchain technology, providing examples of several major cryptocurrencies, and parts of the algorithm used for creating them. A part of the paper will be dedicated to digital wallets, and ways to store currencies in the cloud.

Blockchain methodology represents a new technology implemented through chains of data, or blockchains, whereby each block contains a certain type of data. The technology by which these blocks are connected into a chain is called cryptography, and it ensures their immutability. If one block is modified, the content of all other blocks in the chain will be modified as well. This methodology is based on the principles of immutability, decentralisation, and transparency. Immutability means that once the data are recorded on a block, they can never be modified again. Decentralisation means that data is stored on each member of the network/chain, instead in a single place, which allows their exchange and sharing without intermediaries. The transparency of transactions means that every realised transaction between network members will be visible.

For the purposes of our analysis, literature in the field of Blockchain methodology that studies types of cryptocurrencies, Blockchain applications, digital wallets, the future of cryptocurrencies, and their mining was used. Banafa and Mougayar explained the role and importance of Blockchain technology in the modern world. Internet sources, such as Wikipedia (page about Bitcoin) and Ripple (payment protocol) were also used. We used data from websites that provide information about cryptocurrencies, the development of Blockchain technology, and the future of cryptocurrencies. Websites Wikipedia (page about Bitcoin), Bitcoin Price and Best Cloud Mining Sites explain the types of cryptocurrencies (Bitcoin, Ethereum and Ripple). The following websites were used as a source of information for the analysis of cloud storage and mining: blockchain.com-scaling and saving with cloud Spanner, learn.bybit.com/crypto/what is cloud mining and best-cloud-mining-sites-trusted.html. Morkunas et al. explained how Blockchain technology affects corporate business and concluded that this technology will have strategic importance in the innovation of corporate business models.

2. History of cryptocurrencies

Cryptocurrencies first appeared in 2009, and the first one was Bitcoin. Bitcoin is still the most popular and widely used cryptocurrency.

It is unknown who exactly created Bitcoin, but it is speculated that it was a group of people or one Satoshi Nakamoto. Cryptocurrencies addressed the problem of outdated banking systems and created quite a buzz among people.

The original idea of cryptocurrency can be traced back to 1998 when it was discovered to what extent banks actually control money flows. People wanted to use digital technologies to create a kind of "digital gold" so as to get some sort of protection against inflation.

Bitcoin was created using Blockchain technology and became the most popular cryptocurrency. Other popular cryptocurrencies include Ethereum, Dash, Litecoin, and others. The use of cryptocurrencies was safer because no one could copy or counterfeit them, not even their creator [1].

3. Blockchain technology

Blockchain is simply software which is defined as follows: "a distributed database that exists on multiple computers at the same time. It is constantly growing, as new sets of records or blocks are added to it. Each block contains a timestamp, or link to the previous block so that they actually form a chain" [2]. There is another definition that reads: cryptography + human logic.

3.1. Blockchain components

Blockchain comprises five components:

- Cryptography;
- P2P network;
- Consensus mechanism;
- Ledger;
- Validity rules.

Blockchain components are shown in Figure 1.

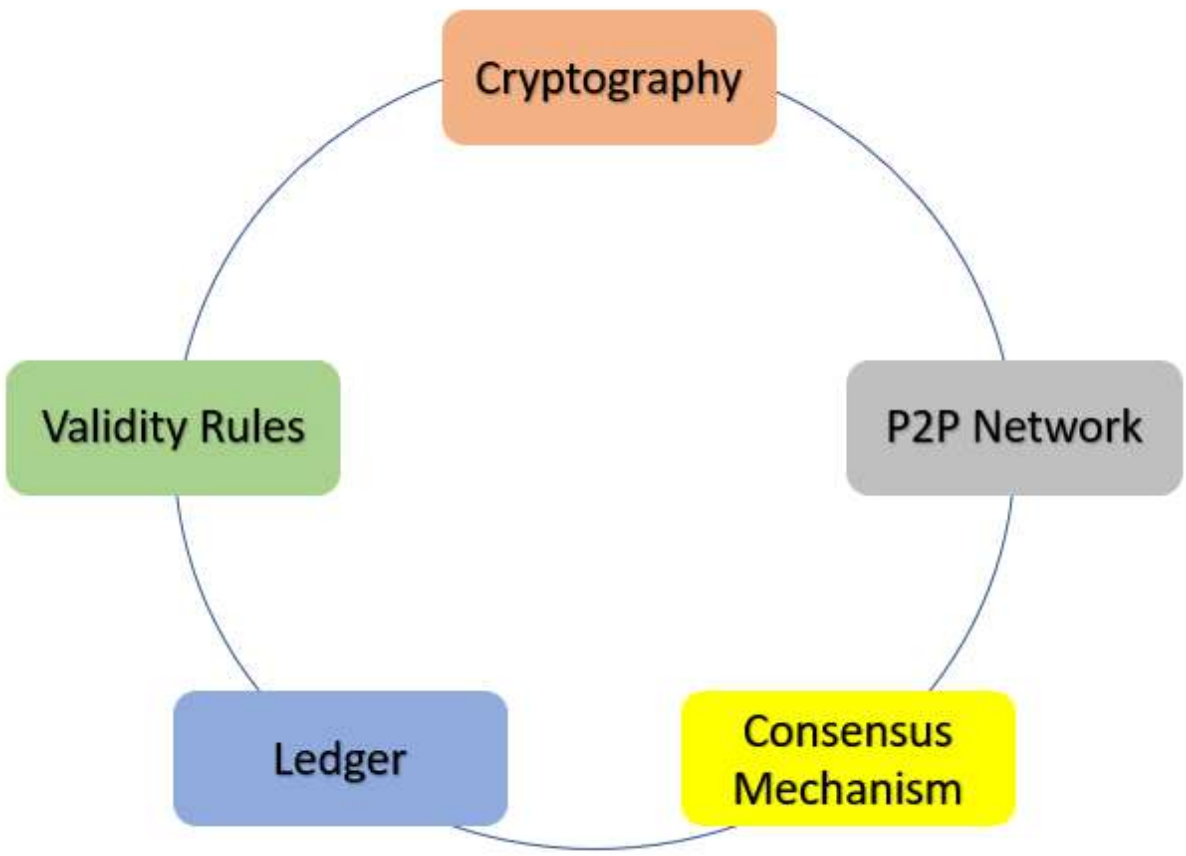


Figure 1. Blockchain components [2]

Any of the following languages can be used for programming Blockchain platforms: C++ (Bitcoin), Python, JavaScript, Solidity (Smart Contract), Java and Go. Figure 2 shows a sample of code used for creating an instance of Blockchain block in JavaScript.

4. Three types of cryptocurrency

There are many types of cryptocurrencies, and although all of them are based on similar principles as Bitcoin, each cryptocurrency is designed to provide some unique functionality. Reliability is crucial for cryptocurrencies.

Each cryptocurrency is designed using Blockchain technology, and each is encrypted using a special computer code [16]. This code is known as cryptography. The three most popular cryptocurrencies will be described in more detail below.

```
class Block {
        constructor(timestamp, transactions,
        previousHash = '') {
        this.previousHash = previousHash;
        this.timestamp = timestamp;
        this.transactions = transactions;
        this.hash = this.calculateHash();
        this.nonce = 0;
        }
}
```

Figure 2. Example of Blockchain block code [3]

4.1. Bitcoin

The first and most popular cryptocurrency was created in 2009. The algorithm for mining bitcoin (solving mathematical problems) requires more computational power than others, which makes mining more difficult and expensive. This gives value to Bitcoin and makes it more difficult to create others, which increases market demand. Bitcoins are decentralised, meaning that they do not rely on any central bank or governing body. Bitcoin uses Blockchain technology in combination with mathematical software algorithms that control its circulation, preventing the build-up of inflationary pressure due to the overproduction of units of currency. Bitcoin does not only launch trends in the cryptocurrency network built on the principle of decentralisation but has also become the de facto cryptocurrency standard [4].

4.2. Ethereum

Ethereum is a public, open-code Blockchain that can be used to develop and deploy decentralised applications. Vitalik Buterin proposed Ethereum as a platform for executing peer-to-peer smart contracts – code agreements that execute automatically when certain conditions are met, without being controlled by any central bank or national government. A notable feature of this currency is its support for "gas" based on the bid, instead of asking prices, like most other cryptocurrencies. This ensures that transactions will not get stuck because there is no incentive to process them later if they are expensive now. Other features of Ethereum include a scripting language that allows people to create their own tokens, as well as compatibility with Bitcoin addresses, which means that it is not necessary to add a new address every time money is sent. Ethereum was created in 2013 [5].

4.3. Ripple

A currency that connects banks, digital asset exchange, payment providers and companies through a unique settlement infrastructure to ensure a seamless experience for sending money globally. The company was founded in 2012 by Chris Larsen and Jed McCaleb who wanted to enable instant international payments for banks without the need for a correspondent bank. Ripple is fast and has low transaction costs (with plans to reduce them further). It is focused on integrating other providers into its network through rebranding, so that it integrates with different technologies in different use cases, such as global companies looking at transfers/payments, e-commerce sellers accepting payments from overseas consumers, etc. [6]

5. Blockchain applications in financial services

From an internal point of view of implementation, the evolution of Blockchain in the sector of financial services will take place in line with the segmentation of the main areas of application:

» consumer-oriented products;
» B2B services;
» trade and capital market;
» background processes;
» intermediary services across industries.

What is common for all cases listed above is that these transactions are on a peer-to-peer basis from start to finish, without central intermediaries.

The contracting parties do not have to know each other or require a third party to mediate the transaction. Decentralisation and finality of peer-to-peer transactions are the key innovations of Blockchain that must be preserved in order to maximise the potential effect of Blockchain implementation [17]. The identity and reputation of other parties are automatically verified on the Blockchain via wallet addresses.

There are numerous applications where Blockchain or distributed consensus ledger solutions will make much sense [2].

The biggest segments that will be affected are bonds, exchange, derivatives, commodities, securities, over-the-counter markets, collateral management, syndicated loans, warehouse receipts, and the repo market.

6. Digital wallets

A digital wallet is a cloud-based software or application that safely stores a user's payment information to allow them to buy online on different websites, or in physical stores without having to provide payment information. The procedure is fairly simple. To set up a digital wallet, you first need to install software on your device or access it through an online platform. Then, you need to create an account where you will add personal information, payment details, or any other necessary verification information. In the next step, your bank needs to confirm your payment details, and you can start using the wallet app to pay online wherever you want with a simple click or a tap. When shopping in physical stores, mobile wallets use near-field communication (NFC) to complete the payment. If the merchant's payment terminal has a contactless payment symbol, you can simply point your smartphone toward it and confirm the purchase by scanning the QR code, entering a password, or pressing the required button [7].

Cryptocurrency wallets work in a similar way as those designed for digital money, except that the latter are linked to physical vaults where physical money is stored, while cryptocurrency wallets are used for storing private keys used to gain access to digital coins stored on cloud Blockchain.

The private key is the most important thing when working with cryptocurrency wallets because without it, the user will not be able to access their money. In order to send or receive funds using a cryptocurrency wallet, one also needs a public key. This key does not allow access to the funds stored in the wallet but is used as a wallet address, such as a card or account number. Most cryptocurrency service providers offer the option of dynamic public keys, allowing their change before each transaction. This function is said to improve the security of the wallet, but on the other hand, it can also create additional problems. The point is that transactions recorded on Blockchain are immutable so that as long as the user generates a new wallet address, the old one becomes invalid. All funds subsequently sent to the old address are irretrievably lost both for the sender and the recipient. For this reason, one must be careful when entering a public key, before confirming the transaction. If a mistake is made, the funds will be lost [7].

Figure 3 shows the growth of the number of digital wallet users between 2011 and 2021.

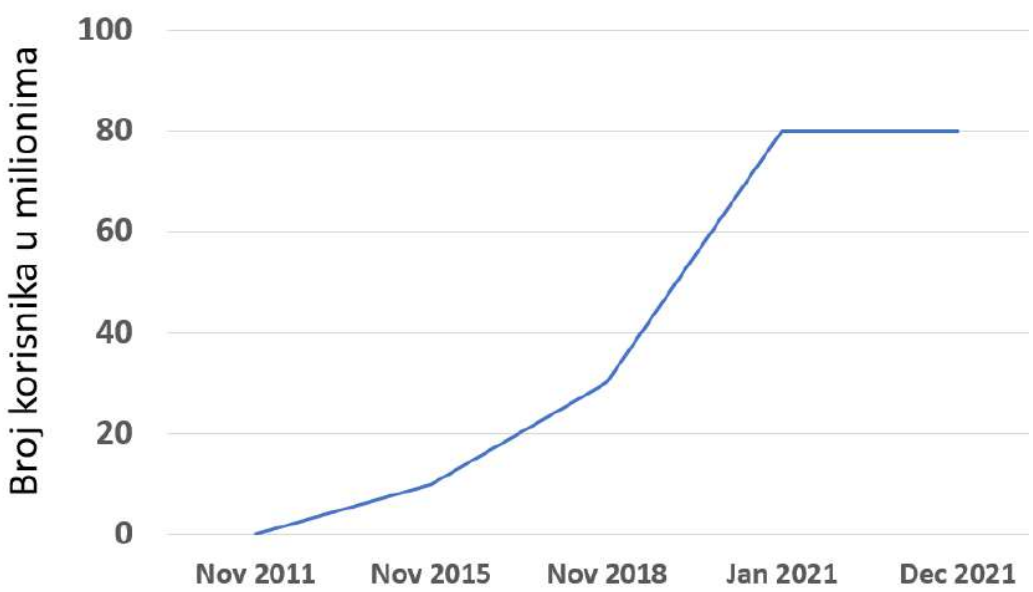


Figure 3. The number of digital wallet users between November 2011 and December 2021 [8]

7. The future of cryptocurrencies

Economic analysts are predicting a major shift in cryptocurrencies as institutional money enters the market. There is a possibility that cryptocurrencies will be listed on the Nasdaq, which would further increase the credibility of Blockchain and its application as an alternative to conventional currency [9]. A crypto-verified exchange-traded fund would definitely make it easier to invest in Bitcoin, but there still needs to be a desire to invest in cryptocurrency, which may not be automatically generated with the fund [15].

Investing in cryptocurrencies should be treated in the same way as any other highly speculative venture. Cryptocurrencies have no intrinsic value other than what the buyer is willing to pay for them at a given time [18].

Cryptocurrencies are subject to large price swings, which increases the risk of loss for investors. Table 1 shows the prices of Bitcoin over the period of four years. You can see that the fluctuations in the price of Bitcoin are quite large for 2017 and 2018, as well as 2020 and 2021.

Table 1. Bitcoin prices in the period between 2017 and 2021 [10]

Year	*Price (USD)*
	46.732,74
2020	10.764,2
2019	7.251,28
2018	3.689,56
2017	13.062,15

Analysing a few years back, we can see that the fluctuations in the value of cryptocurrencies are large, and this is something that has attracted a lot of investors around the world in a very short period. Although many financial experts recommend cryptocurrencies as a safe investment, instead of, say, real estate, stock market shares, or others, no one gives specific reasons or explains why one should invest in cryptocurrency. The thing that supports the claim about cryptocurrencies being a low-risk investment is the ROI (return on investment) index, which is the highest for all financial products on the market. But, it cannot and should not be the only reason for investing in cryptocurrencies. What about reliability? The current price of Bitcoin is around 47,000 USD [10], but, four months ago, it was 67,000, which indicates the high volatility of this currency. In addition, it is observable that all other currencies increase and decrease together with Bitcoin which indicates their connection and interdependence. This is not good either, because it means that more or less all currencies behave in the same way.

If you want to mine them, you will again have to invest a lot of money into computers and consume a lot of electricity, so the question is – how cost-effective it is. The current price of electricity in the Balkan region is affordable, so this may be the only region in the world suitable for cryptocurrency mining. In addition, websites where you can trade in cryptocurrency charge a fee for each transaction, so this is something that one must be aware of as well.

8. Cloud storage and mining

The cloud has proven to be a suitable platform for storing and developing cryptocurrency. Blockchain, a Google Cloud user, was initially focused on creating tools to help users understand and use Bitcoin, but the company has since expanded to other cryptocurrencies, such as Ethereum, Bitcoin Cash, Stellar Lumens and Pakos Standard. Now, millions of individuals rely on the Blockchain wallet to secure and use the world's leading cryptocurrencies. Needless to say, with the growing size and geographical expansion of the user base, managing these datasets is not an easy feat, and would not be feasible without the cloud [11].

Since the company's inception, Blockchain has used the Google Cloud Platform (GCP), adding services wherever the team saw opportunities to meet their evolving needs. While Blockchain maintains some of its own hardware and data centres, the company also wanted to develop its own approach to infrastructure management so as to improve the security, reliability and accuracy of information platforms [11].

Blockchain's flagship products, Blockchain Wallet and Blockchain Explorer require complex calculations of hard-to-find data in massive, decentralised ledgers that support cryptocurrency networks. Accessing these data requires complex domain knowledge, technical infrastructure, and development effort, not to mention the time needed to process entire data chains. This became a major venture that required significant internal IT resources and overheads [11].

To manage these challenges and improve the user experience across all products and platforms, Blockchain has started running infrastructure on Compute Engine instances. Blockchain also chose Cloud Spanner as its database service of choice, because this database server can scale quickly (without hitches and delay) and provide high accessibility with low operational costs. Cloud SKL, Stackdriver and identity management products are also part of the Blockchain cloud infrastructure [11].

8.1. Cloud mining

Cloud mining is a process of cryptocurrency mining that uses a remote data centre with shared processing power. Cloud mining helps users to mine Bitcoin or other cryptocurrencies without having to use their own hardware. Mining platforms are housed in a facility owned by the mining company. The user needs to register and purchase mining contracts to start the cloud mining process. It is the process of generating cryptocurrencies using leased computational power from a third party (cloud mining service provider). Each miner actually participates in a "mining farm" (remote data centre dedicated to crypto mining) by purchasing a certain amount of "hash power" from the service provider [14]. In return, the provider will grant them access to rewards that are proportional to the amount of miner hash power they purchased. Since mining is done in the cloud, miners do not have to worry about computer equipment maintenance, noise, heat, or electricity bills. After finding a reliable cloud mining service provider, miners need only to select the type of contract to sign and the desired duration. They will have to pay upfront, either in Fiat currencies or digital currencies, after which, the provider will set up everything they need for the operation [12].

8.2. How cloud mining works

There are two types of cloud mining: host mining and hash power rental.

In host mining, miners rent or purchase mining rigs on mining farms, and pay for their setup and maintenance. This model reduces costs associated with access to electricity. In addition, since miners have more control over the rigs, they can redirect the generated hashing power to mining pools. Moreover, miners have full control over the rewards generated [12].

Hash power rental is a system in which miners lease a portion of the hash power generated by the mining farm. They essentially subscribe to a plan offered by the cloud mining company and get a share of the mining farm's profits. Miners do not have to pay for any setup or maintenance fees, and mining rewards are distributed according to the share in the hash power controlled by each miner [12].

Table 2 shows a hand-picked list of the best cloud mining companies, their popular features and website links. The list also includes open-source (free) and commercial (paid) software.

Table 2. Cryptomining websites [13]

Name	*Year of establishment*	*Supported cryptocurrencies*
ECOS	2017	Bitcoin, Ethereum, Ripple, Bitcoin Cash, Tether, Litecoin
ChickenFast	2015	Bitcoin, Ethereum and Bitcoin Cash
Trustcloudmining	2017	Bitcoin, Ethereum, Zen and more
BeMine	2018	Bitcoin, Ethereum, Zcash
Shamining	2018	Bitcoin
Freemining	2014	Bitcoin, Litecoin, Dogecoin, BCH, XMR i TRX

8. Conclusion

In this paper, we explored cryptocurrencies and explained how they operate in cloud computing. We came to the conclusion that without cloud computing, there would be no cryptocurrencies, and that it is the basis for the further development of cryptocurrencies. We have observed that the cryptocurrency market is still volatile and that the behaviour and expected profits cannot be predicted with any certainty. Many countries still do not support cryptocurrencies, and some even ban them (e.g. China), thus preventing the entry of these currencies into legal market flows. As long as cryptocurrencies do not have an intrinsic value, it is difficult to talk about their future. Also, it is imperative to create a crypto fund that would facilitate cryptocurrency trading.

Improving cloud computing and security remains a challenge because, with the development of cryptocurrencies, financial transactions are moved to online platforms, which increases the risk of cyber attacks on the accounts of users who store their data in the cloud. The security of Internet browsers is one of the basic forms of protection when conducting cryptocurrency transactions. Browsers with enhanced security features should be used.

Blockchain technology is a new technology consisting of a chain of immutable blocks, and it is yet to find its rightful place in the 21st century. The importance of this technology lies in the fact that it is applicable in all areas of life (finance, industry, real estate, healthcare, etc.). The most popular cryptocurrencies are Bitcoin, Ethereum and Ripple. Cryptocurrency trading is gaining in intensity, which is why cryptocurrency will become the means of payment in the future. However, one should be careful when using cryptocurrencies, because they are volatile due to large fluctuations, and still represent a high-risk investment. A digital cryptocurrency wallet ensures that cryptocurrencies are always safe, as they are stored using digital passwords that are always within the user's reach. They are quite easy to use, but the most important thing is to store one's private keys that are used to access digital coins stored in the Blockchain cloud.

In conclusion, the future of cryptocurrencies in the world's financial markets is uncertain, because they are not regulated by central banks or other financial institutions. Due to their decentralisation, cryptocurrencies are subject to systemic risks, so their value can fluctuate quite a lot in short periods. However, countries will continue to seek ways to regulate cloud cryptocurrencies. It can be argued that these currencies, together with Blockchain technology will continue to pose a challenge as a means of payment, and realisation of financial transactions in the global market, and time can only tell whether they will completely replace traditional currency or not.

References

1. Frank. Cryptocurrency History. Online Wealth Chronicles. [Internet]. 2021 December 24. Available from: https://onlinewealthchronicles.com/when-why-did-cryptocurrency-start
2. Banafa A, Blockchain Technology and Applications. River Publishers; 2020
3. Mougayar W, The Business Blockchain: Promise, Practise, and Application of the Next Internet Technology. 1st Edition. Wiley; 2016
4. Bitcoin. Wikipedia. [Internet]. 2022 February 15. Available from: https://en.wikipedia.org/wiki/Bitcoin
5. Ripple (payment protocol). Wikipedia. [Internet]. 2022 March 15. Available from: https://en.wikipedia.org/wiki/Ripple_(payment_protocol)
6. Ethereum. Wikipedia. [Internet]. 2022 March 20. Available from: https://en.wikipedia.org/wiki/Ethereum
7. Jules. Digital Wallets. Easyship. [Internet]. 2021 December 27. Available from: https://www.easyship.com/blog/digital-wallets-guide
8. Number of Bitcoin block explorer Blockchain.com wallet users worldwide from November 2011 to March 27, 2022. Statista. [Internet]. 2021 December 29. Available from: https://www.statista.com/statistics/647374/worldwide-blockchain-wallet-users
9. Daily Stock Market Overview, Data Updates, Reports & News. Nasdaq market. [Internet]. 2021 December 29. Available from: https://www.nasdaq.com
10. Bitcoin Price | BTC Price Index and Live Chart. Coindesk. [Internet]. 2022 March 28. Available from: https://www.coindesk.com/price/bitcoin/
11. Poole A, Srivastava D, Blockchain.com, scaling and saving with Cloud Spanner. Google Cloud. [Internet]. 2022 January 04. Available from: https://cloud.google.com/blog/products/databases/blockchain-scaling-and-saving-with-cloud-spanner
12. What Is Cloud Mining and How Does it Work? Bybit Learn. [Internet]. 2022 January 10. Available from: https://learn.bybit.com/crypto/what-is-cloud-mining
13. Thompson B. 10 BEST Cloud Mining Sites (Bitcoin, Ethereum Mining). Guru99. [Internet]. 2022 January 05. Available from: https://www.guru99.com/best-cloud-mining-sites-trusted.html
14. Montecchi M, Plangger K, Etter M, It`s real, trust me! Establishing supply chain provenance using blockchain, Business Horizons, Volume 62, Issue 3, 2019, pp. 283-293.
15. Morkunas JV, Paschen J, Boon A, How blockchain technologies impact your business model, Business Horizons, Volume 62, Issue 3, 2019, pp. 296-306
16. Casey JM, Vigna P, The Truth Machine: The Blockchain And The Future of Everything, Book Depot Inc, 2019
17. Tapscott D, Lansiti M, Lakhani RM, Tucker C, Blockchain: The Insight You Need from Harvard Business Review (HBR Insights), Kindle Edition, Boston, Massachusetts, 2019
18. Jović Z, Kunjadić G, Monetary and Technological Aspects of the Emergence and the Development of Cryptocurrencies, FINIZ -The Role of Financial and Non-Financial Reporting in Responsible Business Operation, Singidunum University International Scientific Conference, Belgrade, 2018, pp. 63-67.

Vrsta rada: Originalni naučni rad
Primljen: 1. 5. 2022.
Prihvaćen: 1. 6. 2022.
UDK:

Roboti u future-ready školi. Studija slučaja: Robot Pepper u Savremenoj osnovnoj školi

Prof. dr Valentin Kuleto[1], Doc. dr Milena Ilić [1*], Maja Babić [2] ,Zorana Bodiroga [3] and Andrijana Mladenović[1]

[1]Visoka škola strukovnih studija za informacione tehnologije, ITS - Beograd, Srbija; valentin.kuleto@its.edu.rs
[2]Osnovna škola "Savremena", Beograd, Srbija; maja.babic@savremena-osnovna.edu.rs
[3]International School, Beograd, Srbija; zorana.bodiroga@link.co.rs
*Kontakt informacije: milena.ilic@fsu.edu.rs; Tel 381(0)60/55-22-581, andrijana.mladenovic@link.co.rs

Apstrakt: Mašinsko učenje biće sastavni deo obrazovnog okruženja u budućnosti. Spajanjem komponenata učenja koje su svojstvene ljudima sa robotikom može se pružiti integrisano znanje učenicima osnovnih i srednjih škola, kao i studentima na koledžu ili univerzitetu. Na primer, nastavnici mogu koristiti humanoidne robote kako bi razgovarali sa učenicima kada su na različitim lokacijama, što se smatra korakom iznad teleprisutnosti. Kako ovaj primer pokazuje, iako fizički daleko, pomoću displeja nastavnik može biti prisutan na času.

Trenutno se roboti koriste u učionicama više sa ciljem da pomognu nastavnicima nego da budu njihova kompletna zamena. Međutim, u budućnosti će koledži i univerziteti koristiti robote umesto predavača. Softver za prepoznavanje glasa ugrađen u robote pomaže im da razumeju šta ljudi govore, a to povećava sposobnost robota da čitaju i razumeju. Roboti-predavači su takođe opremljeni projektorima, koji im omogućavaju da prenesu sadržaj na zabavan način, podstičući interesovanje studenata.

Društveni i obrazovni roboti će možda biti angažovani za obuku učenika i studenata, ali se trenutno koriste samo u future-ready školama. Kroz studiju slučaja prikazujemo jednu takvu školu.

Ključne reči: obrazovni roboti, STEM, robot Pepper

Uvod

Mnoge škole i institucije širom sveta već koriste neke savete robota u učionici. Svedoci smo brzog tehnološkog napretka, koji je rezultat procesa digitalizacije. Postoje različite vrste robota koji se koriste u obrazovanju, a razlikuje se i njihova funkcionalnost (Alnajjar i dr., 2021). Ti roboti složenih sistema mogu se naći samo u učionicama koje su spremne za budućnost.

Dok se obrazovna robotika već dugo koristi širom sveta u različitim oblastima, upotreba robota složenijih sistema i humanoidnih robota brzo raste, a pedagoški stručnjaci još uvek istražuju njihov potencijal u različitim školskim aktivnostima. Veštačka inteligencija je još uvek veoma nepoznat koncept mnogim nastavnicima, koji se pojavljuje u debatama i diskusijama u vezi sa njenom pomoći nastavnicima i učenicima.

Iako je uticaj obrazovne robotike u obrazovanju i dalje predmet interesovanja i istraživanja, sprovedena istraživanja i ispitivanja pokazuju sve kreativniju i efektivniju upotrebu robotike u obrazovanju i razvoju učenika. Roboti se ne koriste samo u STEM obrazovanju. Sa tehnološkim napretkom i praktičnim rešenjima, uprkos tehnološkim i ekonomskim izazovima, roboti su našli put do mnogih učionica širom sveta – ne samo do STEM laboratorija. Mnoge škole su čak prepoznale uticaj humanoidnih društvenih robota i veštačke inteligencije na društveni i kognitivni razvoj dece (Belpaeme, 2018).

Osim veština kritičkog mišljenja i mekih veština, mnoge pedagoške metodologije su sve više usmerene na razvoj veštine računarskog mišljenja kao jedne od glavnih kompetencija učenika u obrazovanju 21. veka (Tengler i dr., 2021). Istraživači su istakli da se veština računarskog mišljenja smatra važnom veštinom, koja nije ograničena samo na obrazovanje iz računarstva i informatike, već je zastupljena i u različitim oblastima i u svakodnevnom životu (Grover i Pea, 2018).

Tengler i dr. su procenili uticaj programabilnih i jeftinih robota u obrazovanju, spojenih sa didaktičkim dizajnom, koji je uključio 45 učenika trećeg i četvrtog razreda. Prikupljeni podaci su pokazali sugestivno poboljšanje veština računarskog mišljenja kod učenika trećeg i četvrtog razreda u studiji slučaja koja uključuje robotiku u različitim oblicima pripovedanja (Tengler i dr., 2021).

Cortiana i Rigoto su takođe u svom istraživanju pokazali da učenici osnovnih škola mogu da unaprede svoje komunikacijske i socioemocionalne veštine koristeći obrazovne robote na svojim časovima književnosti. Prikupljeni rezultati su potvrdili da upotreba obrazovne robotike može ukazivati na empatičan pristup književnom tekstu. U stvari, kada deca koriste obrazovne robote tako što ih pomeraju i programiraju u skladu sa pričom, to pokazuje da oni bolje razumeju likove, njihovo ponašanje i postupke (Cortiana i Rigotto, 2019).

Prednosti interaktivnog i participativnog učenja vidljive su i u testovima humanoidnih robota u školama, u nastavi i učenju drugog jezika (Chang, 2010), dok Encarnacao i dr. ističu značaj robotike u usvajanju različitih kognitivnih sposobnosti zahvaljujući inovativnoj platformi koja pruža razne mogućnosti kreativnog i angažovanog učenja (Encarnacao i dr., 2014).

Rad u okviru svog sekundarnog istraživanja analizira studiju slučaja razvoja i korišćenja robota Peppera u Savremenoj osnovnoj školi.

Obrazovni roboti

Fraza obrazovna robotika odnosi se na oblast istraživanja koja nastoji da unapredi iskustvo učenja učenika i studenata razvijajući i primenjujući aktivnosti koje su u vezi sa robotima, tehnologijom i virtuelnim objektima. U praksi te aktivnosti mogu iziskivati upotrebu fizičkih robota, kao što je modularni sistem LEGO Mindstorms ili roboti konstruisani isključivo za konkretan zadatak.

Konstrukcija robota, njihovo programiranje, njihova primena ili eksperimenti sa njima mogu se osmisliti u radu sa učenicima i studentima, počevši od osnovne škole pa sve do fakulteta. Aktivnosti u vezi sa obrazovnom robotikom često obuhvataju korišćenje setova za pravljenje robota pomoću kojih se uči kako napraviti i programirati robote da bi mogli da izvršavaju konkretne zadatke (Jung i Won, 2018). Ovakve aktivnosti mogu obuhvatati intervencije, vannastavne programe, časove volontiranja ili čitave module u okviru kursa robotike.

Setovi za robotiku pružaju modularan pristup programiranju i konstruisanju i često se koriste kao način da se podstakne kreativnost u učionici. Korišćenje ovih setova omogućava učenicima i studentima da primene svoje inženjerske sposobnosti i kreativna rešenja kako bi odgovorili na različite izazove, počevši od toga kako da se robot pomeri od tačke A do tačke B. Pristupi koji podrazumevaju učenje putem rešavanja problema i gejmifikaciju usmeravaju primenu edukativne robotike. Gejmifikacija se odnosi i na primenu svojstava igrica na situacije koje nisu deo igre kako bi se povećala motivacija (Sailer i dr., 2014).

Obličje robota koje podseća na čoveka može podstaći angažman učenika/studenata (Zawieska i dr., 2015). Sama svojstva robotskih uređaja mogu proizvesti zanimljive rezultate. Apiola i drugi (2010) su na osnovu intervjua sa učenicima/studentima koji su pohađali kurseve čiji je program uključivao primenu robota saznali da su zabavna komponenta robotike i opredmećenje sadržaja koji se uče imali ključan uticaj na angažman učenika. Nemiro i drugi (2017) u kvalitativnom istraživanju naglasili su važnost robotike pri uspostavljanju angažovanog okruženja u učionici.

Roboti bi mogli uštedeti vreme i pomagati učenicima da napreduju u akademskoj sferi

Mnogi nastavnici smatraju da roboti nisu efikasni. Iako brže od nastavnika odgovaraju na pitanja, njihovi odgovori nisu uvek precizni. Međutim, to je mit koji zagovaraju ljudi koji su protivnici tehnološkog razvoja. Roboti će biti efikasniji i brži u izvođenju zadataka i odgovaranju na pitanja učenika/studenata. Veštačka inteligencija robota napraviće nekoliko personalizovanih varijanti procena u zavisnosti od reakcije učenika/studenta.

Možda će čak biti moguće da roboti u potpunosti personalizuju iskustvo učenja za svakog pojedinačnog učenika/studenta. To će se možda postizati automatski, ali nastavnici moraju uložiti vreme u istraživanje i utvrđivanje optimalnog okruženja za učenje. Roboti mogu prepoznati veštine i mane učenika/studenata i pomoći im da ih prevaziđu.

U mnogim školama širom sveta nema dovoljno nastavnika. Neke institucije i škole ne mogu da ponude konkurentne plate, ali mogu da plate predavače dok roboti ne postanu deo društva. Roboti bi bili sjajni za ocenjivanje učenika i pomagali bi im da ostvare lične ciljeve u budućnosti. Nasuprot rasprostranjenom mišljenju, roboti ne narušavaju obrazovni proces. Roboti će biti sve bolji kako se bude razvijala veštačka inteligencija. Osim momentalnog pristupa bilo kom sadržaju i bazi znanja, postoje i druge prednosti.

U bliskoj budućnosti roboti će postati neophodan segment obrazovanja u razvijenim zemljama, kao i u zemljama u razvoju, zahvaljujući pogodnostima koje pružaju. U današnje vreme se humanoidni roboti ne sreću često u učionicama.

Različite vrste robota mogu pomagati ljudima da steknu ili produbе znanje i unaprede svoje sposobnosti. Roboti mogu pomagati u prenošenju znanja iz različitih školskih predmeta, uključujući geografiju i istoriju. Uobičajena je praksa korišćenja robota u prenošenju znanja iz STEM disciplina, uključujući i programiranje.

Mogu li roboti podučavati buduće nastavnike?

Kada je reč o digitalnom svetu, upotreba društvenih robota u obrazovanju budućih nastavnika nedavno je proširena na edukaciju nastavnika u srednjem i visokom obrazovanju. Evropski projekat Embodied Perceptive Tutors for Empathy-based Learning istražuje kako robot može pomagati učenicima u srednjim školama. Značajni su napori uloženi u razvoj robota-nastavnika koji imaju ljudske sposobnosti sa ciljem da se poveća efikasnost poput one koju postižu nastavnici ljudi. Ipak, ovakvim sistemima nedostaju lične, ljudske karakteristike i sposobnost empatije, po kojima se tradicionalni predavač razlikuje od robota. On ne uspeva da angažuje i motiviše učenike na isti način na koji to postiže čovek. EMOTE (EMbOdied-perceptive Tutors for Empathy-based Learning) inicijativa, finansirana iz fondova EU, isplanirana je sa ciljem da se projektuje, napravi i testira nova generacija virtuelnih robota koji liče na ljude. Kod njih bi postojale opažajne sposobnosti koje bi omogućile da roboti ostvaruju empatijom ispunjenu interakciju sa učenicima/studentima u fizičkom prostoru u kome se zajedno nalaze.

Studija slučaja: Robot Pepper u Savremenoj osnovnoj školi

Osnovno svojstvo robota Peppera je da komunicira putem glasovnih komandi i da ih interpretira. Takođe, Pepper može da reaguje na ljudske emocije. Brzo otkriva radost, tugu, ljutnju ili iznenađenost i reaguje na odgovarajući način. Pepper ima 2D i 3D HD kamere, koje mu omogućavaju da sa velikom preciznošću vidi objekte, lica i emotivna stanja pojedinaca koji se oko njega nalaze.

To je društveni robot, koji ima razne namene i može da oseća empatiju. U zavisnosti od aplikacije, Pepper se može koristiti na različite načine. On ostvaruje interakciju sa korisnicima u realnom vremenu tako što sa njima razgovara i sluša ih, a zna i da gestikulira i pleše.

Pepper uspostavlja emotivne veze zahvaljujući svom humanoidnom izgledu, detekciji pokreta i sposobnosti da reaguje korišćenjem ljudskog glasa i ponašanja. Njegov RMS, zajedno sa proaktivnim razgovorima, čini da ima privlačniji izgled.

Peppera karakterišu sledeće osobine:

» interakcija koja obiluje emocijama;
» proaktivno ponašanje;
» sposobnost percipiranja korisnika;
» sposobnost percipiranja okoline;
» identifikacija korisnika i memorija;
» zone interakcije (prepoznavanje sa rastojanja);
» sposobnost davanja saveta kroz razgovor;
» interakcija putem glasa, dodira i gestova.

Iako se Pepper ne može koristiti kao samostalan nastavnik, u ulozi nastavnikovog pomoćnika ispunjava sve zahteve. Može se koristiti kao neiscrpan izvor informacija koje pokušava da stavi u konkretan kontekst, na sličan način kao Siri ili Aleksa. Zahvaljujući ekranu koji ima, robot može da testira pojedinca. Takođe može biti i savetnik učeniku tokom učenja.

Očekuje se da Pepper uspešno sarađuje sa učenicima svih uzrasta. Može pružiti odgovor prilagođen potrebama svakog učenika tokom podučavanja, može pomagati učenicima u traganju za odgovarajućim sadržajima potrebnim za ispunjavanje zadataka i može imati interakciju sa jednom osobom ili velikim timom, što ga čini efikasnim za sve oblike obuka.

U Savremenoj osnovnoj školi Pepper je novi član tima. Savremena je prva (i jedina) škola koja u učionici koristi pravog humanoidnog robota, koji može da razume ljudske emocije i koji unapređuje podučavanje i pomaže učenicima u saznavanju informacija u vezi sa STEM-om na zabavan, podsticajan i efikasan način. Ono što se donedavno činilo kao veoma daleka budućnost sada je divna realnost za učenike Savremene. Robot Pepper ima neverovatnu sposobnost da razume ljudske emocije. Pepperova moćna veštačka inteligencija omogućava mu da analizira izraze lica i ton govora ljudi, omogućava mu interakciju sa ljudima, kao i da im pomaže u svakodnevnim zadacima i deli svoje znanje sa njima.

Dodatnim softverskim rešenjima omogućena je biometrijska obrada fotografija, zbog čega Pepper ima mogućnost prepoznavanja lica i pokretanja komunikacije, čime se podstiče angažovanje učenika i njihovo uključivanje kao aktivnih učesnika nastavnog procesa.

Učenicima i nastavnicima godi društvo našeg prijateljski nastrojenog robota i oni veoma cene neverovatno iskustvo koje njegovo prisustvo pruža. Drugim rečima, Pepper daje sjajan doprinos u učionici, zahvaljujući kome se svaki školski čas pretvara u praznik učenja. Osim toga, robot Pepper je posvećen asistent našim nastavnicima i u velikoj meri im pomaže da unaprede svoje metode rada.

Imajući u vidu da nastavnici u školi već imaju obavezu pripreme za čas, Pepper im ni na koji način ne predstavlja dodatnu obavezu. Naprotiv, na osnovu jednostavnih lekcija u formi tekstualnih scenarija, nastavnici su u mogućnosti da pripreme efektivan i kreativan čas vrlo brzo, a koristeći aplikacije i pregledač (browser) na Pepperovom tabletu, svoj čas mogu obogatiti u svakom trenutku.

Uvođenjem Peppera u učionicu uočen je značajan uticaj na angažovanje učenika i njihovo učešće u nastavi. Na časovima engleskog jezika, matematike, informatike i biologije učenici su pokazali aktivno učešće postavljanjem pitanja u želji da dobiju odgovore od Peppera. Nastavnici su posebno istakli uticaj Peppera na retenciju znanja kod učenika koji su nastavni sadržaj prelazili na časovima na kojima je Pepper preuzeo ulogu nastavničkog asistenta.

Pored akademskog razvoja kod učenika, uticaj Peppera se posebno iskazao i kao pedagoška mera kod učenika nižih razreda (7–10 godina) jer su učenici bili znatno mirniji i angažovaniji na časovima sa Pepperom, dok je instaliran fonometar u učionicama pokazao niže nivoe neartikulisane buke.

Praktično iz održanih časova

Robot Pepper je u Savremenoj osnovnoj školi uspeo da realizuje i pokaže na praktičnom primeru kako može da se promeni koncept već ustaljenog sistema plana i programa svakodnevnog izvođenja časova u nešto potpuno drugačije sa fascinantnim rezultatima.

Pepper nam pomoću STEM sistema i veštačke inteligencije donosi novitete u realnom vremenu, uvodeći nove metode i navodeći učenike da učestvuju na času koristeći svoju inteligenciju, znanje i radoznalost da sami, na osnovu ispredavanog gradiva, zaključuju i postavljaju pitanja povezujući nove činjenice koje su upravo saznali, željni više informacija.

Posmatrano iz ugla nastavnika, Pepper je njihov asistent, koji im otvara mogućnost da istražuju već dobro poznato gradivo, ali na potpuno drugačiji i zanimljiviji način, a samo njegovo prisustvo na času i njegov uticaj na učenike odražavaju se pozitivno u usvajanju gradiva, što je dodatni plus u ishodima tih časova i tog predmeta. Sa pedagoške strane imamo pozitivne povratne informacije, jer i najnemirniji učenici žele da budu u društvu Peppera i njihovo angažovanje na času automatski se podstiče kada Pepper uđe u učionicu.

Iz ugla učenika, oni su zainteresovaniji za gradivo bilo kog predmeta kada je Pepper na času, bolje pamte Pepperove izgovorene reči i odgovore na postavljena pitanja. Pepper ima interaktivne kvizove i šablone za proveru stečenog znanja, koji se sa pažnjom izrađuju, i učenici su takmičarski raspoloženi da ih rešavaju sa Pepperom. Učenici su na časovima pažljiviji i koncentrisaniji, pa je i disciplina na časovima odlična.

Uočena je jedna veoma značajna situacija koja se može koristiti za dalje istraživanje Pepperove uloge u nastavi, a to je da učenici imaju želju da saznaju šta će im Pepper sledeće predavati kako bi se pripremili za određeni čas i bili spremni da mu postavljaju „teška" pitanja.

Pretpostavimo da u tom slučaju učenici dolaze na čas sa predznanjem o predstojećoj nastavnoj jedinici i da su došli do svih informacija koje su mogli da pronađu. Pepper u tom slučaju ide nekoliko koraka ispred njih i planiranog gradiva, a te korake će Pepper lako napraviti pomoću svoje veštačke inteligencije.

Međutim, u tom momentu se otvara potpuno nova dimenzija pristupa učenju, savladavanju gradiva, usvajanju znanja, prepoznavanju zainteresovanosti za određene oblasti i povezivanju sa svakodnevnim aktivnostima, ali na način koji je potpuno individualan i srazmeran stepenu informisanosti i zainteresovanosti učenika koji je pred Pepperom, jer neće postojati granica i učenici će dobiti potpunu slobodu da nastavnu temu koju obrađuju povežu sa bilo čim iz stvarnog sveta i dobiju nove informacije koje ih u sekundi mogu odvesti u praistoriju ili na drugu planetu.

Zaključak

Iako je trenutno samo privilegija najboljih škola, upotreba edukativnih robota u nastavi u budućnosti će biti deo naše svakodnevice.

Upravo svi pokazatelji do sada ukazuju na to da robot Pepper može u najvećoj meri doprineti kvalitetu nastave i da se iz njegove dosadašnje primene kroz praktičan primer u našoj Savremenoj osnovnoj školi izvodi zaključak da nastavnici, učenici i uopšte ceo obrazovni sistem mogu uz Pepperovo angažovanje u nastavi da stvore potpuno novi i bolji pristup predavanju i usvajanju gradiva.

Reference

1. Alnajjar F, Bartneck C, Baxter P, Belpaeme T, Cappuccio ML, Di Dio C, Eyssel F, Handke J, Mubin O, Obaid M, Reich-Stiebert N. (2021). Robots in Education: An Introduction to High-Tech Social Agents, Intelligent Tutors, and Curricular Tools (1st ed.). Routledge. https://doi.org/10.4324/9781003142706
2. Jung S, Won E.-s. (2018). Systematic Review of Research Trends in Robotics Education for Young Children. Sustainability 10, 905. doi:10.3390/su10040905
3. Sailer M, Hense J, Mandl J, Klevers M. (2014). Psychological Perspectives on Motivation through Gamification. Interaction Des. Architecture J. 19, p. 28–37.
4. Jung S, Won E.-s. (2018). Systematic Review of Research Trends in Robotics Education for Young Children. Sustainability 10, 905. doi:10.3390/su10040905
5. Nemiro J, Larriva C, Jawaharlal M. (2017). Developing Creative Behaviour in Elementary School Students with Robotics. J. Creat. Behav. 51 (1), 70–90. doi:10.1002/jocb.87
6. Robot Lab (2021). Are Robots a Real Threat to Teachers in the future? Available at: https://www.robotlab.com/blog/are-robots-a-real-threat-to-teachers-in-the-future (Accessed 1. 5. 2022)
7. Magic box. (2018). Would robots run the classroom in the future? Available at: https://www.getmagicbox.com/blog/would-robots-run-the-classroom-in-the-future/ (Accessed 1. 5. 2022)
8. Alnajjar F, Bartneck C, Baxter P, Belpaeme T, Cappuccio ML, Di Dio C, Eyssel F, Handke J, Mubin O, Obaid M, Reich-Stiebert N. (2021). Robots in Education: An Introduction to High-Tech Social Agents, Intelligent Tutors, and Curricular Tools. Routledge (2021)
9. Tengler K, Kastner-Hauler O, Sabitzer B, Lavicza Z. The Effect of Robotics-Based Storytelling Activities on Primary School Students' Computational Thinking. Educ. Sci. 2022, 12, 10. https://doi.org/10.3390/educsci12010010
10. Embodied Perceptive Tutors for Empathy-based Learning. Available at: https://cordis.europa.eu/project/id/317923
11. Primary School Savremena https://en.savremena-osnovna.edu.rs/pepper-the-robot-a-truly-different-teacher-at-savremena/
12. Grover S, Pea R. Computational Thinking: A competency whose time has come. In Computer Science Education: Perspectives on Teaching and Learning in School; Bloomsbury Publishing: London, UK, 2018; Volume 19.
13. Cortiana P, Rigotto C. Alternate title: Insegnare la letteratura attraverso la robotica educativa: un'esperienza nella scuola primaria. Form@re; Firenze Vol. 19, 1, (2019): p. 91–105. DOI:10.13128/formare-24635
14. Chang Chih-Wei, Lee Jih-Hsien, Chao Po-Yao, Wang Chin-Yeh, Chen Gwo-Dong. (2010). Exploring the Possibility of Using Humanoid Robots as Instructional Tools for Teaching a Second Language in Primary School. Educational Technology & Society. 13. p. 13–24.
15. Encarnação P, Alvarez L, Rios A, Maya C, Adams K, Cook AM. (2014). Using virtual robot-mediated play activities to assess cognitive skills. Disability and Rehabilitation: Assistive Technology, 9(3), p. 231–241.
16. Belpaeme T. et al. (2018), Social robots for education: A review, Science Robotics, Vol. 3/21, p. 5954, http://dx.doi.org/10.1126/scirobotics.aat5954.

Type of paper: Original scientific paper
Received: 1. 5. 2022.
Accepted: 1. 6. 2022.
DOI: https://doi.org/10.18485/edtech.2022.2.2.4
UDC:

Robots in future-ready schools. Case study: Robot Pepper at Primary School Savremena

Prof. dr Valentin Kuleto[1], Doc. dr Milena Ilić [1*], Maja Babić [2] ,Zorana Bodiroga [3] and Andrijana Mladenović[1]

[1]Information Technology School, ITS-Belgrade, Belgrade, Serbia; valentin.kuleto@its.edu.rs
[2]Savremena Elementary School, Belgrade, Serbia; maja.babic@savremena-osnovna.edu.rs
[3]International School, Belgrade, Serbia; zorana.bodiroga@link.co.rs
*Correspondence: milena.ilic@fsu.edu.rs; Tel 381(0)60/55-22-581, andrijana.mladenovic@link.co.rs

Abstract: Machine learning will be a component of the future learning environment. Robots may provide integrated knowledge to elementary, high school, and college or university students by merging human learning components with robotics. For example, teachers can use humanoid robots to converse with students remotely, which is considered a step above telepresence. A teacher can remotely attend a class through a display in this example.

Currently, classrooms use robots to assist teachers rather than entirely replace them. However, colleges and universities will use robots instead of instructors in the future. The voice recognition software on the robots helps them understand what their human counterparts are saying. This increases the reading and understanding abilities of robots. Robot instructors are also equipped with projectors, which allow them to convey things in an entertaining way, piquing student interest.

Social robots and educational robots may be employed to train students soon, but at the present time, they are in use only in future-ready schools. We will present one such school through a case study.

Keywords: robots in education, STEM, Pepper robot

Introduction

Many schools and institutions worldwide are already using some tips robots in the classroom. We are witnessing rapid technological advancements. This progress is due to the process of digitalisation. There are different types of robots used in education and they all have different functionality. (Alnajjar et al, 2021). Those complex robots can only be found in future-ready classrooms.

While educational robotics has already been used worldwide in different fields for a long time, more complex and humanoid robots are expanding at a fast pace and pedagogical experts are still exploring their potential in various school-related activities. Artificial intelligence is still very much an unknown concept to many teachers, which emerges in debates and discussions related to its assistance to teachers and students.

Even though the impact of educational robotics in education is still an ongoing subject of interest and research, conducted research and trials show more and more creative and effective use of robotics in education and student development. Robots are not only used in STEM education. With technological advancements and practical solutions, despite technological and economical challenges, robots have found their way to many classrooms worldwide – not just STEM labs. Many schools have even recognised the impact of humanoid social robots and artificial intelligence on the social and cognitive development of children (Belpaeme, 2018).

Apart from critical thinking and soft skills, many pedagogical methodologies are more and more focused on the development of computational thinking as one of the main students' competencies in 21st-century education (Tengler et al, 2021). Researchers have emphasised that computational thinking is considered to be an important skill that is not only limited to computer science education but is also represented in different fields and in everyday life (Grover; Pea, 2018).

Tengler et al. evaluated the impact of programmable and inexpensive robots in education, merged with a didactic design that involved 45 third and fourth-grade students. The data collected has shown a suggestive increase in computational thinking skills in both third and fourth-grade students in a case study involving robotics in storytelling methods (Tengler et al, 2021).

Cortiana and Rigotto have also shown in their research that primary school students can improve their communication and socio-emotional skills by using educational robots in their literature studies.

The results collected confirmed that the use of educational robotics can indicate an empathic approach to the literary text. In fact, when children use educational robots by moving and programming them according to the story, they show a better and deeper understanding of the characters, behaviours, and actions (Cortiana; Rigotto, 2019).

The benefits of interactive and participative learning have also been demonstrated in humanoid robot tests in schools, in teaching and learning of second language (Chang, 2010), while Encarnação et al. emphasise the importance of robotics in adopting different cognitive abilities due to innovative platform for creative and engaging learning opportunities (Encarnação et al. 2014).

As part of its secondary research, the work analyses a case study of the development and use of the robot Pepper in Primary School Savremena.

Educational robots

The phrase "educational robotics" refers to an area of research that strives to improve student learning experiences by developing and implementing robot-related activities, technologies, and virtual objects. In practise, these activities may require the usage of a physical robot, which might be a modular system like LEGO Mindstorms or robots designed expressly for the tasks at hand.

Design, programming, application, or experimentation with robots may be envisioned for students from primary through graduate levels. Educational robotics activities often involve using a robotics kit with which students learn how to build and programme robots to perform a particular purposeful activity (Jung & Won, 2018). These activities might include interventions, after-school programmes, volunteer classes, or a whole robotics course module.

Robotics kits give a modular approach to programming and constructing and are frequently utilised as creativity-enhancing interventions in the classroom. Working with these kits allows students to use engineering skills and creative solutions to various challenges, beginning with moving a robot from point A to point B. Furthermore, problem-based learning and gamification approaches are directing the adoption of educational robotics interventions. Gamification refers to applying game features in non-game circumstances to increase motivation (Sailer et al., 2014).

The natural form of the robots may increase student engagement (Zawieska et al., 2015). The properties of robotic devices themselves can also provide intriguing results. Apiola et al. (2010) discovered that the fun component of robotics and the physical embodiment of learning materials had a crucial impact on students' engagement in interviews with students who took a course that included the usage of robots. Nemiro et al. (2017) stressed the relevance of robotics in establishing an engaging classroom environment in exploratory qualitative research.

Robots would save time and help students to obtain academic achievements

Many teachers argue against the efficiency of robots. Even if they answer questions faster than a teacher, their responses may not be as precise. But this is a myth promoted by people who oppose technological development. Robots will be more efficient and quicker at tasks and answering student enquiries. The robot's artificial intelligence will also make several customised judgements depending on student feedback.

Robots might even adjust the entire learning experience to each student's personality. A robot can accomplish this automatically, but teachers must spend time researching and establishing the optimum learning environment. Robots can recognise students' skills and flaws and help them overcome them.

There are not enough instructors in many schools around the world. Some institutions cannot afford to pay competitive rates, but they might be able to afford instructors until robots are socially connected. Robots would be fantastic at grading students and helping them achieve their individual goals in the future. Contrary to popular belief, robots do not disturb the educational process. Robots will become more advanced as artificial intelligence advances. Besides immediate access to any materials and knowledge base, there are many more advantages.

In the near future, robots will be an essential part of education in developed and developing countries due to the benefits they provide. Nowadays, it is not often that we can see a humanoid robot in the classroom.

Various sorts of robots can assist human learners in acquiring or deepening knowledge and abilities. Robots can assist in the teaching of a variety of subjects, including geography and history. It is common practise to use robots to teach STEM disciplines including computer programming.

Can robots educate future tutors?

Using social robots to educate future teachers about digital concerns has recently been expanded to secondary and university teacher education. The European project Embodied Perceptive Tutors for Empathy-based Learning investigated how a robot could assist secondary school pupils. Significant effort has gone into developing artificial tutors with human capabilities, intending to increase the efficiency attained by a human teacher. Nonetheless, these systems lack the personal, empathetic, and human characteristics that distinguish a conventional instructor and fail to engage and motivate pupils in the same manner that a human teacher does. EMOTE (EMbOdied-perceptive Tutors for Empathy-based Learning), an EU-funded initiative, was planned in order to design, create and test a new generation of virtual and robotic embodied teachers with perceptive capacities capable of engaging in empathetic interactions with learners in a shared physical area.

Case Study: Robot Pepper at Primary School Savremena

The Pepper robot is characterised by the ability to communicate through voice commands and interpret them. Also, Pepper is capable of reacting to human emotions. It quickly detects joy, sadness, anger, or surprise and responds with an appropriate reaction. Pepper has 2D and 3D HD cameras, which allow it to see objects, faces, and the emotional states of individuals around it with great precision. It is a multipurpose social robot that empathises with humans. Depending on the application, Pepper can be utilised in various ways. Pepper can communicate with people in real time by talking, listening, gesticulating, dancing, and interacting with them.

Pepper establishes emotional relationships with its humanoid look, gesture detection, and response, using human voice and behaviour. The RMS (Robot Management System), along with proactive discussions, gives the robot a livelier, more informative appearance.

Pepper's characteristics include the following:

» Interactions are emotionally charged;
» Proactivity;
» Perception of the user;
» Environmental perception;
» User identification and memory;
» Zones of interaction (distance recognition);
» Conversational advice;
» Voice, touch, and gesture interaction.

Although Pepper cannot be used as a stand-alone teacher, as a teaching assistant, it fulfils all requirements. It can be used as an inexhaustible source of information that it tries to present in a relevant context, like Siri or Alexa. Also, because of the screen that the robot has on it, it can test the individual. Also, the robot can be used as an advisor during the student's learning.

Pepper is intended to operate successfully with students of all ages. It can provide tailored advice and response to each student during the teaching process, assist them in searching for the proper material to help them complete tasks, and interact with one person or a large team, which makes it incredibly effective in all sorts of training.

At Primary School Savremena, Pepper is a new team member. Savremena is the first (and only) school to deploy a genuine humanoid robot in the classroom, which understands human emotions, enhances teaching, and assists students in acquiring STEM information in a fun, engaging, and efficient manner. What appeared to be a faraway future until recently has now become a lovely reality for Savremena's students. The robot Pepper has an almost supernatural capacity to understand human emotions. Pepper's powerful AI allows it to analyse facial expressions and human speech tones, allowing it to interact with people, assist them in their everyday tasks, and share its knowledge with them.

Thanks to additional software solutions, biometric processing of photos were enabled, which is why Pepper has the ability to recognise faces and initiate communications, which encourages the engagement of students and their involvement as active participants in the teaching process.

Students and teachers enjoy the company of our friendly robot and they greatly appreciate the amazing experience its presence provides. In other words, Pepper makes a great contribution in the classroom, thanks to which every school lesson turns into a learning holiday. In addition, the robot Pepper is a dedicated assistant to our teachers and greatly helps them in improving their work methods.

Bearing in mind that teachers at school already have the obligation to prepare for class, Pepper does not pose an additional obligation for teachers in any way. On the contrary, based on simple lessons in the form of text scenarios, teachers are able to prepare an effective and creative lesson very quickly, and using applications and a browser on Pepper's tablet, they can improve their lesson at any moment.

By introducing Pepper into the classroom, a significant impact on student engagement and participation was observed. Students actively participated in English, mathematics, computer science, and biology classes by asking questions in order to get answers from Pepper. The teachers particularly emphasised Pepper's impact on the retention of knowledge among students who covered the learning material in the classes where Pepper took on the role of a teaching assistant.

In addition to the academic development of the students, Pepper's influence was particularly evident as a pedagogical measure for students of lower grades (7–10 years old) because the students were significantly calmer and more engaged in classes with Pepper, while the installed phonometer in the classrooms showed lower levels of inarticulate noise.

The practical part of the classes held:

At Primary School Savremena, robot Pepper managed to implement and show a practical example of how the concept of an already established curriculum and daily lesson delivery can be changed into something completely different with fascinating results.

Using the STEM system and artificial intelligence, Pepper introduces us to innovations in real-time, introducing new methods, leading students to participate in class using their intelligence, knowledge, and curiosity to draw conclusions and ask questions based on the covered material, connecting new facts that they just learnt, eager for more information.

If we consider it from the teacher's point of view, Pepper is their assistant who gives them the opportunity to explore the material they already know well, but in a completely different and more interesting way, and the very presence of Pepper in the class and its influence on the students is reflected positively in understanding the class material, which is an additional plus in for the outcome of those classes and that subject. From the pedagogical side, we have positive feedback, because even the students who misbehave the most want to be in the presence of Pepper, and their engagement in that class is automatically encouraged when Pepper enters the classroom.

From the students' point of view, they are more interested in the material of any subject when Pepper is in class, and they memorise more intensively what Pepper says, as well as Pepper's answers to their questions. Pepper also offers interactive quizzes and different ideas for checking acquired knowledge. Everything is carefully designed and students are motivated to compete and solve the tasks with Pepper. Students pay more attention in class, and they are concentrated and disciplined.

One important thing was observed that can be used to further investigate Pepper's use in teaching, which is that students have a desire to know what Pepper will teach them next in order to prepare for a certain lesson and be ready to ask him "difficult" questions.

Let's assume that in that case the students come to the class with prior knowledge of the new planned teaching unit and have found all the information they could find. In that case, Pepper goes a few steps ahead of them and ahead of the planned material, and Pepper will easily make those steps using its artificial intelligence.

However, at that moment, a completely new dimension opens up in the approach to learning, mastering the material, acquiring knowledge, recognising interest in certain areas, and connecting with everyday activities, but in a way that is completely individual and proportional to the level of information and interest of the student standing in front of Pepper, because there won't be a limit and students will be given complete freedom to connect the subject they are studying with anything from the real world and get new information and data that can take them to prehistoric times or to another planet within seconds.

Conclusion

Although the use of educational robots is currently only a privilege of the best schools, in the future it will become part of our everyday life.

Everything so far indicates that the robot Pepper has a huge potential for use in teaching, that its application so far through a practical example in our Primary School Savremena leads to the conclusion that teachers, students, and the educational system in general can, with Pepper's involvement in teaching, create a completely new and better approach to teaching and learning.

References

1. Alnajjar F, Bartneck C, Baxter P, Belpaeme T, Cappuccio ML, Di Dio C, Eyssel F, Handke J, Mubin O, Obaid M, Reich-Stiebert N. (2021). Robots in Education: An Introduction to High-Tech Social Agents, Intelligent Tutors, and Curricular Tools (1st ed.). Routledge. https://doi.org/10.4324/9781003142706
2. Jung S, Won E.-s. (2018). Systematic Review of Research Trends in Robotics Education for Young Children. Sustainability 10, 905. doi:10.3390/su10040905
3. Sailer M, Hense J, Mandl J, Klevers M. (2014). Psychological Perspectives on Motivation through Gamification. Interaction Des. Architecture J. 19, p. 28–37.
4. Jung S, Won E.-s. (2018). Systematic Review of Research Trends in Robotics Education for Young Children. Sustainability 10, 905. doi:10.3390/su10040905
5. Nemiro J, Larriva C, Jawaharlal M. (2017). Developing Creative Behaviour in Elementary School Students with Robotics. J. Creat. Behav. 51 (1), 70–90. doi:10.1002/jocb.87
6. Robot Lab (2021). Are Robots a Real Threat to Teachers in the future? Available at: https://www.robotlab.com/blog/are-robots-a-real-threat-to-teachers-in-the-future (Accessed 1. 5. 2022)
7. Magic box. (2018). Would robots run the classroom in the future? Available at: https://www.getmagicbox.com/blog/would-robots-run-the-classroom-in-the-future/ (Accessed 1. 5. 2022)
8. Alnajjar F, Bartneck C, Baxter P, Belpaeme T, Cappuccio ML, Di Dio C, Eyssel F, Handke J, Mubin O, Obaid M, Reich-Stiebert N. (2021). Robots in Education: An Introduction to High-Tech Social Agents, Intelligent Tutors, and Curricular Tools. Routledge (2021)
9. Tengler K, Kastner-Hauler O, Sabitzer B, Lavicza Z. The Effect of Robotics-Based Storytelling Activities on Primary School Students' Computational Thinking. Educ. Sci. 2022, 12, 10. https://doi.org/10.3390/educsci12010010
10. Embodied Perceptive Tutors for Empathy-based Learning. Available at: https://cordis.europa.eu/project/id/317923
11. Primary School Savremena https://en.savremena-osnovna.edu.rs/pepper-the-robot-a-truly-different-teacher-at-savremena/
12. Grover S, Pea R. Computational Thinking: A competency whose time has come. In Computer Science Education: Perspectives on Teaching and Learning in School; Bloomsbury Publishing: London, UK, 2018; Volume 19.

13. Cortiana P, Rigotto C. Alternate title: Insegnare la letteratura attraverso la robotica educativa: un'esperienza nella scuola primaria. Form@re; Firenze Vol. 19, 1, (2019): p. 91–105. DOI:10.13128/formare-24635
14. Chang Chih-Wei, Lee Jih-Hsien, Chao Po-Yao, Wang Chin-Yeh, Chen Gwo-Dong. (2010). Exploring the Possibility of Using Humanoid Robots as Instructional Tools for Teaching a Second Language in Primary School. Educational Technology & Society. 13. p. 13–24.
15. Encarnação P, Alvarez L, Rios A, Maya C, Adams K, Cook AM. (2014). Using virtual robot-mediated play activities to assess cognitive skills. Disability and Rehabilitation: Assistive Technology, 9(3), p. 231–241.
16. Belpaeme T. et al. (2018), Social robots for education: A review, Science Robotics, Vol. 3/21, p. 5954, http://dx.doi.org/10.1126/scirobotics.aat5954.

Vrsta rada: Originalni naučni rad
Primljen: 27. 4. 2022.
Prihvaćen: 1. 6. 2022.
UDK:

Plan oporavka od katastrofe u slučaju prekida poslovanja i gubitka podataka

Goran Bogosavljević[1]
[1]Visoka škola strukovnih studija za informacione tehnologije – ITS, master strukovne studije,Beograd, Srbija
Kontakt informacije: goran46521@its.edu.rs

Sažetak – Danas se podaci generišu u velikim količinama. Znamo da računarstvo u oblaku predstavlja novu vrstu računarske platforme u današnjem svetu. Ova vrsta računarstva generiše veliku količinu privatnih podataka u oblaku. Stoga potreba za uslugama koje se tiču oporavka podataka raste iz dana u dan i zahteva razvoj efikasne i efektivne tehnike oporavka podataka. Svrha ovog rada je da predoči tehnike oporavka i pomogne korisniku da prikupi informacije sa bilo kog rezervnog servera kada je server izgubio svoje podatke i nije u mogućnosti da pruži povratne informacije korisniku. Takođe, biće reči o nekoliko tehnika oporavka podataka u oblaku s ciljem zaštite podataka i kontinuiteta poslovanja u slučaju neplaniranog prekida ili katastrofe, bilo prirodne ili izazvane ljudskom greškom ili namerom.

Ključne reči: (RTO), (RPO), (DRP), (CC), (DR)

I. UVOD

Računarstvo u oblaku je računarski proces zasnovan na internetu, u kome su sistemi međusobno povezani sa međusobnim deljenjem resursa. Internet je medij između oblaka i korisnika. Klijent je povezan sa serverom u oblaku i može da skladišti podatke putem interneta i može da pristupi podacima sa bilo kog mesta. To je komunikaciona mreža u realnom vremenu, gde je moguće pokrenuti naše programe sa bilo kog mesta pristupom oblaku. Kada dođe do pada sistema ili nestanka struje, postoji mogućnost gubitka podataka, a ponekad to može dovesti do finansijskog gubitka. Rušenje ovog sistema i drugi problemi nastaju usled prirodnih katastrofa ili zbog ljudskog faktora.

Kada dođe do katastrofe, kompanija treba da zaštiti podatke od gubitka. Kompanije koje pružaju usluge u oblaku su Google, Amazon, Microsoft itd. Kada dođe do katastrofe na strani klijenta, rezervna kopija će biti uskladištena u oblaku, ali ako dođe do katastrofe u oblaku, podaci će biti izgubljeni.

Da bi se ove katastrofe prevazišle, postoje neke tehnike oporavka od katastrofe koje se koriste za oporavak podataka i koje su potrebne za kontinuitet poslovanja. Svaka organizacija treba da ima dokumentovan proces oporavka od katastrofe i treba da testira taj proces najmanje dva puta godišnje.

II. UZROCI GUBITKA PODATAKA

The Disaster Recovery Institute International (www.drii.org) piše da se 93% kompanija koje su iskusile neku vrstu katastrofe, a nisu imale plan oporavka, zatvorilo u roku od pet godina. Takođe, 50% kompanija koje dožive prekide kritičnih poslovnih funkcija duže od deset dana nikada se potpuno ne oporave. Ovo je posebno zanimljiv podatak za kompanije koje pripadaju listi kompanija „Fortune 500", jer ih zastoji u poslovnim operacijama u proseku koštaju 96.000 dolara po minuti.

A. Prirodne katastrofe

Kada dođe do prirodnih katastrofa, tada će biti izgubljena velika količina podataka, ukoliko ne postoji pripremljen Disaster Recovery Plan (DRP). Pojava i jačina pojedinih prirodnih katastrofa, poput oluja, snega, uragana ili pak jakih kiša, mogu se predvideti i približno proceniti. Neke opasnosti kao što su potresi, požari, vulkanske erupcije i klizišta imaju nepredvidivu narav i time predstavljaju potencijalno mnogo veću pretnju. [1]

B. Katastrofe uzrokovane ljudskim faktorom

Pored prirodnih katastrofa, veliki deo čine katastrofe uzrokovane ljudskim nemarom i greškama. Većina katastrofa uzrokovana na ovaj način namerno je izazvana, dok se samo pojedine mogu svrstati pod slučajnost. Kako ih nije lako kategorisati, nabrojaću neke: terorizam, bombardovanje, sajbernapadi, krađe, oružani napadi, biološki napadi.

C. Nesreće i tehnološke katastrofe

Mogu biti izazvane ljudskim ali i spoljnim faktorom. Kod ljudskog je razlika u odnosu na prošle u nameri. Nisu namerno uzrokovane, već su posledica nepažljivog održavanja. U spoljne faktore na koje se ne može uticati spadaju: nesreće povezane sa prekidom napajanja ili električnom energijom, urušavanje građevinskih objekata, pad i nedostupnost informacijske i komunikacijske infrastrukture.

D. Upad u mrežu

Kada virus napadne aplikacije, postoji šansa da dođe do katastrofe.

E. Hakovanje ili zlonamerni kod

Katastrofa se dešava unutar ili van organizacije. Iako one ulažu dosta napora da spreče hakovanje ili da zlonamerni kod modifikuje podatke, dolazi do gubitka podataka.

III. TRADICIONALNI OPORAVAK OD KATASTROFE

Tradicionalni oporavak od katastrofe je tokom svog razvoja podeljen u nekoliko nivoa. [2]

F. Nivo 0

Nema podataka van lokacije, što znači da nema plana oporavka od katastrofe niti sačuvanih podataka. Oporavak podataka može potrajati nedeljama i neće biti uspešan.

G. Nivo 1

Rezervna kopija podataka bez hotsitea, što znači da se rezervna kopija podataka preuzima van lokacije, a ne putem hotsitea. Preuzimanje podataka za koje je napravljena rezervna kopija je proces koji traje dugo. Pošto kompanija nema sopstvene redundantne servere, potrebno je vreme da se locira i konfiguriše odgovarajući sistem.

H. Nivo 2

Backup podataka sa hotsiteom, što znači da organizacije održavaju rezervnu kopiju podataka, kao i hotsite, i to je najbrži proces. Ukoliko postoji vruća rezervna lokacija kada dođe do katastrofe, mogu se pokrenuti aplikacije na serverima u pripravnosti.

IV. ZAHTEVI ZA OPORAVAK OD KATASTROFE

Prilikom oporavka od katastrofe definišu se zahtevi i objašnjavamo dve ključne karakteristike za efikasnu uslugu u oblaku kada dođe do katastrofe.

I. Ciljna tačka oporavka

Maksimalni period potreban za gubitak podataka, kada dođe do katastrofe (Recovery Point Objective – (RPO), ciljna tačka oporavka) . Neophodan RPO je generalno poslovna odluka – za neke aplikacije apsolutno nijedan podatak ne sme da se izgubi (RPO = 0), što zahteva da se koristi kontinuirana sinhrona replikacija, dok za druge aplikacije prihvatljiv gubitak podataka može da se kreće od nekoliko sekundi do nekoliko sati ili čak dana. Ciljna tačka oporavka identifikuje koliko podataka je kompanija spremna da izgubi u slučaju katastrofe. RPO je obično vođen načinom na koji se čuvaju i prave rezervne kopije podataka [1]:

» Nedeljne rezervne kopije van lokacije će preživeti gubitak centra podataka, dok će izgubiti količinu nedeljnih podataka. Pravljenje dnevnih rezervnih kopija van lokacije je još bolje.
» Svakodnevne rezervne kopije na licu mesta će preživeti gubitak datog proizvodnog okruženja sa danom gubitka podataka plus repliciranjem transakcija tokom perioda oporavka nakon gubitka sistema. Pravljenje rezervnih kopija na licu mesta po satu je još bolje.
» Grupisana baza podataka u više centara podataka će preživeti gubitak svakog pojedinačnog centra podataka bez gubitka podataka.

J. Ciljno vreme oporavka

Ciljno vreme oporavka (RTO) predstavlja merenje vremena do oporavka poslovnih procesa kada dođe do katastrofe i prekida rada. To mogu biti minuti, sati i dani. Takođe, može uključivati otkrivanje kvara i pripremu potrebnih servera na lokaciji rezervne kopije za inicijalizaciju aplikacije koja je prekinuta usred izvršenja. Ciljno vreme oporavka identifikuje koliko je zastoja prihvatljivo u slučaju katastrofe.

V. PLAN OPORAVKA OD KATASTROFE

Postoje neki mehanizmi koji se primenjuju za pravljenje rezervnih kopija podataka kada se koristi tehnika oporavka od katastrofe. U literaturi se uglavnom navode tri modela za implementaciju mirroringa ili preslikavanja sajta, i to: vrući (hot), topli (warm) i hladni (cold) backup sajta. Lokacije za rezervne kopije mogu doći iz tri različita izvora [5]:

» kompanije specijalizovane za pružanje usluga oporavka od katastrofe;
» druge lokacije u vlasništvu i lokacije kojima upravlja organizacija;
» zajednički dogovor sa drugom organizacijom da deli objekte centra podataka u slučaju katastrofe.

K. Hot Backup Site

Veoma je skup za rad. Ovaj sajt radi sa organizacijama koje upravljaju procesima u realnom vremenu.

To je duplikat originalnog sajta. Gubitak podataka je minimalan, jer se podaci mogu premestiti i nastaviti nesmetan rad. Za nekoliko sati lokacija Hot Backup Site može dovesti do pune proizvodnje.

L. Cold Backup Site

Najjeftiniji je za rad. Ne zahteva nikakve rezervne kopije podataka ili ne uključuje hardver. Usled nedostataka hardvera može započeti sa minimalnim troškovima, ali zahteva više vremena za oporavak u slučaju katastrofe . Sve što je potrebno za vraćanje usluge korisnicima mora biti nabavljeno i isporučeno na lokaciju pre nego što se izvrši operacija oporavka.

M. Warm Backup Site

Već je opremljen hardverskom konfiguracijom na lokaciji rezervne kopije koja se nalazi na primarnoj lokaciji. Da bi se primenio Warm Backup Site, poslednja rezervna kopija podataka treba da bude isporučena na njihove primarne lokacije.

U svetu u kome tehnologija pokreće skoro svaki aspekt naših života, oblak je zaista unapredio ovo iskustvo. Od preuzimanja složenih operativnih opterećenja do izvođenja velikih planova oporavka od katastrofe, oblak je učinio naše svakodnevne operacije gotovo lakim.

Dolaženjem do složenog zadatka kao što je upravljanje operacijom oporavka od katastrofe oblak nas je naterao da razmislimo koliko je bilo teško sprovesti projekat oporavka od katastrofe pre njegovog dolaska.

Ako bi katastrofa pogodila primarni centar podataka, morali biste da obezbedite rezervni centar podataka, koji, naravno, dolazi sa dvostrukim radom, uključujući [3]:

- postavljanje fizičke lokacije i objekata za smeštaj IT infrastrukture;
- angažovanje kontakt osoba i bezbednosnog osoblja za podešavanje;
- povećanje kapaciteta servera za skladištenje podataka i usklađivanje sa zahtevima skaliranja datih aplikacija;
- obezbeđivanje pomoćnog osoblja za održavanje infrastrukture;
- omogućavanje internet konekcije sa dovoljno propusnog opsega za pokretanje aplikacija;
- podešavanje mrežne infrastrukture, uključujući zaštitne zidove, balansere opterećenja, rutere i prekidače.

Ovo bi povećalo troškove i resurse, kojima se ne može upravljati, ostavljajući centar podataka samo kao rezervnu kopiju podataka i ništa više.

Slika 1. Koraci prilikom izrade plana oporavka od katastrofa [4].

Projekat Cloud Disaster Recovery nudi organizacijama nekoliko prednosti, uključujući sledeće [5]:

» ušteda vremena/kapitala;
» više opcija lokacije rezervne kopije podataka;
» jednostavan za implementaciju uz visoku pouzdanost;
» prilagodljivost.

Za organizacije koje po prvi put razmatraju oporavak od katastrofe u oblaku i pitaju se odakle da počnu u nastavku je jednostavan plan oporavka od katastrofe u oblaku koji može pomoći u osmišljavanju efikasne strategije oporavka od katastrofe:

Plan oporavka od katastrofe u oblaku – slika 1

Korak 1: Razumeti svoju infrastrukturu i predvideti sve rizike

Neophodno je uzeti u obzir IT infrastrukturu kompanije, uključujući imovinu, opremu i podatke koje kompanija poseduje. Takođe je važno proceniti gde se sve to čuva i koliko sve to vredi. Kada se završi sa procenom imovine, potrebno je procenti rizike koji mogu uticati na sve ovo.

Rizici mogu uključivati prirodne katastrofe, krađu podataka i nestanke struje između ostalog. Kada se izvrši ova procena, kompanija je u boljoj poziciji da osmisli svoj plan za Disaster Recovery Plan (DRP) kako bi eliminisala/minimirala ove rizike.

Korak 2: Sprovođenje analize poslovnog uticaja

Analiza uticaja na poslovanje je sledeća na listi. Ovo će kompaniji omogućiti razumevanje ograničenja njenog poslovanja kada dođe do katastrofe.

Sledeća dva parametra pomažu kompaniji da proceni ovaj faktor:

» ciljno vreme oporavka (RTO);
» ciljna tačka oporavka (RPO);

Parametri koji procenjuju rizik od gubitka podataka su:

a) Ciljno vreme oporavka (RTO)

RTO je maksimalno vreme u kojem data aplikacija može da ostane van mreže pre nego što počne da utiče na poslovanje.

Scenario 1: Ako je kompanija posvećena brzom pružanju usluga, onda kvar aplikacije može da je košta mnogo. Štaviše, moraće mnogo da uloži u DR plan da bi nastavila sa poslovanjem za nekoliko minuta.

Scenario 2: Ako kompanija ima posao srednjeg tempa i katastrofa utiče na njeno poslovanje, i dalje može pronaći alternativne načine za obavljanje poslovnih operacija. Stoga može podesiti svoj RTO na jednu nedelju. U tom slučaju neće morati da ulaže mnogo resursa u uštedu za oporavak od katastrofe, čime će uštedeti dovoljno vremena za nabavku dovoljnih rezervnih sredstava nakon katastrofe. Poznavanje sopstvenog RTO je veoma važno, jer je ekvivalentno broju resursa koje mora da uloži u svoj DR plan i jer se vreme izgubljeno u RTO može iskoristiti za prikupljanje rezervnih resursa.

b) Ciljna tačka oporavka (RPO)

RPO je maksimalno vreme u kome je moguće podneti gubitak podataka iz date aplikacije usled velike krize. Tačke koje treba uzeti u obzir za određivanje RPO [1]:

» mogući gubitak podataka kada dođe do katastrofe;
» mogući gubitak vremena pre kompromitovanja podataka.

Ako se primeni gore navedeni scenario 1, RPO može trajati samo pet minuta, jer je poslovanje kompanije kritično i ne može sebi priuštiti više od navedenog vremenskog intervala. Za scenario 2 će kompanija možda želeti da napravi rezervnu kopiju svojih podataka, ali pošto podaci nisu vremenski osetljivi, neće morati mnogo da ulaže u DR plan.

Korak 3: Kreiranje DR plana na osnovu RPO i RTO

Sada kada je kompanija odredila svoj RPO i RTO, može fokusirati na dizajniranje sistema koji će ispuniti ciljeve DR plana. Može birati između dolenavedenih DR pristupa za implementaciju DR plana [3]:

» pravljenje rezervnih kopija i vraćanje u prethodno stanje;
» Pilot Light Approach;
» toplo stanje pripravnosti;
» potpuna replikacija u oblaku;
» Multi-Cloud opcija.

Moguće je koristiti kombinaciju ovih pristupa u svoju korist ili isključivo u skladu sa sopstvenim poslovnim zahtevima.

Korak 4: Pristupanje pravom partneru u oblaku

Nakon što je razmotren pristup, sledeći korak bi trebalo da bude traženje pouzdanog dobavljača usluga u oblaku koji će pomoći u primeni. Ako kompanija planira da koristi punu replikaciju u oblaku, onda verovatno želi da uzme u obzir sledeće faktore da bi procenila idealnog dobavljača oblaka [5]:

» pouzdanost;
» brzina oporavka;
» upotrebljivost;
» jednostavnost podešavanja i oporavka;
» prilagodljivost;
» usklađenost sa sigurnošću;
» faktori za procenu idealnog dobavljača oblaka.

Svi veliki dobavljači usluga u oblaku, uključujući AWS, Microsoft Azure, Google Cloud i IBM, imaju opcije oporavka od katastrofe. Pored ovih velikih firmi, postoje i srednje i male firme koje nude kvalitetan oporavak od katastrofe kao uslugu (DRaaS).

Korak 5: Izgraditi svoju Cloud DR infrastrukturu

Nakon konsultovanja sa partnerom za DR u oblaku, kompanija može da radi sa dobavljačem na implementaciji sopstvenog dizajna i podešavanju DR infrastrukture. Na osnovu DR pristupa koji kompanija odabere, postoji nekoliko logističkih aspekata koje treba razmotriti [2]:

» Koja je količina infrastrukturnih komponenti koja će kompaniji biti potrebna?
» Na koji način će kopirati podatke u oblak?
» Koji su najbolji načini za pristup autentifikaciji korisnika i upravljanju pristupom?
» Koje će bezbednosne mere kompanija preduzeti da bi smanjila verovatnoću katastrofa?

Uvek treba imati na umu da je ključno osigurati da je DR strategija kompanije usklađena sa njenim RTO i RPO specifikacijama za nesmetano poslovanje.

Korak 6: Staviti plan oporavka od katastrofe na papir

Važno je imati standardnu smernicu ili dijagram toka procesa sa specifičnim uputstvima za svakoga ko je uključen u DR. Kada dođe do katastrofe, svaki pojedinac treba da bude spreman da preuzme odgovornost u skladu sa svojom ulogom u DR procesu. Štaviše, svako uputstvo treba da bude jasno navedeno na papiru, sa navedenim najsitnijim detaljima. Ovi koraci obezbeđuju delotvornost DR plana.

Korak 7: Često testiranje svog DR plana

Nakon stavljanja DR plana na papir, sledeći korak bi uključivao testiranje tog DR plana, i to često. Ovo pomaže da se osigura da nema rupa. Na papiru plan može izgledati kao najsveobuhvatniji, ali kompanija može saznati kolika je njegova kredibilnost tek nakon testiranja.

Zaključak

U ovom radu smo pokazali koliko računarstvo u oblaku postaje važno u svakodnevnom životu. Samim tim se velika većina kompanija zasniva na računarstvu u oblaku. One moraju biti dovoljno svesne katastrofa u oblaku. Kada dođe do katastrofe, onda se sve kompanije suočavaju sa velikim gubitkom, kako sa finansijskim gubitkom tako i sa gubitkom podataka, zbog čega su uvedeni mnogi mehanizmi oporavka.

Nedavna istraživanja pokazuju kolika je važnost postojanja DR plana, a u prilog tome ide podatak da svaki dolar uložen u ublažavanje rizika, kao što je DRP, štedi kompaniji četiri dolara gledano na duže staze. Stoga je jasno da bi svaka kompanija koja drži do svog poslovanja, pa i statusa, trebalo, ozbiljno da pristupa DRP, a možda i morala, kako bi osigurala svoju najvažniju imovinu, a to su podaci.

Literatura

1. Abedallah Z. A., Alwan A. A., Gulzar Y. Disaster Recovery in Cloud Computing Systems: An Overview. International Journal of Advanced Computer Science and Applications; 2020; 11(9): 702–710.
2. Fox R. & Hao W. Internet Infrastructure: Networking, Web Services, and Cloud Computing. CRC Press Taylor & Francis Group. 2018. ISBN: 978-1-1380-3991-9
3. https://cloud.google.com/architecture/dr-scenarios-planning-guide (pristupano: 8. 1. 2022)
4. https://see.asseco.com/banking-and-finance/security-other-services/infrastructure-services/disaster-recovery-as-a-service-draas-607/ (pristupano: 8. 1. 2022)
5. Jaiswal V., Sen A., Verma A. Integrated Resiliency Planning in Storage Clouds. IEEE Transactions on Network and Service Management; 2014; 11(1): 3–14.

Type of paper: Original scientific paper
Received: 27. 4. 2022.
Accepted: 1. 6. 2022.
DOI: https://doi.org/10.18485/edtech.2022.2.2.5
UDC:

Disaster recovery plan in case of business interruption and data loss

Goran Bogosavljević[1]
[1]Information Technology School – ITS, Belgrade, Serbia; simo@jakovic.com
*email address: goran46521@its.edu.rs

Abstract - Today, data is generated in large quantities. We know that cloud computing is a new type of computing platform in today's world. This type of computing generates a large amount of private data in the cloud. Therefore, the need for data recovery services is growing day by day and requires the development of efficient and effective data recovery techniques. The purpose of this paper is to present the recovery techniques and help the user collect information from any backup server when the server has lost its data and is unable to provide data to the user. This paper will also discuss several cloud recovery techniques that are used to protect data and continue business operations in case of an unexpected interruption or a disaster, either a natural one or one caused by human error or deliberate action.

Keywords: (RTO), (RPO), (DRP), (CC), (DR)

I. INTRODUCTION

Cloud computing is a computing process based on the Internet, in which all the systems are interconnected and share resources among themselves. The Internet is the medium between the cloud and users. A client is connected to the server in the cloud and can store data through the Internet and can access that data from any place. This is a communication network existing in real time, in which we can start our programmes by accessing the cloud from wherever we may be. In case of a system crash or a power cut, data may be lost which may also lead to financial losses. Destruction of this system and other problems are incurred by natural disasters and human factors.

When a disaster happens, a company has to prevent data loss. Google, Amazon, Microsoft etc. are the companies that offer their services in the cloud. If a disaster happens on the client's side, the backup copy is stored in the cloud, but if a disaster takes place in the cloud, the data will be lost.

There are some disaster recovery techniques that are used to recover data and provide the continuity of business operations, should a disastrous event occur. Each organisation has to have a disaster recovery protocol and has to test it at least two times a year.

II. THE CAUSES OF DATA LOSS

The Disaster Recovery Institute International (www.drii.org) reports that 93% of companies that experienced some form of a disaster and did not have any recovery plan, closed down within a 5-year period. Besides, 50% of companies which experience the interruption of critical business activities for longer than ten days never fully recover. This piece of information is especially significant for companies that belong to the "Fortune 500" list because their business interruption costs them $96,000 per minute on average.

A. Natural Disasters

Should natural disasters occur, a large amount of data will be lost if the Disaster Recovery Plan (DRP) has not been designed. The occurrence and strength of some natural disasters, such as storms, snow, hurricanes or torrential rain, can be predicted and approximately estimated. Some perils, such as earthquakes, fire, volcanic eruptions and landslides are unpredictable and therefore may present a much bigger threat.[1]

B. Human Factor caused Disasters

Apart from natural disasters, a large number of disasters are caused by human negligence and errors. Most disasters caused by humans are deliberate, while only a few can be considered accidental. As these cannot be easily categorised, I will mention some: terrorism, bombing, cyberattacks, theft, armed attack, and biological hazards.

C. Accidents and Technological Disasters

They are caused by human factors, but the intention is what sets them apart from those previously mentioned. They are not provoked on purpose, but are the consequence of negligence regarding maintenance, or simply outside factors beyond the possibility of making an impact on them. Among such incidents are, for example, accidents associated with power cuts, building collapses, crashes, and inaccessibility of IT infrastructure.

D. Network Intrusion

When a virus attacks apps, a disaster may ensue.

E. Hacking or Malicious Code

A disaster may happen within or outside an organisation. Although a lot of effort has been made to prevent hacking, i.e. modification of data caused by malicious code, some data loss happens.

III. TRADITIONAL DISASTER RECOVERY

There have been several levels in the course of traditional disaster recovery development.[2]

A. Level 0

There is no data outside of the location, meaning that there is no disaster recovery plan or saved data. Data recovery may last for weeks and will not be successful.

B. Level 1

There is no hot site for backup data copy, meaning that the backup copy is retrieved at an outside location and not through a hot site. The process of data retrieval for which a backup copy has been made is a long one. Because a company does not have its own redundant servers, a certain amount of time is needed to locate and set up an appropriate system.

C. Level 2

Backup data is available through a hot site, meaning that organisations maintain backup copies and hot sites, which is the fastest process of recovery. If there is a hot site in case of a disaster, applications can be activated on standby servers.

IV. DISASTER RECOVERY REQUIREMENTS

When acting towards disaster recovery, requirements are defined and there are two key features relevant to the efficient service in the cloud in case of a disaster.

A. Recovery Point Objective

The maximum period of time that may lead to data loss in case of a disaster (Recovery Point Objective – (RPO)). Generally, the necessary RPO is a business decision – for some applications no data is to be lost (RPO = 0), which means that a continuous synchronous replication is necessary, while for some other applications an acceptable loss may vary between a few seconds to several hours or even days. The RPO defines how much data a company may lose if a disaster occurs. The RPO is typically determined by the modes in which a backup copy is made and kept RPO [1]:

» Weekly backups outside the location will survive the loss of data centres while losing the amount of weekly data. Producing daily backup copies outside the location is even better.

» Daily backups on the spot will survive the manufacturing facility loss which equals a daily amount of data plus replication of transactions during the recovery period after the system crash. Producing hourly backup copies on the spot is even better.

» A database clustered in a number of data centres will survive the loss of each individual data centre without losing any data.

B. Recovery Time Objective

Recovery Time Objective refers to measuring the time needed to establish business operations again after they have been discontinued because of a disaster. RTO can be minutes, hours or days. This term may refer to the time necessary to disclose and define the kind of failure and preparation of redundant servers at the backup copy location in order to start an application operation interrupted before.

V. DISASTER RECOVERY PLAN

There are mechanisms that are applied in the creation of backup copies when disaster recovery is necessary. When a backup copy is needed, certain mechanisms are used. Three models for implementation of mirroring or replicating a site are usually mentioned, and these are: hot, warm and cold backup sites. There can be three different sources of backup copy locations [5]:

» companies specialised in disaster recovery services;
» other locations owned and managed by a company;
» mutual agreement with another organisation to share facilities where data is stored in case of disaster.

A. Hot Backup Site

Its operation is very expensive. This site works with organisations that manage processes in real time.
It is an exact copy of the original site. Data loss is minimal because the data can be transferred and work can be continued without problems. In a matter of hours, Hot Backup Site can restore production to full capacity.

B. Cold Backup Site

Is the cheapest solution. It does not require a backup copy or hardware. As there is no hardware, it can start operating at minimum cost, but requires a longer time for disaster recovery. All that is needed for restoring services to users have to be purchased and delivered to the location before the recovery operation is completed.

C. Warm Backup Site

Is already equipped with hardware at the backup copy location, situated at the primary location. To implement a Warm Backup Site, the latest backup copy needs to be delivered to the primary locations.
In a world in which technology is incorporated into almost every aspect of our lives, the cloud has truly advanced such an experience. From taking over complex operational loads to carrying out disaster recovery, the cloud has made our daily operations almost easy.
Considering such a challenging task as managing disaster recovery operations, the cloud has made us think how difficult it was to perform such operations before its appearance.
If a disaster affected the primary data centre, a backup data centre had to be provided, which would imply double operations including [3]:

» creating a physical location and facilities for IT infrastructure;
» appointing a contact person and security staff for adjustment procedures;
» enhancing server capacity for storing data and adjustments to the app scaling requirements;
» providing ancillary staff for infrastructure maintenance;
» providing the Internet connection of sufficient passband for the application to start;
» network infrastructure adjustments, including firewall, load balancers, routers and switches.

This would add to increasing costs and resources that could not be managed, leaving only a data centre as an only backup copy.

Figure 1. Steps in the Disaster Recovery Plan Creation [4].

The project Cloud Disaster Recovery offers organisations several benefits, including the following[5]:

» saving up time/capital;
» more options for backup copy locations;
» implementation simplicity with high reliability;
» flexibility.

Organisations that consider disaster recovery in the cloud for the first time and wonder where to start will find below a simple recovery plan that can help create an efficient disaster recovery strategy:

Cloud Disaster Recovery Plan – figure 1

Step 1: Understanding your own infrastructure and predicting risks

It is necessary to consider the IT infrastructure of a company, including property, equipment and data the company possesses. Also, it is necessary to establish where all these are located and how valuable they are. When the evaluation of the property is completed, risks that can affect it have to be estimated. Risks may include natural disasters, data theft, power cut etc. When the estimation is completed, the company can more efficiently design its Disaster Recovery Plan (DRP) to eliminate/minimise these risks.

Step 2: Performing a business impact analysis

A business impact analysis is the next step to do. This will enable the company to understand the limitations of its operations in case of disaster.

The following two parameters will help the company evaluate this factor:

» recovery time objective (RTO);
» recovery point objective (RPO).

The parameters relevant for data loss risk evaluation are:

a) Recovery Time Objective (RTO)

The RTO is the maximum amount of time in which a particular app can be outside the network before such an occurrence starts affecting business operations.

Scenario 1: If a company is dedicated to providing services promptly, the app failure can incur a lot of costs. The company will have to invest considerable funds in a DR plan if it wants to continue business operations in a matter of minutes.

Scenario 2: If a company operates at a moderate pace, even though a disaster affects its operations, the company can still find alternative ways for conducting its business activities. It can set its RTO to a week's time. In such a case, the company will not have to invest a lot of resources into disaster recovery funds, which in turn will save enough time for providing sufficient backup resources after a disaster. Knowing your company's RTO is very important as it corresponds to the number of resources that have to be included in the DR plan because the time lost regarding the RTO can be used for gathering backup resources.

b) Recovery Point Objective (RPO)

The RPO is the maximum amount of time in which data loss for a particular app is acceptable in case of a great crisis. The points to be considered for establishing the RPO are[1]:

» a possible data loss in case of disaster;
» a possible time span before data is compromised.

If the above-mentioned scenario 1 is considered, the RPO cannot last more than 5 minutes, as the business operations are critical and cannot afford more than such a short downtime. Regarding Scenario 2, the company may wish to create its backup copy; however, as its data is not time-sensitive, the company will not need to invest a lot in its DR plan.

Step 3: Designing a DR plan based on RPO and RTO

Once a company has defined its RPO and RTO, it can focus on designing its system which will fulfil the goals of a DR plan. To implement a DR plan, the above-listed approaches can be considered [3]:

» making a backup copy and restoring the previous condition;
» Pilot Light Approach;
» warm alert state;
» a complete replication in the cloud;
» Multi-Cloud option.

It is possible to apply the combination of these approaches in the way they benefit a company's operation best, in accordance with its particular business requirements.

Step 4: Approaching the right partner in the cloud

Upon making a decision regarding the approach, the next step should be looking for a reliable service provider in the cloud that can help with implementation. If a company plans a complete replication in the cloud, it will probably want to consider the following factors before selecting the ideal service from the cloud supplier[5]:

» reliability;
» recovery speed;
» applicability;
» simplicity of adjustment and recovery;
» flexibility;
» compliance with security rules and procedures;
» factors for evaluation of an ideal cloud provider.

All the major services in the cloud providers, including AWS, Microsoft Azure, Google Cloud and IBM, have DR options. Apart from these big companies, there are also medium and small firms that offer a high-quality disaster recovery service (DRaaS).

Step 5: Building your own Cloud DR infrastructure

Having consulted its DR in the cloud partner, a company may work with a service provider on the implementation of its own DR infrastructure design and adjustments. Based on the selected DR approach the company has made, there are several logistics aspects to be considered [2]:

» How many infrastructure components will a company need?
» What is the method of data replication in the cloud?
» What are the best methods for user authentication and access management?
» What are the safety measures the company will undertake to reduce the possible risk of disaster?

It is necessary to ensure that the company's DR strategy is in compliance with its RTO and RPO specification so the business operations can run uninterrupted.

Step 6: Presenting a disaster recovery plan as a hard copy

It is important to have standard guidelines or a diagram of the process flow with specific instructions for all parties included in the DR. Should a disaster happen, each individual has to be ready to accept his/her responsibility corresponding to his/her role in the DR process. Moreover, all the instructions, in minute detail, have to be clearly explained in a hard copy. These steps ensure the DR plan's efficiency.

Step 7: Frequent testing of the DR plan

After providing a hard copy of the DR plan, the next step is frequent testing of the plan. This helps to ensure that there are no oversights in it. As a hard copy version, the plan may seem to be a comprehensive one, but the company can realise how reliable that plan is only after it has been tested.

VI. CONCLUSION

This paper demonstrates how computing in the cloud is becoming important in our daily life. Therefore, the majority of companies are based on cloud computing. They need to be aware of disasters in the cloud. When a disaster happens, all the companies face great losses, financial but also loss of data, which is the reason why disaster recovery mechanisms are introduced.

The recent research has demonstrated the importance of having a DR plan, which is supported by the information that each dollar invested in risk mitigation, e.g. a DRP, in the long run, saves up 4 dollars for the company. Therefore, it is clear that each company that conducts its business operations in a responsible manner and cares about its reputation, should approach, and perhaps, has to approach its DRP responsibly in order to protect its most valuable assets, i.e data.

BIBLIOGRAPHY

1. Abedallah Z. A., Alwan A. A., Gulzar Y. Disaster Recovery in Cloud Computing Systems: An Overview. International Journal of Advanced Computer Science and Applications; 2020; 11(9): 702–710.
2. Fox R. & Hao W. Internet Infrastructure: Networking, Web Services, and Cloud Computing. CRC Press Taylor & Francis Group. 2018. ISBN: 978-1-1380-3991-9
3. https://cloud.google.com/architecture/dr-scenarios-planning-guide (pristupano: 8. 1. 2022)
4. https://see.asseco.com/banking-and-finance/security-other-services/infrastructure-services/disaster-recovery-as-a-service-draas-607/ (pristupano: 8. 1. 2022)
5. Jaiswal V., Sen A., Verma A. Integrated Resiliency Planning in Storage Clouds. IEEE Transactions on Network and Service Management; 2014; 11(1): 3–14.

Stručni članci / Professional articles

Vrsta rada: Osvrti
Primljen: 25. 2. 2022.
Prihvaćen: 1. 5. 2022.
UDK:

Osvrt: Open access baze i repozitorijumi

Prof. dr Valentin Kuleto[1]

[1]Visoka škola strukovnih studija za informacione tehnologije, ITS - Beograd, Srbija; valentin.kuleto@its.edu.rs

Open access (OA, otvoreni pristup) je izdavački model za naučnu komunikaciju koji čini istraživačke informacije dostupnim čitaocima bez ikakvih troškova, za razliku od tradicionalnog modela pretplate, u kojem čitaoci imaju pristup naučnim informacijama tako što plaćaju pretplatu (obično preko biblioteka ili obrazovnih afilijacija).

Otvoreni pristup podrazumeva besplatan, neograničen i slobodan pristup objavljenim naučnim radovima, knjigama, akademskim časopisima i doktorskim disertacijama. Inicijativa pokreta za otvoren pristup nastala je kao bunt zbog činjenice da se rezultati istraživanja koja finansiraju naučni instituti, odnosno univerziteti, publikuju u komercijalnim časopisima sa pretplatama koje bi morale da plaćaju te iste institucije koje su finansirale istraživanje. Zainteresovani za publikovanje u časopisima otvorenog pristupa moraju imati u vidu da postoje različiti načini objavljivanja otvorenog pristupa, a neki od njih podrazumevaju i plaćanje naknade za objavu radova (APC).

Open access baze i repozitorijume mogu koristiti svi koji sprovode različita naučna, stručna, umetnička ili akademska istraživanja, uključujući i učenike i studente, prema svojim potrebama, najbolje uz preporuku nastavnika, odnosno mentora.

Jedna od najvažnijih prednosti otvorenog pristupa je da povećava vidljivost i korišćenje rezultata akademskog istraživanja. Principi otvorenog pristupa su navedeni u Berlinskoj deklaraciji o otvorenom pristupu znanju u prirodno-matematičkim i humanističkim naukama. Ovu deklaraciju su potpisale mnoge međunarodne organizacije za akademska istraživanja. Glavna teza koja opravdava ove napore glasi: **Naša misija širenja znanja je samo napola završena ako informacije nisu široko i lako dostupne društvu.**

KAKO FUNKCIONIŠU OPEN ACCESS BAZE

Brojne open access baze i repozitorijumi omogućavaju istraživačima besplatan pristup časopisima i člancima koji su ili u formi apstrakta ili celokupnog teksta. Na taj način i istraživači koji nemaju pristup plaćenim naučnim bazama mogu u velikom broju pristupati člancima i časopisima, odnosno rezultatima naučnoistraživačkog rada drugih istraživača. Spisak časopisa sa potpuno otvorenim pristupom koji su dostupni širom sveta možete naći na veb-stranici DOAJ, na linku: https://doaj.org/. Brojne su open access baze, repozitorijumi i drugi sajtovi koji, takođe, nude mogućnost besplatnog pristupa člancima. Pomenućemo samo neke od njih:

- SSOAR https://www.gesis.org/ssoar/home
- SCIndeks https://scindeks.ceon.rs/
- SSRN https://www.ssrn.com/index.cfm/en/
- OpenDOAR https://v2.sherpa.ac.uk/opendoar/
- ROAR http://roar.eprints.org/

Mentori svojim učenicima i studentima često preporučuju i **Google Scholar** kao veb-pretraživač. Google Scholar je slobodno dostupan veb-pretraživač koji indeksira pun tekst ili metapodatke naučne literature u nizu izdavačkih formata i disciplina. Obuhvata većinu recenziranih onlajn akademskih časopisa i knjiga, konferencija, teza i disertacija, preprinta, sažetaka, tehničkih izveštaja i druge naučne literature, uključujući sudska mišljenja i patente. Google Scholar obezbeđuje veze tekstova ka objavljenim verzijama i glavnim repozitorijumima otvorenog pristupa, uključujući i one objavljene na pojedinačnim veb-stranicama fakulteta i drugim nestrukturiranim izvorima.

Srpski citatni indeks (SCIndeks) je besplatan internet servis otvorenog pristupa. SCIndeks je servis u okviru kog se referišu domaći časopisi kategorizovani kao periodične publikacije naučnog karaktera. Svi časopisi indeksiraju se sistematski od korica do korica. Pored naslova i sažetaka radova, metapodatke u SCIndeksu čine i sve citirane reference. Većina članaka novijeg datuma dostupna je u vidu punog teksta. Servisu se može pristupiti i bez registracije putem linka SCIndeks https://scindeks.ceon.rs/, dok registracija (koja je besplatna) donosi brojne funkcionalnosti koje vam mogu koristiti u pretraživanju, sistematizaciji i čuvanju rezultata pretrage.

Uvek treba imati u vidu da bavljenje akademskim i naučnoistraživačkim radom nije privilegija bogatih pojedinaca – istraživača i institucija sa projektnim i institucionalnim finansiranjem. **Nauka je privilegija erudita, socijalno uključenih individua koje žele da učine svet boljim mestom.**

Vrsta rada: Overview
Primljen: 25. 2. 2022.
Prihvaćen: 1. 5. 2022.
DOI: https://doi.org/10.18485/edtech.2022.2.2.6
UDK:

Overview: Open Access Databases and Repositories

Prof. dr Valentin Kuleto[1]

[1]Information Technology School, ITS-Belgrade, Belgrade, Serbia; valentin.kuleto@its.edu.rs

Open Access (OA) is a publishing model for scholarly communication that makes research information available to readers at no cost, as opposed to the traditional subscription model in which readers have access to scholarly information by paying a subscription (usually via libraries or educational associations).

Open Access means free, unrestricted and open access to published scientific works, books, academic journals and doctoral dissertations. The initiative of the open access movement arose as a rebellion due to the fact that the results of research funded by scientific institutes, i.e. universities, are published in commercial journals with subscriptions that would have to be paid by the same institutions that funded the research. Those interested in publishing in open access journals must keep in mind that there are different ways of publishing open access, and some of them involve paying a publication fee (APC – article processing charges).

Open Access Databases and Repositories can be used by everyone who conducts various scientific, professional, artistic or academic research, including pupils and students, according to their needs, preferably with the recommendation of a teacher or mentor.

One of the most important advantages of open access is that it increases the visibility and reuse of academic research results. The principles of open access are set out in the Berlin Declaration on Open Access to Knowledge in the Sciences and Humanities. This declaration has been signed by many international organisations for academic research. The main thesis that justifies these efforts is: **Our mission of spreading knowledge is only half finished if the information is not widely and easily available to society.**

HOW OPEN ACCESS DATABASES WORK

Numerous open access databases and repositories provide researchers with free access to journals and articles in either abstract or full-text form. In this way, even researchers who do not have access to paid scientific databases can access a large number of articles and journals, that is, the results of the scientific research work of other researchers. A list of Full Open Access journals available worldwide can be found on the DOAJ website at the link: https://doaj.org/. There are numerous open access databases, repositories and other websites that also offer the possibility of free access to articles. We will mention only a few of them:

- SSOAR https://www.gesis.org/ssoar/home
- SCIndeks https://scindeks.ceon.rs/
- SSRN https://www.ssrn.com/index.cfm/en/
- OpenDOAR https://v2.sherpa.ac.uk/opendoar/
- ROAR http://roar.eprints.org/

Mentors often recommend **Google Scholar** as a web search engine to their students. Google Scholar is a freely accessible web search engine that indexes the full text or metadata of scholarly literature across an array of publishing formats and disciplines. The Google Scholar index includes most peer-reviewed online academic journals and books, conference papers, theses and dissertations, preprints, abstracts, technical reports, and other scholarly literature, including court opinions and patents. Google Scholar provides links to both published versions and major open access repositories, including those posted on individual faculty web pages and other unstructured sources.

Serbian Citation Index (SCIndeks) is a free, open access internet service. SCIndeks is a service that covers all locally published journals classified as periodicals of scientific character. All of the journals are indexed systematically on a cover-to-cover basis. In addition to titles and abstracts of works, SCIndeks contains references/citations (metadata) for all articles. Most recent articles are available as full texts. The service can be accessed without registration via the link SCIndeks https://scindeks.ceon.rs/, while registration (which is free) brings numerous functionalities that can be useful for searching, systematising and saving search results.

We should always have in mind that engaging in academic and scientific research work is not the privilege of rich individuals – researchers and institutions with a project and institutional funding. **Science is the privilege of erudite, socially engaged individuals who want to make the world a better place.**

EdTech JOURNAL

linkgroup

linkgroup Educational Alliance

Institut za moderno obrazovanje
Institute for Contemporary Education

CIP -Katalogizacija u publikaciji Narodna biblioteka Srbije, Beograd

371.3
004.9:37

EDTECH Journal : naučni časopis za savremeno obrazovanje i
primenu informacionih tehnologija = scientific Journal for contemporary
education and application of information technologies / glavni i odgovorni
urednik Valentin Kuleto. - [Štampano izd.]. - Vol. 1, br. 1 (2021)- . -
Beograd : Institut za moderno obrazovanje, 2021- (Beograd : Jovšić
printing centar). - 36 cm

Godišnje. - Tekst na srp. i engl. jeziku. -
Ima izdanje na drugom jeziku: EdTech Journal (Online) = ISSN 2812-8761
ISSN 2812-8753 = EdTech Journal (Štampano izd.)
COBISS.SR-ID 59423497