

UNIVERSITATEA BABEȘ-BOLYAI CLUJ-NAPOCA  
FACULTATEA DE MATEMATICĂ ȘI INFORMATICĂ  
SPECIALIZAREA INFORMATICĂ

## LUCRARE DE LICENȚĂ

### Aplicații de rețele sociale

Conducător științific  
Lect. Dr. Lazăr Ioan

*Absolvent*  
*Suciu Sergiu-Eduard*

2024



---

## ABSTRACT

---

A project involves complex actions pursued by individuals or groups to achieve specific goals. These actions are composed of various activities whose completion is crucial for reaching the project's objectives. Factors like time, resources, and knowledge influence the completion of these activities, making the project more complex as more factors are considered. Consequently, managing the project becomes more challenging, reducing the likelihood of achieving the desired outcomes.

Therefore, having a well-structured plan is essential for successful project completion. This plan outlines how resources are utilized, activities are scheduled, and goals are pursued. Given the significance of projects in modern life, extensive research has been conducted to address various issues in project planning.

In the first chapter, which also serves as the introduction, I discussed the issues that I will address in the paper, as well as the project's goals and objectives. This section provided a solid foundation for understanding the context and overall direction of the research.

In the second chapter, I made a comparison between various social networks and discussed communication protocols, which are essential aspects for the development of my application. I analyzed how different social networks function and explored the necessary protocols to ensure efficient communication within the application. In the third chapter, I addressed social network security, discussing common security issues and the measures we can take to protect ourselves. I presented concrete examples of vulnerabilities and offered solutions to minimize the risks associated with using social networks.

In the fourth chapter, I detailed my thesis and the implementation process of the application. I described the technologies used and explained the steps taken to develop and complete the project. This section provided a detailed look at how theory is applied in practice, demonstrating the integration of knowledge accumulated in the previous chapters. Therefore, the project's structure facilitated a comprehensive and integrated approach, providing a profound understanding of social networks, security issues, and the technologies used to develop an efficient and secure application.

This work is the product of my own efforts. I have neither given nor received unauthorized assistance in completing it.

# Cuprins

<b>1</b>	<b>Introducere</b>	<b>1</b>
1.1	Context și importanță . . . . .	1
1.2	Probleme abordate . . . . .	2
1.3	Scopul și obiectivele lucrării . . . . .	3
<b>2</b>	<b>Rețele sociale</b>	<b>5</b>
2.1	Introducere . . . . .	5
2.2	Tipuri de rețele sociale . . . . .	6
2.3	Istoria rețelelor de socializare . . . . .	7
2.4	Protocoale de comunicare . . . . .	9
2.4.1	Protocoale de comunicare cu fir . . . . .	9
2.4.2	Protocoalele de comunicare fără fir . . . . .	10
<b>3</b>	<b>Securitatea rețelelor sociale</b>	<b>12</b>
3.1	Introducere . . . . .	12
3.2	Vulnerabilități de securitate . . . . .	13
3.2.1	Cross-Site Request Forgery . . . . .	13
3.2.2	Cross-site scripting . . . . .	14
3.2.3	SQL injection . . . . .	15
3.3	Tehnici de atac . . . . .	16
3.3.1	Clickjacking . . . . .	17
3.3.2	Session Hijacking . . . . .	18
3.3.3	Man-in-the-Middle (MitM) . . . . .	19
<b>4</b>	<b>Proiect</b>	<b>21</b>
4.1	Analiză . . . . .	21
4.2	Proiectare . . . . .	25
4.3	Tehnologii și Framework-uri . . . . .	30
4.4	Backend . . . . .	31
4.4.1	C# . . . . .	31
4.4.2	.NET . . . . .	32

4.4.3	Entity Framework . . . . .	32
4.5	Frontend . . . . .	33
4.5.1	Typescript . . . . .	33
4.5.2	React.js . . . . .	34
4.5.3	Next.js . . . . .	34
4.5.4	MaterialUI . . . . .	35
4.6	Baza de date . . . . .	35
4.7	Manual de utilizare . . . . .	36
<b>5</b>	<b>Concluzii</b>	<b>46</b>
	<b>Bibliografie</b>	<b>47</b>

# Capitolul 1

## Introducere

### 1.1 Context și importanță

Rețelele sociale au cunoscut o ascensiune rapidă în ultimele decenii, evoluând de la simple platforme de comunicare la complexe ecosisteme digitale care influențează toate aspectele vieții umane. La finalul anilor 1990, site-uri precum SixDegrees (1997) și Friendster (2002) au deschis calea pentru conectarea utilizatorilor pe baza intereselor comune. Cu toate acestea, adevărata explozie a rețelelor sociale a avut loc odată cu apariția Facebook în 2004, aducând standarde noi în interactivitate și partajarea de conținut între utilizatori. Pe parcursul anilor, platforme precum Twitter (2006), Instagram (2010) și Snapchat (2011) au adus diversitate în peisajul rețelelor sociale, introducând noi funcționalități și evidențiind importanța mediului mobil. Potrivit unui studiu de caz realizat de către Brooke Auxier și Monica Anderson [Bro], se poate observa că aproximativ 72% dintre americani folosesc cel puțin o platformă de rețea de socializare, iar la nivel global, numărul utilizatorilor de rețele sociale a depășit 4.59 miliarde în 2022, și tinde să crească spre aproape 6 miliarde până în 2027, conform Statista într-un articol publicat de către Stacy Jo Dixon [Sta].

În prezent rețelele de socializare nu s-au limitat doar la creșterea interacțiunii sociale, ci au demonstrat capacitatea lor de a influența evenimente majore, precum mișcările politice și campaniile electorale, ca în timpul Primăverii Arabe din 2011 studiu realizat de către Reda Benkirane în *The Alchemy of Revolution: The Role of Social Networks and New Media in the Arab Spring* [Ben12].

Totodată, rețelele sociale sunt esențiale și pentru afaceri și educație, acestea făcând mai ușoară atât comunicarea între persoane cât și partajarea materialelor didactice necesare studierii. Conform articolului realizat de către Casimir C. Barczyk și Doris G. Duncan [BD11], s-a realizat un studiu conform căruia rețelele sociale au schimbat modul în care se colaborează în mediul academic și în domeniul Managementului Resurselor Umane (MRU), eliminând barierele existente și facilitând conexiu-

nile globale. Aceste platforme permit studenților și cercetătorilor să colaboreze și să comunice fără probleme, depășind limitele geografice. În plus, în organizații, social media este folosită pentru recrutare, interacționarea cu angajații și dezvoltarea profesională. În cadrul cursurilor de MRU, integrarea mediilor de socializare este crucială pentru pregătirea angajaților pentru cerințele pieței actuale. Astfel, rețelele sociale devin un instrument esențial pentru schimbul de informații, stimularea discuțiilor și îmbunătățirea relațiilor cu angajații.

Prin urmare, dezvoltarea unei noi aplicații de rețele sociale în acest context nu este doar relevantă, ci și crucială pentru a răspunde nevoilor în continuă evoluție ale utilizatorilor și pentru a exploata noile tehnologii emergente. Aceasta ar putea oferi soluții îmbunătățite pentru probleme actuale precum gestionarea confidențialității datelor și combaterea dezinformării, contribuind astfel la un mediu digital mai sigur și mai constructiv.

## 1.2 Probleme abordate

Avansul rapid al tehnologiei digitale și extinderea rețelelor sociale au modificat în mod fundamental interacțiunile sociale și modul în care avem acces la informație. În acest context, problema abordată în această lucrare se concentrează pe nevoia de a dezvolta o aplicație de rețele sociale care să răspundă în mod eficient cerințelor și preocupărilor utilizatorilor din zilele noastre.

Coform [RSL<sup>+</sup>17], unul dintre principalele aspecte care necesită atenție în dezvoltarea acestei aplicații este creșterea volumului de informații și de dezinformare. Cu o cantitate vastă de conținut disponibilă online, utilizatorii se confruntă adesea cu dificultatea de a naviga prin mulțimea de informații și de a identifica sursele de încredere, astfel făcându-i pe acestia ținte atractive pentru atacuri cibernetice, incluzând spam, malware, socialbots.

Pe lângă aceasta, preocupările legate de protecția datelor personale și securitatea informațiilor reprezintă un alt aspect important în cadrul rețelelor sociale, neglijența acestui aspect putând să ducă la furtul de identitate a unui utilizator. Într-o eră în care datele personale sunt adesea colectate și folosite fără consimțământul explicit al utilizatorilor, este esențial să dezvoltăm soluții care să asigure o protecție adecvată a confidențialității și securității informațiilor personale.

Alte două aspecte importante pe care le regăsim în articolul [Hay14], de care ar trebui să ținem cont este experiența utilizatorilor pe aplicație (UX) și interfața cu care aceștia interacționează (UI). Aceste aspecte menționate mai sus pot constitui o problemă majoră în rândul aplicațiilor din ziua de azi, având în vedere că rețele de socializare sunt folosite de toate categoriile de vârstă. După cum reiese și din articolul [QRA<sup>+</sup>20], aceste aspecte sunt importante deoarece multitudinea de date cu care

se înglobează interfața utilizatorului poate provoca confuzie în rândul utilizatorilor, astfel rectificarea acestora poate duce la îmbunătățirea experienței utilizatorilor, creșterea adopției și retenției și accesibilitate universală.

## 1.3 Scopul și obiectivele lucrării

Scopul acestei lucrări este de a proiecta, dezvolta și evalua o aplicație de rețele sociale inovatoare, care să aducă o contribuție semnificativă în domeniul interacțiunilor online și să răspundă nevoilor actuale ale utilizatorilor. În mod specific, se urmărește crearea unei platforme care să ofere o experiență interactivă și angajantă, bazată pe cele mai recente tehnologii și bune practici de design și dezvoltare software. Această aplicație va fi concepută pentru a promova comunicarea autentică, conexiunile interpersonale și participarea comunitară, contribuind astfel la crearea unui mediu online mai pozitiv și mai îmbogățit pentru utilizatori.

Pe lângă scopul lucrării, obiectivele reprezintă motivația acesteia, fiind acțiunile necesare pentru realizarea aspirațiilor propuse sau a problemelor abordate. Obiectivele acestei lucrări sunt următoarele:

### 1. Analiza nevoilor utilizatorilor

Analiza profundă a nevoilor utilizatorilor în ceea ce privește rețelele sociale este crucială pentru dezvoltarea unei platforme care să răspundă eficient și eficace cerințelor acestora. Prin intermediul studiilor de piață, sondajelor și analizelor de date, putem investiga în profunzime pentru a înțelege cu adevărat ce își doresc utilizatorii de la o rețea socială și cum putem să le satisfacem aceste dorințe. De exemplu, un studiu de piață amănunțit poate dezvălui că utilizatorii doresc o platformă care să le ofere un mediu sigur pentru a interacționa cu prietenii și familia, dar și să le ofere posibilitatea de a descoperi și conecta cu persoane noi pe baza intereselor comune. De asemenea, putem identifica tendințe și comportamente de utilizare care să ne ajute să proiectăm funcționalități și caracteristici care să răspundă nevoilor și preferințelor utilizatorilor.

### 2. Inovare în funcționalitate și design

Inovarea în funcționalitate și design este esențială pentru a păstra utilizatorii angajați și interesați de o platformă de socializare. Aceasta implică nu numai implementarea unor caracteristici și facilități noi, ci și proiectarea unei interfețe atractivă și intuitive care să ofere o experiență plăcută și captivantă utilizatorilor. De exemplu, putem să introducem funcții inovatoare, cum ar fi chat-ul video în timp real sau un bot AI interactiv, care să aducă valoare adăugată



experienței utilizatorilor și să îi încurajeze să revină pe platformă în mod regulat. În același timp, putem să ne concentrăm pe designul interfeței utilizator pentru a o face ușor de navigat și plăcută din punct de vedere vizual, folosind culori, fonturi și elemente grafice care să sporească atractivitatea și intuitivitatea.

### 3. Securitate și protecția datelor

Asigurarea securității și protecției datelor personale ale utilizatorilor este o prioritate absolută în dezvoltarea unei rețele sociale de succes. Implementarea unor măsuri robuste de securitate cibernetică, cum ar fi criptarea datelor sensibile, autentificarea puternică a utilizatorilor și monitorizarea activității neautorizate, este esențială pentru a preveni accesul neautorizat și exploatarea datelor personale. De exemplu, putem să folosim tehnologii avansate de criptare pentru a proteja mesajele și datele utilizatorilor împotriva interceptării și accesului neautorizat, și putem să implementăm controale stricte de securitate pentru a preveni eventualele amenințări cibernetice. Este important să oferim utilizatorilor încrederea că datele lor sunt în siguranță și că pot utiliza platforma fără griji în ceea ce privește securitatea și confidențialitatea informațiilor lor personale.

### 4. Evaluare și feedback continuu

Colectarea și analizarea continuă a feedback-ului utilizatorilor sunt esențiale pentru a înțelege nevoile și preferințele acestora și pentru a îmbunătăți constant experiența pe platformă. Prin intermediul testelor de utilizabilitate, sondajelor de satisfacție și analizelor de date, putem identifica punctele forte și slabe ale aplicației și putem lua măsuri pentru a îmbunătăți continuu experiența utilizatorilor. De exemplu, un sondaj de satisfacție detaliat ar putea evidenția aspectele care sunt apreciate de utilizatori și aspectele care necesită îmbunătățiri, iar aceste informații ar putea fi folosite pentru a ghida dezvoltarea viitoare a aplicației. Este important să demonstrăm că luăm în serios feedback-ul utilizatorilor și că suntem dedicați îmbunătățirii continue a platformei pentru a răspunde nevoilor și așteptărilor lor în continuă schimbare.

# Capitolul 2

## Rețele sociale

### 2.1 Introducere

Rețelele sociale sunt construite pe baza profilurilor personale, facilitând utilizatorilor să-și prezinte identitatea și interesele lor. Aceste profiluri devin nodurile unei rețele complexe de conexiuni, permițând oamenilor să se conecteze cu alții din întreaga lume prin mesaje, postări și comentarii.

Deși inițial văzute ca simple platforme de divertisment și socializare, aceste rețelele au devenit instrumente esențiale pentru schimbul de informații și dezvoltarea personală. Ele au un impact semnificativ asupra activității sociale, permițând oamenilor să descopere informații importante și să participe la discuții despre probleme sociale. De asemenea, acestea au generat schimbări semnificative în peisajul economic și cultural, devenind instrumente esențiale pentru marketing și promovare pentru afaceri de toate dimensiunile.

Cu toate acestea, există și unele dezavantaje ale rețelelor sociale. Probleme precum dependența de tehnologie, scăderea calității relațiilor interpersonale offline și preocupările legate de confidențialitatea datelor necesită atenție și reglementare. Este esențial să găsim un echilibru între utilizarea rețelelor sociale și viața offline, prioritarizând relațiile autentice și responsabilitatea online.

Utilizatorii trebuie să fie conștienți de impactul pe care îl au rețelele de socializare asupra lor și asupra celor din jur, consumând și distribuind informații cu grijă și având o atitudine responsabilă în mediul online. Este important ca societatea să exploreze și să dezvolte modalități de reglementare și gestionare a utilizării rețelelor sociale pentru a promova bunăstarea și progresul comun. Implementarea unor politici și legi care protejează confidențialitatea datelor și combat dezinformarea, împreună cu promovarea unor practici de utilizare sănătoase și etice, sunt imperative pentru asigurarea unui mediu online pozitiv și sigur.

## 2.2 Tipuri de rețele sociale

Rețelele sociale joacă un rol crucial în lumea interconectată de astăzi, modelând modul în care persoanele interacționează, își împărtășesc informațiile și își construiesc relațiile. Când vorbim despre tipurile de rețele sociale, le putem categorisi în funcție de diverse criterii, cum ar fi scopul lor, structura și funcționalitatea lor.

O modalitate de a clasifica rețelele sociale este după scopul lor. De exemplu, unele rețele sociale sunt concepute pentru networking-ul profesional, cum ar fi LinkedIn, unde utilizatorii se conectează cu colegii și profesioniștii din industrie pentru a-și îmbunătăți oportunitățile de carieră [MW11]. Pe de altă parte, platforme precum Facebook, Instagram și Twitter sunt mai concentrate pe conexiunile personale, împărtășind actualizări, fotografii și interacționând cu prietenii și urmăritorii.

O altă modalitate de a clasifica rețelele sociale este după structura lor. Unele rețele sunt bazate pe legături puternice, reprezentând relații strânse cu familia și prietenii, în timp ce altele sunt construite pe legături slabe, conectând indivizii cu cunoștințe și colegi [Val10]. Facebook, cu accentul său pe conectarea cu persoanele pe care le cunoști deja, se încadrează mai mult în categoria legăturilor puternice. În contrast, Twitter, cu natura sa deschisă și publică, tinde să faciliteze legăturile slabe, permițând utilizatorilor să urmărească și să interacționeze cu o gamă largă de persoane, inclusiv străini și celebrități. Instagram, cunoscut pentru conținutul său vizual și povestirea prin imagini și videoclipuri, oferă o platformă unică pentru utilizatori să se exprime creativ [Zag13]. Spre deosebire de Facebook și Twitter, accentul Instagramului pe comunicarea vizuală stimulează un tip diferit de angajament și interacțiune între utilizatori. Accentul platformei pe estetică și povestirea vizuală o deosebește de natura bogată în text a Twitter-ului și de partajarea mai cuprinzătoare a conținutului pe Facebook.

Atunci când comparăm cele trei rețele de socializare, este esențial să luăm în considerare și tipurile de interacțiuni și conținuturile pe care le prioritizează.

- Facebook, este una dintre primele și cele mai utilizate rețele sociale. Aceasta oferă o gamă largă de funcționalități pentru partajarea actualizărilor, fotografiilor, videoclipurilor și linkurilor [SLT10]. Utilizatorii pot să se conecteze cu prietenii, să se alăture grupurilor și să urmărească pagini în funcție de interesele lor. Fluxul de știri al platformei, bazat pe algoritmi, își propune să prezinte utilizatorilor conținut de la persoane și pagini cu care interacționează cel mai mult.
- Instagram se concentrează pe povestirea vizuală și pe estetică. Aceasta îl face o opțiune populară pentru partajarea fotografiilor și a videoclipurilor cu legende creative și hashtag-uri [Zag13]. Accentul platformei pe conținutul vizual a

transformat-o într-un centru pentru influenceri, branduri și creatori pentru a-și prezenta munca și pentru a interacționa cu o audiență orientată vizual. Pagina Explore și funcțiile de hashtag-uri ale Instagramului permit utilizatorilor să descopere conținut nou și să se conecteze cu persoane care au interese comune.

- Twitter este cunoscut pentru actualizările în timp real și pentru postările limitate la un număr de caractere, încurajează comunicarea rapidă și concisă între utilizatori [Val10]. Utilizarea de hashtag-uri, retweet-uri și menționări pe platformă permite descoperirea ușoară a subiectelor la modă și interacțiunea cu o audiență mai largă. Natura lea deschisă a Twitter-ului îl face o opțiune populară pentru diseminarea știrilor, conversații publice și networking cu persoane din afara cercului social imediat al utilizatorului.

## 2.3 Istoria rețelelor de socializare

Istoria dezvoltării aplicațiilor de rețele sociale este o călătorie fascinantă care a schimbat felul în care ne conectăm și interacționăm cu alții în epoca digitală. Site-urile de rețele sociale, așa cum le-au definit Ellison și Boyd în 2007, sunt servicii online care permit oamenilor să-și facă un profil public sau semi-public într-un sistem bine definit, să facă o listă cu alte persoane cu care sunt conectate și să vadă și să exploreze lista lor de conexiuni și a altora din sistem [BE07].

Evoluția rețelelor sociale poate fi urmărită încă de la începuturile internetului, când au apărut platforme precum SixDegrees.com la sfârșitul anilor 1990, care permiteau utilizatorilor să-și creeze profiluri și să se conecteze cu alții online. La începutul anilor 2000, platformele de socializare online au cunoscut o creștere exponențială. Această creștere a fost alimentată de apariția marilor platforme de socializare precum Facebook, Instagram, Twitter și Snapchat în jurul anului 2010 [MRCD17]. Aceste platforme au revoluționat modul în care oamenii se conectează între ei și își împărtășesc informațiile devenind o parte integrantă a vieții oamenilor de zi cu zi, în special pentru tineri, care le folosesc în diverse scopuri, cum ar fi partajarea de fotografii, videoclipuri, sentimente și păstrarea la curent cu evenimentele și tendințele actuale [DH19]. Acest moment a marcat debutul unei noi perioade în comunicare și interacțiune socială, deschizând drumul pentru dezvoltarea unor aplicații de rețele sociale mai avansate în decursul anilor.

Un aspect important al evoluției rețelelor sociale este analiza structurii și dinamicii lor. Cercetători precum Barabási, Jeong, Néda și Ravasz în 2002 au studiat rețeaua socială a colaborărilor științifice, descoperind că aceste rețele au proprietăți scale-free și se schimbă în timp [BJN<sup>+</sup>02]. Aceste cercetări au oferit informații importante despre modul în care rețelele sociale cresc și se modifică, evidențiind importanța

înțelegerii mecanismelor care stau la baza evoluției lor.

Diferite studii cum ar fi cel realizat de Kossinets și Watts în 2006, au contribuit, de asemenea, la înțelegerea evoluției rețelelor sociale. Analizând o rețea socială dinamică a studenților, aceștia au identificat că evoluția rețelei este influențată de diverse factori, inclusiv închiderea ciclurilor scurte de rețea [KW06]. Această cercetare subliniază natura complexă a dinamicii rețelelor sociale și necesitatea unei monitorizări și analize continue pentru a înțelege evoluția lor. Dezvoltarea analizei rețelelor sociale ca domeniu de studiu a jucat, de asemenea, un rol semnificativ în formarea evoluției aplicațiilor de rețele sociale. Lucrarea lui Freeman din 2011 evidențiază gama largă de aplicații ale analizei rețelelor sociale și importanța crescândă în diverse discipline [Fre11]. Prin furnizarea unui cadru pentru înțelegerea structurii și comportamentului rețelelor sociale, analiza rețelelor sociale a pregătit terenul pentru dezvoltarea unor instrumente și tehnologii mai avansate pentru studierea și valorificarea conexiunilor sociale.

Pe măsură ce rețelele sociale online au devenit din ce în ce mai răspândite, cercetătorii s-au concentrat pe studierea structurii și evoluției acestora. Kumar, Novak și Tomkins în 2006 au propus un model de atașament preferențial bazat pe evoluția rețelelor sociale online, aducând lumină asupra mecanismelor care stau la baza creșterii platformelor precum Flickr și Myspace [KNT06]. Înțelegerea modelelor structurale și a dinamicii evolutive a rețelelor sociale online este crucială pentru proiectarea de strategii eficiente pentru implicarea utilizatorilor și diseminarea conținutului.

În ultimii ani, domeniul analizei rețelelor sociale a cunoscut progrese semnificative în modele și metode. Carrington, Scott și Wasserman în 2005 au subliniat importanța cercetării și inovației continue în analiza rețelelor sociale, construind pe realizările anterioare și explorând noi direcții pentru studierea conexiunilor sociale [CSW05]. Prin dezvoltarea de modele și metode robuste, cercetătorii pot obține o înțelegere mai profundă a complexităților rețelelor sociale și a evoluției lor în timp. Provocările și oportunitățile prezentate de media socială au, de asemenea, modelat evoluția aplicațiilor de rețele sociale. Kaplan și Haenlein în 2010 au evidențiat rolul Web 2.0 ca platformă pentru evoluția mediilor sociale, accentuând natura colaborativă a interacțiunilor online și apariția unor noi rețele de comunicare [KH10]. Platformele de social media au revoluționat modul în care împărtășim informații, ne conectăm cu alții și ne implicăm în comunitățile online, conducând evoluția continuă a aplicațiilor de rețele sociale.

## 2.4 Protocoale de comunicare

Protocoalele de comunicare joacă un rol esențial în facilitarea interacțiunilor eficiente în cadrul sistemelor informatice. Aceste protocoale definesc regulile și convențiile pentru transmiterea datelor între dispozitive, asigurând o comunicare fără probleme. Modelul CCITT X.400, conform lui Dorregeest în articolul [vSD88], este un cadru fundamental pentru definirea serviciilor și protocoalelor de e-mail electronic, evidențiind importanța practicilor standardizate în manipularea mesajelor. Această combinație între modele teoretice și instrumente practice subliniază rolul critic al protocoalelor de comunicare în asigurarea unui flux eficient și fiabil al informațiilor.

În paralel, cercetarea menționată de Jong [dJS00] subliniază importanța metodelor de evaluare utilizate în protocoalele de comunicare. Validitatea metodelor de evaluare, compoziția și dimensiunea eșantionului, precum și implementarea rezultatelor sunt aspecte cruciale pentru evaluarea eficacității acestor protocoale. De asemenea, studiul abordat de Haak [VdHDJ03] explorează utilizarea protocoalelor de gândire în voce pentru testarea utilității în documentele de instruire și interfețele. Înțelegerea detaliilor diferitelor protocoale de comunicare și a metodelor de evaluare este esențială pentru asigurarea unui schimb eficient și fără probleme al informațiilor în medii diverse. Prin analizarea critică a acestor perspective, se pot obține informații în diversele strategii care pot fi folosite pentru a evalua și îmbunătăți protocoalele de comunicare. Prin investigații empirice și studii comparative, cercetătorii pot rafina înțelegerea lor a diferitelor protocoale de comunicare, contribuind în cele din urmă la structuri de comunicare mai eficiente și mai eficace în diferite domenii.

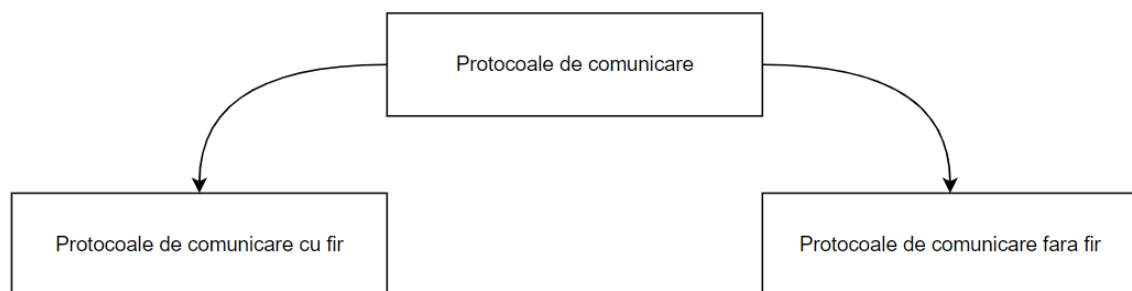


Figura 2.1: Tipuri de protocoale de comunicare

### 2.4.1 Protocoale de comunicare cu fir

Cercetarea în protocoalele de comunicare prin cablu joacă un rol fundamental în modelarea eficienței și fiabilității comunicațiilor în rețea. În timp ce rețelele fără fir domină adesea discuțiile în peisajele moderne de conectivitate, înțelegerea caracteristicilor și cerințelor distincte ale protocoalelor de comunicare prin cablu este cru-

cială. Rețelele Ad Hoc Mobile (MANETs) reprezintă un domeniu cheie în care nodurile fără fir formează dinamic rețele fără o administrație centralizată, necesitând protocoale de rutare robuste pentru a se adapta naturii dinamice a acestor rețele [AOS10]. Explorarea acestor domenii oferă informații valoroase în evoluția și complexitatea protocoalelor de comunicare, îmbunătățind în cele din urmă performanța rețelei și experiența utilizatorului.

### 2.4.2 Protocoalele de comunicare fără fir

Diverse tipuri de protocoale de comunicare fără fir joacă un rol critic în sistemele de rețelistică moderne, în special în rețelele Ad Hoc Mobile (MANETs) și rețelele de senzori fără fir (WSNs). Emergența MANETs, așa cum este descrisă în [AOS10], semnifică o schimbare către medii de comunicare dinamice și descentralizate, în care nodurile formează autonom rețele. În cadrul acestor rețele, alegerea protocoalelor de rutare este integrală pentru a permite căi de comunicare eficiente care să se adapteze naturii dinamice a rețelei.

Pe de altă parte, WSNs se confruntă cu provocarea de a optimiza acoperirea pentru a monitoriza eficient câmpurile de senzori, așa cum este evidențiat în [ESSH19]. Taxonomia propusă pentru protocoalele de acoperire în WSNs subliniază importanța protocoalelor care abordează optimizarea acoperirii la diferite etape ale rețelei. Pentru cercetătorii și practicienii din domeniul protocoalelor de comunicare fără fir, aceste studii aduc lumină asupra diverselor provocări și abordări în proiectarea unor sisteme de comunicare robuste și eficiente pentru arhitecturile de rețele variate.

Studiul protocoalelor de comunicare a arătat că există diverse tipuri disponibile, fiecare cu punctele sale forte și limitele sale. Înțelegerea acestor diferențe este crucială pentru a asigura o comunicare eficientă și sigură în diferite medii de rețea. Prin compararea caracteristicilor diferitelor protocoale, cum ar fi TCP/IP, HTTP, FTP, SMTP, POP3 și IMAP, devine evident că fiecare servește scopuri specifice și se adresează nevoilor distincte. În timp ce TCP/IP este esențial pentru a asigura fiabilitatea comunicației de la un capăt la altul, HTTP permite transferul de documente hiper-text peste web, iar FTP facilitează transferurile de fișiere. Extinzând această gamă de opțiuni, protocoalele specifice pentru e-mail, cum sunt SMTP, POP3 și IMAP, fiecare aduce funcționalități adaptate la necesități diferite ale utilizatorilor și organizațiilor.

- SMTP este esențial pentru trimiterea și livrarea mesajelor de e-mail între servere, având un rol crucial în fluxul de mesaje pe Internet. Este orientat pe mesaje și eficientizează livrarea de la un client la serverul destinatar, fără a oferi funcționalități de gestionare sau păstrare a mesajelor pe server. Fiind un standard IETF, SMTP este robust și larg acceptat în infrastructura globală de

e-mail.

- POP3 este un protocol simplu, orientat spre descărcarea și gestionarea locală a e-mailurilor, eliminând mesajele de pe server după descărcare. Este ideal pentru utilizatorii care accesează e-mailul de pe un singur dispozitiv, oferind un control complet asupra mesajelor stocate local.
- IMAP este un protocol care permite o gestionare mai flexibilă și avansată a e-mailurilor, păstrând mesajele pe servere, ceea ce permite utilizatorilor să le acceseze și să le sincronizeze de pe mai multe dispozitive. Este orientat spre acces și gestionare, facilitând o vizualizare consistentă a mesajelor indiferent de platforma utilizată.

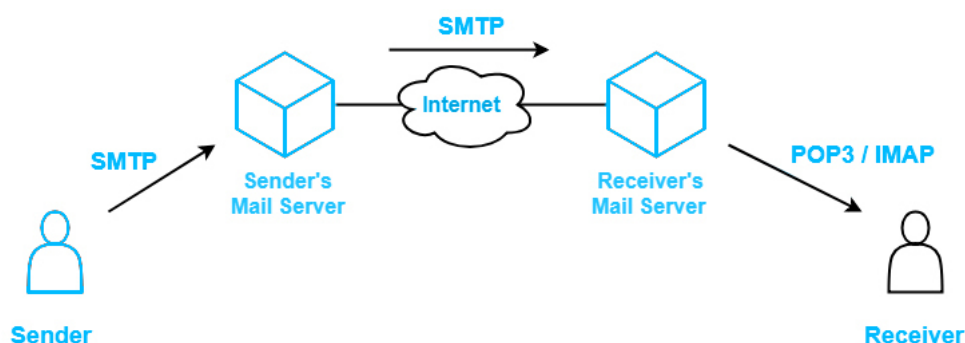


Figura 2.2: Protocoale de comunicare  
[ima]

În plus, evoluția protocoalelor de comunicare continuă să modeleze modul în care informația este schimbată și transmisă în rețele. Fiecare protocol își are locul său într-o structură de rețea bine planificată, asigurându-se că necesitățile de comunicare specifice sunt satisfăcute eficient și sigur.



# Capitolul 3

## Securitatea rețelelor sociale

### 3.1 Introducere

Securitatea în aplicațiile de rețele sociale este un aspect critic, dat fiind creșterea utilizării acestor platforme online. Protejarea datelor și a confidențialității utilizatorilor este esențială pentru a menține încrederea și pentru a contracara eventuale amenințări. Cercetătorii subliniază importanța abordării problemelor de securitate în mediul online al rețelelor sociale pentru a asigura protecția informațiilor utilizatorilor.

Una dintre cele mai mari preocupări în ceea ce privește securitatea rețelelor de socializare este protecția datelor personale. Multe platforme colectează o cantitate imensă de informații despre utilizatori, inclusiv date personale, preferințe, locație și chiar activități online. Aceste date pot fi expuse riscului de abuz sau furt de identitate, dacă nu sunt gestionate corespunzător și securizate eficient. Această problemă a fost reglementată prin adaugarea regulamentului General privind Protecția Datelor (GDPR). Regulamentul GDPR este o reglementare europeană semnificativă care își propune să îmbunătățească protecția datelor și confidențialitatea pentru persoanele din Uniunea Europeană și Spațiul Economic European. Aceasta înlocuiește Directiva privind Protecția Datelor, care a fost considerată inadecvată în atingerea unor standarde consistente de protecție a datelor în întreaga UE [VVdB17].

Un alt aspect important este securitatea cibernetică. Rețelele de socializare sunt adesea vizate de atacuri cibernetice, cum ar fi phishing-ul și hacking-ul.

- Atacurile de phishing implică adesea înșelarea persoanelor pentru a dezvălui informații confidențiale, cum ar fi datele de autentificare sau detalii financiare, folosindu-se de mascarea drept o entitate de încredere. O regulă crucială în cibernetică este să fii vigilent împotriva încercărilor de phishing, în special cele care ar putea proveni de la servere web compromise. Rămânând informat despre cele mai recente tactici de phishing și fiind precaut în interacțiunile

cu emailuri sau site-uri web suspecte, indivizii pot reduce riscul de a cădea victimă în astfel de atacuri [GTP22].

- Pe de altă parte, hacking-ul, care implică accesul neautorizat la sistemele de calcul sau rețele, reprezintă o amenințare gravă pentru securitatea cibernetică. Hackerii pot exploata vulnerabilitățile din sisteme pentru a efectua diverse activități malițioase, inclusiv găzduirea de pagini de phishing pe site-uri web legitime. Prin urmare, organizațiile și indivizii trebuie să prioritizeze măsuri de securitate cibernetică, cum ar fi actualizările regulate ale sistemului, folosirea unei parole puternice și monitorizarea rețelei pentru a preveni incidentele de hacking [Kos20].

## 3.2 Vulnerabilități de securitate

În mediul online, securitatea rețelilor de socializare este o preocupare centrală, pe măsură ce utilizatorii devin tot mai dependenți de aceste platforme pentru comunicare și interacțiune socială. Protejarea datelor personale și a confidențialității este crucială pentru a asigura un mediu online sigur și încrezător. Aceste platforme se confruntă cu diverse vulnerabilități de securitate, precum Cross-Site Request Forgery (CSRF), Cross-Site Scripting (XSS) și SQL Injection, care pot fi exploatare de către atacatori pentru a compromite integritatea și confidențialitatea datelor utilizatorilor.

### 3.2.1 Cross-Site Request Forgery

Cross-Site Request Forgery (CSRF) 3.1 este o vulnerabilitate de securitate întâlnită în aplicațiile web, care permite atacatorilor să manipuleze utilizatorii să execute acțiuni nedorite în numele lor pe site-uri unde aceștia sunt autentificați. Această problemă a fost subiectul unor numeroase studii și cercetări, deoarece poate avea consecințe grave pentru securitatea datelor și confidențialitatea utilizatorilor.

Pentru a contracara această amenințare, comunitatea de securitate informatică a dezvoltat mai multe strategii și tehnici. De exemplu, unele abordări implică utilizarea de token-uri speciale (CSRF tokens) pentru a valida cererile HTTP, astfel încât să fie mai dificil pentru atacatori să trimită cereri false în numele utilizatorilor [Agr23]. Alte metode includ detectarea automată a atacurilor CSRF folosind tehnici de învățare automată și analiză a datelor, precum și validarea strictă a cererilor pentru a asigura că acestea provin de la surse de încredere.

În plus, s-a acordat o atenție deosebită securității aplicațiilor JavaScript, deoarece acestea sunt susceptibile la atacuri CSRF din cauza naturii lor interactivă și a

dependenței de interacțiunea cu serverele web. Îmbunătățirea securității framework-urilor JavaScript și a implementării corecte a protecției CSRF în acestea a fost un obiectiv important al cercetării în domeniu [PC21].

Un alt aspect important al combaterii CSRF este utilizarea de cookie-uri Same-Site, care pot limita expunerea la acest tip de atacuri prin restricționarea trimerii cookie-urilor către alte site-uri. În timp ce aceste tehnici și strategii sunt eficiente în prevenirea atacurilor CSRF, este esențial să existe o conștientizare continuă a acestei vulnerabilități și a modurilor de protejare împotriva acesteia în comunitatea de dezvoltatori și utilizatori de aplicații web. De asemenea, sunt necesare eforturi continue pentru a identifica și remedia noi vulnerabilități și pentru a răspunde la evoluția tacticilor și tehnologiilor folosite de către atacatori.

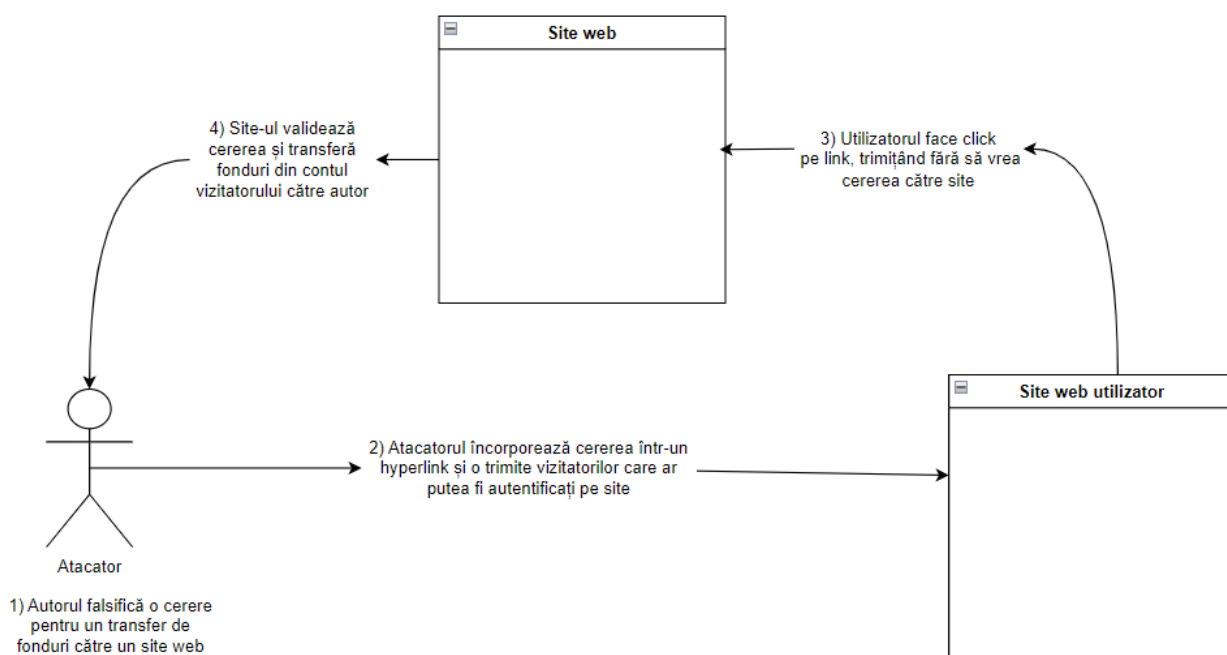


Figura 3.1: Cross-Site Request Forgery

### 3.2.2 Cross-site scripting

Cross-site scripting (XSS) este un tip de atac cibernetic care folosește breșe în aplicațiile web pentru a introduce scripturi malefice în pagini web, afectând utilizatorii care le vizualizează. Aceste scripturi pot fura date sensibile, vandaliza site-uri sau redirecționa utilizatorii către pagini periculoase.

Există două tipuri principale de XSS: cel reflectat, care apare prin URL-uri modificate, și cel stocat, care implică inserarea de scripturi direct în aplicație. Ambele pot cauza daune serioase și pun în pericol securitatea aplicațiilor web.

Pentru a realiza acest atac, atacatorul inserează cod JavaScript malițios în paginile web, iar acest cod este ulterior executat în browserul utilizatorilor care accesează

acele pagini. Atacatorul poate folosi această oportunitate pentru a fura cookie-urile de autentificare ale utilizatorilor, pentru a redirecționa utilizatorii către site-uri frauduloase sau pentru a compromite datele personale. În același timp victima trebuie să interacționeze cu site-ul în care este injectat codul JavaScript 3.2

Pentru a combate atacurile XSS, au fost dezvoltate tehnici de detecție și prevenție, inclusiv folosirea de algoritmi de învățare automată. Aceste tehnici se bazează pe cunoștințe despre amenințări și metode inteligente de detecție pentru a identifica și contracara vulnerabilitățile XSS [Gro07].

În plus, investigația digitală joacă un rol important în studierea atacurilor XSS și în strângerea de dovezi pentru a înțelege mai bine impactul acestora. Cu toate eforturile de combatere a acestor atacuri, este nevoie de cercetare continuă pentru a dezvolta metode mai eficiente de prevenire și detectare.

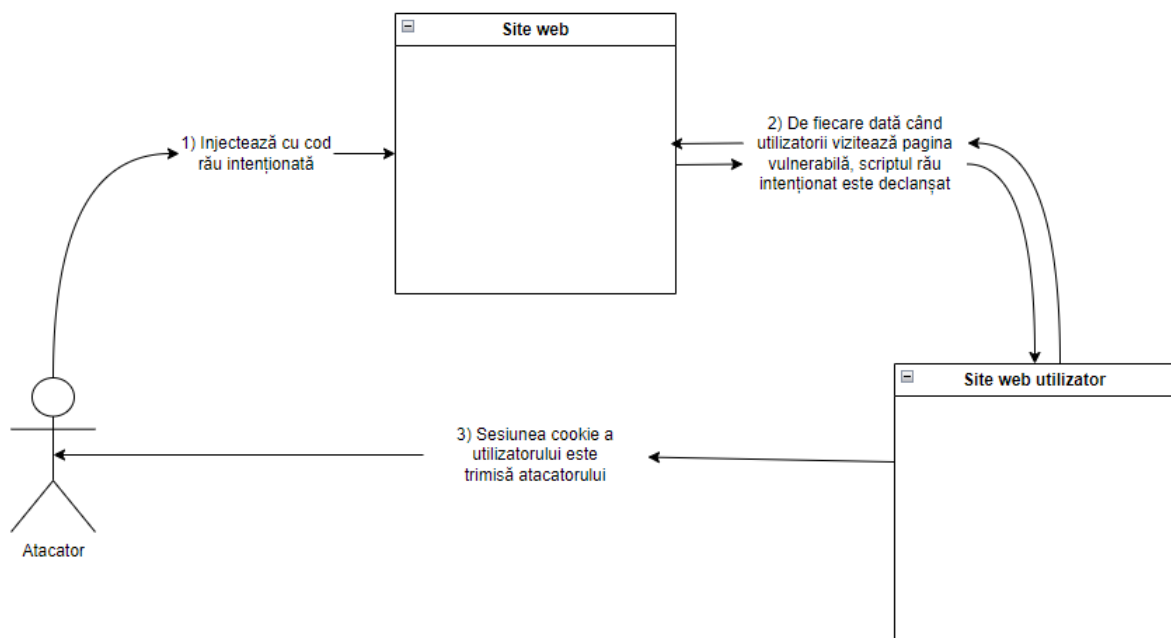


Figura 3.2: Cross-site scripting

### 3.2.3 SQL injection

Atacurile de injectare SQL sunt extrem de periculoase și pot avea consecințe grave pentru securitatea și integritatea datelor unei aplicații web. Atunci când un atacator reușește să efectueze o astfel de injectare, el poate să obțină acces neautorizat la baza de date a aplicației, să extragă sau să modifice datele sensibile stocate acolo și să compromită întregul sistem. Aceste atacuri pot duce la expunerea informațiilor personale ale utilizatorilor, la pierderea de date importante sau chiar la deteriorarea reputației unei companii. Din acest motiv, prevenirea și detecția atacurilor de injectare SQL sunt prioritare în securitatea aplicațiilor web, iar dezvoltatorii și ad-

ministratorii de sisteme trebuie să fie conștienți de vulnerabilitățile potențiale și să implementeze măsuri adecvate pentru a le contracara.

Pentru a realiza acest atac, atacatorul introduce comenzi SQL malițioase în câmpurile de intrare ale unei aplicații web, în scopul de a obține acces neautorizat la datele din baza de date sau de a modifica informațiile existente. Victima, fără să știe, furnizează date care sunt apoi manipulate de către atacator pentru a executa comenzi SQL 3.3.

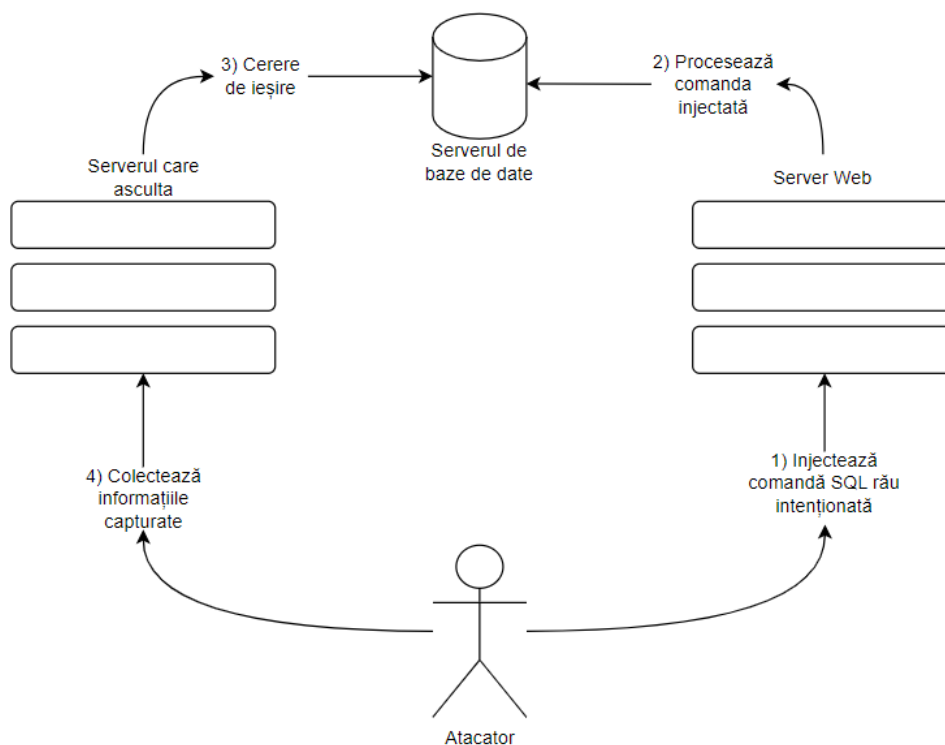


Figura 3.3: SQL Injection

Tehnicile de prevenire includ folosirea parametrizării query-urilor SQL, validarea strictă a datelor de intrare și utilizarea unor soluții de securitate precum firewalls de aplicații web și sisteme de detecție a intruziunilor. De asemenea, monitorizarea constantă a activității aplicației și actualizarea regulată a software-ului sunt esențiale pentru a menține un nivel înalt de securitate și pentru a preveni eventualele încercări de injectare SQL. [CS09].

### 3.3 Tehnici de atac

Pe lângă vulnerabilitățile obișnuite precum Cross-Site Request Forgery (CSRF), Cross-Site Scripting (XSS) și SQL Injection, rețelele de socializare sunt afectate și de tehnici de manipulare și atacuri, precum Clickjacking, Session Hijacking și Man-in-the-Middle (MitM). Aceste tactici sunt direcționate către comunicarea și sesiunile uti-

lizatorilor în cadrul acestor platforme, crescând riscul de acces neautorizat la date sau de interceptare a informațiilor transmise. Este vitală înțelegerea și gestionarea acestor amenințări pentru a asigura un mediu online sigur și protejat pentru toți utilizatorii.

### 3.3.1 Clickjacking

Clickjacking este un tip de atac cibernetic în care un site web rău intenționat îi înșală pe utilizatori să facă clic pe ceva diferit de ceea ce percep ei, adesea suprapunând conținutul malefic peste un site legitim sau făcând conținutul malefic transparent astfel încât utilizatorul să interacționeze cu el fără să știe. Acest atac poate duce la diverse consecințe, cum ar fi răspândirea de mesaje false pe platforme de socializare precum Twitter, Facebook, Instagram, furtul de informații sensibile sau inițierea de acțiuni neautorizate fără consimțământul utilizatorului.

Pentru a realiza acest atac, atacatorul creează o pagină web care conține un element invizibil sau opac, suprapus peste conținutul dorit de victima sa. Atunci când victima face clic pe conținutul aparent normal, de fapt face clic pe elementul suprapus, ceea ce îi permite atacatorului să dirijeze acțiunea utilizatorului către un scop diferit de cel inițial prevăzut 3.4.

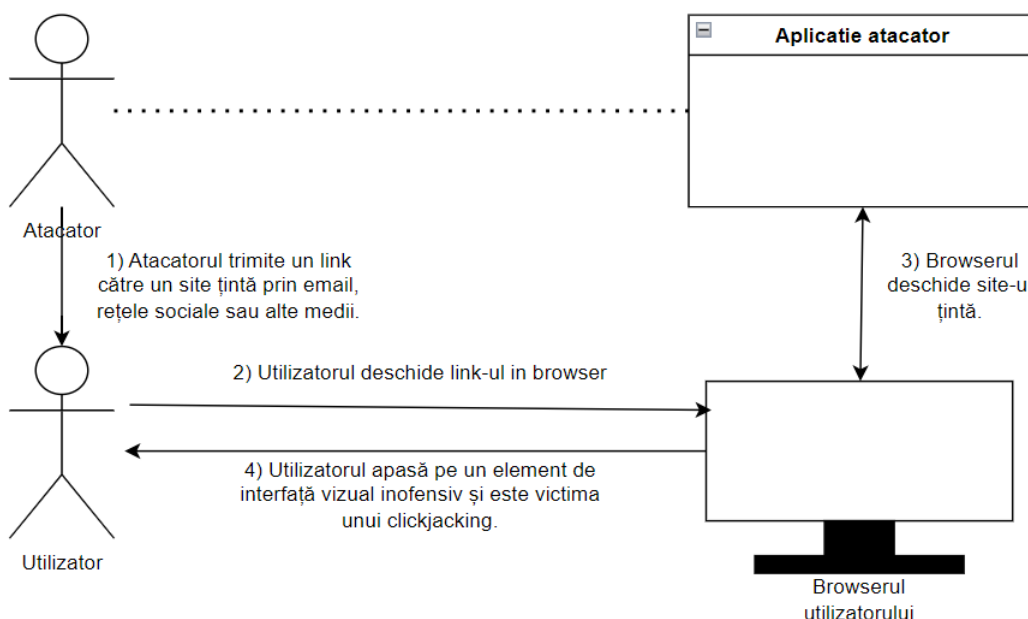


Figura 3.4: Clickjacking

Cercetătorii au dezvoltat o varietate de tehnici și soluții pentru a detecta și preveni atacurile de clickjacking, o tactică de fraudă cibernetică. De exemplu, Clicksafe este un mecanism de securitate specializat în oferirea unei protecții robuste împotriva acestor atacuri, asigurând o experiență mai sigură utilizatorilor. În același

context, ProClick reprezintă un cadru sofisticat care analizează conținutul cererilor și al paginilor de răspuns la nivel de proxy, detectând și blocând potențialele amenințări de clickjacking în aplicațiile web [HMW<sup>+</sup>12].

### 3.3.2 Session Hijacking

Hijacking-ul de sesiune este un atac cibernetic în care un atacator neautorizat preia controlul sesiunii unui utilizator pe un sistem informatic, dobândind acces la informații sensibile și capacitatea de a se autentifica ca și utilizatorul respectiv. Consecințele pot fi grave, deoarece atacatorul poate să fure date personale sau să efectueze acțiuni neautorizate în numele utilizatorului.

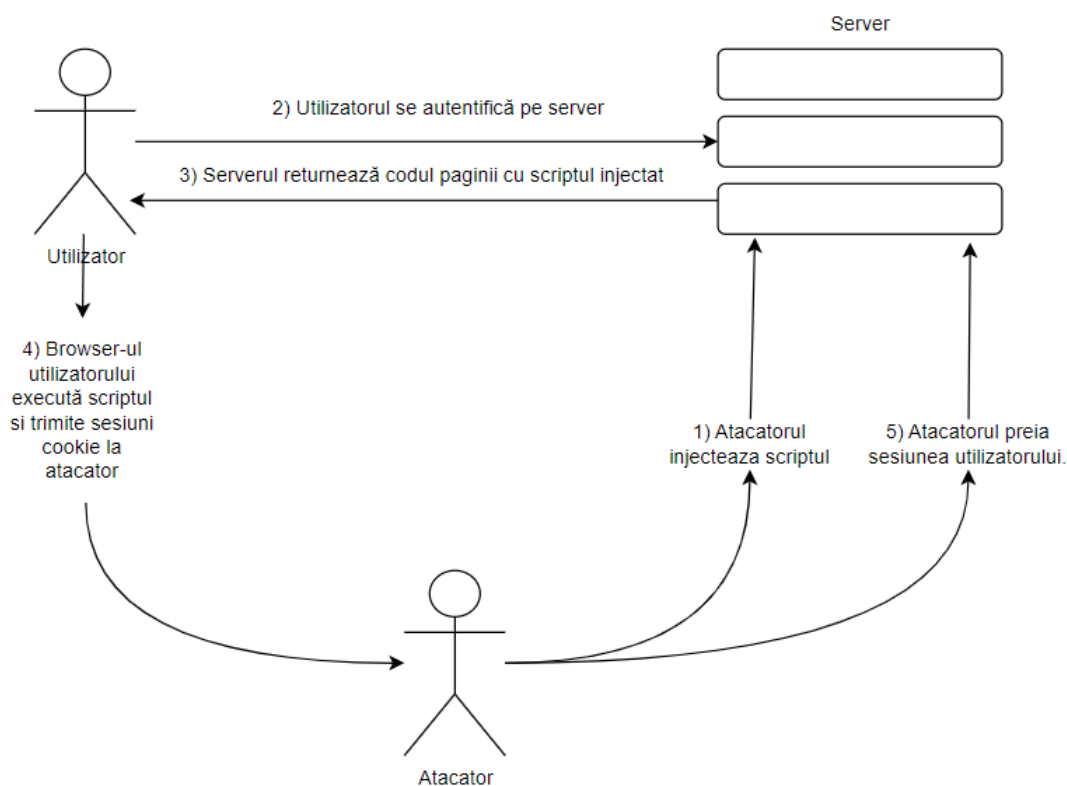


Figura 3.5: Session Hijacking

Pentru a realiza acest atac, atacatorul monitorizează traficul de rețea pe o rețea Wi-Fi publică și interceptează comunicațiile între victimă și server. Acesta identifică o sesiune activă, cum ar fi o sesiune de autentificare pe un site web, și interceptează cookie-urile de sesiune trimise de server către browserul victimei în timpul autentificării. Prin acest lucru, atacatorul obține un token de autentificare sau alte date de sesiune, care îi permit să preia controlul asupra sesiunii utilizatorului. În același timp, victima, neștiind că este supravegheată, navighează pe internet și interacționează cu aplicații web, inclusiv autentificându-se pe site-uri. Fără să-și dea seama, victima furnizează date care sunt interceptate și folosite de către ataca-

tor pentru a accesa conturile și datele personale. Atacatorul poate apoi să efectueze acțiuni neautorizate în numele victimei, cum ar fi plasarea de comenzi frauduloase sau furtul de informații 3.5.

Pentru a preveni atacurile, se folosesc diverse tehnici și soluții, precum tokenuri de autentificare fără stare și patch-uri de securitate pentru browsere. Este crucial să se ia în considerare vulnerabilitățile din conexiunile SSL/TLS, deoarece atacatorii le pot exploata pentru a intercepta și manipula comunicările între utilizatori și servere [JST15].

### 3.3.3 Man-in-the-Middle (MitM)

Un atac Man-in-the-Middle (MitM) este o formă sofisticată de atac cibernetic în care un atacator interceptează comunicarea între două sau mai multe părți și poate să o monitorizeze, să o modifice sau chiar să o întrerupă fără ca niciuna dintre părți să fie conștientă de aceasta. Atacatorul se inserează astfel în fluxul de comunicare, devenind un intermediar neinvitat între cei implicați.

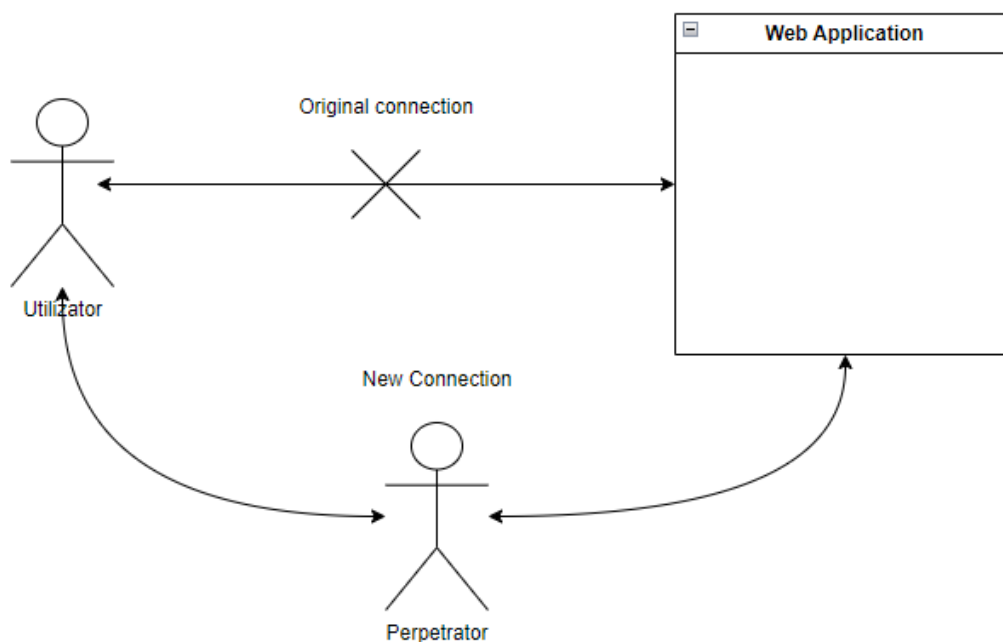


Figura 3.6: MitM

Acest tip de atac este extrem de periculos, deoarece permite atacatorului să obțină acces la informații sensibile, cum ar fi parole, date financiare sau alte date personale. De asemenea, atacatorul poate să modifice datele transmise între părți, să înlocuiască informațiile sau să creeze comunicări false pentru a manipula acțiunile părților implicate.

Există mai multe modalități prin care un atac MitM poate fi efectuat. Una dintre cele mai comune este prin intermediul unei rețele de calculatoare, unde atacatorul se



află între utilizator și serverul cu care comunică utilizatorul. Atacatorul poate să utilizeze tehnici precum ARP spoofing sau DNS spoofing pentru a dirija traficul către propriul său dispozitiv, unde poate să intercepteze și să modifice datele [Mal19] 3.6.

Alte modalități de a efectua un atac MitM includ utilizarea de programe malware instalate pe dispozitivul unui utilizator sau chiar infiltrarea în infrastructura unei rețele fără fir pentru a intercepta comunicările.

Pentru a preveni atacurile MitM, este esențial să se utilizeze protocoale de securitate puternice, cum ar fi HTTPS pentru comunicarea pe web, să se implementeze soluții de autentificare și criptare robuste și să se fie atenți la semnele de avertisment ale unui posibil atac, cum ar fi avertismentele browserului cu privire la certificate de securitate nevalide sau alte semne de conectare nesigură. De asemenea, este important să se păstreze software-ul și dispozitivele actualizate pentru a proteja împotriva vulnerabilităților cunoscute care ar putea fi exploatare de atacatori [MAST19].



În imaginea 4.1 este prezentată diagrama cazurilor de utilizare, care ilustrează interacțiunile dintre actorii principali (Utilizator și Admin) și aplicația Visi cu diverse funcționalități ale sistemului. Utilizatorii pot efectua operațiuni precum login, logout, creare și modificare a contului, vizualizarea și trimiterea mesajelor, gestionarea conversațiilor și vizualizarea altor utilizatori. Adminii au acces la funcționalități suplimentare, incluzând blocarea și deblocarea utilizatorilor, modificarea rolurilor, filtrarea și ștergerea utilizatorilor, și gestionarea rolurilor.

Aceste funcționalități sunt esențiale pentru o administrare eficientă a accesului și interacțiunilor în cadrul aplicației, asigurând o gestionare detaliată a drepturilor și activităților utilizatorilor, spre exemplu:

- Creare cont

Procesul de creare a unui cont este un pas esențial în gestionarea utilizatorilor într-un sistem. Utilizatorii completează un formular cu detalii personale, cum ar fi numele, adresa de email, și parola. Acest proces asigură că fiecare utilizator își poate crea un profil unic care va fi folosit în toate interacțiunile cu sistemul. După completarea formularului, informațiile sunt verificate și, dacă sunt acceptate, contul este creat în sistem. Utilizatorul poate apoi efectua login, accesând funcționalitățile sistemului conform rolului și permisiunilor atribuite.

- Login și Logout

Procesul de login permite utilizatorilor să acceseze conturile personale prin introducerea numelui de utilizator și a parolei. Aceasta este prima linie de apărare împotriva accesului neautorizat, asigurând că numai proprietarul contului poate accesa informațiile și funcționalitățile disponibile. Odată autentificați, utilizatorii pot naviga în sistem, efectua diverse acțiuni și modifica setările conform nevoilor lor.

Logout-ul este un proces simplu dar important, care se finalizează cu deconectarea utilizatorului din sistem.

- Modificare parolă

Schimbarea parolei este o funcționalitate standard în cadrul gestionării securității conturilor. Utilizatorii pot alege să-și schimbe parola prin accesarea setărilor contului, unde trebuie să dea pe un buton pentru a se deschide o fereastră unde trebuie să introducă o parolă nouă.

Acest proces este important pentru menținerea securității contului, permițând utilizatorilor să își actualizeze periodic parolele pentru a preveni accesul neautorizat. După actualizare, utilizatorul va trebui să folosească noua parolă pentru toate sesiunile viitoare de login.

- Vizualizare și Modificare informații cont

Utilizatorii au posibilitatea de a vizualiza și modifica informațiile asociate contului lor, cum ar fi numele, prenumele și numele de utilizator. Accesul la această secțiune se face prin panoul de control al utilizatorului, unde informațiile pot fi revizuite și ajustate după necesitate.

- Ștergere cont

Ștergerea contului este o opțiune disponibilă utilizatorilor care doresc să renunțe la serviciile sistemului. Acest proces se inițiază din setările contului, unde utilizatorul poate selecta opțiunea de a-și șterge permanent contul și toate datele asociate acestuia.

Aceasta este o decizie semnificativă, deoarece odată efectuată, acțiunea este ireversibilă. Sistemul va solicita confirmări multiple pentru a asigura că utilizatorul înțelege consecințele și este sigur de decizia sa de a proceda cu ștergerea.

- Trimitere și Vizualizare mesaje

Utilizatorii pot comunica între ei prin sistemul de mesagerie, selectând un utilizator din lista de utilizatori ai aplicației, scriind un mesaj și trimițându-l. Această funcționalitate facilitează interacțiunea directă între utilizatori, fiind esențială pentru colaborare sau comunicare personală.

Vizualizarea mesajelor permite utilizatorilor să urmărească istoricul conversațiilor, să răspundă la mesaje sau să continue dialoguri anterioare, oferind o modalitate eficientă de gestionare a comunicărilor.

- Adăugare conversație

Inițierea unei conversații noi este o funcție accesibilă din interfața de mesagerie, unde utilizatorii pot selecta unul sau mai mulți participanți din lista de utilizatori pentru a începe o discuție.

După selecția participanților și eventuala configurare a unui titlu pentru conversație, sesiunea de dialog este activată, permițând participanților să comunice în timp real.

- Modificare conversație

Utilizatorii pot modifica conversațiile existente pentru a răspunde schimbărilor în dinamica grupului sau a discuției. Acest lucru poate include adăugarea sau eliminarea participanților, schimbarea titlului conversației. Ștergere conversație

Ștergerea unei conversații este o opțiune disponibilă pentru utilizatori pentru a elimina discuții care nu mai sunt relevante sau necesare. Acest proces este simplu, implicând selecția conversației și confirmarea acțiunii de ștergere.

- Filtrare conversații

Filtrarea conversațiilor permite utilizatorilor să localizeze rapid discuții specifice folosind criterii precum numele participantului, numele conversației, numărul de participanți.

Utilizatorii pot accesa opțiunile de filtrare direct din interfața de conversații, unde pot introduce parametrii de căutare și vizualiza rezultatele imediat. Aceasta economisește timp și eficientizează gestionarea comunicațiilor, mai ales în contextul în care volumul conversațiilor este mare.

- Vizualizare utilizatori

Funcția de vizualizare a utilizatorilor permite accesul la o listă completă a tuturor persoanelor înregistrate în sistem. Acesta este un instrument util pentru a identifica și selecta interlocutori pentru mesaje.

Prin această funcționalitate, utilizatorii pot vedea informații de bază despre alți membri ai sistemului, facilitând colaborarea și comunicarea.

- Filtrare utilizatori

Filtrarea utilizatorilor este o extensie a funcției de vizualizare, permițând utilizatorilor să restrângă lista afișată pe baza unor criterii precum numele de utilizator. Aceasta facilitează găsirea rapidă a utilizatorilor pentru inițierea conversațiilor.

- Blocare și Deblocare utilizator

Administratorii au autoritatea de a restricționa accesul utilizatorilor la sistem, fie din cauze disciplinare, fie pentru alte probleme de conformitate. Blocarea este un instrument de control important care asigură menținerea unui mediu sigur și respectuos pentru toți utilizatorii.

Când un utilizator este blocat, acesta nu mai poate accesa sistemul sau interacționa cu alți utilizatori. Procesul de deblocare, pe de altă parte, este aplicat după ce problema care a condus la blocare a fost rectificată, permițând utilizatorului să revină în sistem.

- Modificare rol utilizator

Modificarea rolului unui utilizator este o capacitate administrativă care permite ajustarea nivelurilor de acces ale utilizatorilor în sistem. Acest lucru poate include promovarea unui utilizator la statutul de administrator.

Administratorii selectează utilizatorii din lista sistemului și ajustează rolurile acestora printr-un panou de control administrativ. Acest proces asigură că fiecare utilizator al aplicației are acces pe aplicație în funcție de rolul atribuit.

- Ștergere utilizatori

Administratorii pot de asemenea să șteargă utilizatori din sistem, fie ca răspuns la cererile acestora, fie ca o măsură disciplinară pentru încălcări grave ale regulilor comunității. Procesul de ștergere a unui utilizator este definitiv și implică eliminarea tuturor datelor asociate cu contul respectiv din baza de date.

Ștergerea unui utilizator se face printr-o procedură controlată, cu verificări suplimentare pentru a asigura că această acțiune este justificată și necesară.

- Vizualizare roluri

Administratorii au capacitatea de a revizui toate rolurile disponibile în sistem printr-o interfață dedicată în panoul de administrare. Aceasta listă include detalii despre fiecare rol, precum numele rolului și o descriere generală a permisiunilor asociate acestuia. Accesul la această funcționalitate permite o gestionare eficientă a drepturilor de acces, esențială pentru securitatea și eficiența sistemului.

- Adăugare și Modificare rol

Procesul de adăugare a unui nou rol permite administratorilor să definească un set specific de permisiuni care va determina ce acțiuni poate efectua un utilizator asociat cu acest rol. Aceasta este o parte vitală a gestionării securității sistemului, permițând adaptarea accesului la resurse în funcție de necesitățile organizaționale și de schimbările în politica de securitate.

Modificarea unui rol existent este la fel de importantă, oferind flexibilitatea de a ajusta permisiunile pe măsură ce nevoile aplicației se schimbă. Administratorul selectează rolul dorit din lista disponibilă, modifică permisiunile printr-un formular interactiv, și salvează schimbările.

- Ștergere rol

Ștergerea unui rol este o acțiune care trebuie tratată cu prudență deoarece poate avea implicații semnificative asupra structurii de acces a sistemului. Acest proces începe cu identificarea rolului care nu mai este necesar sau care a fost configurat incorect. Administratorul accesează secțiunea de roluri, selectează rolul în cauză și inițiază procedura de ștergere.

## 4.2 Proiectare

Pentru a gestiona eficient datele utilizatorilor și a asigura funcționalitatea rețelei de socializare Visi, am utilizat Microsoft SQL Server Management Studio (SSMS) ca

sistem de gestionare a bazelor de date. SSMS oferă un set robust de instrumente pentru administrarea bazelor de date, facilitând atât dezvoltarea, cât și întreținerea sistemului de date.

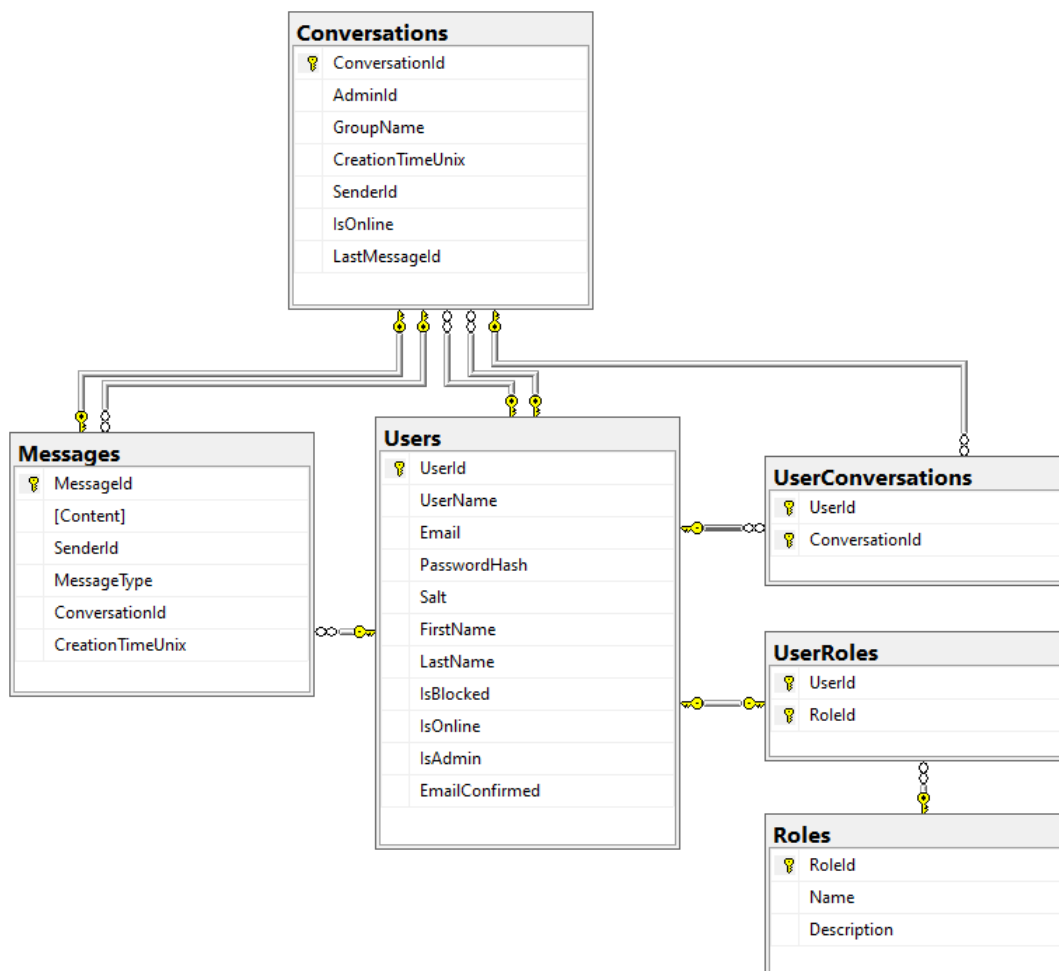


Figura 4.2: Diagrama bazei de date

Baza de date a platformei Visi 4.2e este organizată în mai multe tabele, fiecare având un rol specific în stocarea și gestionarea informațiilor pentru funcționarea platformei.

- **Users**: Acest tabel este esențial pentru gestionarea informațiilor de bază ale utilizatorilor și securitatea conturilor lor.
- **Roles**: Acest tabel permite definirea și gestionarea diferitelor roluri pe platformă, facilitând atribuirea de permisiuni specifice fiecărui tip de utilizator.
- **UserRoles**: Acest tabel gestionează relația many-to-many dintre utilizatori și roluri. Acesta permite atribuirea mai multor roluri unui utilizator și asocierea mai multor utilizatori cu un anumit rol.

- **Conversations:** Acest tabel stochează informații despre conversațiile începute cu anumiți utilizatori.
- **UserConversations:** Acest tabel gestionează relația many-to-many dintre utilizatori și conversații. Acesta permite atribuirea mai multor conversații unui utilizator și asocierea mai multor utilizatori cu o anumită conversație.
- **Messages:** Acest tabel stochează informații despre mesajele trimise în cadrul conversațiilor.

Relațiile dintre tabele sunt gestionate prin chei străine (Foreign Keys), care asigură integritatea datelor și consistența relațiilor între diferitele tabele. În cazul de față, tabela **UserRoles** conține chei străine ce leagă **UserId** din tabela **Users** și **RoleId** din tabela **Roles**. Acest mecanism garantează că fiecare utilizator asociat cu un rol există în tabela **Users** și fiecare rol atribuit unui utilizator există în tabela **Roles**. De asemenea, relațiile dintre **Messages**, **Conversations** și **Users** sunt gestionate prin chei străine: **Messages** are o cheie străină **SenderId** care se referă la **UserId** din tabela **Users** și o cheie străină **ConversationId** care se referă la **ConversationId** din tabela **Conversations**; **Conversations** are o cheie străină **AdminId** care se referă la **UserId** din tabela **Users**; iar **UserConversations** are chei străine **UserId** și **ConversationId** care se referă la **UserId** din tabela **Users** și **ConversationId** din tabela **Conversations**.

Proiectul **VisiProject** este structurat într-o arhitectură modulară, unde fiecare modul are un rol specific în cadrul aplicației. Această abordare modulară permite o organizare clară și separarea responsabilităților, facilitând dezvoltarea, întreținerea și scalabilitatea sistemului. După cum se poate observa în imaginea 4.3, modulele proiectului **VisiProject** sunt următoarele:

- **VisiProject.Contracts:** Acest modul conține definițiile contractelor utilizate în aplicație. Contractele sunt interfețele și clasele care definesc structura datelor și comportamentele așteptate între diferitele componente ale sistemului. Acestea asigură un mod standardizat de comunicare între modulele aplicației.
- **VisiProject.API:** Modulul API expune funcționalitățile aplicației către clienții externi. Acesta gestionează cererile HTTP și maparea acestora către logica aplicației. Modulul API se bazează pe contractele definite în **VisiProject.Contracts** pentru a asigura consistența și integritatea datelor transmise între client și server.
- **VisiProject.Infrastructure:** Acest modul conține implementările infrastructurii necesare pentru funcționarea aplicației. Include accesul la baza de date și alte resurse externe. Modulul de infrastructură este crucial pentru persistența datelor.



- VisiProject.Notifications: Modulul de notificări gestionează trimiterea emailurilor către utilizatori. Modulul se bazează pe infrastructura definită pentru a asigura livrarea corectă și la timp a emailurilor.
- VisiProject.Host: Modulul Host este punctul de intrare în aplicație. Acesta configurează și pornește aplicația, inițializând toate celelalte module necesare.

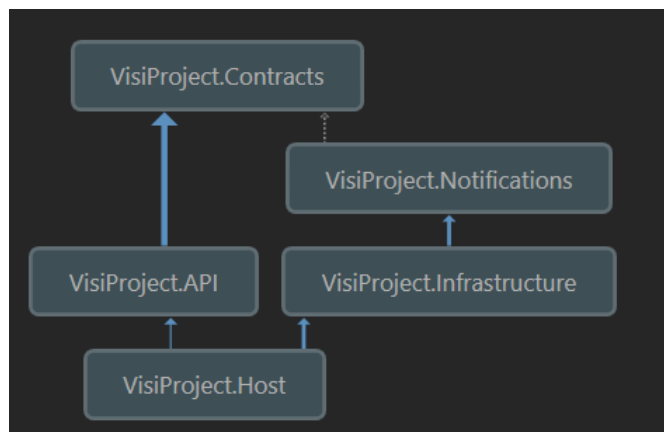


Figura 4.3: Diagrama claselor de dependente

Având în vedere complexitatea aplicației, diagramele de secvență fac mai ușoară vizualizarea interacțiunii utilizatorilor cu aplicația.

În imaginea 4.4 este prezentată diagrama de secvență pentru ștergerea unui utilizator, ilustrând cum un administrator șterge un utilizator. Cererea este procesată prin AdminUserController și UserService, iar utilizatorul este eliminat din baza de date de către UserStore, actualizându-se lista de utilizatori în DashboardAdmin.

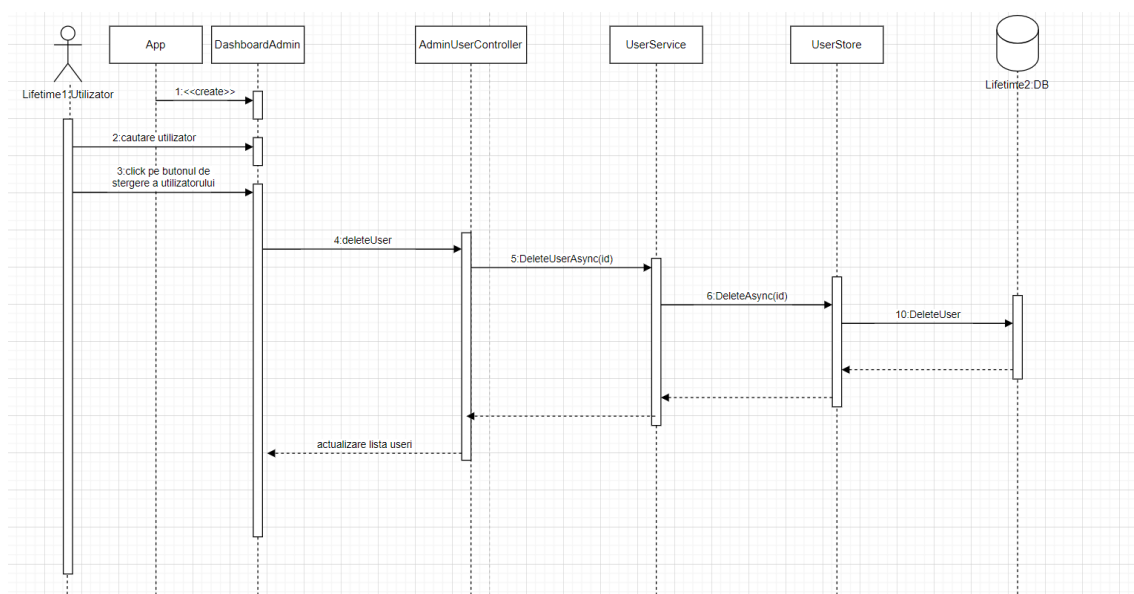


Figura 4.4: Diagrama de secvență pentru ștergerea unui utilizator

În imaginea 4.5 este prezentată diagrama de secvență pentru adăugarea unei conversații noi ilustrând cum utilizatorul adaugă o conversație. După adăugarea conversației lista de conversații se va actualiza în DashboardUser.

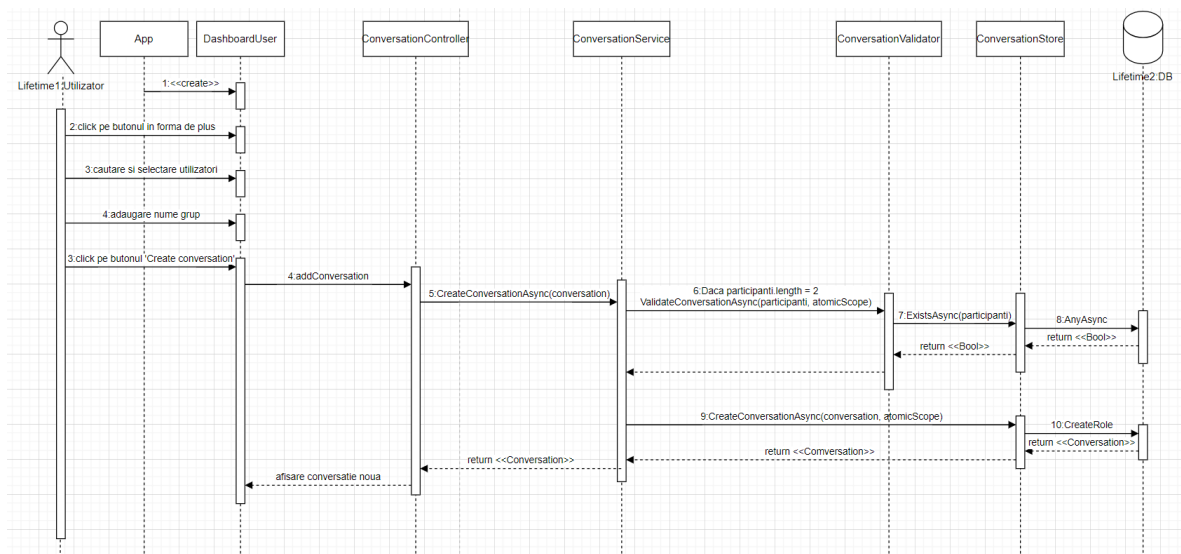


Figura 4.5: Diagrama de secvență pentru adăugarea unei conversații noi

În imaginea 4.6 este prezentată diagrama de secvență pentru autentificarea utilizatorului ilustrând cum utilizatorul se autentifică în aplicație, fiind redirecționat către o pagină destinată rolului său.

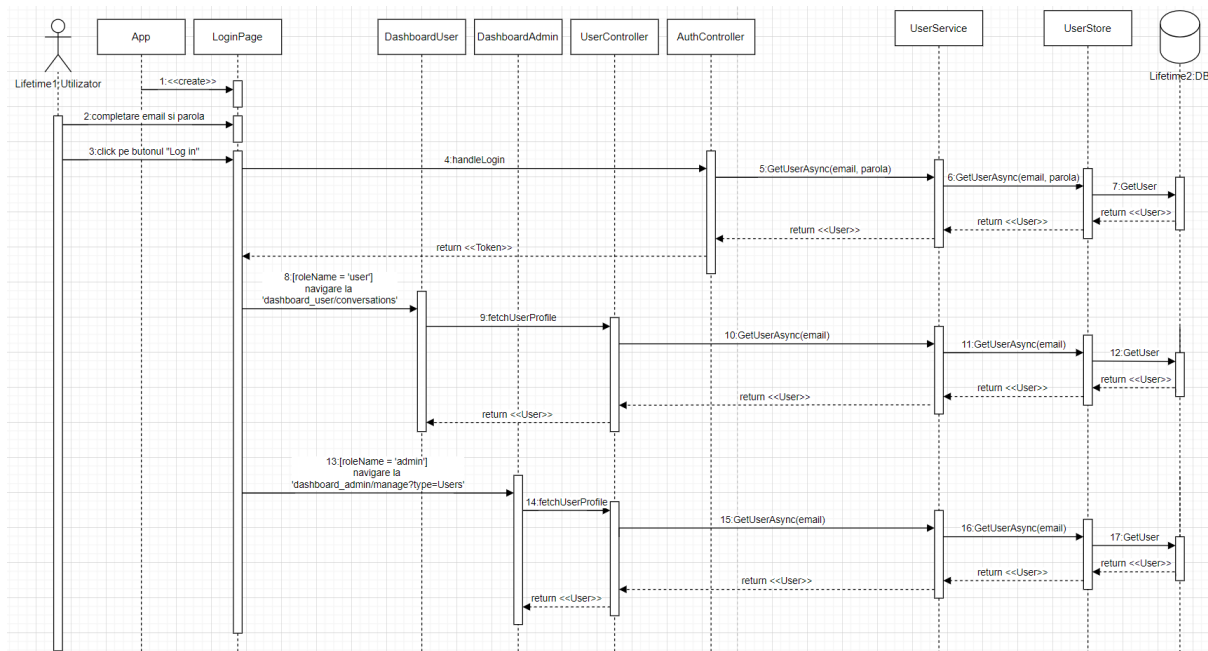


Figura 4.6: Diagrama de secvență pentru logare

În imaginea 4.7 este prezentată diagrama de secvență pentru procesul de creare a unui rol nou de către un administrator. După adăugare noul rol este afișat în

DashboardAdmin astfel lista de roluri fiind actualizată.

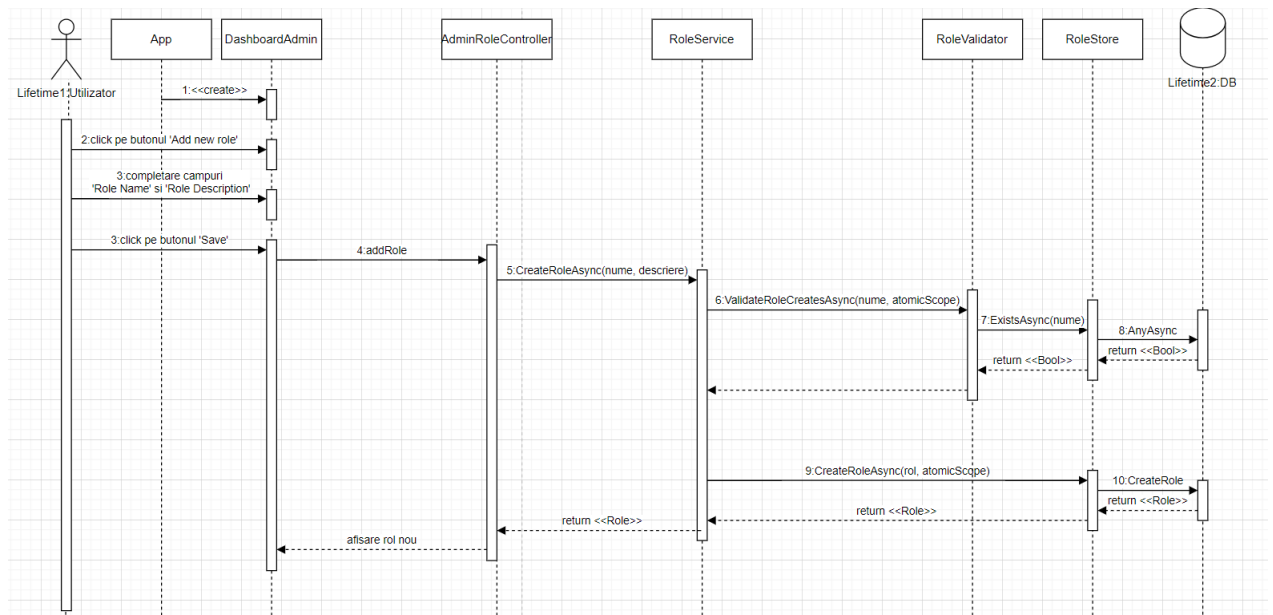


Figura 4.7: Diagrama de secvență pentru adăugarea unui rol nou

### 4.3 Tehnologii și Framework-uri

În cursul dezvoltării unei aplicații sofisticate și eficiente, am făcut uz de o selecție riguroasă de tehnologii de ultimă generație pentru a asigura o performanță optimă și o experiență de utilizare remarcabilă. În acest context, am adoptat o abordare meticuloasă, selectând cu grijă tehnologii precum C# și Typescript, două limbaje de programare cunoscute pentru robustețea și versatilitatea lor, în vederea implementării unui cod fiabil și eficient.

Pentru partea care se ocupă de funcționalitățile de bază ale aplicației, am optat pentru framework-urile .NET, React.js și Next.js. Alegând aceste tehnologii, am combinat fiabilitatea și puterea framework-ului .NET cu reactivitatea și interactivitatea aduse de React.js și Next.js în partea de frontend. Pentru a completa această structură, am integrat MaterialUI, asigurându-ne astfel că utilizatorii vor beneficia de un design plăcut și de o experiență vizuală îmbunătățită.

Pentru gestionarea datelor într-un mod eficient și securizat s-a ales Entity Framework. Acesta a furnizat un set robust de instrumente pentru interacțiunea cu baza de date, asigurând accesibilitatea și manipularea datelor într-un mod eficient. Pentru administrarea și gestionarea bazei de date, s-a ales să se lucreze cu SQL Server Management Studio (SSMS). Acesta a oferit un mediu familiar și puternic pentru administrarea și vizualizarea datelor, permițând efectuarea unor operațiuni complexe de gestionare a bazei de date într-un mod intuitiv și eficient. Prin utilizarea

acestor două tehnologii împreună, s-a reușit construirea și gestionarea cu succes a întregii infrastructuri a bazei de date în cadrul aplicației.

Această selecție atentă de tehnologii și framework-uri a reprezentat baza solidă a aplicației, furnizând un sistem robust, scalabil și ușor de administrat.

## 4.4 Backend

### 4.4.1 C#

C# a fost introdus pentru prima dată în 2000 ca parte a inițiativei .NET a Microsoft, cu scopul de a oferi un limbaj modern de programare orientat pe obiect pentru construirea aplicațiilor robuste și scalabile. Limbajul a fost proiectat de Anders Hejlsberg, care este cunoscut și pentru munca sa la Turbo Pascal și Delphi. Influența C++ și Java este evidentă în sintaxa și structura C#, făcându-l familiar dezvoltatorilor proveniți din aceste medii. Deși C# a fost inițial dezvoltat pentru platforma Windows, versatilitatea sa se extinde mult dincolo de ecosistemul Microsoft. Cu introducerea .NET Core și ulterior .NET 5, C# a adoptat dezvoltarea cross-platform, permițând dezvoltatorilor să scrie cod care rulează perfect pe Windows, macOS și Linux. Această independență de platformă a deschis noi posibilități pentru construirea aplicațiilor care se adaptează la medii și audiențe diverse [HTWG08].

Una dintre caracteristicile definitorii ale C# este sistemul său de tipizare puternic, care asigură siguranța tipului și ajută la prevenirea erorilor comune de programare la timpul compilării. Această caracteristică, împreună cu colectarea de gunoi pentru gestionarea memoriei, contribuie la reputația C#-ului de a fi un limbaj fiabil și sigur pentru dezvoltarea sistemelor software complexe.

C# este larg utilizat în diverse domenii, inclusiv dezvoltarea web, dezvoltarea de jocuri, dezvoltarea de aplicații mobile și software pentru întreprinderi. Odată cu apariția tehnologiilor precum Xamarin, C# a devenit, de asemenea, o alegere populară pentru dezvoltarea cross-platform, permițând dezvoltatorilor să scrie cod o singură dată și să-l implementeze pe mai multe platforme. Totodată, acesta se remarcă prin sintaxa sa elegantă și intuitivă, care este proiectată pentru a fi ușor de citit și scris. Structura sa, bazată pe clase și obiecte, urmează principiile programării orientate pe obiecte (OOP), promovând modularitatea și scalabilitatea în dezvoltarea de software [HTWG08].

În domeniul dezvoltării web, C# este adesea folosit în combinație cu ASP.NET, un framework puternic pentru aplicații web care permite dezvoltatorilor să construiască site-uri web dinamice și interactive. Integrarea C# cu ASP.NET oferă un mediu robust pentru crearea aplicațiilor web scalabile cu funcționalitate bogată. De-a lungul anilor, C# s-a adaptat la peisajul schimbător al dezvoltării software, introducând

o multitudine de caracteristici și inovații ale limbajului. De la construcții de limbaj precum LINQ (Language Integrated Query) pentru interogarea structurilor de date până la modele de programare asincronă cu `async/await`, C# continuă să se adapteze la tendințele și paradigmele emergente. Adățiile recente precum înregistrările, potrivirea modelelor și tipurile de referință nullable îmbunătățesc în continuare productivitatea dezvoltatorului și claritatea codului.

#### 4.4.2 .NET

Framework-ul .NET, creat inițial de Microsoft, este o componentă esențială în domeniul dezvoltării software, oferind o platformă completă pentru construirea și rularea diverselor aplicații. Cu o istorie care se întinde pe parcursul a peste două decenii, Framework-ul .NET a devenit unul dintre cele mai populare și influente cadre software din industria IT.

O trăsătură distinctivă a Framework-ului .NET este abordarea sa flexibilă față de limbajele de programare. .NET suportă multiple limbaje de programare, inclusiv C#, F# și Visual Basic, permițând dezvoltatorilor să aleagă limbajul cel mai potrivit pentru proiectele lor.

În plus, Framework-ul .NET se remarcă prin arhitectura sa modulară și versatilitatea. Cu componente precum Common Language Runtime (CLR) și Framework Class Library (FCL), .NET oferă un set bogat de funcționalități și instrumente care facilitează dezvoltarea și îmbunătățesc performanța aplicațiilor. De asemenea, .NET este compatibil cu diverse platforme, inclusiv Windows, Linux și macOS, permițând dezvoltatorilor să creeze aplicații care rulează pe o gamă largă de dispozitive și sisteme [TL03].

#### 4.4.3 Entity Framework

Entity Framework reprezintă un instrument puternic în dezvoltarea software, care permite programatorilor să gestioneze bazele de date folosind concepte de programare orientată pe obiecte. Prin intermediul său, se furnizează un nivel de abstractizare care permite dezvoltatorilor să interacționeze cu bazele de date folosind structuri de limbaj familiare, cum ar fi clasele și obiectele. Această metodă simplifică codul de acces la date și reduce necesitatea de a scrie interogări SQL complexe direct.

Unul dintre avantajele majore ale Entity Framework constă în abilitatea sa de a mapea tabelele bazei de date în clase .NET, facilitând astfel lucrul cu datele într-un mod orientat pe obiecte. Acest lucru este posibil prin intermediul modelelor, care reflectă structura tabelor bazei de date în codul aplicației. Prin definirea acestor

modele, dezvoltatorii pot efectua operații CRUD (Create, Read, Update, Delete) pe baza de date fără a fi nevoie să scrie interogări SQL explicit.

Entity Framework oferă, de asemenea, o serie de caracteristici și funcționalități care îmbunătățesc experiența de dezvoltare. De exemplu, suportă LINQ (Language Integrated Query), permițând programatorilor să scrie interogări folosind sintaxa C# sau VB.NET, făcând astfel interacțiunea cu baza de date mai intuitivă și mai sigură. În plus, Entity Framework susține funcționalități precum dezvoltarea bazată pe cod, unde schema bazei de date este generată pe baza modelului de domeniu al aplicației, și migrațiile de bază de date, care ajută la gestionarea modificărilor schemei bazei de date în timp [Ler10].

## 4.5 Frontend

### 4.5.1 Typescript

TypeScript este un limbaj de programare dezvoltat de Microsoft, care își propune să îmbunătățească și să sprijine dezvoltarea JavaScriptului. Nu este menit să fie un limbaj nou în sine, ci mai degrabă un superset al JavaScriptului, oferind funcționalități suplimentare precum tipizarea statică opțională și programarea orientată pe obiecte bazată pe clase. Acest lucru înseamnă că codul TypeScript poate fi compilat în JavaScript simplu, permițând dezvoltatorilor să beneficieze de avantajele tipizării statice, în timp ce își îndreaptă atenția către mediul de rulare JavaScript, omniprezent.

Unul dintre avantajele cheie ale TypeScriptului este sistemul său de tipuri statice, care permite dezvoltatorilor să identifice erori la timpul compilării în loc de timpul de rulare. Prin specificarea tipurilor pentru variabile, funcții și alte entități din cod, dezvoltatorii pot asigura o calitate mai bună a codului, o întreținere îmbunătățită și suport sporit pentru instrumente, ducând la aplicații mai robuste și scalabile.

În plus față de tipizarea statică, TypeScript introduce, de asemenea, funcționalități precum interfețele, clasele și modulele, care sunt întâlnite în mod obișnuit în limbajele tradiționale orientate pe obiecte, precum Java și C#. Acest lucru face ca TypeScript să fie o unealtă puternică pentru construirea aplicațiilor la scară largă, oferind dezvoltatorilor structuri și modele de proiectare familiare pentru a organiza și structura codul eficient. În plus, sistemul de tipuri al TypeScriptului este conceput să fie flexibil și expresiv, permițând dezvoltatorilor să creeze definiții de tipuri complexe care să modeleze cu exactitate logica lor de domeniu. Acest lucru permite dezvoltatorilor să scrie cod mai auto-descriptiv și ușor de întreținut, reducând probabilitatea de apariție a bug-urilor și facilitând înțelegerea și analiza codului.

Un alt aspect important al TypeScriptului este interoperabilitatea sa cu codul și bibliotecile JavaScript existente. TypeScript permite dezvoltatorilor să introducă

treptat adnotări de tipuri în baza lor de cod JavaScript, permitând o tranziție lină către un mediu cu tipuri statice fără a fi nevoie de o rescriere completă. Acest abordaj de adoptare progresivă este deosebit de benefic pentru proiectele mari cu baze de cod JavaScript vechi, deoarece permite dezvoltatorilor să profite de avantajele TypeScriptului fără a perturba fluxurile de lucru existente [Che19].

### 4.5.2 React.js

React.js este o bibliotecă puternică de JavaScript care și-a câștigat o popularitate imensă în ultimii ani pentru construirea interfețelor de utilizator dinamice și interactive pentru aplicațiile web. Oferă o arhitectură bazată pe componente care permite dezvoltatorilor să creeze componente UI reutilizabile, facilitând astfel procesul de dezvoltare și întreținere. React.js este cunoscut pentru tehnicile sale de optimizare a performanței, cum ar fi randarea virtuală a DOM-ului, care ajută la îmbunătățirea vitezei generale și a reactivității aplicațiilor web.

Una dintre caracteristicile cheie ale React.js este capacitatea sa de a crea atât componente de clasă, cât și componente funcționale, cunoscute sub numele de Hooks. Componentele de clasă sunt componente React tradiționale care extind clasa React, în timp ce componentele funcționale sunt mai simple și mai ușoare, făcându-le mai ușor de utilizat și înțeles. Introducerea Hooks în React.js a îmbunătățit în continuare capacitățile componentelor funcționale, permițându-le să folosească starea și alte caracteristici React fără a fi nevoie să scrie o clasă [Din22].

### 4.5.3 Next.js

Next.js este un cadru puternic care a câștigat o popularitate semnificativă în dezvoltarea web modernă datorită capacității sale de a îmbunătăți performanța și SEO-ul site-urilor web prin diverse tehnici de optimizare. Dezvoltatorii petrec adesea o cantitate considerabilă de timp și efort integrând multiple tehnologii pentru a construi o aplicație web completă. Next.js simplifică acest proces prin organizarea ordonată a pachetelor și oferind un abordaj structurat în dezvoltarea web.

Unul dintre avantajele cheie ale Next.js este capacitatea sa de a implementa Regenerarea Statică Incrementală (ISR), care permite actualizări de conținut dinamic fără a sacrifica performanța. Prin folosirea Next.js, dezvoltatorii pot construi aplicații web scalabile, de înaltă performanță și moderne care prioritizează experiența utilizatorului și satisfacția dezvoltatorului [Din22].

#### 4.5.4 MaterialUI

Material-UI reprezintă un cadru popular de interfață de utilizator care integrează Design-ul Material al Google, oferind o paletă variată de componente și unelte pentru crearea aplicațiilor web vizual atrăgătoare și responsive. Cunoscut pentru flexibilitatea sa, simplitatea în utilizare și documentația detaliată, Material-UI este alegerea preferată a mulți dezvoltatori din ecosistemul React.

Unul dintre punctele forte ale Material-UI constă în respectarea principiilor Design-ului Material, un cadru de design elaborat de Google care se concentrează pe crearea unei experiențe consistente și intuitive pentru utilizatori, indiferent de platformă sau dispozitiv. Prin utilizarea componentelor Material-UI, dezvoltatorii pot crea interfețe care urmează aceste ghiduri de design, rezultând aplicații nu doar plăcute vizual, ci și prietenoase cu utilizatorul.

În plus, Material-UI pune la dispoziție o gamă variată de componente pre-construite, precum butoane, carduri, meniuri și casete de dialog, care contribuie semnificativ la accelerarea procesului de dezvoltare. Aceste componente sunt concepute să fie personalizabile și responsive, permițând dezvoltatorilor să creeze interfețe adaptabile la diferite dimensiuni și orientări de ecran. Flexibilitatea oferită de Material-UI este extrem de valoroasă în contextul actual al utilizării multiple a dispozitivelor, unde utilizatorii accesează aplicațiile de pe o gamă variată de dispozitive, inclusiv smartphone-uri, tablete și computere desktop [RM20].

### 4.6 Baza de date

SQL Server Management Studio (SSMS), dezvoltat de Microsoft, este o unealtă esențială în gestionarea eficientă a bazelor de date SQL Server. Cu o interfață intuitivă și puternică, SSMS oferă dezvoltatorilor și administratorilor un set complet de instrumente pentru dezvoltare, administrare și întreținere. Prin intermediul său, utilizatorii pot interacționa cu bazele de date folosind construcții familiare de limbaj, simplificând astfel codul de acces la date și reducând necesitatea de a scrie interogări SQL complexe. Cu un editor puternic de interogări T-SQL și un designer vizual pentru obiectele bazei de date, SSMS facilitează dezvoltarea și modificarea structurilor de date. De asemenea, oferă un set de instrumente pentru administrarea serverului și optimizarea performanței bazei de date, precum și integrarea cu servicii Microsoft și sisteme de control al versiunilor pentru gestionarea eficientă a bazelor de date în mediul cloud și colaborarea la proiecte [Ser].



## 4.7 Manual de utilizare

La începutul site-ului, utilizatorul va fi întâmpinat de o pagină de logare intuitivă și ușor de utilizat 4.8, care conține trei butoane principale: "Forgot password?", "Sign up for Visi", și "Log in". În plus, utilizatorul are opțiunea de a se conecta prin intermediul contului său de Google, oferind o modalitate rapidă și convenabilă de acces, chiar dacă nu are un cont Visi.

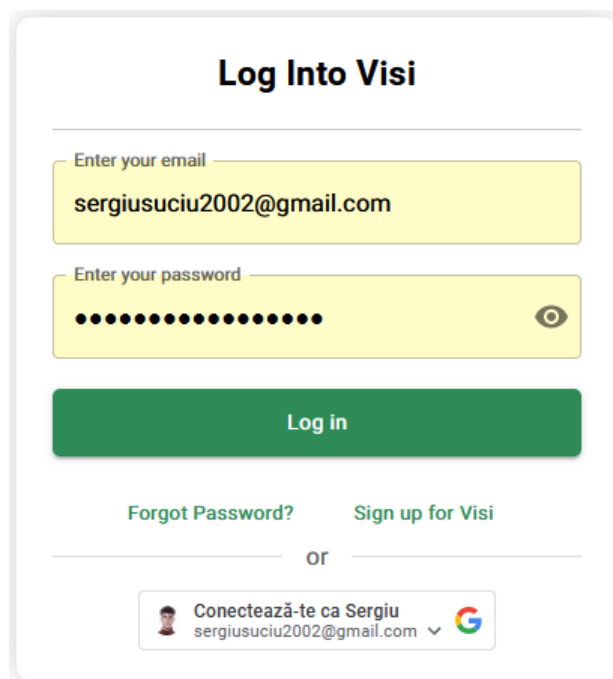


Figura 4.8: Pagina de logare

Dacă utilizatorul apasă pe butonul "Sign up for Visi", va fi redirecționat automat către pagina de înregistrare, unde va putea să își creeze un nou cont prin completarea unor câmpuri precum nume, email și parolă.

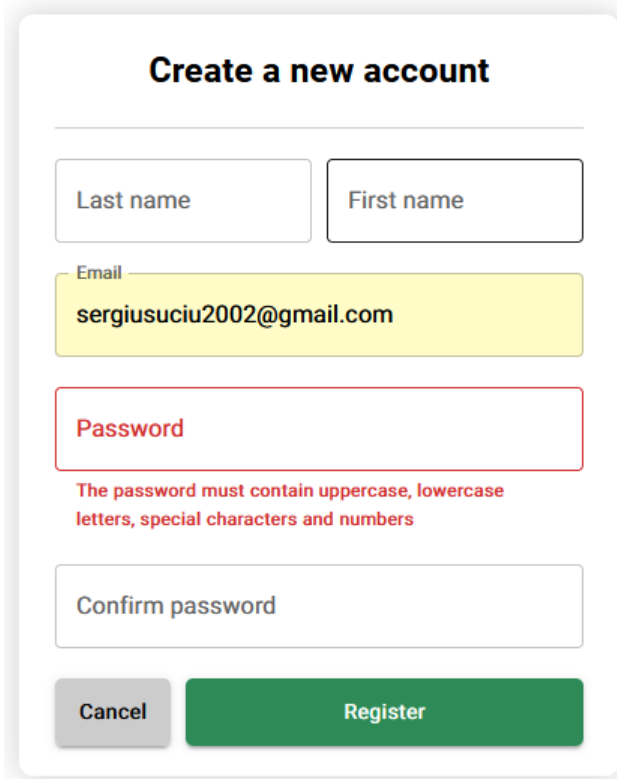
În cazul în care utilizatorul a uitat parola și apasă pe butonul "Forgot password?", va fi redirecționat către pagina de resetare a parolei. Aici, va trebui să introducă adresa de email asociată contului său, urmând să primească instrucțiuni detaliate prin email pentru resetarea parolei.

Dacă utilizatorul apasă pe butonul "Log in", acesta va fi redirecționat către pagina de început a site-ului, unde va avea acces complet la toate funcționalitățile și serviciile oferite. Pagina de început va afișa un dashboard personalizat, cu informații relevante și opțiuni pentru a naviga ușor prin diferitele secțiuni ale site-ului.

Această pagină de logare este concepută pentru a oferi utilizatorului o experiență simplă și eficientă, asigurând accesul rapid la contul său și facilitând procesele de înregistrare și recuperare a parolei.

Pagina de înregistrare a site-ului Visi 4.9 este proiectată pentru a oferi utiliza-

torului o experiență simplă și sigură de creare a unui cont nou. Aceasta include câmpurile obligatorii: Last Name (Nume de familie), First Name (Prenume), Email (Adresa de email), Password (Parolă) și Confirm Password (Confirmare parolă). Aceste câmpuri trebuie completate corect pentru a finaliza procesul de înregistrare.



The image shows a web form titled "Create a new account". It contains several input fields: "Last name" and "First name" (side-by-side), "Email" (containing "sergiusuciu2002@gmail.com"), "Password" (with a red border and a red error message below it: "The password must contain uppercase, lowercase letters, special characters and numbers"), and "Confirm password". At the bottom are two buttons: "Cancel" (grey) and "Register" (green).

Figura 4.9: Pagina de înregistrare

Butonul "Register" este folosit pentru a trimite formularul după ce toate câmpurile sunt completate. Dacă datele sunt corecte și valide, contul va fi creat cu succes și utilizatorului îi va apărea un mesaj care îi va sugera că i-a fost trimis un email de confirmare a adresei de email 4.10. Utilizatorul va trebui să verifice emailul pentru a confirma adresa și pentru a finaliza activarea contului.

Butonul "Cancel" permite utilizatorului să renunțe la procesul de înregistrare. La apăsarea acestui buton, utilizatorul va fi redirectionat înapoi la pagina de logare, fără a salva informațiile introduse în formularul de înregistrare. Aceasta oferă utilizatorului flexibilitatea de a ieși din procesul de înregistrare fără a fi nevoit să completeze toate câmpurile dacă decide să nu continue.

Validarea câmpurilor este esențială pentru asigurarea unei experiențe de înregistrare fără probleme. Câmpurile Last Name și First Name trebuie completate cu numele și prenumele utilizatorului, iar dacă sunt lăsate necompletate sau conțin caractere nepermise, va apărea un mesaj de eroare în roșu. Adresa de email trebuie să fie într-un

format valid (de exemplu, exemplu@domeniu.com); orice email invalid sau câmp necompletat va genera un mesaj de eroare. Parola trebuie să îndeplinească anumite criterii de securitate, cum ar fi o lungime minimă și includerea unor caractere speciale, cifre și litere mari și mici. Orice parolă care nu îndeplinește aceste criterii sau un câmp lăsat necompletat va duce la afișarea unui mesaj de eroare în roșu. Câmpul Confirm Password trebuie să corespundă exact cu parola introdusă inițial; orice nepotrivire între parole va fi indicată printr-un mesaj de eroare, informând utilizatorul că parolele nu se potrivesc.

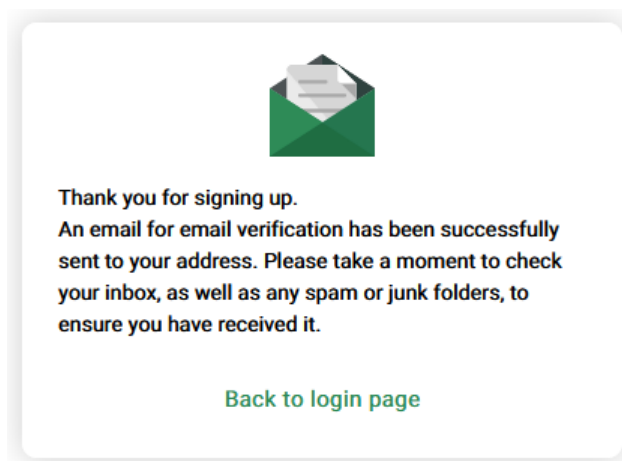


Figura 4.10: Mesaj pentru trimiterea mailului de resetare a parolei

În imaginea 4.11, se poate observa un email primit după înregistrare unui utilizator. Acesta include un buton etichetat "Confirm Email Address". Apăsarea acestui buton redirecționează utilizatorul către o pagină care indică statusul confirmării emailului.

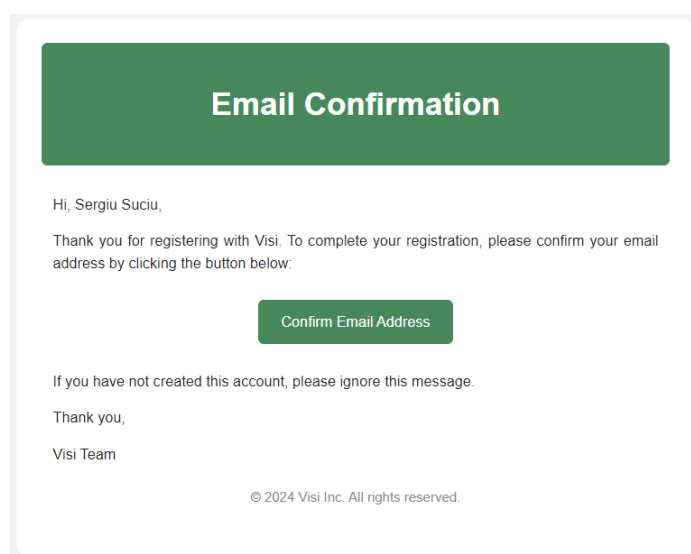


Figura 4.11: E-mail pentru confirmare email

Pagina de resetare a parolei de pe platforma Visi 4.12 este concepută pentru a oferi utilizatorilor o soluție rapidă și sigură în situația în care au uitat parola contului lor. Această pagină anunță acțiunea pe care un utilizator trebuie să o facă pentru a-și reseta parola, astfel interfața simplă a paginii solicită doar adresa de email asociată contului, permițând utilizatorilor să inițieze procesul de resetare a parolei în doar câțiva pași simpli. În plus, pagina este echipată cu două butoane esențiale: "Cancel", care oferă utilizatorului opțiunea de a renunța la proces și de a reveni la paginile anterioare, și "Reset Password", care declanșează procesul de resetare a parolei.

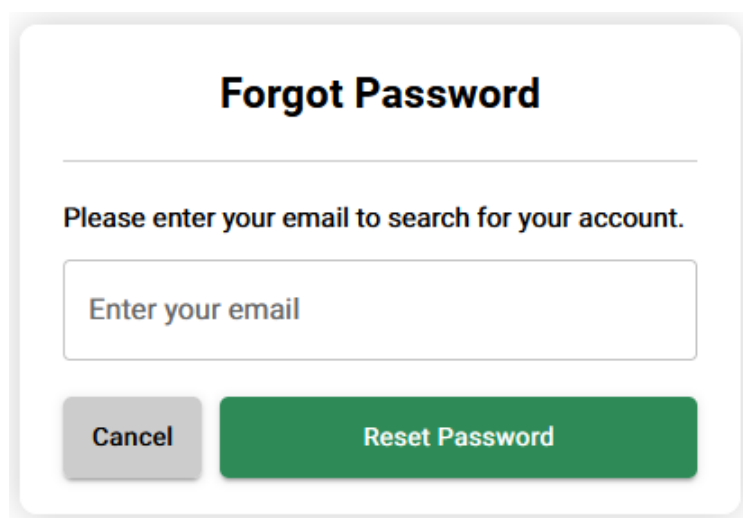


Figura 4.12: Pagina pentru resetarea parolei

După ce utilizatorul apasă pe butonul "Reset Password", acesta va primi imediat un mesaj de confirmare că un email pentru resetarea parolei a fost trimis la adresa de email furnizată 4.13.

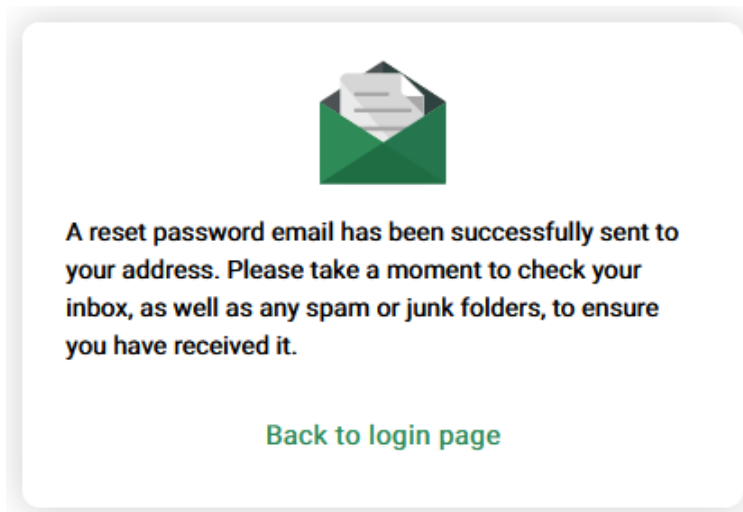


Figura 4.13: Mesaj pentru trimiterea mailului de resetare a parolei

În imaginea 4.14, se poate observa un email primit de un utilizator care a solicitat resetarea parolei, conținând un buton etichetat "Change Password". Apăsând acest buton, utilizatorul este redirecționat către o pagină web care confirmă dacă resetarea parolei a fost realizată cu succes sau nu.

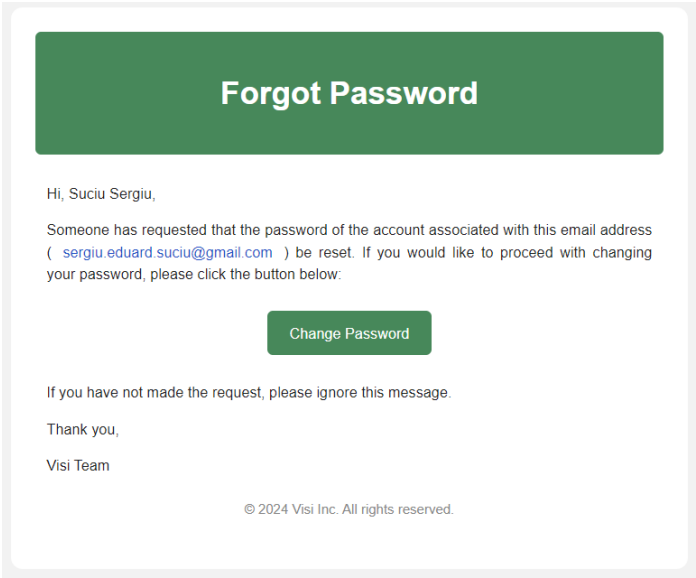


Figura 4.14: E-mail pentru resetarea parolei

Pagina de administrare a platformei Visi oferă administratorilor un set cuprinzător de instrumente pentru gestionarea utilizatorilor și a rolurilor. În imaginea 4.15, se poate observa că administratorul are capacitatea de a șterge utilizatori sau de a bloca și debloca utilizatori.

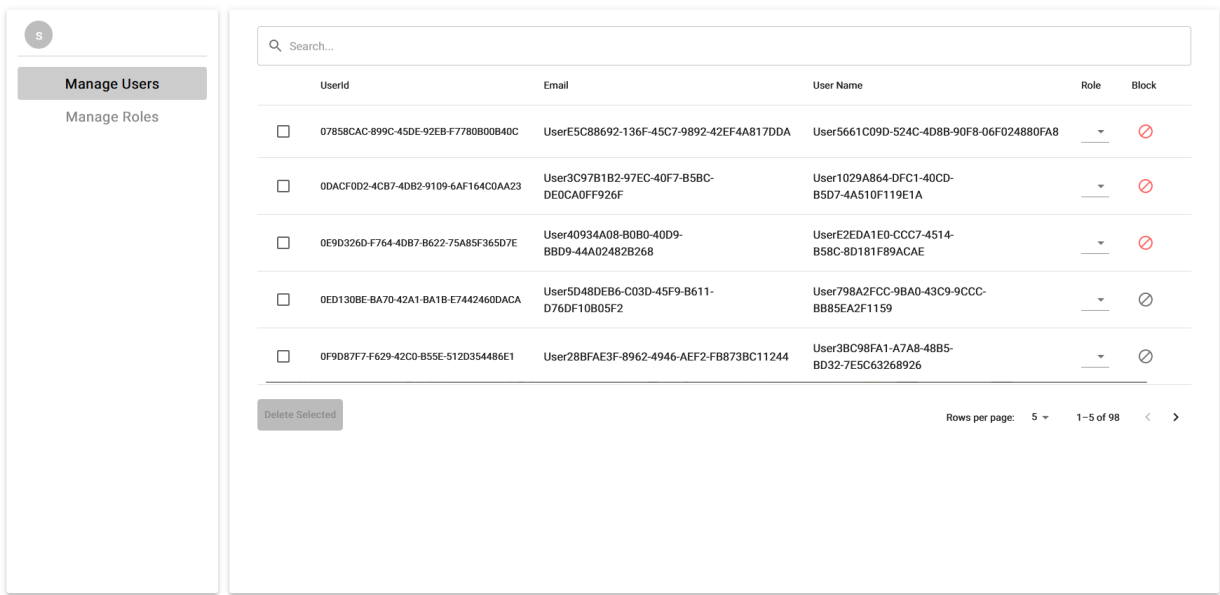


Figura 4.15: Pagina pentru modificarea utilizatorilor

Dacă un utilizator este blocat, acesta va primi un email de notificare care va sugera că administratorul i-a blocat contul 4.16.

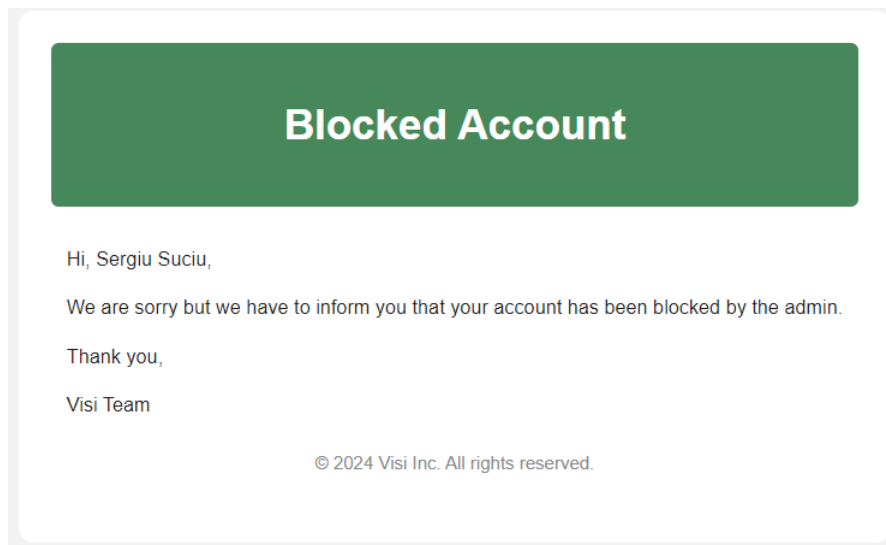


Figura 4.16: E-mail pentru blocare a utilizatorului

Similar, dacă un utilizator este deblocat, acesta va primi un email care va sugera că administratorul i-a deblocat contul 4.17. Aceste funcționalități sunt esențiale pentru a menține controlul asupra accesului și comportamentului utilizatorilor pe platformă.

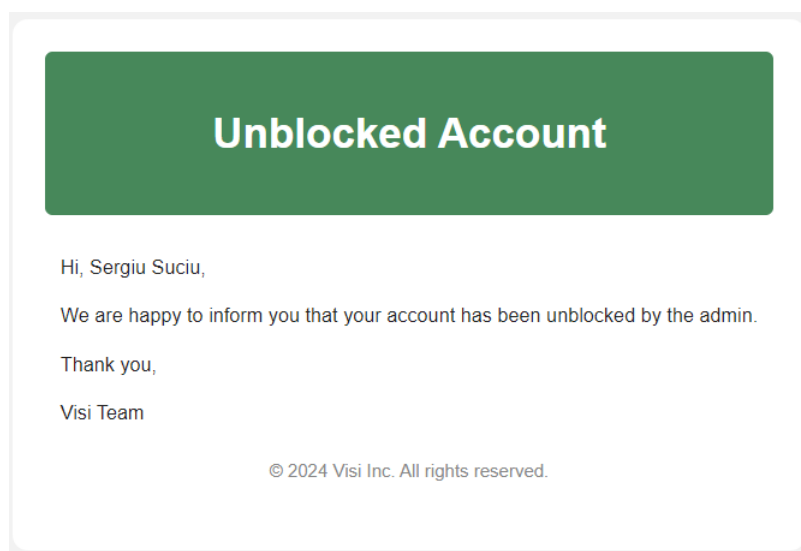


Figura 4.17: E-mail pentru deblocare a utilizatorului

În imaginea 4.18, administratorul poate gestiona rolurile utilizatorilor și poate vizualiza lista completă a rolurilor disponibile în sistem. Aceasta include atât rolurile standard predefinite cât și cele personalizate, oferind astfel o flexibilitate mai mare în administrarea accesului utilizatorilor.

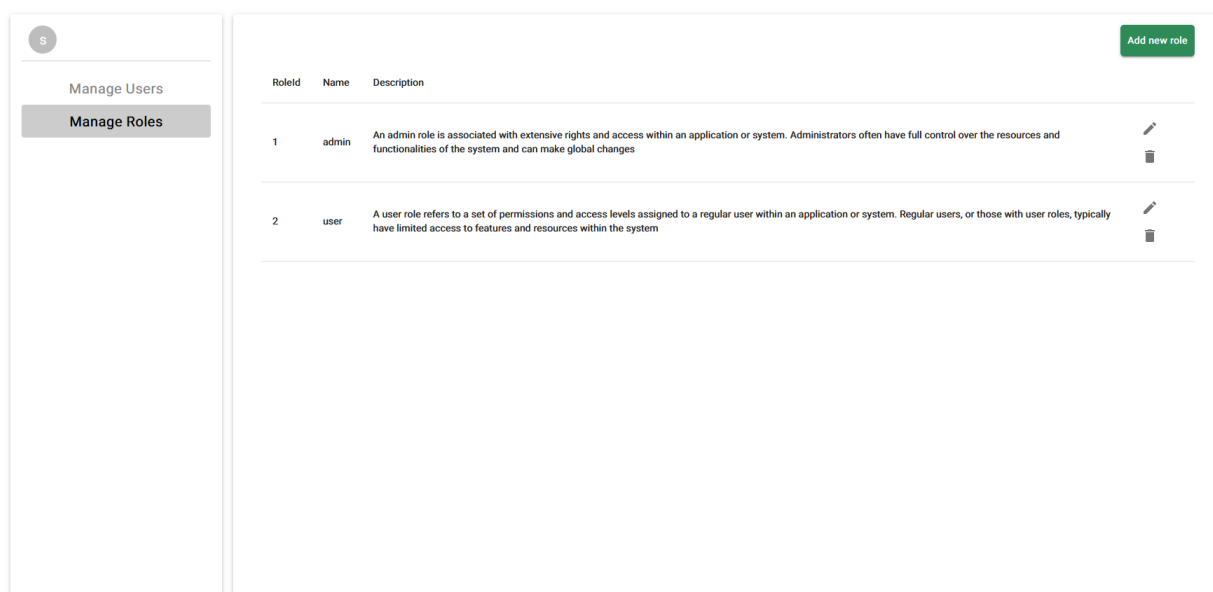


Figura 4.18: Pagina pentru modificarea rolurilor

Pe această pagină, prin apăsarea butonului "Add new role", administratorul poate adăuga un nou rol. Când acest buton este apăsător, se va deschide o fereastră nouă în care trebuie să completeze câmpurile "Role Name" (Nume rol) și "Role Description" (Descriere rol) 4.19.

### Add New Role

Please enter the details for the new role:

Role Name

Role Description

If you want to add the new role click Save button.

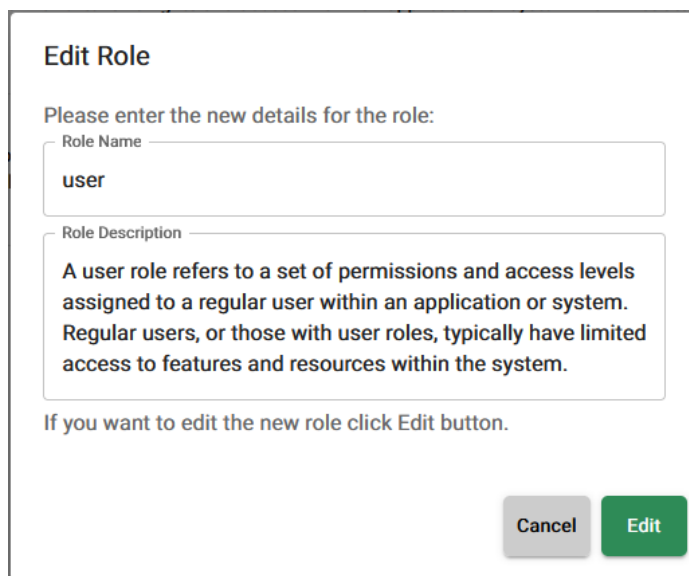
Cancel

Save

Figura 4.19: Pagina pentru adaugarea unui rol

De asemenea, pentru a edita un rol existent, administratorul poate apăsa pe butonul în formă de creion aflat în dreptul fiecărui rol. La apăsarea acestui buton, se va deschide o fereastră nouă în care administratorul trebuie să completeze sau să mo-

difice câmpurile "Role Name" și "Role Description" 4.20. Aceasta permite ajustarea detaliilor și permisiunilor rolului, asigurându-se că structura de autoritate și acces este mereu actualizată și corespunzătoare nevoilor platformei.



**Edit Role**

Please enter the new details for the role:

Role Name

Role Description

If you want to edit the new role click Edit button.

Figura 4.20: Pagina pentru modificarea unui rol

În imagine 4.21 este prezentată interfața aplicației Visi, care este structurată pentru a facilita comunicarea eficientă între utilizatori. Interfața este împărțită în două secțiuni principale: bara laterală din stânga și fereastra principală din dreapta.

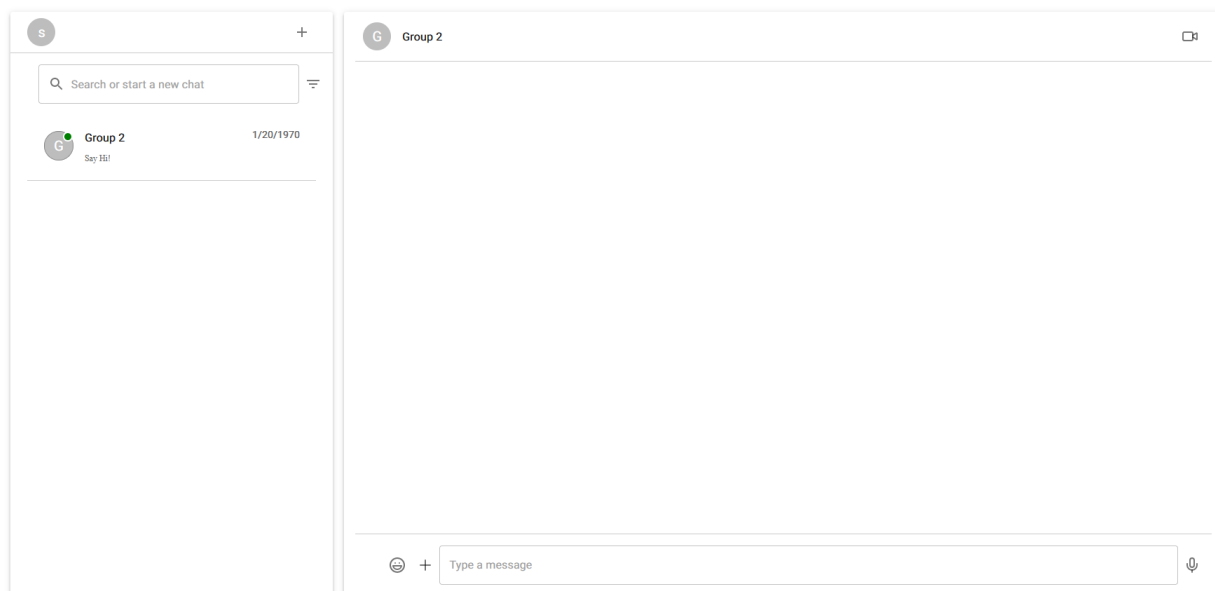


Figura 4.21: Pagina pentru gestionarea conversațiilor user-ului logat

De asemenea, butonul "+" le permite utilizatorilor să adauge o conversație nouă și să caute alți utilizatori cu care să înceapă o discuție 4.22. Câmpul de căutare de sub



butonul "+" oferă o modalitate rapidă de a naviga între conversațiile existente, care sunt afișate mai jos în listă, fiecare conversație fiind reprezentată printr-un rezumat al activităților recente.

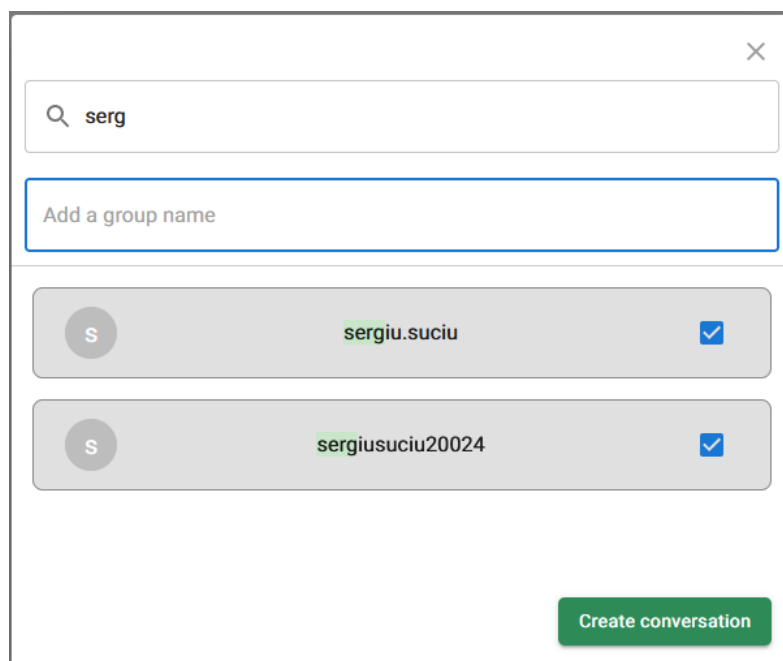


Figura 4.22: Pagina pentru adaugarea unei conversatii

Dacă utilizatorul face clic pe avatarul din stânga sus, se va deschide o fereastră detaliată. Această fereastră oferă o vizualizare cuprinzătoare a informațiilor despre cont, inclusiv detalii configurabile, cum ar fi numele de utilizator, adresa de email și alte preferințe personale 4.23.

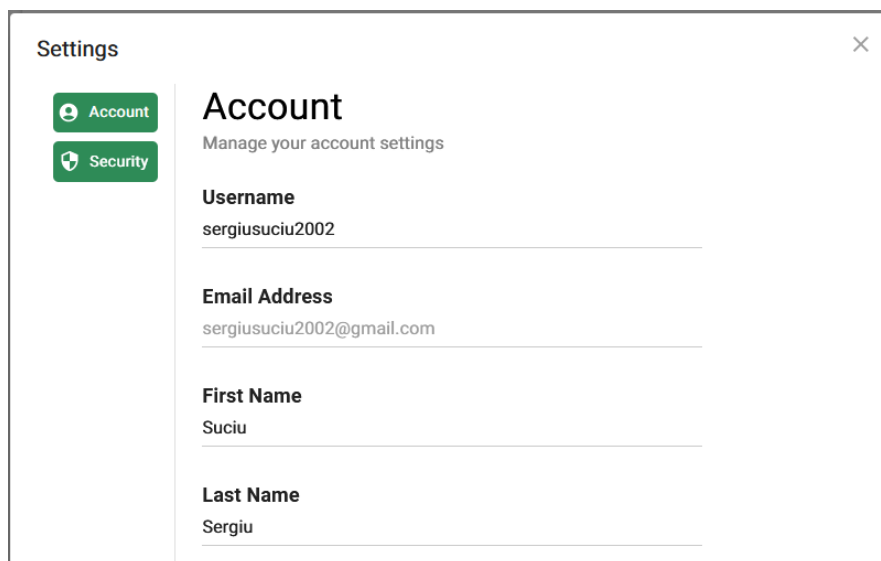


Figura 4.23: Pagina pentru vizualizarea setarilor de cont

Pe lângă acestea, sunt afișate și detalii de securitate 4.24, care includ informații

specifice despre rolul utilizatorului în aplicație și permisiunile asociate acestuia. Aceste informații de securitate clarifică ce acțiuni și funcții sunt disponibile utilizatorului pe platformă, contribuind astfel la o administrare mai eficientă și transparentă a accesului.

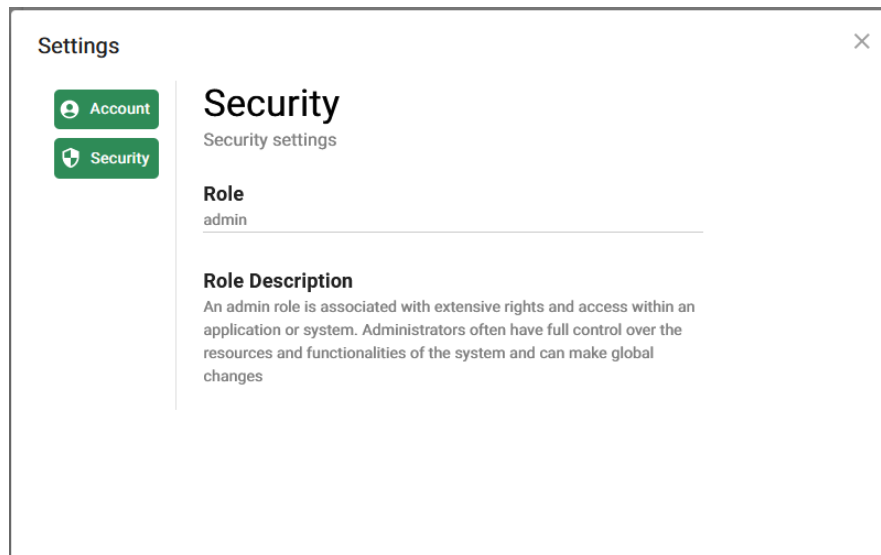


Figura 4.24: Pagina pentru vizualizarea setarilor de securitate

Fereastra principală din dreapta este dedicată afișării detaliilor conversației selectate. Aici, utilizatorii pot vedea istoricul complet al mesajelor și pot continua discuția. Butonul de cameră video, plasat în colțul din dreapta sus, permite inițierea unui apel video, oferind posibilitatea de a comunica vizual, nu doar prin text. Acest aspect îmbogățește experiența utilizatorilor, făcând comunicarea mai personală și directă. De asemenea, utilizatorii au la dispoziție un câmp de introducere a mesajelor în partea de jos a ferestrei principale, unde pot scrie și trimite mesaje text. Câmpul de introducere a mesajelor include opțiuni pentru trimiterea de emoji-uri, oferind astfel flexibilitate și diversitate în comunicare.

# Capitolul 5

## Concluzii

În această lucrare am analizat impactul semnificativ al tehnologiei digitale și al rețelelor sociale asupra interacțiunilor sociale și accesului la informație, evidențiind necesitatea unei aplicații de rețele sociale adaptate nevoilor moderne. În dezvoltarea aplicației, au stat la baza cele patru aspecte precizate la începutul lucrării: gestionarea informațiilor și combaterea dezinformării, securitatea și confidențialitatea datelor, îmbunătățirea experienței utilizatorilor și optimizarea interfeței.

În subcapitolul 2.2 am investigat diversitatea rețelelor sociale și am evidențiat rolurile distincte pe care le îndeplinesc în cadrul mediului digital. Această diversitate de funcționalități a fost pusă în evidență printr-o paralelă între aplicațiile Twitter, Instagram și Facebook, subliniind modul unic în care fiecare platformă facilitează exprimarea personală, conectarea și interacțiunea, astfel observandu-se importanța experienței utilizatorilor și optimizarea interfeței, acestea două favorizând adoptarea pe scară largă a aplicației.

Așa cum a fost menționat când au fost propuse obiectivele lucrării, securitatea reprezintă o bază foarte importantă pentru o rețea de socializare. Importanța acesteia a fost evidențiată în subcapitolele 3.2 și 3.3 printr-o clasificare a problemelor de securitate, astfel reieșind că amenințările cibernetice, precum hacking-ul și phishing-ul, subliniază necesitatea unor măsuri stricte de securitate cibernetică, cum ar fi actualizările regulate ale sistemului, parole puternice și monitorizarea constantă a rețelelor. Astfel prin analiza amănunțită a acestor aspecte s-a remarcat importanța contribuției lor la buna dezvoltare a unei rețele de socializare care să prospere pe termen îndelungat.

# Bibliografie

- [Agr23] Shobhit Agrawal. Mitigating cross-site request forgery (csrf) attacks using reinforcement learning and predictive analytics. *Applied Research in Artificial Intelligence and Cloud Computing*, 6(9):17–30, 2023.
- [AOS10] Saleh Ali K Al-Omari and Putra Sumari. An overview of mobile ad hoc networks for the existing protocols and applications. *arXiv preprint arXiv:1003.3565*, 2010.
- [BD11] Casimir C Barczyk and Doris G Duncan. Social networking media as a tool for teaching business administration courses. *International Journal of Humanities and Social Science*, 1(17):267–276, 2011.
- [BE07] Danah M Boyd and Nicole B Ellison. Social network sites: Definition, history, and scholarship. *Journal of computer-mediated Communication*, 13(1):210–230, 2007.
- [Ben12] Reda Benkirane. The alchemy of revolution: The role of social networks and new media in the arab spring. *GCSP Policy Paper*, 7(1), 2012.
- [BJN<sup>+</sup>02] Albert-Laszlo Barabási, Hawoong Jeong, Zoltan Néda, Erzsebet Ravasz, Andras Schubert, and Tamas Vicsek. Evolution of the social network of scientific collaborations. *Physica A: Statistical mechanics and its applications*, 311(3-4):590–614, 2002.
- [Bro] Brooke Auxier and Monica Anderson. Social Media Use in 2021. <https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/>. Online.
- [Che19] Boris Cherny. *Programming TypeScript: making your JavaScript applications scale*. O'Reilly Media, 2019.
- [CS09] Justin Clarke-Salt. *SQL injection attacks and defense*. Elsevier, 2009.
- [CSW05] Peter J Carrington, John Scott, and Stanley Wasserman. *Models and methods in social network analysis*, volume 28. Cambridge university press, 2005.

- 
- [DH19] Shreya Desai and Meng Han. Social media content analytics beyond the text: A case study of university branding in instagram. In *Proceedings of the 2019 ACM Southeast Conference*, pages 94–101, 2019.
- [Din22] Zerihun Dinku. React. js vs. next. js. 2022.
- [dJS00] Meno de Jong and Peter J Schellens. Toward a document evaluation methodology: What does research tell us about the validity and reliability of evaluation methods? *IEEE Transactions on professional communication*, 43(3):242–260, 2000.
- [ESSH19] Riham Elhabyan, Wei Shi, and Marc St-Hilaire. Coverage protocols for wireless sensor networks: Review and future directions. *Journal of Communications and Networks*, 21(1):45–60, 2019.
- [Fre11] Linton C Freeman. The development of social network analysis—with an emphasis on recent events. *The Sage handbook of social network analysis*, 21(3):26–39, 2011.
- [Gro07] Jeremiah Grossman. *XSS attacks: cross site scripting exploits and defense*. Syngress, 2007.
- [GTP22] Adam Kavon Ghazi-Tehrani and Henry N Pontell. Phishing evolves: Analyzing the enduring cybercrime. In *The New Technology of Financial Crime*, pages 35–61. Routledge, 2022.
- [Hay14] Jackie R Hayes. User interface design for online social media. 2014.
- [HMW<sup>+</sup>12] Lin-Shung Huang, Alex Moshchuk, Helen J Wang, Stuart Schecter, and Collin Jackson. Clickjacking: Attacks and defenses. In *21st USENIX Security Symposium (USENIX Security 12)*, pages 413–428, 2012.
- [HTWG08] Anders Hejlsberg, Mads Torgersen, Scott Wiltamuth, and Peter Golde. *The C# programming language*. Pearson Education, 2008.
- [ima] <https://lh6.googleusercontent.com/vTO2aDiByNAYWmZEcnv9gQ0jU3yfoRDYx13YC4ADogqiR3lQWisWiT8QNCRTcqC4VpeBRqG5MObs-ir>. at 19:03 pm Sat, 27th April 24.
- [JST15] Vineeta Jain, Divya Rishi Sahu, and Deepak Singh Tomar. Session hijacking: Threat analysis and countermeasures. In *Int. Conf. on Futuristic Trends in Computational Analysis and Knowledge Management*, 2015.
-

- [KH10] Andreas M Kaplan and Michael Haenlein. Users of the world, unite! the challenges and opportunities of social media. *Business horizons*, 53(1):59–68, 2010.
- [KNT06] Ravi Kumar, Jasmine Novak, and Andrew Tomkins. Structure and evolution of online social networks. In *Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 611–617, 2006.
- [Kos20] Jeff Kosseff. Hacking cybersecurity law. *U. Ill. L. Rev.*, page 811, 2020.
- [KW06] Gueorgi Kossinets and Duncan J Watts. Empirical analysis of an evolving social network. *science*, 311(5757):88–90, 2006.
- [Ler10] Julia Lerman. *Programming Entity Framework: Building Data Centric Apps with the ADO. NET Entity Framework*. " O'Reilly Media, Inc.", 2010.
- [Mal19] Avijit Mallik. Man-in-the-middle-attack: Understanding in simple words. *Cyberspace: Jurnal Pendidikan Teknologi Informatika*, 2(2):109–134, 2019.
- [MAST19] A Mallik, A Ahsan, MMZ Shahadat, and JC Tsou. Understanding man-in-the-middle-attack through survey of literature. *Indonesian Journal of Computing, Engineering, and Design*, 1(1):44–56, 2019.
- [MRCD17] Tushar Maheshwari, Aishwarya N Reganti, Tanmoy Chakraborty, and Amitava Das. Socio-ethnic ingredients of social network communities. In *Companion of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, pages 235–238, 2017.
- [MW11] Alexandra Marin and Barry Wellman. Social network analysis: An introduction. *The SAGE handbook of social network analysis*, pages 11–25, 2011.
- [PC21] Ksenia Peguero and Xiuzhen Cheng. Csrp protection in javascript frameworks and the security of javascript applications. *High-Confidence Computing*, 1(2):100035, 2021.
- [QRA<sup>+</sup>20] Daniela Quiñones, Cristian Rusu, Diego Arancibia, Sebastián González, and María José Saavedra. Snuxh: A set of social network user experience heuristics. *Applied Sciences*, 10(18):6547, 2020.
- [RM20] Prateek Rawat and Archana N Mahajan. Reactjs: a modern web development framework. *International Journal of Innovative Science and Research Technology*, 5(11):698–702, 2020.

- [RSL<sup>+</sup>17] Shailendra Rathore, Pradip Kumar Sharma, Vincenzo Loia, Young-Sik Jeong, and Jong Hyuk Park. Social network security: Issues, challenges, threats, and solutions. *Information sciences*, 421:43–69, 2017.
- [Ser] SQL Server. Sql server management studio.
- [SLT10] Michael Szell, Renaud Lambiotte, and Stefan Thurner. Multirelational organization of large-scale social networks in an online world. *Proceedings of the National Academy of Sciences*, 107(31):13636–13641, 2010.
- [Sta] Stacy Jo Dixon. Number of global social network users 2017-2027. <https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/>. Online.
- [TL03] Thuan L Thai and Hoang Lam. . *NET framework essentials*. " O'Reilly Media, Inc.", 2003.
- [Val10] Thomas W Valente. *Social networks and health: Models, methods, and applications*. Oxford University Press, 2010.
- [VdHDJ03] Maaïke J Van den Haak and Menno DT De Jong. Exploring two methods of usability testing: concurrent versus retrospective think-aloud protocols. In *IEEE International Professional Communication Conference, 2003. IPCC 2003. Proceedings.*, pages 3–pp. IEEE, 2003.
- [vSD88] Marten van SINDEREN and Evert Dorregeest. A critical analysis of the x. 400 model of message handling systems. *Computer standards & interfaces*, 7(4):363–375, 1988.
- [VVdB17] Paul Voigt and Axel Von dem Bussche. The eu general data protection regulation (gdpr). *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, 10(3152676):10–5555, 2017.
- [Zag13] Melanie E Zaglia. Brand communities embedded in social networks. *Journal of business research*, 66(2):216–223, 2013.