Sistem de online banking

Echipa:

Sarariu Liviu-Dan 333CC

Dragoi Stefan 333CC

Sandu Cristian Andrei 333CC

Radu Toma 333CC

Cuprins

1. Introducere
    1.1 Scopul sistemului
    1.2 Documente referinte

2. Obiective de proiectare

3. Arhitectura propusa
    3.1 Prezentarea generala a arhitecturii sistemului
    3.2 Decompozitia in subsisteme si responsabilitatile fiecarui subsistem
    3.3 Distributia subsistemelor pe platforme hardware/software
    3.4 Managementul datelor persistente
    3.5 Controlul accesului utilizatorilor la sistem
    3.6 Conditiile limita (cazurile de utilizare limita)

1. Introducere

1.1 Scopul sistemului

Aplicatia reprezintă un sistem de online banking. Această aplicație urmărește să integreze mai multe operațiuni uzuale, precum transferuri bancare, consultarea soldului și obținerea extraselor de cont, deschiderea unui cont de economii și transferul între contul curent și cel de economii, gestionarea cardurilor și aprobarea plăților către comercianți. Utilitarul prezintă un grad înalt de securitate, autentificarea realizându-se în doi pași, atât prin parola introdusă de client dar și printr-un cod generat printr-o aplicație pentru smartphone. Sistemul va oferi de asemenea conturi privilegiate pentru personalul băncii care vor realiza acțiuni asupra conturilor clienților și să obțină statistici despre tranzacțiile efectuate. Vor exista și conturi pentru comercianți, care vor accepta plata cu cardul.

1.2 Documente referinte

Mai multe detalii despre cerinte, actorii care interactioneaza cu sistemul si diferitele cazuri de utilizare pot fi consultate in Documentul de Specificare a Cerintelor.

2. Obiective de proiectare

Scopurile urmarite in dezvoltarea sistemului:

- usurinta in utilizare a sistemului(utilizatorii nu trebuie sa fie neaparat persoane tehnice)
- siguranta si securitatea sistemului(toti utilizatorii vor folosi autentificare in 2 pasi)
- portabilitatea (interfata utilizatorilor va fi un site web, respectiv un autentificator pe dispozitivul lor Android, sistemul putand fi astfel accesat de la orice sistem capabil sa ruleze un browser web)
- extensibilitatea (suport pentru diferite platforme mobile va putea fi introdus relativ usor, fara modificarea codului existent)

3. Arhitectura propusa

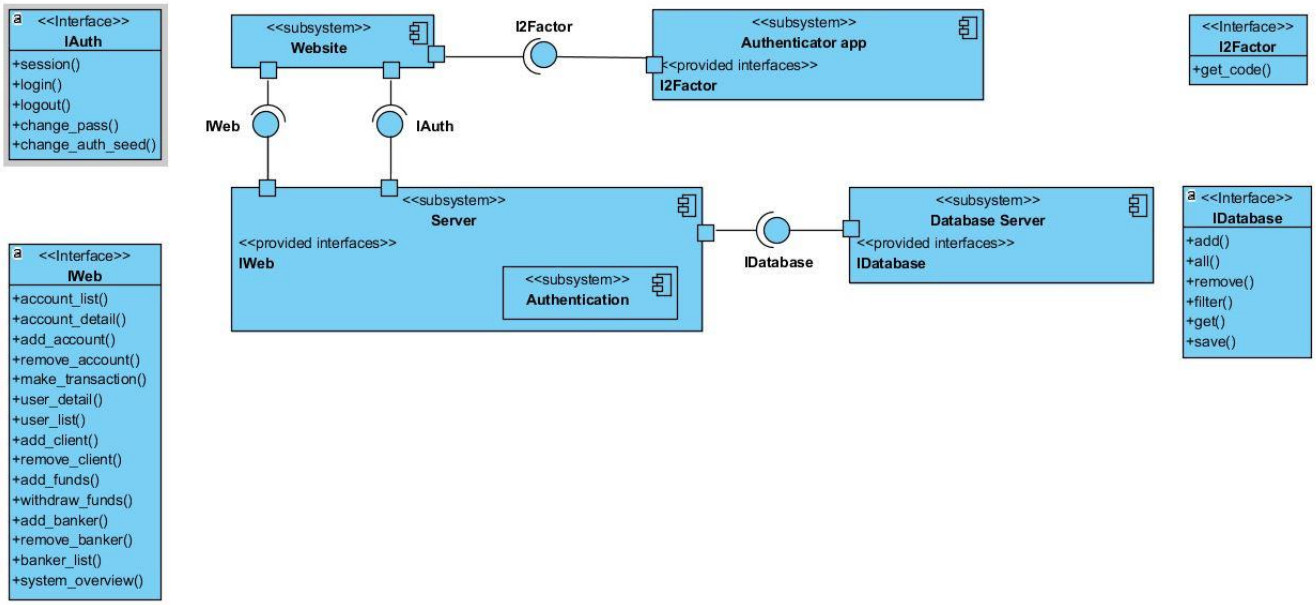
3.1 Prezentarea generala a arhitecturii sistemului

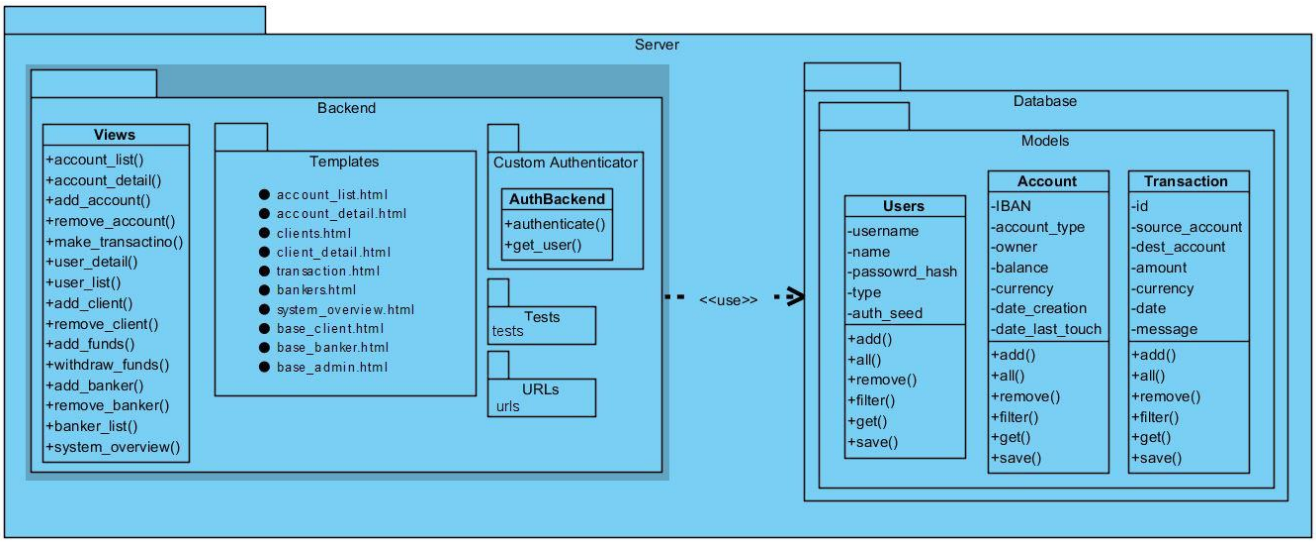
Sistemul de online banking se bazeaza pe 4 subsisteme relativ independente:

a) Site-ul web - interfata de interactiune cu sistemul de online banking. Implementat folosind template-uri HTML Django si Bootstrap pentru stilizare. Ofera functiile precizate in documentul de specificare a cerintelor. Diferite tipuri de utilizatori vor putea accesa seturi diferite de pagini, in functie de permisiuni.
b) Aplicatia de autentificare Android - va avea un ID/seed unic asociat utilizatorului, va genera un cod(bazat pe un timestamp obtinut de la acelasi server NTP ca serverul central) pe care utilizatorul va fi nevoit sa il introduca la autentificare. Acelasi cod va fi generat si de catre server pentru a confirma identitatea utilizatorului.
c) Subsistemul de baze de date - implementat ca o baza de date MySQL ; fiecarui model specificat in models.py ii va corespunde un tabel in baza de date. Este incapsulat in serverul central.

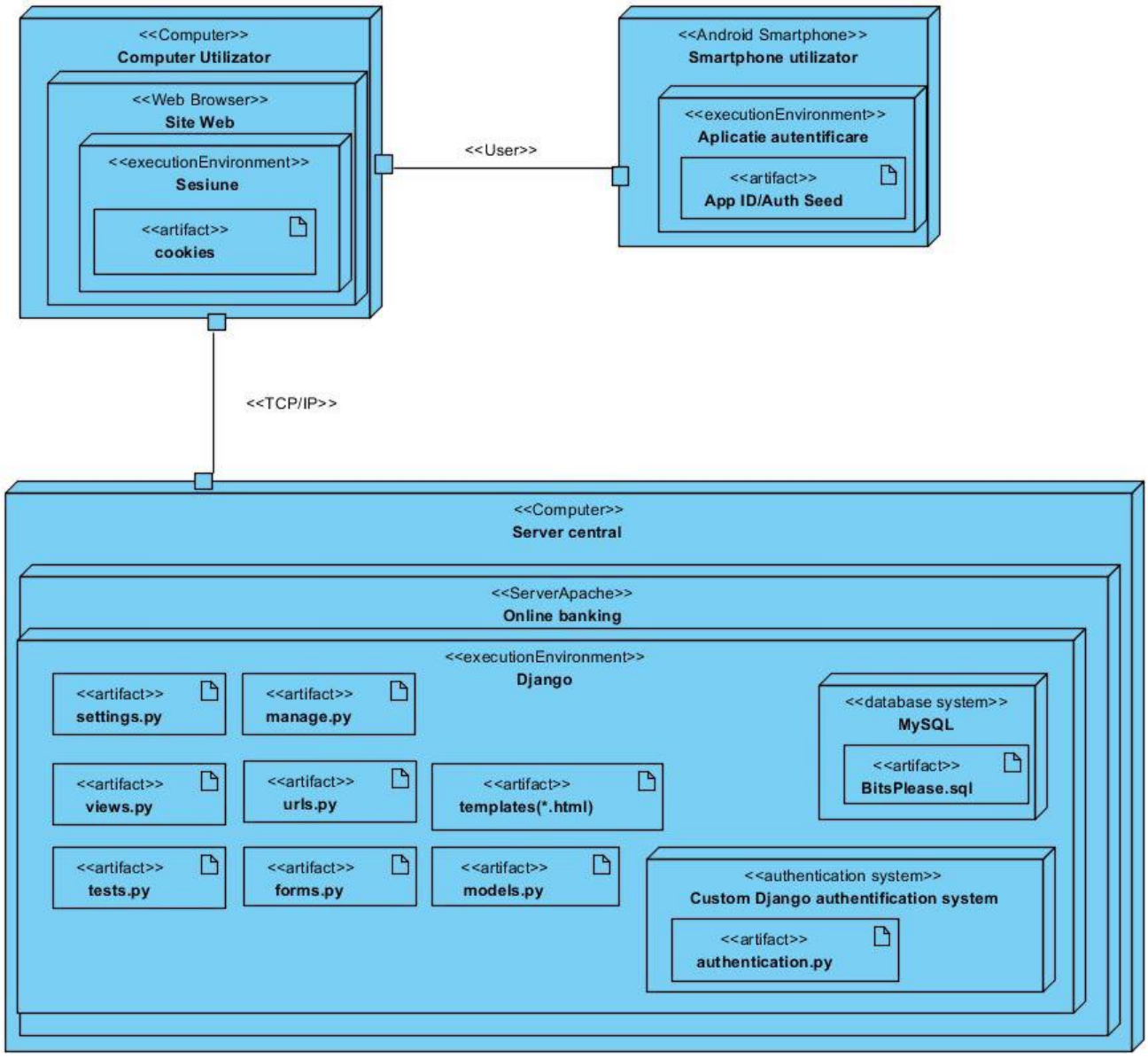
d) Subsistemul de autentificare - inlocuieste backend-ul default de autentificare al Django, pentru a putea oferi functionalitati aditionale(de ex. 2-factor authentication). Este incapsulat in serverul central.
e) Serverul central - este backend-ul aplicatiei noastre, implementat in Python3, folosind framework-ul Django. Asigura intreaga functionalitate a aplicatiei. In varianta finala, va rula pe un webserver Apache.

3.2 Decompozitia in subsisteme si responsabilitatile fiecarui subsistem

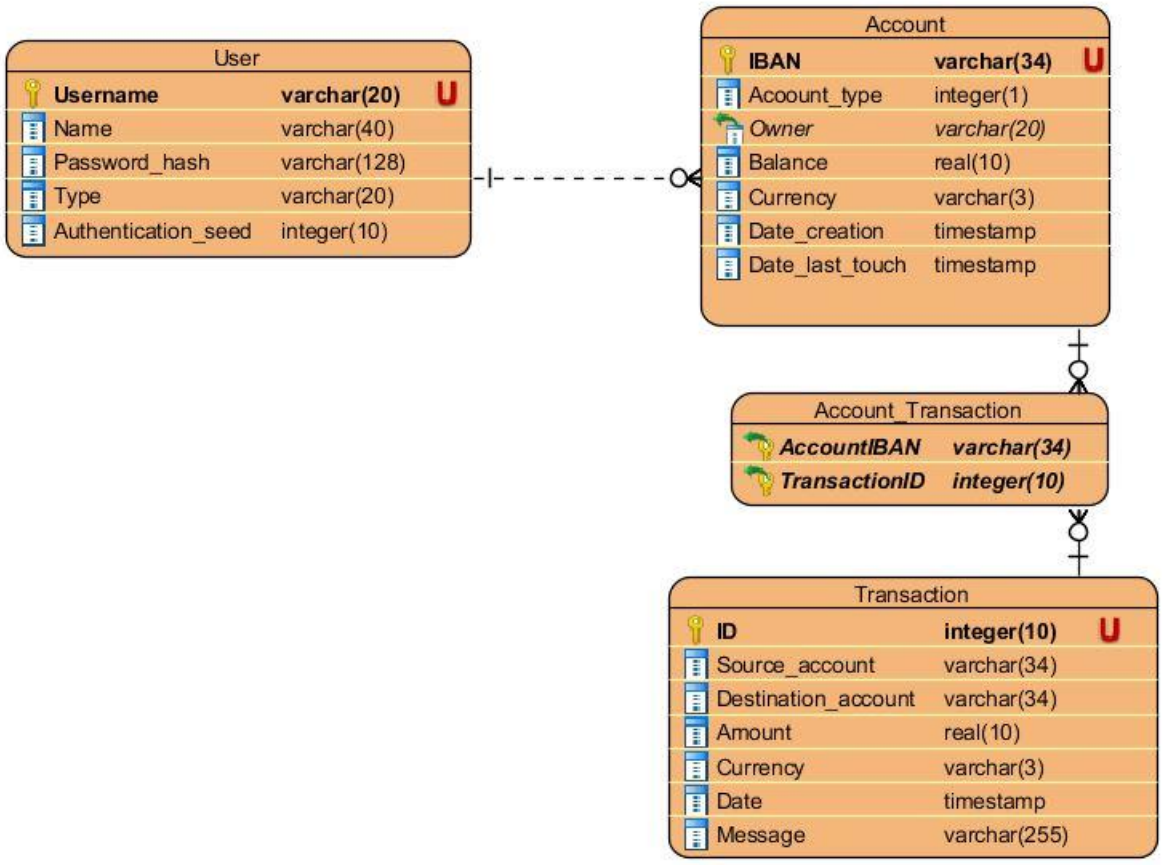




3.3 Distributia subsistemelor pe platforme hardware/software



3.4 Managementul datelor persistente



3.5 Controlul accesului utilizatorilor la sistem

Autentificarea utilizatorilor in sistem se va face in 2 pasi: clientii obisnuiti vor folosi autentificatorul Android pentru generarea unui cod de verificare, in timp ce comerciantii, bancherii si administratorii vor fi verificati pe baza adresei IP.

Fiecare categorie de utilizatori are acces la diferite operatii, backend-ul fiind cel care verifica tipul utilizatorului si are grija sa ii ofere doar functionalitatile proprii:

a) Client - autentificare, tranzactii online, obtinere extras de cont, adaugare/eliminare conturi
b) Comerciant - autentificare, tranzactii online(solicitare plata de la un client), obtinere extras de cont
c) Bancher - autentificare, depunere/retragere numerar, adaugare/eliminare client din sistem
d) Administrator - autentificare, obtinere statistici/raport sistem bancar, adaugare/eliminare bancher din sistem

3.6 Conditiile limita (cazurile de utilizare limita)

- Ceasul serverului si cel al telefonului pe care ruleaza aplicatia de autentificare two factor pot sa nu fie exact sincronizate, desi isi iau timestampul de la acelasi server NTP (poate exista riscul ca diferenta sa fie chiar de cateva secunde), rezultand ca aplicatia genereaza un cod iar serverul alt cod. Din aceasta cauza in generarea codurilor de autentificare timestampul actual se va trunchia la un timestamp multiplu de 30 secunde. In primele si ultimele secunde(perioada determinata de diferenta dintre ceasul serverului si al telefonului) din intervalul de 30 secunde pot aparea diferente intre codul serverului si al telefonului, caz in care autentificarea va esua. Utilizatorului trebuie doar sa incerce sa se logheze inca odata, sansele ca si acum sa pice in intervalul de desincronizare fiind foarte mici si scazand substantial cu fiecare incercare de logare succesiva.

- Se inregistreaza incercari repetate de fortare a autentificarii: este necesara blocarea contului respectiv.

- Defectarea dispozitivelor de stocare: datele vor fi stocate pe mai multe dispozitive pentru a asigura redundanta.