

Abstract

Lista figurilor

Figura 1: Schemă design.....	9
Figura 2: Arhitectura detaliată a sistemului	11
Figura 3: Interacțiunea utilizatorului cu sistemul.....	12
Figura 4: Diagrama de activitate a interacțiunii utilizatorului cu sistemul	13
Figura 5: Structura unei componente angular	16
Figura 6: Structura aplicației web	17
Figura 7: Codul de rutare	18
Figura 8: Reprezentarea lampei	19
Figura 9: Structura serverului Java	21
Figura 10: Dependența la baza de date, definită pom.xml	22
Figura 11: Procedura responsabilă de conectarea la un dispozitiv.....	23
Figura 12: Comenzile protocolului de comunicare	25
Figura 13: Comanda pentru generarea certificatului SSL/TLS.....	28
Figura 14: Captură a comunicației dintre server și un dispozitiv	29
Figura 15: Documentația interactivă a server-ului.....	30
Figura 16: Documentarea unei metode	31
Figura 17: Observarea traficului HTTP dintre aplicația web și server	32
Figura 18: Makefile-ul dispozitivului lampă	34
Figura 19: Conținutul scriptul ce pornește toate dispozitivele simultan	34
Figura 20: KY-008 Modulul senzor laser.....	35
Figura 21: KY-016 Modul LED cu 3 culori	36
Figura 22: KY-019 Modul releu 5V.....	36
Figura 23: KY-011 Modul LED cu 2 culori	36

Lista tabelelor

Tabelul 1: Definirea protocolului de comunicare.....	26
--	----

Cuprins

Abstract	i
Lista figurilor.....	ii
Lista tabelelor.....	ii
Cuprins	iii
Introducere.....	1
Context	1
Motivație	1
Ce este „Smart Home”?	2
Facilitățile traiului într-o casă inteligentă.....	3
Provocări	5
1. Contribuții	7
2. Arhitectura sistemului.....	8
2.1. Proiectare	8
2.2. Detalii arhitecturale.....	10
2.3. Exemplificare scenarii, cazuri de utilizare și fluxuri de activități.....	12
3. Implementare.....	15
3.1. Modulul 1 – Aplicația web.....	15
3.1.1. Structura proiectului	16
3.1.2. Rutarea	17
3.1.3. Serviciul de autentificare.....	19
3.1.4. Librării folosite.....	19
3.2. Modulul 2 – Server REST Java.....	20
3.2.1. Structura proiectului	20
3.2.2. Server REST.....	22
3.2.3. Managerul de dispozitive și protocolul de comunicare	24
3.2.4. Securitatea serverului	26
3.2.5. Unelte folosite.....	29
3.3. Modulul 3 – Dispozitivele „inteligente”	33
3.3.1. Interacțiunea cu Raspberry Pi	33
3.3.2. Dispozitive implementate	35
3.3.2.1. Laser de securitate	35
3.3.2.2. Lampă.....	35
3.3.2.3. Încuietoare a ușii.....	36
3.3.2.4. Bec.....	36

4.	Direcții de viitor	37
	Concluziile lucrării	38
	Bibliografie	39

Introducere

Context

Persoanele își petrec cea mai mare parte a timpului la domiciliu sau la locul de muncă; pentru mulți, aceste locuri sunt sanctuarele lor. Pe parcursul secolului al XX-lea, progresele tehnologice au contribuit la sporirea confortului și protecției oferite de casele noastre. Observațiile asupra mediului casnic și modelarea comportamentului său sunt utile în a face mediile mai inteligente și mai receptive la nevoile noastre. Progresele recente au adus o astfel de „inteligență ambientală” mai aproape de realitate. Chiar dacă idea de casă inteligentă există de ceva vreme, case inteligente reale există doar de puțin timp.

De la miniaturizarea microprocesoarelor, puterea de calcul a fost încorporată în obiecte familiare, cum ar fi aparatele de uz casnic și dispozitivele mobile, regăsindu-se aproape la toate nivelurile societății. Inteligența ambientală extinde noțiunea de calcul pentru a oferi suport personalizat și automatizat în viețile noastre.

Ideea [de casă inteligentă] este următoarea: software-ul de calculator joacă rolul unui agent inteligent ce percepe starea mediul fizic și a rezidenților utilizând senzori, raționează în legătură cu starea acestora folosind tehnici de inteligență artificială și apoi ia măsuri pentru a atinge obiectivele specificate, cum ar fi maximizarea confortului locuitorilor, minimizarea consumul de resurse și menținerea sănătății și siguranței locuinței și a locuitorilor. [1]

Motivație

Primele case inteligente au fost idei, nu construcții reale. Timp de decenii, literatura științifico-fantastică a explorat ideea automatizării locuințelor. Producători prolifici, cum ar fi Ray Bradbury¹, și-au imaginat un viitor în care casele vor fi interactive. În scurta povestire a lui Bradbury, „There Will Come Soft Rain”², se descrie o casă automată care continuă să funcționeze chiar și după ce oamenii au dispărut. Sună un pic înfricoșător, până când luați în considerare beneficiile reale ale automatizării locuințelor, iar apoi ideea devine mai mult confortabilă decât descurajatoare.

¹ Ray Douglas Bradbury (n. 22 August 1920 – d. 5 Iunie 2012): scriitor de romane științifico-fantastice, fantezie, horror și mister.

² „Va veni ploaie ușoară”: povestire scurta publicată pe data de 6 Mai 1950.

Atunci când nu sunteți acasă, aveți tot felul de suspiciuni care vă îngrijorează? Am oprit cafetiera? Am închis ușa de la intrare? Oare am lăsat apă aprinsă în baie? Cu o locuință inteligentă, aceste îngrijorări nu-și mai au locul. Puteți afla informații despre locuința dumneavoastră folosindu-vă de tabletă, telefon sau calculator personal. Puteți conecta dispozitivele și aparatele de la domiciliu pentru a comunica cu ele. De altfel, dispozitivele pot fi programate pentru a comunica între ele.

Lucrare de față își propune implementarea ideii de casă inteligentă și aducerea la cunoștiință, prin exemple practice, a avantajelor folosirii unui astfel de sistem. În exemplele oferite, voi folosi drept locuință inteligentă un Raspberry Pi³ 2, Model B, iar dispozitivele controlate de utilizator vor fi module arduino⁴.

Inovația acestei lucrări constă în implementarea unui sistem de la zero, cu o arhitectură unică, folosind tehnologii de ultimă generație. Arhitectura sistemului este formată din 3 componente: partea de front-end⁵ care are drept scop interacțiunea eficientă și facilă cu utilizatorul; partea de back-end⁶ ce constă într-un server java care se ocupă de managementul utilizatorilor și al dispozitivelor, oferind siguranță, încredere și eficiență; partea de dispozitive ale utilizatorului ce folosește un protocol de comunicare securizată cu partea de back-end. Protocolul de comunicare oferă un management al erorilor foarte strict pentru a ține utilizatorul la curent cu starea dispozitivelor chiar și în cazuri de excepție.

Ce este „Smart Home”?

„Smart Home”⁷ este termenul utilizat în mod obișnuit pentru a defini o reședință care are iluminat, încălzire, aer condiționat, televizoare, calculatoare, sisteme audio și video de divertisment, sisteme de securitate și camere de luat vederi capabile să comunice între ele și pot fi controlate de la distanță: din orice cameră din casă, precum și din orice locație din lume, prin telefon sau prin internet.

Smart home este un sistem care oferă deținătorilor locuinței confort, securitate, eficiență energetică (costuri de operare scăzute) și comoditate în orice moment, indiferent dacă este cineva acasă sau nu.

³ Raspberry Pi: <https://www.raspberrypi.org/>

⁴ Modul arduino: este un circuit hardware complex, adus la o formă compactă pentru utilizare, cu o interfață de conexiune simplă, ce necesită doar atasarea unor fire între placă și circuit.

⁵ Front-end: Parte a site-ului pe care o putem vedea și cu care interacționează vizitatorii.

⁶ Back-end: Locul unde se administrează informația. De obicei este format din server și bază de date.

⁷ Smart Home: Echivalentul acestui termen în limba română este „Casă Inteligentă”.

Instalarea de produse inteligente oferă locuinței și ocupanților săi diverse beneficii - aceleași avantaje pe care tehnologia și computerele personale le-au adus în ultimii 30 de ani - confort și economii de timp, bani și energie. [2]

Facilitățile traiului într-o casă inteligentă

Multora nu le place ideea de „Smart Home” considerând că va fi prea costisitoare, greu de folosit, sau nu vor avea suficient control asupra propriului mediu. Cu toate acestea, casele inteligente devin foarte accesibile, datorită opțiunii de a construi puțin câte puțin, înglobând părțile într-un proiect mare, lăsându-se loc pentru îmbunătățiri viitoare. Fiecare dispozitiv vă stă la dispoziție pentru a vă face viața mai confortabilă.

În continuare voi enumera câteva motive pentru care ar trebui luați în considerare un smart home: [3]

1. Confort

Una dintre cele mai bune părți ale locuinței inteligente este că o puteți configura pentru a corespunde cu exactitate necesităților dumneavoastră. Lampa trebuie să fie configurată la o luminozitate corectă, nu prea luminoasă, dar nici prea întunecată. Puteți chiar să setați aprinderea luminilor treptat, evitând astfel blițul brusc de lumină orbitoare.

Puteți să setați o melodie liniștită atunci când alarmele se sting dimineața, astfel încât să vă treziți într-o atmosferă plăcută. Puteți amplasa difuzoarele în mai multe încăperi pentru a fi programate să difuzeze diferite melodii la diferite volume, astfel încât să puteți asculta mereu ceea ce doriți în orice loc din casă.

De asemenea, aveți posibilitatea ca temperatura casei să fie menținută la valoarea optimă. Instalația de încălzire și climatizare poate fi controlată de la distanță printr-un termostat, astfel încât în casă să nu fie niciodată prea rece sau prea cald.

2. Securitate

Există nenumărate motive pentru care o casă inteligentă vă poate menține în siguranță. Puteți avea senzori specifici pentru a detecta imediat mișcarea, cum ar fi noaptea sau în timp ce vă aflați la serviciu. Dacă detectorii de mișcare sunt avertizați, vi se poate trimite o notificare telefonului dumneavoastră și/sau se pot aprinde luminile pentru a da impresia că sunteți treaz, acest lucru sperându-l pe potențialul spărgător.

Puteți avea senzori pe ferestre și uși, astfel încât să știți dacă au fost deschise sau dacă au fost distruse.

O mulțime de case inteligente au camere video instalate care vă permit să monitorizați orice cameră utilizând dispozitivul inteligent sau terminalul de perete. Puteți seta secțiuni ale ecranului pentru a detecta mișcarea, astfel încât un animal de companie sau un copac în vânt să nu declanșeze alarma.

Dacă vă montați alarme „inteligente” de incendiu, puteți primi notificări despre potențiale incendii, indiferent dacă vă aflați în casă sau la locul de muncă. Dacă știți că este o alarmă falsă, puteți opri alarma printr-o simplă atingere de ecran, în loc să urcați pe un scaun și să vă întindeți pentru a ajunge la butonul de alarmă.

Mai mult, dacă plecați vreodată în vacanță puteți alege între a obține personal notificări despre cazurile excepționale sau a fi transmise unui vecin ori unui membru al familiei.

3. Ușor de utilizat

Partea cea mai convenabilă a unei locuințe inteligente este că fiecare parte a casei ar putea fi doar la o atingere de ecran(sau apăsarea unei taste) distanță. Fie că este vorba de telefonul tău inteligent, tabletă, calculator personal sau un terminal montat în perete.

Când te pregătești să dormi, puteți opri orice lumină din casă doar prin apăsarea unui buton. Puteți să vă uitați la ecranul dumneavoastră și să vedeți că toate ușile și ferestrele sunt blocate, astfel încât să nu trebuiască să mergeți și să le verificați pe fiecare în parte.

Puteți chiar crea setări pentru grupuri de dispozitive, de exemplu, când porniți televizorul, luminile se diminuează automat sau sunetul se aprinde odată cu televizorul. Dimineata puteți seta încălzirea, luminile, muzica pentru a se aprinde când vă ridicați din pat, fără să trebuiască să faceți nimic.

4. Accesibilitate

Casele inteligente oferă un ajutor imens pentru persoanele cu diverse dizabilități. Oamenii care nu văd pot avea interfață vocală cu care pot controla televizoarele, luminile, încălzirea, orice dispozitiv ce este conectat la electricitate și internet. Pentru persoanele cu dizabilități, precum deficiențe musculare, activarea comutatoarelor de lumină sau alarmei de incendiu se poate dovedi a fi un lucru dificil, dacă nu chiar imposibil. Acum, astfel de dispozitive, se pot controla folosind un telefon sau o tabletă. Pentru cineva într-un scaun cu roțile se poate configura deschiderea și închiderea ușilor automat folosind senzori.

Programele pot avea setări personalizate în funcție de utilizatori, astfel scutindu-i de preocupări triviale, cum ar fi setarea zilnică a încălzirii sau luminii.

Familiile care au un membru în vârstă sau poate pe cineva ce suferă de o boală precum Alzheimer⁸ pot avea senzori instalați în casă pentru a fi mai simplă monitorizarea de la distanță a persoanelor în nevoie. Se pot crea alerte care să informeze în caz că ușa frontală este deschisă pe timp de noapte, pot fi atașați senzori la chei pentru a afla dacă se rătăcesc și nu sunt unde vă așteptați să fie. De altfel, se pot crea alerte de inundații în camerele de bucătărie, baie, chiar și monitorizarea casetelor de pastile pentru a vă asigura că sunt luate în fiecare zi.

De asemenea, pot fi instalate cu ușurință butoane de panică, în cazul în care a existat un accident în casă, iar familia sau personalul de îngrijire poate fi anunțat imediat, scutind persoana în nevoie să telefoneze pentru ajutor.

Provocări

O casă inteligentă poate fi un coșmar pentru acei oameni ce nu se simt confortabil cu tehnologia de ultimă generație.

Unul dintre blocajele esențiale în instalarea unui sistem smart home este menținerea echilibrului dintre complexitatea și gradul de dificultate al utilizării lui. Dacă este exasperant de utilizat, atunci o să vă facă viața mai grea în loc să o facă mai ușoară. Când planificați sistemul, este important să luați în considerare câțiva factori:

- Ce tipuri de componente fac parte din sistem? Sunt de bază, de dimensiuni mici sau impunătoare, cum ar fi un sistem de alarmă sau o cameră video?
- Cât de intuitiv va fi sistemul pentru un non-utilizator?
- Dispozitivul îndeplinește o nevoie sau este doar o fantezie și potențial o jucărie frustrantă?
- Câți oameni vor fi nevoiți să utilizeze sistemul?
- Cine va ști cum să opereze sistemul? Cine va ști cum să mențină sistemul și să remedieze eșecurile?
- Cât de ușor este să faceți schimbări în interfață? De exemplu, dacă casa ta este programată să te trezească la 7 dimineața, cum o vei lăsa să știe că ești deplasat peste noapte la birou sau că dorești să dormi mai mult într-o sâmbătă?

Din aceste motive, ar putea fi mai ușor să începeți cu o rețea foarte simplă și apoi să o extindeți atunci când sunt necesare sau dorite îmbunătățiri. Ca multe dintre noile tehnologii, casele inteligente necesită o investiție semnificativă atât în bani, cât și în timp. În caz contrar,

⁸ Alzheimer: tip de demență care cauzează probleme cu memoria, gândirea și comportamentul.

dacă nu aveți nici bani, nici timp, ați putea dori să rămâneți la casa dumneavoastră „veche” și „neinteligentă”.

Înainte de a cumpăra, verificați recenziile despre produse. Există o mulțime de produse care fac promisiuni înalte, dar în lumea reală nu au succes. Și dacă sunteți un utilizator de smartphone, luați în considerare produsele care apar și care au construite pentru ele o aplicație smartphone bine revizuită. Unele aplicații sunt atât de greoaie sau complicate încât provoacă mai multe dureri de cap decât vă ușurează viața.

Casele inteligente vin, de asemenea, cu unele probleme de securitate. Hackerii care găsesc o modalitate de a accesa rețeaua internă pot să dezactiveze sistemele de alarmă, luminile, lăsând locuința vulnerabilă la o spargere. De asemenea, ar putea provoca neplăceri, cum ar fi aprinderea și închiderea rapidă a dispozitivelor electronice, ceea ce ar putea dăuna funcționării sau, într-un caz extrem, ar putea provoca un incendiu.

Producătorii produselor electronice de uz casnic își îmbunătățesc liniile de producție, în speranța că automatizarea locuințelor va ajunge în sfârșit să se realizeze în masă. Mulțumită smartphone-urilor, tabletelor și numeroaselor aplicații de automatizare a locuințelor, disponibile acum, există o șansă că trendul va atrage mai mulți utilizatori.

Asta pentru că, în ciuda atâtor progrese tehnologice, nu există încă un sistem standard pentru automatizarea tuturor acestor gadgeturi⁹. Fără un astfel de standard, mulți consumatori sunt supuși riscului de a cheltui sute sau mii de dolari pe produse care vor sfârși depășite sau inutilizabile într-un scurt timp.

Desigur, se pune problema dacă o persoană are nevoie de toată această tehnologie. Societatea noastră este într-adevăr atât de leneșă și comodă încât nu putem apăsa pe un comutator de lumină? Indiferent de răspunsul acestei întrebări, această tehnologie are drept scop satisfacerea altelor puncte de interes, și anume: datorită timpului pe care îl vom economisi din automatizarea locuinței, vom avea timp de mai multe activități mai puțin triviale. [4]

⁹ Gadget: obiect tehnologic mic care îndeplinește o anumită funcție, de obicei fiind ceva nou.

1. Contribuții

2. Arhitectura sistemului

2.1. Proiectare

În ceea ce urmează o să descriu planul pe care l-am abordat pentru a pune în practică ideea de Smart Home.

Sistemul trebuie să fie accesibil din orice locație din lume, din această cauză am ales ca interfața pentru utilizator să fie o aplicație web. Aplicația poate fi accesată de pe telefon, tabletă, calculator personal atât timp cât există conexiune la internet; ceea ce nu ar fi fost la fel de accesibil cu o aplicație Android sau iOS.

Pentru ca dispozitivele din casa dumneavoastră să nu fie accesate de persoane neautorizate, fiecare utilizator va avea un cont personal, ce va fi accesat pe baza unor credențiale.

Partea de back-end, altfel spus serverul de back-end, trebuie să ofere:

- un mediu persistent de stocare a datelor;
- înregistrarea, autentificarea¹⁰ și managementul utilizatorilor;
- înregistrarea și controlul dispozitivelor expuse de utilizator;
- managementul conexiunilor dispozitivelor: inițiere, comunicare propriu zisă, finalizare;
- stabilirea unui protocol de comunicare cu dispozitivele „smart”.

Odată stabilite responsabilitățile serverului de back-end, mai rămâne de stabilit modalitatea de conectare a dispozitivelor smart cu partea de back-end și implementarea lor propriu-zisă.

Ce limbaj trebuie folosit pentru a programa cât mai multe tipuri de dispozitive, dacă nu chiar toate dispozitivele posibile? Am ales Java deoarece este un limbaj independent de platforma de lucru, aceeași aplicație rulând fără nicio modificare și fără a necesita recompilarea ei pe sisteme de operare diferite cum ar fi Windows, Linux, Mac OS, după cum se înțelege și din sloganul Java „*Write once, run everywhere*”. Alte calități sunt: simplitate, robustețe, garbage collector¹¹, portabilitate.

Prin urmare dispozitivele trebuie să poată rula cod sursă scris în Java și ar trebui să aibă o conexiune la internet, având în vedere că acestea trebuie controlate de la distanță.

¹⁰ Autentificarea: Are drept scop stabilirea identității actorilor care doresc să comunice sigur în rețea.

¹¹ Garbage collector: Program care face managementul memoriei interne automat.

Comunicarea cu serverul de back-end ar trebui să fie criptată astfel încât un posibil atacator să nu poată descifra nimic din ceea ce se transmite pe rețea. În plus, se pune și problema de certificare a serverului și evitare a unui posibil atac de tip „Man-in-the-Middle”¹². O să descriu în continuare acest tip de atac aplicat pe acest sistem. Un atacator a aflat protocolul de comunicare a serverului cu dispozitivele. Un dispozitiv al unui utilizator este conectat la internet și primește o cerere de conectare de la atacator, care pretinde că este serverul de back-end. Dacă nu ar fi nici o metodă de identificare a serverului real, atunci întreg sistemul este compromis, atacatorul având posibilitatea sa controleze orice dispozitiv disponibil.

Prin urmare, pentru a evita o astfel de problemă, ce dovedește sistemul a fi inutilizabil, am să folosesc protocolul criptografic SSL(Secure Sockets Layer)/TLS (Transport Layer Security)¹³ între server și client. SSL/TLS este un protocol criptografic care poate asigura confidențialitate, integritatea mesajelor și autentificarea părților. SSL/TLS acționează asupra unui flux TCP(Transport Control Protocol) și oferă servicii nivelurilor superioare.

În Figura 1 de mai jos este reprezentată o schiță pentru design-ului sistemului.

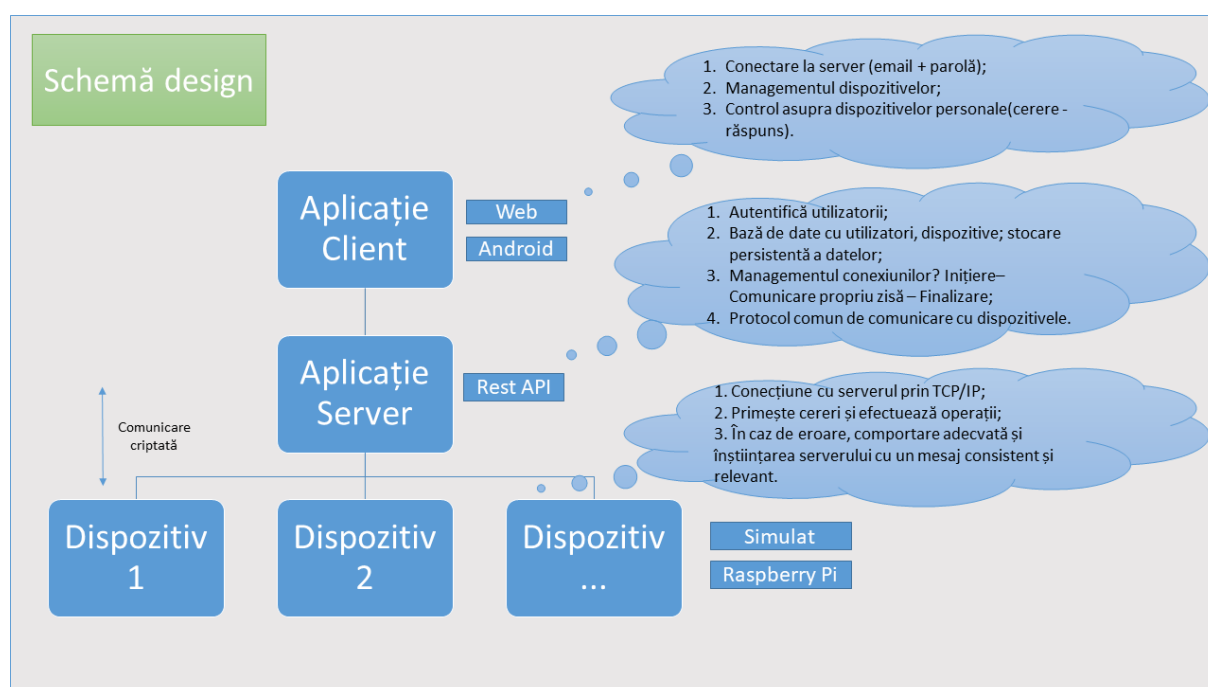


Figura 1: Schemă design

¹² Man-in-the-middle: detalii aici: <https://arxiv.org/ftp/arxiv/papers/1504/1504.02115.pdf>

¹³ SSL/TLS: Când protocolul SSL a fost standardizat de către IETF, a fost redenumit în TLS.

2.2. Detalii arhitecturale

În urma proiectării s-a conturat o arhitectură formată din trei module principale. Primul modul constă într-o aplicație web care are drept scop principal comunicarea și interacțiunea cu utilizatorul. Al doilea modul este o aplicație Java, ce servește pe post de server, fiind „creierul sistemului”. Am numit acest modul astfel deoarece face legătura între ceea ce vede utilizatorul și cum se desfășoară firul logic al acțiunilor în spate. Al treilea modul este format din aplicații client ce vor juca rolul de dispozitive din cadrul unei case inteligente.

Utilizatorul interacționează cu sistemul prin intermediul primului modul, aplicația web. Aplicația structurează informațiile necesare utilizatorului astfel încât interacțiunea cu dispozitivele personale să fie cât mai simplă și facilă.

Modulul al doilea este responsabil în oferirea de răspunsuri pentru toate cererile ce vor veni de la utilizator, prin intermediul aplicației web. Paradigma de programare a serverului este REST(Representational State Transfer). REST este un stil arhitectural de dezvoltare al aplicațiilor Web cu focalizare asupra reprezentării datelor. Rezultatul unei procesări conduce la obținerea unei reprezentări a unei resurse. Formatul reprezentării e desemnat de tipuri MIME(Multipurpose Internet Mail Extensions) text/html, text/xml, text/csv, application/json, image/png, etc. Clienții (e.g., navigatoare Web, roboți, player-e etc.) interacționează cu reprezentările resurselor via verbe: „accesează” – GET, „modifică” – POST, „șterge” – DELETE, ș.a.m.d. . [5] Am ales această paradigma de programare deoarece oferă o separare între client și server, vizibilitate, scalabilitate, api-ul¹⁴ REST fiind mereu independent de tipul de platformă sau limbajul de programare folosit.

Modulul al treilea, responsabil de dispozitivele inteligente, va fi simulat folosind un Raspberry Pi și module arduino. Un Raspberry Pi este, după cum îl prezintă producătorii, un microcomputer de dimensiunile unui card de credit, fiind cel mai mic și ieftin computer din lume. Un modul arduino este un circuit hardware complex, adus la o formă compactă pentru utilizare, ce are o interfață de conexiune simplistă necesitând doar atașarea unor fire între placă și circuit. Producătorul modulului oferă informații despre funcționalitatea pinilor de ieșire și modul lor de conexiune. Am ales aceste componente pentru că, în primul rând, este ieftin din punct de vedere financiar. În al doilea rând, module arduino oferă o interacțiune minimală cu dispozitivele hardware. În al treilea rând, Raspberry Pi oferă un mediu pentru crearea dispozitivelor foarte ușor și plăcut de utilizat. Pentru programarea dispozitivelor arduino am folosit o bibliotecă pentru controlarea fluxului de intrare ieșire a unui Raspberry Pi, Pi4J [6].

¹⁴ API: Application Programming Interface

Figura 2, conține arhitectura detaliată a sistemului. După cum se poate observa, sistemul folosește o arhitectură bazată pe niveluri. Fiecare nivel efectuează anumite operații și oferă funcționalități nivelelor superioare. Comunicarea între niveluri se realizează astfel:

- aplicația client comunică cu aplicația server via verbe HTTP(Hyper Text Transfer Protocol), schimbând resurse în format MIME.
- aplicația server comunică cu dispozitivele conectate la Raspberry Pi printr-un protocol definit peste TCP, ce urmărește pattern-ul cerere-răspuns.

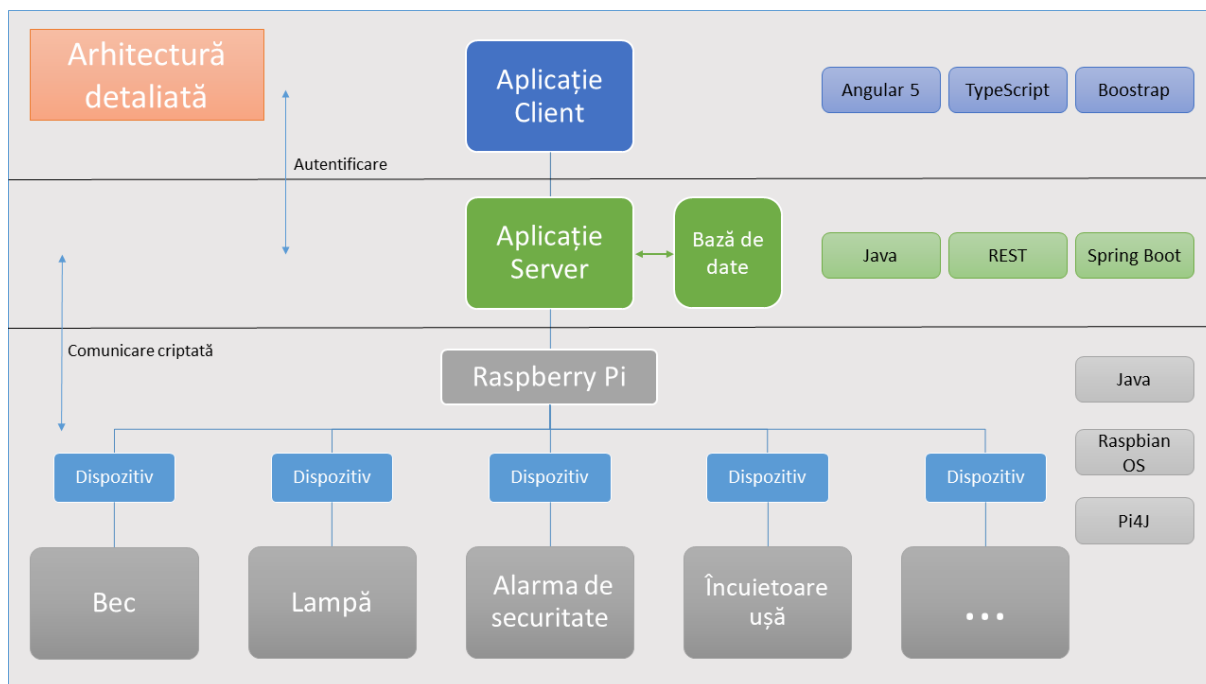


Figura 2: Arhitectura detaliată a sistemului

Scopul protocolul de comunicare este de a îndeplini următoarele funcționalități:

- Crearea și finalizarea unei conexiuni cu dispozitivul;
- Testarea conexiunii;
- Aflarea statusului dispozitivului;
- Aflarea tipului de dispozitiv;
- Interogarea parametrilor pe care dispozitivul îi acceptă;
- Setarea anumitor configurări;
- Interogarea valorilor curente.

Atunci când se construiește un dispozitiv trebuie stabiliți parametri personalizați. Parametrii unui dispozitiv nu vor fi cunoscuți apriori de către serverul Java. După ce se face conexiunea cu dispozitivul se vor afla parametrii acestuia în urma unei interogări aplicate dispozitivului. Acest lucru face protocolul de comunicare dinamic, o eventuală schimbare a

parametrilor nu va afecta în niciun fel comunicarea dintre server și client. Totuși, aplicația web va fi afectată, deoarece acolo este necesară cunoșterea exactă a numelui parametrului ce este primit.

2.3. Exemplificare scenarii, cazuri de utilizare și fluxuri de activități

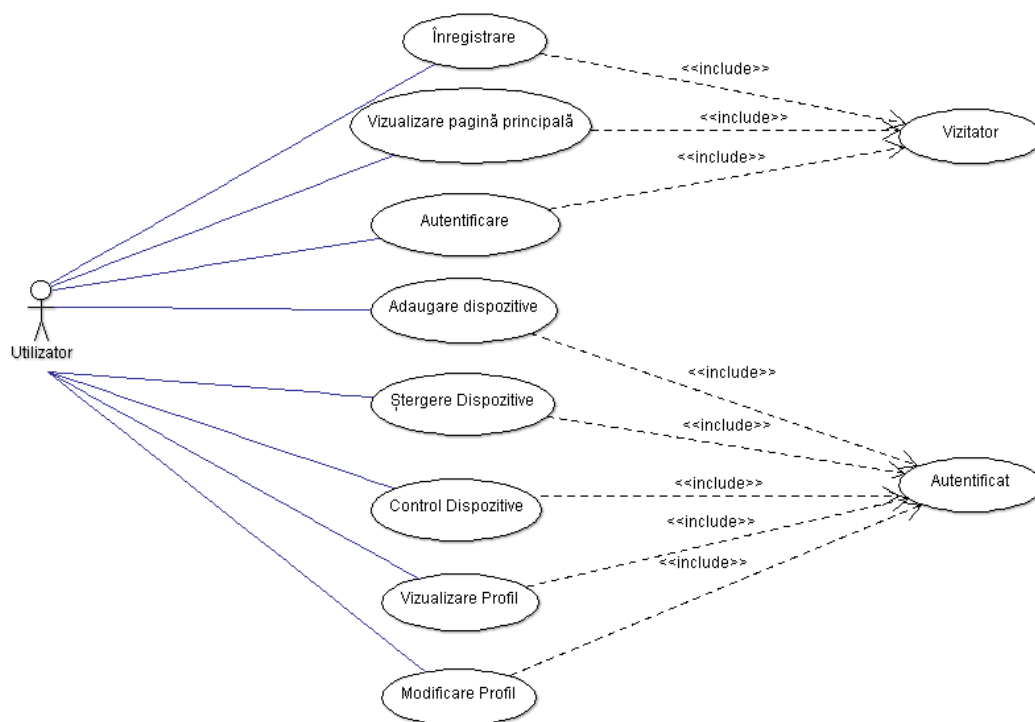


Figura 3: Interacțiunea utilizatorului cu sistemul

Figura 3, de mai sus, conține o diagramă cu cazurile de utilizare a sistemului. Utilizatorul poate să se înregistreze, să vizualizeze pagina principală și să se autentifice(login) dacă este un utilizator vizitator. El nu o să poată accesa alte funcționalități ale sistemului.

Utilizatorul autentificat poate să adauge, să șteargă și să programeze dispozitivele. În plus poate să își vizualizeze profilul și să îl modifice.

Figura 4, localizată mai jos, reprezintă o diagramă de activitate. Această diagramă arată fluxul de activitate rezultat din interacțiunea utilizatorului cu sistemul. Fluxul diagramei este de sus în jos. De exemplu, conectarea la un dispozitiv este poziționată la baza diagramei deoarece trebuie efectuată o secvență de pași până ajunge la aceasta. Evenimentele sunt aranjate cronologic în felul următor: logarea utilizatorului, vizualizarea listei de dispozitive, alegerea

unui dispozitiv din listă, selectarea opțiunii de management al dispozitivului și în cele din urmă conectarea efectivă la un dispozitiv.

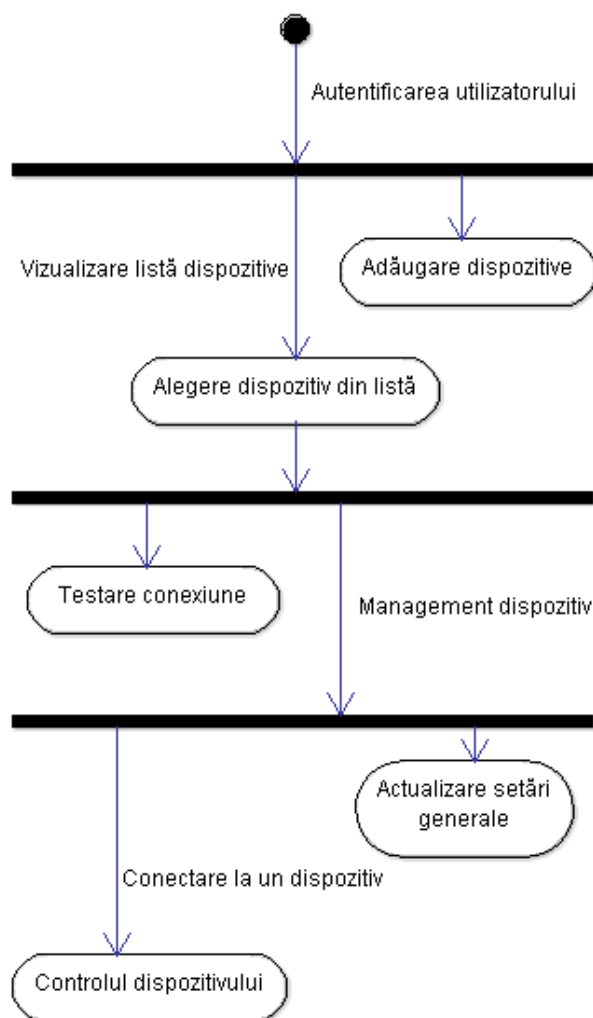


Figura 4: Diagrama de activitate a interacțiunii utilizatorului cu sistemul

Un scenariu important ține de managementul conexiunilor dispozitivelor. Utilizatorul efectuează manual conectarea la dispozitive, prin apăsarea butonului „Connect” de pe interfața grafică. La deconectare deja încep să apară unele întrebări. Cazul ideal este când utilizatorul apasă pe butonul de deconectare înainte să închidă pagina sau să iasă din cont, asigurându-se astfel că dispozitivul este închis. Ce se întâmplă atunci când se conectează la dispozitiv și apoi închide tab-ul din browser? Sau iese din cont? Sau chiar închide browser-ul? Aceste cazuri trebuie tratate corespunzător pentru a nu consuma resurse inutile sau a defecta dispozitivele. În primul rând o modalitatea de a trata anumite cazuri este folosind interceptarea de evenimente cum ar fi închiderea tabului, ieșirea din cont, închiderea browser-ului.

Din cauza dependențelor dintre evenimente și mediul de lucru, cum ar fi browser-ul folosit de client în accesarea site-ului web, o soluție independentă de mediu de lucru ar fi folosirea unui mecanism de expirare a unei unități de timp prestabilite. Un astfel de mecanism va acționa pe partea de server, pentru a avea control complet. Mecanismul va funcționa în următorul mod: atunci când un utilizator se va conecta la un dispozitiv sau va face o setare dispozitivului, un timer(cronometru) va fi activat. Dacă utilizatorul face o acțiune în timp ce timer-ul este activ, atunci se va relua număratoarea de la început. Timer-ul va avea o valoare inițială prestabilită, de exemplu – 20 de minute. Sumarizând, comportamentul rezultat este: dacă utilizatorul nu face nici o operație asupra unui dispozitiv, într-un interval mai mare de 20 de minute, atunci conexiunea cu dispozitivul este încheiată, fără a afecta starea pe care o avea înainte de deconectare. Astfel, am obținut un comportament sigur, independent de browser, ce asigură managementul eficient al resurselor.

3. Implementare

3.1. Modulul 1 – Aplicația web

Modulul de aplicație web este foarte important, deoarece utilizatorul va interacționa cu sistemul folosind interfața web. Pentru ca experiența utilizatorului să fie plăcută și agreabilă, atunci când interacționează cu sistemul, am contruit un design bazat pe următoarele principii:

- *intuitiv*. Atunci când utilizatorul folosește aplicația să nu fie nevoit să citească pagini întregi din manualul aplicației pentru a ști cum se efectuează o operație simplă.
- *modern*. Folosirea tehnologiilor de ultimă generație oferă o experiență plăcută utilizatorului, datorită faptului că noile tehnologii sunt construite în funcție de feedback-ul utilizatorilor.
- *simplist*. Un design poate să înglobeze diverse funcționalități, însă poate eșua în a fi simplu de utilizat. De exemplu, dacă paginile sunt prea încărcate, setarea anumitor opțiuni devine un proces mult prea complicat.
- *responsive*. Design responsive înseamnă capacitatea unui site web de a își adapta conținutul în funcție de dimensiunea dispozitivului de pe care este accesat. Acest lucru duce la atragerea utilizatorilor ce folosesc dispozitive mobile.

Prin urmare, am hotărât să folosesc pentru acest modul două dintre cele mai populare tehnologii web: Angular¹⁵ și Bootstrap¹⁶.

Am ales Angular pentru că este o platformă ce ajută la crearea aplicațiilor SPA¹⁷. Datorită acestui fapt, pagina este fragmentată în mai multe componente ce se încarcă dinamic atunci când utilizatorul interacționează cu aplicația. Această abordare bazată pe componente face ca aplicația să se încarce foarte rapid, să fie modularizată, evitând duplicarea codului.

Apoi, am ales Bootstrap deoarece oferă un suport foarte bun în crearea de site-uri responsive, o documentație foarte bine structurată, cu exemple relevante, ceea ce face developmentul foarte rapid.

¹⁵ Angular: <https://cli.angular.io/>

¹⁶ Bootstrap: <https://getbootstrap.com/>

¹⁷ Single-page application: Aplicație ce interacționează cu utilizatorul rescriind dinamic pagina curentă, în loc să încarce pagini întregi primite de la server.

3.1.1. Structura proiectului

În Figura 5 se poate observa structura unei componente Angular. O componentă conține un fișier .css¹⁸, unul .html¹⁹ și altul .ts²⁰. Acest mod de structurare permite unei componente să nu depindă de altă componentă, astfel reducând cuplajul din interiorul aplicației.

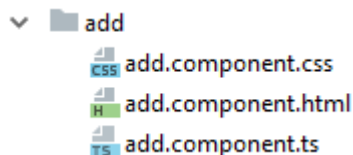


Figura 5: Structura unei componente angular

Prin definiție, cuplajul este măsura gradului de interdependență a claselor. Reformulând această definiție pentru contextul curent, cuplajul este gradul de dependență a unei componente de altă componentă. O componentă are un cuplaj redus dacă nu depinde de multe alte componente.

În Figura 6 se poate observa structura aplicației web, ce conține următoarele module:

- *backendservice*: conține un serviciu responsabil de cererile asincrone către serverul Java și alt serviciu ce este responsabil de autentificarea utilizatorului când se încearcă accesarea anumitor funcționalități;
- *device*: conține componente ce descriu operațiile ce pot fi aplicate asupra dispozitivelor: add – adăugare, manage – management, view – vizualizare;
- *deviceTypes*: conține mai multe componente ce descriu interfețele specifice în funcție de dispozitive: lampă, laser de securitate, încuietorea ușii, bec, etc;
- *footer*: definește subsolul site-ului;
- *header*: definește antetul site-ului. Antetul conține meniul principal;
- *home*: componentă responsabilă de pagina principală;
- *login*: componentă ce se ocupă de autentificarea utilizatorului;
- *notfound*: componentă ce va apărea de fiecare dată când utilizatorul va încerca să acceseze o resursă ce nu este disponibilă;
- *profile*: componentă ce se ocupă de managementul profilului utilizatorului;
- *register*: componenta cu care interacționează utilizatorul când se înregistrează.

¹⁸ Cascade Style Sheets(foaie de stiluri CSS): standard pentru formatarea elementelor unui document html.

¹⁹ Hyper Text Markup Language: limbajul principal al Web-ului pentru crearea de conținut ce poate fi utilizat oriunde.

²⁰ TypeScript: limbaj puternic tipizat, orientat obiect, compilat, superset al lui JavaScript.

3.1.2. Rutarea

Pentru a explica ce este rutarea este necesară definirea termenului „view”. O grupare de elemente prezentate utilizatorului ce se creează și se distrug împreună formează un view.

Rutarea constă în navigarea între view-uri, pe măsură ce utilizatorii execută operații în aplicație.

Figura 7 conține codul responsabil de rutare. Ideea principală constă în definirea unui router²¹ care va fi inclus în modulul aplicației. El va efectua rutarea pe componenta specificată. Obiectul ce conține rutele este o listă, iar în interior conține dicționare ce au următorul format: *path, component, canActivate*. *Path* conține un string cu url²²-ul relativ la aplicație. *Component* definește ce clasă o să fie încărcată, iar *canActivate* definește dacă se poate accesa sau nu ruta respectivă. Dacă *canActivate* lipsește, atunci se poate accesa ruta fără nici o restricție, altfel se va decide dacă se poate sau nu accesa ruta.

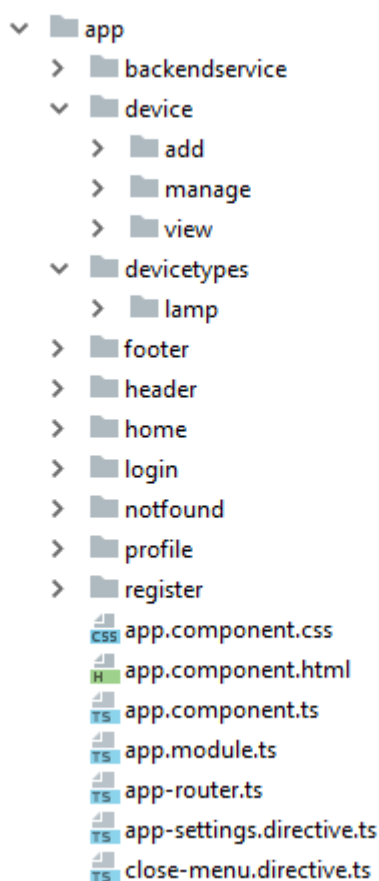


Figura 6: Structura aplicației web

²¹ Obiect responsabil cu navigarea de pe un view pe următorul view.

²² URL (Uniform Resource Locator): localizator uniform de resurse.

```

export const router: Routes = [
  {path: '', component: HomeComponent},
  {path: 'home', component: HomeComponent},
  {path: 'login', component: LoginComponent},
  {path: 'register', component: RegisterComponent},
  {path: 'profile', component: ProfileComponent, canActivate: [AuthGuard]},
  {path: 'devices', component: ViewComponent, canActivate: [AuthGuard]},
  {path: 'devices/add', component: AddComponent, canActivate: [AuthGuard]},
  {path: 'devices/manage/:id', component: ManageComponent, canActivate:
[AuthGuard]},
  {path: '**', component: NotFoundComponent},
];

export const RouterGlobal: ModuleWithProviders =
RouterModule.forRoot(router);

```

Figura 7: Codul de rutare

Consider oportună explicarea path-urilor „**”, „devices/manage/:id” întrucât sunt path-uri speciale. „**” este folosit pentru a controla rutele invalide, ceea ce o să declanșeze componenta `NotFound`, indicându-i utilizatorului, într-o manieră elegantă, faptul că a introdus un link greșit. „devices/manage/:id” are scopul de a capta rutele de forma: <http://localhost:4200/devices/manage/7018dea9-8cb6-4677-a5ea-cfb743ee4dca>, unde „7018dea9-8cb6-4677-a5ea-cfb743ee4dca” este id-ul unui dispozitiv. Se folosește „:id” pentru a avea acces direct la id, evitând astfel parsarea url-ului.

De exemplu, dacă aplicația rulează pe host-ul local, la portul 4200, și utilizatorul introduce în browser următorul url: <http://localhost:4200/home>, atunci, conform router-ului definit, se va încărca componenta `HomeComponent`, fără nicio restricție de accesare. Dacă se introduce în browser url-ul: <http://localhost:4200/profile>, atunci ar trebui să se încarce `ProfileComponent`. Totuși, `AuthGuard` va lua decizia finală dacă se poate sau nu accesa componenta. O să explic în următoarea secțiune ce este `AuthGuard` și care este rolul lui.

3.1.3. Serviciul de autentificare

Într-o aplicație web, există rute publice și rute ce pot fi accesate doar dacă sunt satisfăcute anumite condiții. Una dintre aceste condiții este ca utilizatorul să fie autentificat. Acesta este și cazul de față, AuthGuard fiind un serviciu care verifică utilizatorul este autentificat atunci când accesează anumite rute.

Paginile publice din aceasă aplicație sunt: pagina principală, pagina de autentificare, pagina de înregistrare. Paginile verificate de serviciu sunt: pagina de profil și paginile ce țin de dispozitive. Este necesară verificarea stării utilizatorului, deoarece utilizatorul vizitator (neautentificat) nu are acces la principalele funcționalități oferite de aplicație, pentru aceasta fiind nevoie de un profil înregistrat, însoțit de autentificarea propriu-zisă.

3.1.4. Librării folosite

În crearea aplicației am folosit următoarele librării:

- ngx-toastr [7]
- highcharts [8]
- fontawesome [9]

Ngx-toastr este o librărie ce am folosit-o pentru a afișa mesaje toast utilizatorilor. Un mesaj toast este un mesaj scurt afișat într-un pop-up. Toast-ul dispare automat după un anumit timp sau poate fi închis manual de către utilizator. Am folosit toast-uri pentru a afișa mesaje de diferite tipuri utilizatorilor. Mesajele afișate pot fi de următoarele tipuri: eroare, informare, success, avertizare. Un exemplu de mesaj afișat utilizatorului este un mesaj de eroare, atunci când se încearcă conectarea la un dispozitiv dar nu se reușește din diverse motive tehnice.

HighCharts oferă suport pentru grafice create în javascript. Am integrat un grafic, prezent în Figura 8, în design-ul interfeței obiectului lampă, mai precis pentru funcționalitatea de a seta o anumită culoare. Motivul pentru care am ales această librărie este de a oferi utilizatorului o experiență mai bună, întrucât această reprezentare mi se pare a fi cea mai aproape de realitate, în ceea ce privește interacțiunea cu o lampă.

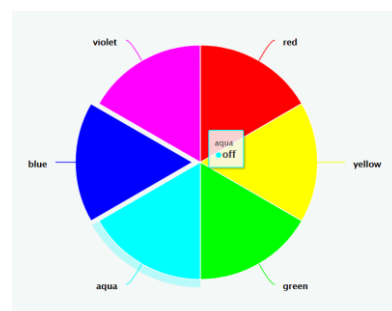


Figura 8: Reprezentarea lampei

FontAwesome este folosit pentru gama largă de pictograme oferite. DETALIERE

3.2. Modulul 2 – Server REST Java

După cum am menționat și la începutul subcapitolului „Detalii arhitecturale”, acest modul este „creierul sistemului” deoarece face legătura între ceea ce vede utilizatorul și cum se desfășoară firul logic al acțiunilor în spate.

Am ales să folosesc pentru acest server Spring Boot²³, un framework de Java foarte popular în construirea de aplicații web și enterprise. Nu este prima dată când interacționez cu acest framework, rămânând cu un gust plăcut după fiecare proiect scris utilizând acest framework.

Paradigma de programare a serverului este REST²⁴. REST este un stil arhitectural de dezvoltare al aplicațiilor Web cu focalizare asupra reprezentării datelor. Rezultatul unei procesări conduce la obținerea unei reprezentări a unei resurse. Formatul reprezentării e desemnat de tipuri MIME²⁵ text/html, text/xml, text/csv, application/json, image/png, etc. Clienții (e.g., navigatoare Web, roboți, player-e etc.) interacționează cu reprezentările resurselor via verbe „accesează” : GET, „modifică” : POST, „șterge” : DELETE, șamd. [5] Motivul pentru care am ales această paradigma de programare deoarece oferă o separare între client și server, vizibilitate, scalabilitate, api-ul REST este mereu independent de tipul de platformă sau limbajul de programare folosit.

3.2.1. Structura proiectului

În Figura 9 se poate observa structura serverului Java, ce este formată din:

- *controllers*: o colecție de controllere sunt responsabile cu preluarea cererilor de la client gestionând resursele necesare satisfacerii cererilor;
- *dtos*: acronim pentru „Data Transfer Object”, folosite pentru a încapsula date ce vor fi trimise între server și aplicația web;
- *entities*: pachet ce conține o colecție de entități din baza de date. Entitățile sunt obiecte ce pot exista independent;
- *hal*: acronim pentru „Hardware Abstraction Layer”. Acest pachet este folosit pentru comunicarea cu dispozitivele inteligente;
- *repositories*: pachet ce conține mai multe colecții de date. Am folosit această abordare pentru a evita dublare logicii în accesul la date;

²³ Spring Boot: <https://spring.io/projects/spring-boot>

²⁴ REST: https://www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm

²⁵ MIME: <https://www.iana.org/assignments/media-types/media-types.xhtml>

- *security*: pachet responsabil cu securitatea serverului, conține filtre http și partea de autentificare;
- *service*: pachet ce conține serviciile utilizate în server cum ar fi: managerul de dispozitive sau serviciul responsabil cu utilizatorii;
- *SwaggerConfig*: clasă responsabilă cu configurarea Swagger-ului²⁶;
- *Application.properties*: fișier responsabil cu configurări ale aplicație. Aici se găsesc configurări cum ar fi: portul la care rulează serverul, șirul de caractere ce reprezintă conexiunea la baza de date, numele utilizatorului ce poate accesa baza de date, ș.a.m.d.

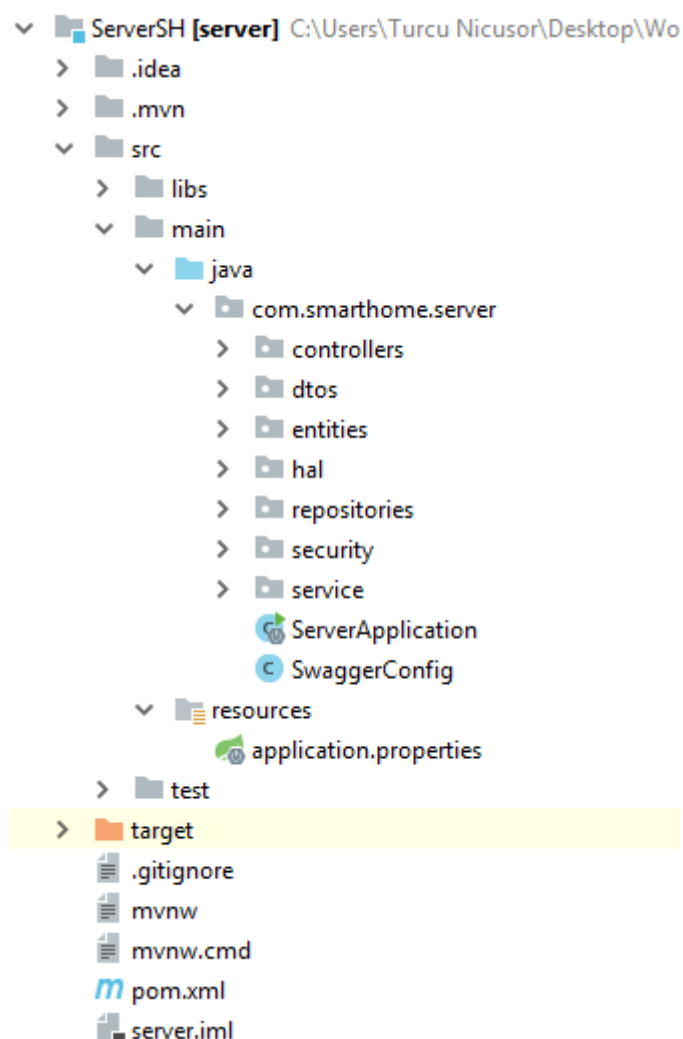


Figura 9: Structura serverului Java

²⁶ Swagger: <https://swagger.io>

Fișierul pom.xml conține dependențele din cadrul server-ului. Ele sunt specificate în format xml, după cum se vede și în Figura 10. Atunci când se specifică dependențele, se caută online, după ce au fost găsite, se salvează și la nivel local.

```
<dependency>

    <groupId>mysql</groupId>

    <artifactId>mysql-connector-java</artifactId>

    <scope>runtime</scope>

</dependency>
```

Figura 10: Dependența la baza de date, definită pom.xml

3.2.2. Server REST

Programarea la nivel de server necesită cunoașterea unei anumite terminologii. Termenii pe care îi voi explica vor fi următorii: repository, entități, DTO(data transfer object), controller, bază de date.

O bază de date se poate defini în 2 moduri. În general, o bază de date este organizarea unei colecții de date, indiferent de tipul lor. Mai teoretic, o bază de date este un sistem electronic care permite ca datele să fie ușor accesate, modificate și actualizate.

DTO(data transfer object), în traducere obiect de transfer de date, este termenul desemnat pentru a defini un obiect ce încapsulează date ce sunt trimise de la un subsistem la altul. În cazul meu, un dto este folosit pentru a transfera informații între server și aplicația web.

O entitate este orice obiect pe care dorim să îl păstrăm într-o bază de date. Entitățile pot fi: concepte concrete, abstracte, recunoscute; evenimente, lucruri, locuri, etc. Exemple clasice ce sunt folosite deseori și în exemplificări sunt: angajat, student, profesor. Din punct de vedere informatic, o entitate este o tabelă din baza de date relațională.

Un repository este o abstractizare asupra unei baze de date. Permite utilizarea obiectele, fără a avea nevoie să știi cum se face managementul lor în spate. Două dintre avantajele folosirii sunt: existența un singur loc unde se fac modificări în accesul datelor precum și existența unui singur loc responsabil pentru mai multe tabele.

Un controller face de obicei, doar un lucru: primește o intrare și generează rezultat. Mai detaliat, un controller primește cererile utilizatorului, apoi delegă de obicei un serviciu în a rezolva cererea, iar când cererea se rezolvă, el răspunde cu mesajul corespunzător.

Acum că am terminat definirea de termeni, voi continua explicarea construcției serverului.

Atunci când un utilizator efectuează o operație pe partea de aplicație web, atunci un cerere va fi trimisă serverului. Prima componentă întâlnită va fi filtrul http. Filtrul http este descris în subcapitolul 3.2.4 Securitate. Apoi cererea trece de la filtrele http la controller-ul corespunzător. În aplicație există trei controllere: pentru dispozitive, utilizatori, și pentru autentificarea utilizatorilor. Fiecare controller are o responsabilitate exactă.

Figura 11, de mai jos, conține procedura responsabilă de conectarea la un dispozitiv. „@PutMapping” este o adnotare ce are următoarea semnificație: metoda se apelează atunci când verbul http din cerere este PUT. Calea „/connect” reprezintă url-ul relativ la metodă. Această metodă necesită în antetul HTTP token-ul de autorizare, pentru identificarea utilizatorului ce a făcut cererea, iar ca parametru de interogare, id-ul dispozitivului, pentru identificare dispozitivului la care de dorește conectarea. Metoda aparține controller-ului „DevicesController” de aceea, url-ul complet prin care va fi accesată această metodă este: [http://localhost:9000/device/connect?device=hash dispozitiv](http://localhost:9000/device/connect?device=hash_dispozitiv).

```
@PutMapping("/connect")

    ResponseEntity connect(@RequestHeader("Authorization") String token,
    @RequestParam("device") String hash) {

        ResponseEntity response = checkDevice(token, hash);

        if (response.getStatusCode() != HttpStatus.OK) return response;

        try {

            deviceManager.getHalDevice(hash).connect();

        } catch (Exception e) {

            return
ResponseEntity.status(HttpStatus.EXPECTATION_FAILED).body("Connect failed.
Reason: " + e.getMessage());

        }

        return ResponseEntity.status(HttpStatus.OK).body("");

    }
```

Figura 11: Procedura responsabilă de conectarea la un dispozitiv

Metoda verifică mai întâi ca dispozitivul să existe și ca utilizatorul să aibe drept să îl acceseze, iar apoi se delegă responsabilitatea managerului de dispozitive ce va efectua operația de conectare. Metoda `checkDevice` nu este inclusă în blocul `try catch` pentru că face o verificare a condițiilor minime de continuare execuției metodei. Blocul `try catch` tratează cazurile de excepție, returnând aplicației web un mesaj corespunzător. În cazul în care totul merge conform planului, atunci se va apela ultima linie din metodă, care va întoarce un status `http 200`, adică totul s-a realizat cu succes, conectarea la dispozitiv fiind reușită.

Repository-urile le-am folosit în accesarea datelor corespunzătoare utilizatorilor și dispozitivelor necesare. Datele preluate sunt sub formă de entități, definite corespunzător, fiind extrase dintr-o bază de date. Pentru baza de date am folosit MySQL²⁷, toate setările de conectare fiind definite în fișierul „`application.properties`”.

Un exemplu de dto folosite este dto-ul de înregistrare. El are următorii membrii privați: *firstName*, *lastName*, *email*, *password*. Fiecare membru are validare corespunzătoare, de exemplu, la câmpul de email se verifică formatul email-ului să fie valid. Acest obiect se completează după ce utilizatorul completează formularul de înregistrare, apoi se trimite serverului care procesează corespunzător cererea.

3.2.3. Managerul de dispozitive și protocolul de comunicare

Pentru interacțiunea facilă cu dispozitivele, am creat un manager de dispozitive. Așa cum îi spune și numele, el are rolul de administrare a dispozitivelor. Acest manager o să interacționeze cu toate obiectele de tip dispozitiv și cu ajutorul lui dispozitivele vor fi programate.

Managerul de dispozitive folosește un mecanism de cache, descris în ceea ce urmează. Atunci când un utilizator se autentifică, toate dispozitivele lui, existente în baza de date, se vor încărca într-un `HashMap` intern. Cache-ul este necesar deoarece o conexiune trebuie inițiată cu dispozitivul atunci când clientul o solicită. Această stare a conexiunii trebuie menținută corespunzător.

După ce utilizatorul se autentifică, orice operație asupra unui dispozitiv este delegată managerului de dispozitive, ce are acces la toate operațiile expuse de clasa `HalDevice`.

La deconectarea utilizatorului, se va încheia comunicarea cu toate dispozitive la care utilizatorul este conectat, iar apoi se vor scoate toate dispozitivele utilizatorului din cache.

²⁷ MySQL: <https://www.mysql.com/>

HalDevice este clasa ce implementează protocolul de comunicare cu dispozitivele. Protocolul este de tip cerere răspuns. Mesajele transmise sunt fluxuri de octeți. Pentru a identifica comanda, mai întâi se trimite antetul reprezentat de un octet ce va indica comanda, iar apoi conținutul cererii. Protocolul de comunicare are comenzile definite în Figura 12. Primele două comenzi reprezintă răspunsurile posibile: succes sau eroare, următoarele șapte reprezentând cererile ce se pot efectua.

În caz de eroare, după octetul pentru protocol, se trimite și mesajul de eroare corespunzător. Atunci când acest mesaj ajunge pe partea de server se va arunca o excepție creată din mesajul primit, ce va fi tratată corespunzător din logica serverului.

Celelalte comenzi sunt implementate identic, primul octet este identificatorul comenzii, octeții următori având semnificații diferite, în funcție comandă.

```
public class Protocol {

    public static final byte EXCEPTION = 101;

    public static final byte SUCCESS = 109;

    public static final byte OPEN = 102;

    public static final byte CLOSE = 103;

    public static final byte IS_OPENED = 104;

    public static final byte GET_TYPE = 105;

    public static final byte GET_PARAMS = 106;

    public static final byte COMMAND = 107;

    public static final byte QUERY_DATA = 108;

}
```

Figura 12: Comenzile protocolului de comunicare

<i>Metodă</i>	Descriere	Cerere	Răspuns
<i>Open</i>	Comandă ce va deschide dispozitivul.	Doar octetul de comandă.	Octet de success. În caz contrar, octet de eroare urmat de mesaj.
<i>Close</i>	Comandă ce va închide dispozitivul.	Doar octetul de comandă.	Octet de success. În caz contrar, octet de eroare urmat de mesaj.

<i>IsOpen</i>	Verifică dacă dispozitivul este conectat.	Doar octetul de comandă.	Octet de succes urmat de o valoare booleană. În caz contrar, octet de eroare urmat de mesaj.
<i>GetType</i>	Cere tipul dispozitivului.	Doar octetul de comandă.	Octet de succes urmat de un șir de caractere ce semnifică tipul dispozitivului. În caz contrar, octet de eroare urmat de mesaj.
<i>GetAcceptedParams</i>	Cere parametrii configurabili ai dispozitivului. Ei vor fi de forma: nume, tipul parametrului și dacă este de citire sau de scriere.	Doar octetul de comandă.	Octet de succes urmat de un șir de parametrii separați prin „;”. Un parametru este de forma: „cheie=boolean;tip”. Valoarea booleană semnifică dacă parametrul este doar de citire sau nu. În caz contrar, octet de eroare urmat de mesaj.
<i>Command</i>	Programează dispozitivul.	Octetul de comandă urmat de o secvență de perechi cheie=valoare separate prin „;”.	Octet de succes. În caz contrar, octet de eroare urmat de mesaj.
<i>QueryData</i>	Cere valorile parametrilor dispozitivului.	Octetul de comandă urmat de numele parametrilor separați prin „;”.	Octet de succes urmat de un șir valori de forma „cheie=valoare”, separate prin „;”. În caz contrar, octet de eroare urmat de mesaj.

Tabelul 1: Definirea protocolului de comunicare

Tabelul 1, de mai sus, conține definirea protocolului de comunicare. Coloanele cerere și răspuns se referă la ce se trimite pe rețea atunci când se solicită operație, respectiv răspunsul corespunzător cererii.

Securitatea dintre server și dispozitive va fi prezentată în capitolul următor.

3.2.4. Securitatea serverului

Din punct de vedere al securității între server și client folosesc autorizarea bazată pe token-uri de access. În autentificarea bazată pe token-uri, se asigură că fiecare cerere către server conține un token semnat, pe care serverul îl va verifica pentru autenticitate, iar doar apoi

va raspunde la cerere. Un token este o secvență de informație care nu are nici o însemnătate singură, dar combinată cu sistemul de tokenizare joacă un rol vital în securitatea serverului.

Atunci când un utilizator dorește să se autentifice, cererea este trimisă de la aplicația web la server. Serverul primește cererea, verifică dacă utilizatorul este înregistrat, apoi verifică dacă parola se potrivește. Dacă toți acești pași se termină cu succes atunci utilizatorul este autorizat, prin urmare serverul generează un token ce este trimis drept răspuns aplicației web. Din acest punct aplicația web are tokenul de autorizare și o să îl folosească la fiecare cerere către server. Un token expiră la un timp presabilit de către server.

Din cauză că după autentificare aplicația web trimite la fiecare cerere token-ul primit, am creat un filtru http care interceptează toate cererile de la aplicația web, în afară de autentificare și de înregistrare, și verifică existența token-ului în header-ul http. Dacă se efectuează cererea și se trimite fără token, atunci serverul răspunde că utilizatorul nu este autorizat în efectuarea operațiunii dorite. Dacă se trimite token dar după verificarea serverului este invalid, același răspuns se va trimite. Doar în cazul în care tokenul este valid, cererea trece la metoda din controller ce o să execute acțiunea dorită.

Tokenul creat de server este semnat folosind HMAC-SHA-512²⁸.

Din cauza faptului că token-ul se trimite ca antet http există posibilitatea ca el să fie recepționat de un atacator. Acest lucru este posibil pentru ca momentan se folosește protocolul HTTP, unde antetele http sunt trimise în clar peste retea.

Dacă se folosește HTTPS(Secure Hyper Text Transfer Protocol), nu vor mai fi astfel de probleme. HTTPS are o fază de inițiere unde se negociază criptarea între serverul web și browser-ul web. Apoi tot traficul este trimis criptat, în loc să fie trimis în clar, dar este în esență același lucru ca traficul HTTP, dar cu avantaje de securitate. [10]

Referitor la securitatea între server și client, așa cum am precizat și în capitolul de arhitectură a sistemului, folosesc protocolul criptografic SSL/TLS. Pentru a folosi protocolul criptografic SSL/TLS este nevoie de un certificat SSL/TLS. Certificatul este un fișier de dimensiune redusă ce leagă cheia criptografică de informațiile unei organizații. Avantajele folosirii acestui protocol sunt [11]:

- criptează datele sensibile. Datele trimise folosind acest protocol sunt criptate, fiind ilizibile pentru cei ce nu au cheia.
- asigură că informația este trimisă la destinatarul real. Certificatul SSL/TLS acționează sub forma unui handshake între browser-ele care comunică.

²⁸ HMAC-SHA-512: <https://tools.ietf.org/html/rfc4868>

Handshake-ul reprezintă un termen criptografic ce semnifică un proces automat de negociere între doi participanți pentru stabilirea protocolului de comunicare înainte de începerea comunicării propriu-zise.

- apără împotriva escrocherilor. Escrocherii au foarte mari dificultăți în crearea unei replici autentice a unui certificat SSL/TLS.
- oferă confidențialitate și încredere.

Pentru conectarea SSL/TLS am folosit pachetul `javax.net.ssl`. Pe partea de dispozitive am folosit clasa `SSLServerSocketFactory` pentru a crea un socket. Serverul obține socket-urile pentru conectarea la dispozitive din clasa `SSLSocketFactory`. Serverul și dispozitivele trebuie să specifice locația certificatului SSL/TLS folosit. În plus, dispozitivele trebuie să specifice și parola certificatului SSL/TLS.

Figura 13 conține comanda prin care am generat certificatul SSL/TLS. Când comanda se rulează următoarele informații vor fi cerute: numele și prenumele, numele unității organizatoriale, numele organizației, numele orașului/localității, numele țării, prescurtarea țării. Apoi se va cere introducerea unei parole care mai apoi trebuie confirmată.

```
keytool -genkey -keyalg RSA -alias smarthome -keystore secret_key -storepass  
„*****” -validity 360 -keysize 2048
```

Figura 13: Comanda pentru generarea certificatului SSL/TLS

Figura 14 reprezintă o captură de ecran dintre comunicația dintre server și un dispozitiv. Această captură a fost realizată folosind programul Wireshark²⁹. Un dispozitiv este online fiind conectat la Raspberry P. Traficul din captură este filtrat după ip-ul `169.254.207.167` și port-ul `8000`, ce aparțin dispozitivului. Ip-ul `169.254.207.167` este ip-ul de conexiune al serverului.

Captura indică toate mesajele ce se transmit pe rețea atunci când utilizatorul apasă pe butonul *Connect* în interfața web.

În figură se pot observa 4 secțiuni:

- Secțiunea 1: stabilirea conexiunii TCP/IP între server și dispozitiv.
- Secțiunea 2: negocierea protocolului SSL/TLS.
- Secțiunea 3: comunicarea inițială cu dispozitivul. Serverul cere tipul dispozitivului, ce parametrii acceptă, respectiv valorile curente ale parametrilor.

²⁹ Wireshark: <https://www.wireshark.org/>

- Secțiunea 4: conține datele în format hexazecimal, în partea stângă, respectiv datele în format ASCII, în partea dreaptă, referitoare la mesajul cu numărul 518. După cum se observă nu se înțelege nimic din ceea ce se transmite pe rețea.

No.	Source	Destination	Protocol	Info
1.	493 169.254.48.113	169.254.207.167	TCP	51776 → 8000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
	494 169.254.207.167	169.254.48.113	TCP	8000 → 51776 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
	495 169.254.48.113	169.254.207.167	TCP	51776 → 8000 [ACK] Seq=1 Ack=1 Win=65536 Len=0
	496 169.254.48.113	169.254.207.167	TLSv1.2	Client Hello
	497 169.254.207.167	169.254.48.113	TCP	8000 → 51776 [ACK] Seq=1 Ack=199 Win=30336 Len=0
	501 169.254.207.167	169.254.48.113	TLSv1.2	Server Hello, Certificate, Server Key Exchange, Server Hello Done
2.	502 169.254.48.113	169.254.207.167	TLSv1.2	Client Key Exchange
	503 169.254.207.167	169.254.48.113	TCP	8000 → 51776 [ACK] Seq=1204 Ack=338 Win=31360 Len=0
	504 169.254.48.113	169.254.207.167	TLSv1.2	Change Cipher Spec
	505 169.254.207.167	169.254.48.113	TCP	8000 → 51776 [ACK] Seq=1204 Ack=344 Win=31360 Len=0
	506 169.254.48.113	169.254.207.167	TLSv1.2	Encrypted Handshake Message
	507 169.254.207.167	169.254.48.113	TCP	8000 → 51776 [ACK] Seq=1204 Ack=429 Win=31360 Len=0
	508 169.254.207.167	169.254.48.113	TLSv1.2	Change Cipher Spec
	509 169.254.48.113	169.254.207.167	TCP	51776 → 8000 [ACK] Seq=429 Ack=1210 Win=64256 Len=0
	510 169.254.207.167	169.254.48.113	TLSv1.2	Encrypted Handshake Message
	511 169.254.48.113	169.254.207.167	TLSv1.2	Application Data
	512 169.254.207.167	169.254.48.113	TCP	8000 → 51776 [ACK] Seq=1295 Ack=498 Win=31360 Len=0
	513 169.254.207.167	169.254.48.113	TLSv1.2	Application Data
3.	517 169.254.48.113	169.254.207.167	TLSv1.2	Application Data
	518 169.254.207.167	169.254.48.113	TLSv1.2	Application Data
	519 169.254.48.113	169.254.207.167	TLSv1.2	Application Data
	520 169.254.207.167	169.254.48.113	TLSv1.2	Application Data
	521 169.254.48.113	169.254.207.167	TLSv1.2	Application Data
	522 169.254.207.167	169.254.48.113	TLSv1.2	Application Data
	528 169.254.48.113	169.254.207.167	TCP	51776 → 8000 [ACK] Seq=721 Ack=1651 Win=65280 Len=0

> Frame 518: 171 bytes on wire (1368 bits), 171 bytes captured (1368 bits) on interface 0
 > Ethernet II, Src: Raspberr_0a:f0:6b (b8:27:eb:0a:f0:6b), Dst: TanakaS/_0c:27:1d (00:05:0f:0c:27:1d)
 > Internet Protocol Version 4, Src: 169.254.207.167, Dst: 169.254.48.113
 > Transmission Control Protocol, Src Port: 8000, Dst Port: 51776, Seq: 1364, Ack: 567, Len: 117
 > Secure Sockets Layer

0000	00 05 0f 0c 27 1d b8 27	eb 0a f0 6b 08 00 45 00'...k..E
0010	00 9d 98 b7 40 00 40 06	4d 8e a9 fe cf a7 a9 fe	...@.@. M.....
0020	30 71 1f 40 ca 40 af 77	0d f5 ba d1 d9 4a 50 18	0q.@.@-wJP
0030	00 f5 1b 49 00 00 17 03	03 00 70 e0 3c 04 f7 04	...I.....p<...
0040	ff a0 c9 80 5c 59 b8 25	b4 8f 74 67 b0 b2 21 8a	...V-% ..tg..!

Figura 14: Captură a comunicației dintre server și un dispozitiv

3.2.5. Unelte folosite

În dezvoltarea aplicației server am folosit două unelte ce m-au ajutat foarte mult: swagger și ngrok.

Swagger

Swagger permite descrierea structurii API-ului dorit astfel încât și masinile să poată le poată citi. Prin citirea structurii API-ului se poate contrui automat o documentație interactivă și frumoasă. De asemenea se pot genera automat biblioteci, în mai multe limbi, pentru a explora și alte posibilități cum ar fi testarea automată. [12]

Am folosit Swagger pentru a genera o documentație interactivă a server-ului, și mai ales pentru a putea testa serverul interactiv fără nevoia existenței modulului de aplicație web. Figura 15 surprinde o parte din interfața expusă de swagger unde se observă documentația interactivă a server-ului. Se pot observa ce controllere există, iar în interiorul fiecărui controller se pot

vedea metodele ce pot fi accesate. Verbele http prin care se pot accesa fiecare metodă sunt marcate corespunzător.

Figura 16 surprinde o altă din interfața swagger, ce conține documentarea metodei de ștergere a unui dispozitiv. Metoda necesită 2 parametrii: Authorization și device. În partea dreaptă apare tipul de parametru necesitat, antet http respectiv interogarea a resursei, dar și tipul de dată necesar. În secțiunea „Curl” se afișează request-ul corespunzător cu metoda: ce antete http se pun, care este url-ul corespunzător.

authentication-controller : Authentication Controller			Show/Hide	List Operations	Expand Operations
POST	/login	login			
POST	/register	register			
devices-controller : Devices Controller			Show/Hide	List Operations	Expand Operations
DELETE	/device	delete			
GET	/device	findByHash			
POST	/device	add			
PUT	/device	edit			
GET	/device/all	getAll			
PUT	/device/close	close			
PUT	/device/connect	connect			
PUT	/device/disconnect	disconnect			
PUT	/device/open	open			
POST	/device/setParams	setParams			
PUT	/device/testConnection	testConnection			
user-controller : User Controller			Show/Hide	List Operations	Expand Operations
POST	/user/logout	logout			
GET	/user/profile	profile			
POST	/user/profile	changeProfile			

Figura 15: Documentația interactivă a server-ului

devices-controller : Devices Controller
Show/Hide List Operations Expand Operations

DELETE /device delete

Response Class (Status 200)
OK

Response Content Type */*

Parameters

Parameter	Value	Description	Parameter Type	Data Type
Authorization	Bearer eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJ0dXJjdW5pY2tAZ2	Authorization	header	string
device	7018dea9-8cb6-4677-a5ea-cfb743ee4dca	device	query	string

Response Messages
Try it out! [Hide Response](#)

Curl

```
curl -X DELETE --header 'Accept: application/json' --header 'Authorization: Bearer eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJ0dXJjdW5pY2tAZ2'
```

Request URL

```
http://localhost:9000/device?device=7018dea9-8cb6-4677-a5ea-cfb743ee4dca
```

Figura 16: Documentarea unei metode

Aceste informații sunt foarte folositoare la definirea API-ului deoarece, o metodă poate fii definită greșit. Drept urmare, atunci când se va folosi swagger să se testeze dacă metoda merge se va vedea foarte ușor dacă metoda este greșit definită sau nu, sau dacă nu funcționează corespunzător.

Ngrok

Este un software ce permite dezvoltatorilor să expună la internet un server web ce rulează pe mașina locală. Oferă o interfață web în timp real unde poate observa tot traficul HTTP care rulează peste tunelurile folosite. [13]

Motivul pentru care am folosit ngrok este de a verifica aplicația web ca face cererile protrivite în accesarea resurselor oferite de server. Am avut cazuri când cererea către server pe care o făceam era greșită, deși eu credeam că este corectă, și comunicarea între ei nu funcționa.

Figura 17 reprezintă o porțiune a unei capturi de ecran, în interfața web oferită de ngrok. În partea stângă se pot vedea cererile ce s-au făcut serverului. Cererea „GET /device/all” este selectată, de aceea în partea dreaptă apare în format text conținutul cererii.

3.3. Modulul 3 – Dispozitivele „inteligente”

Din punct de vedere software dispozitivele inteligente trebuie să folosească un limbaj puternic, ce poate programa cât mai multe tipuri de clienți posibili. Din aceste considerente am ales Java, ce este un limbaj independent de platforma de lucru, portabil, simplu, robust.

Dispozitivele o să comunice cu serverul Java prin TCP, folosind protocolul criptografic SSL/TLS. Protocol SSL/TLS necesită un certificat SSL/TLS, de aceea am generat unul și l-am inclus în serverul Java și în aplicațiile dispozitivelor. Apoi, comunicarea efectivă între server și dispozitive este stabilită folosind un protocolul de comunicare definit în capitolul „3.2.3. Managerul de dispozitive și protocolul de comunicare”.

Pentru a simula dispozitivele inteligente am folosit un Raspberry Pi 2, Model B. El este de dimensiunile unui card de credit, ieftin, cu o varietate de sisteme de operare ce pot fi instalate. La Raspberry am conectat module arduino, acele module reprezentând efectiv dispozitivele inteligente.

3.3.1. Interacțiunea cu Raspberry Pi

Primul lucru pe care a trebuit să îl fac, a fost instalare de sistem de operare. Am instalat sistemul de operare oficial pentru toate modelele de Raspberry, Raspbian. Acest lucru l-am realizat folosind un monitor alternativ ce l-am conectat la portul de HDMI(High-Definition Multimedia Interface). Dar, din cauză că monitor nu îmi aparținea, a trebuit să găsesc o modalitate de conectare direct din calculatorul personal. Așa că am conectat un cablu din portul de ethernet al calculatorului la portul de ethernet al raspberry-ului. Apoi am scanat rețeaua internă a laptopului, am găsit hostname-ul „raspberrypi” cu ip-ul corespunzător.

După, am configurat VNC³⁰-ul, un sistem de împărtășire a desktop-ului către alt computer. Am făcut acest lucru pentru a putea avea o interfață grafică atunci când mă conectez la Raspberry. Apoi am deconectat monitorul și am realizat prima conexiune folosind prin VNC, știind ip-ul static. Raspberry-ul era conectat prin ethernet la calculator, dar nu aveam conexiune la internet din cadrul acestuia. Acest lucru nu m-a incomodat până nu a trebuit să scriu primul dispozitiv. Atunci mi-am dat seama că am nevoie de o librărie java, ce oferă suport în controlul pinilor de pe Raspberry. Dar nu puteam să configurez librăria deoarece nu aveam conexiune la internet.

³⁰ VNC: Vritual Network Computing

Din această cauză am configurat partajarea unei conexiuni wifi de la computer la Raspberry Pi folosind un cablu ethernet. Acest tutorial mi-a fost de ajutor: <https://www.hackster.io/Anwaarullah/sharing-wifi-with-raspberry-pi-using-a-lan-cable-ae1f44>. După această configurare, Raspberry-ul își va lua un ip dinamic, de aceea înainte de conectare trebuie scanată rețeaua calculatorului între anumite clase de ip-uri. După, având acces la internet, am facut update la sistemul de operare și am instalat libraria Java Pi4J.

Pentru a automatiza cât de mult posibil compilarea și rularea dispozitivelor am definit makefile-uri pentru fiecare dintre ele. Apoi am scris un script care ce folosește aceste makefile-uri pentru a porni fiecare dispozitiv în câte un terminal, în paralel.

```
compile:

    javac -classpath .:classes:/opt/pi4j/lib/'*' -d . Lamp.java

run:

    java -classpath .:classes:/opt/pi4j/lib/'*' Lamp lamp $(ip) 8000 0 1 2
```

Figura 18: Makefile-ul dispozitivului lampă

Figura 18 reprezintă makefile-ul dispozitivului lampă. El are două părți: compilare și rulare. Din cauză că folosesc librăria Pi4J trebuie să adaug în classpath, la rulare și la compilare, JAR-urile librăriei Pi4J.

```
#!/bin/bash

lxterm -e 'bash -c "cd DoorLock/src && make compile; make ip=$(hostname -I) run"' &

lxterm -e 'bash -c "cd Lamp/src && make compile; make ip=$(hostname -I) run"' &

lxterm -e 'bash -c "cd SecurityLaser/src && make compile; make ip=$(hostname -I) run"' &

lxterm -e 'bash -c "cd LightBulb/src && make compile; make ip=$(hostname -I) run"'
```

Figura 19: Conținutul scriptul ce pornește toate dispozitivele simultan

În Figura 19 se găsește conținutul scriptului ce pornește toate dispozitivele simultan. În urma rulării acestui script se vor deschide în paralel 4 terminale ce vor compila codul corespunzător dispozitivului, apoi vor pornește dispozitivele.

3.3.2. Dispozitive implementate

În contruirea dispozitivelor, partea cea mai importantă este definirea parametrilor personalizați. Parametrii unui dispozitiv nu vor fi cunoscuți apriori de către serverul Java. Vor fi aflați abia după ce se realizează conexiunea cu dispozitivul. Ei trebuie definiți cu atenție pentru fiecare dispozitiv, fiind sugestivi în denumire și îndeplinind o operație clară.

Am ales această idee de design deoarece protocolul de comunicare devine astfel mai dinamic, numele și numărul parametrilor unui dispozitiv fiind cunoscut la momentul execuției programului. Un alt motiv, mai practic, constă în faptul că dispozitivele nu sunt neapărat contruite de aceeași producător și în plus implementările nu o să fie livrate toate odată. Unele o să fi gata mai devreme, altele mai târziu. Dacă în logica serverului s-ar ține cont de tipul de dispozitiv și de parametrii lui, atunci ar fi prea mare cuplajul între server și aplicațiile client, și la orice dispozitiv nou ar trebui modificat și recompilat serverul.

Pentru dispozitivele implementate am folosit module arduino la partea de hardware și librăria Java Pi4J pe partea de software.

În continuare voi descrie ce dispozitive am implementat.

3.3.2.1. Laser de securitate



Figura 20: KY-008 Modulul senzor laser³¹

3.3.2.2. Lampă

³¹ Imagine preluată. Sursa: <https://www.fasttech.com/product/1219301-keyes-ky-008-arduino-compatible-650nm-laser>



Figura 21: KY-016 Modul LED cu 3 culori³²

3.3.2.3. Încuietoare a ușii



Figura 22: KY-019 Modul releu 5V³³

3.3.2.4. Bec

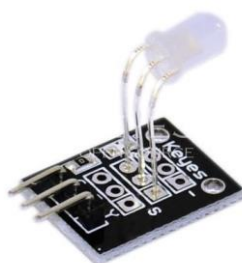


Figura 23: KY-011 Modul LED cu 2 culori³⁴

³² Imagine preluată. Sursa: <https://piandmore.wordpress.com/2016/02/10/nodemcu-ky-016-3-color-led>

³³ Imagine preluată. Sursa: https://tkkrlab.nl/wiki/Arduino_KY-019_5V_relay_module

³⁴ Imagine preluată. Sursa: <https://www.newegg.com/Product/Product.aspx?Item=1FS-002B-000B7>

4. Direcții de viitor

Concluziile lucrării

Bibliografie

- [1] D. J. Cook, „How Smart Is Your Home?,” *Science (New York, NY)*, vol. 335, nr. 6076, pp. 1579-1581, 2012.
- [2] ***, „What is a Smart Home,” n.d. n.d. c2018. [Interactiv]. Available: <https://www.smarthomeusa.com/smarthome/>. [Accesat 3 06 2018].
- [3] Homeoftech, „7 Benefits of living in a smart home,” 24 05 2016. [Interactiv]. Available: <http://homeoftechnologies.co.uk/7-benefits-of-living-in-a-smart-home/>. [Accesat 03 06 2018].
- [4] N. C. Molly Edmonds, „How Smart Homes Work,” 25 03 2008. [Interactiv]. Available: <https://home.howstuffworks.com/smart-home6.htm>. [Accesat 03 07 2018].
- [5] B. Sabin-Corneliu, „Dezvoltarea de aplicații Web prin REST,” [Interactiv]. Available: <https://profs.info.uaic.ro/~busaco/teach/courses/web/presentations/web11ServiciiWeb-REST.pdf>. [Accesat 13 06 2018].
- [6] D. S. Robert Savage, „The Pi4J Project,” [Interactiv]. Available: <http://pi4j.com/index.html>.
- [7] S. Cooper, „ngx-toastr,” [Interactiv]. Available: <https://github.com/scttcper/ngx-toastr>. [Accesat 04 05 2018].
- [8] „Highcharts,” [Interactiv]. Available: <https://www.highcharts.com/>.
- [9] Komei, „Angular5 Fontawesome,” [Interactiv]. Available: <https://github.com/travelist/angular2-fontawesome>. [Accesat 25 05 2018].
- [10] B. Pollard, „Secure websites with HTTPS,” 25 02 2018. [Interactiv]. Available: <https://www.tunetheweb.com/security/https/>.
- [11] **, „The importance of SSL - Top 6 advantages,” Clear Vertical Ltd. 8259274, [Interactiv]. Available: <https://www.clearvertical.co.uk/the-importance-and-advantages-of-ssl/>.
- [12] SmartBear Software, „Swagger,” [Interactiv]. Available: <https://swagger.io/>.
- [13] inconshreveable, „ngrok,” [Interactiv]. Available: <https://ngrok.com/>.