

# Securitatea și confidențialitatea datelor în contextul aplicațiilor mobile

Ghimpu Lucian Eduard

May 7, 2019

CONDUCĂTOR ȘTIINȚIFIC

DR. CZIBULA ISTVAN, PROFESOR UNIVERSITAR

# Contents

|          |   |           |
|----------|---|-----------|
| <b>1</b> | <b>Introducere</b>  | <b>3</b>  |
| 1.1      | Introducere . . . . .   | 3         |
| 1.2      | Ecosistemul aplicațiilor mobile . . . . .   | 3         |
| 1.3      | GDPR . . . . .  | 3         |
| <b>2</b> | <b>Securitatea și confidențialitatea datelor în contextul aplicațiilor mobile</b> | <b>3</b>  |
| 2.1      | Autentificarea și înregistrarea . . . . .   | 3         |
| 2.1.1    | Ceva introducere * . . . . .  | 4         |
| 2.1.2    | JWT . . . . .   | 5         |
| 2.1.3    | Autentificare prin senzori biometrici . . . . .                                   | 7         |
| 2.1.4    | Autentificare prin factori multipli . . . . .                                     | 8         |
| 2.2      | Permisuni . . . . .   | 10        |
| 2.3      | Canale de comunicare . . . . .  | 12        |
| 2.3.1    | HTTP și HTTPS . . . . .   | 12        |
| 2.3.2    | SMS . . . . .   | 13        |
| 2.3.3    | WebSocket . . . . .   | 14        |
| 2.4      | Persistența datelor . . . . .   | 15        |
| 2.4.1    | Metode de persistare a datelor . . . . .  | 15        |
| 2.4.2    | Criptografie . . . . .  | 16        |
| <b>3</b> | <b>Medicarium</b>   | <b>18</b> |
| 3.1      | Analiza aplicației . . . . .  | 18        |
| 3.1.1    | Problematica . . . . .  | 18        |
| 3.1.2    | Cazuri de utilizare . . . . .   | 19        |
| 3.2      | Proiectarea aplicației . . . . .  | 20        |
| 3.2.1    | Arhitectura . . . . .   | 20        |
| 3.2.2    | UML ceva??? . . . . .   | 21        |
| 3.3      | Implementarea aplicației - Serverul și serviciile . . . . .                       | 21        |
| 3.3.1    | Server REST . . . . .   | 21        |
| 3.3.2    | Node.js . . . . .   | 23        |
| 3.3.3    | MongoDB . . . . .   | 24        |
| 3.3.4    | Autentificare în doi pași . . . . .   | 24        |
| 3.4      | Implementarea aplicației - Clientul mobil . . . . .                               | 24        |
| 3.4.1    | Android Jetpack . . . . .   | 24        |
| 3.4.2    | Kotlin . . . . .  | 24        |

|          |                                     |           |
|----------|-------------------------------------|-----------|
| 3.4.3    | Autentificarea . . . . .            | 24        |
| 3.4.4    | Securitatea aplicației . . . . .    | 24        |
| 3.4.5    | Gestionarea permisiunilor . . . . . | 24        |
| 3.4.6    | Gestionarea fișierelor . . . . .    | 24        |
| 3.5      | Testarea . . . . .                  | 24        |
| <b>4</b> | <b>Manual de utilizare</b>          | <b>24</b> |
| <b>5</b> | <b>Concluzii</b>                    | <b>24</b> |
| <b>6</b> | <b>Bibliografie</b>                 | <b>25</b> |

# **1 Introducere**

## **1.1 Introducere**

## **1.2 Ecosistemul aplicațiilor mobile**

## **1.3 GDPR**

# **2 Securitatea și confidențialitatea datelor în contextul aplicațiilor mobile**

## **2.1 Autentificarea și înregistrarea**

### 2.1.1 Ceva introducere \*

Indiferent că vorbim de aplicații web, desktop sau mobile, majoritatea folosesc o metodă de autentificare. Autentificarea și înregistrarea stau la baza problematicei securității datelor. În clasamentul OWASP Top 10 din 2017 [1], problemele legate de autentificare și gestiunea sesiunii, sunt clasate pe locul 2. Iar în clasamentul OWASP top 10 Mobile din 2016 [2], autentificare nesigură și autorizarea necorespunzătoare sunt clasate pe locul 4, respectiv 6.

Unicitatea aplicațiilor mobile este dată de faptul că un dispozitiv mobil poate deveni accesibil oricărui persoane datorită portabilității lor. Un dispozitiv mobil poate fi furat, pierdut sau accesat temporal de o persoană necunoscută fără permisiunea posesorului. Prin urmare nevoia de un sistem de autentificare robust este mandatorie atunci când vorbim de aplicații care gestionează date sensibile (aplicații financiare, sociale, medicale, etc. . . ).

În cadrul aplicațiilor mobile, autentificarea se poate face prin mai multe metode. De la simpla autentificare prin utilizator și parolă, până la utilizarea de senzori biometrici. Mitigari clasice precum impunerea unei parole sigure rămân valabile și în contextul aplicațiilor mobile.

Pentru alegerea metodei de autentificare trebuie să ne punem în primă instanța următoarele două întrebări:

- Care este scopul aplicației? O aplicație care notifica utilizatorul despre starea meteo poate că nu ar avea nevoie de autentificare prin senzori biometrici.
- Aplicația gestionează date confidențiale? Un exemplu potrivit ar fi o aplicație precum BT pay, care gestionează contul curent al unui utilizator, se folosește de mai multe metode de autentificare, o dată prin datele de logare, iar apoi prin senzori biometrici.

După ce ne este clar care este scopul aplicației și cu ce fel de date lucrează, putem include una sau mai multe metode de autentificare bazate după următorii factori:

1. Ceva ce utilizatorul știe (parolă, pin etc. . . )
2. Ceva ce îl definește pe utilizator (amprenta, retina)

### 3. Ceva ce utilizatorul deține (parole generate temporal)



Figure 1: Metode de autentificare [3]

#### 2.1.2 JWT

Majoritatea aplicațiilor de azi se folosesc de cea mai simplă formă de autentificare, prin folosirea de credentiale (ceva ce utilizatorul știe) și unui token de acces (ceva ce utilizatorul deține). Utilizatorul își creează cont pentru o anumită aplicație, folosește credentialele pentru a se loga, cererea de autentificare ajunge la server unde se verifică credentialele iar apoi se generează un token care va fi folosit de utilizator pentru a accesa diferite resurse în aplicație.

Scenariu descris anterior se referă la folosirea de JWT (JSON Web Token), un standard (RFC 7519) [4] adoptat de multe aplicații mobile în zilele noastre. JSON Web Token este o metodă sigură de autorizare a transferului de informații între două părți [5], de obicei clientul mobil și serverul la care se face cererea. Clientul revendică de la server o dovadă, un token, care apoi este folosit de client pentru a accesa diferite resurse.

Din punct de vedere tehnic, un JWT are următoarea formă 11111.22222.33333 și este alcătuit din 3 părți:

1. Antetul (Header)
2. Datele utile (Payload)
3. Semnătura (Signature)

#### HEADER: ALGORITHM & TOKEN TYPE

---

```
{  
  "alg": "HS256",  
  "typ": "JWT"  
}
```

Figure 2: Antetul unui JWT, alcatuit din tipul de algoritm de înregistrare (HS256) și tipul de token (JWT).

#### PAYLOAD: DATA

---

```
{  
  "numar": "1234567890",  
  "nume": "John Doe",  
  "admin": false  
}
```

Figure 3: Partea utilă al unui JWT conține date sau permisiuni pe care clientul le are.

#### VERIFY SIGNATURE


```
HMACSHA256(  
  base64UrlEncode(header) + "." +  
  base64UrlEncode(payload),  
  your-256-bit-secret  
)  secret base64 encoded
```

Figure 4: Semnătura unui JWT este alcătuită din antetul encodat, datele encodeate, algoritmul folosit în antet și un secret. Semnătura are rolul de a oferi o metodă de verificare pentru a asigura ca conținutul nu a fost modificat

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJudW1hcnI6IjEyMzQ1Njc4OTAiLCJudW1lIjoiaSm9obiBEb2UiLCJkYXRhIjoxNTE2MjM5MDIyfQ.uEE41yzcc12Z1Tp0J20NwLbg_js4sMq6ikJRue87QUo
```

Figure 5: JWT va fi format în final de 3 siruri de caractere de tip Base64-URL separate prin punct.

O dată ce clientul deține un token, acesta trebuie tratat cu multă grijă în cadrul unei aplicații. Acesta poate fi folosit mai apoi în antetul tuturor

cererilor de tip HTTP sub formă "Authorization: Bearer {token}", din acest motiv cel mai probabil se dorește salvarea token-ului în memoria locală a dispozitivului pentru a putea fi apoi folosit în viitor. Acesta poate fi criptat iar la rândul lui la nivelul clientului, deși în mod nativ atât pe android cât și pe ios există metode sigure de stocare a datelor de tip primitiv (Shared-Preferences în mod private pe Android și keychain pe iOS).

Pentru un nivel și mai mare de siguranță, se poate limita durata de timp pe care este valabil un token. Spre exemplu aplicația BT Pay folosește un token care este valid tip de 10-15 minute. După ce token-ul expiră, utilizatorul este nevoit să se autentifice din nou.

Avantajul principal pe care îl oferă JWT este facilitatea prin care se demarează tot procesul de revendicare a datelor sau drepturile de la un server de către client. Un alt aspect important îl reprezintă faptul că în spate, totul se produce folosit obiecte de tipul JSON, fapt ce îl face extrem de ușor de implementat și folosit în orice limbaj de programare.

### **2.1.3 Autentificare prin senzori biometrici**

Biometria este termenul tehnic folosit pentru măsurătorile și calculele făcute legate de corpul uman. Se folosește de metrici legate de caracteristicile umane. În cazul dezvoltării de software, biometria este folosită pentru autentificare.

Autentificarea prin senzori biometrici se folosește de un factor moștenit, ceva ce îl definește pe utilizator și prin urmare este una dintre cele mai comode și rapide metode de autentificare. Mai mult decât atât, datele biometrice precum aprență sunt greu de furat sau compromis.

Din ce în ce mai multe aplicații încep să folosească autentificare prin senzori biometrici, un factor major îl joacă faptul că în ultimi ani, capacitățile hardware ale dispozitivelor mobile a crescut exponențial, telefoanele vin încorporate cu diferinți senzori biometrici precum: senzori de amprenta și recunoaștere facială (iris și rețină).

Metricile biometrice pot varia de la caracteristici fizice până la aspecte ale comportamentului unei persoane. În cea ce privește dispozitivele mobile putem idetifica trei tipuri de autentificari biometrice:

1. Senzor de amprentă, extrem de sigur deoarece fiecare individ are o amprentă unică.

2. Recunoașterea vocii, avantajoasă deoarece nu necesită hardware în plus dar nepotrivit pentru situații unde utilizatorul trebuie să păstreze liniștea.
3. Recunoaștere facială, la fel ca cea a vocii, nu necesită hardware adițional dar nepotrivit pentru locuri în care luminozitatea este scăzută.

Utilizarea senzorilor biometrici implică anumite aspecte de care un dezvoltator de aplicații mobile trebuie să țină cont:

- Verificarea ca dispozitivul mobil este încorporat cu senzorii folosiți, în cazul în care un dispozitiv nu are senzorii biometrici, dezvoltator trebuie să ofere o metodă alternativă de autentificare. [6]
- Cererea de permisiunea pentru folosirea senzorilor.
- Verificarea datele biometrice asociate dispozitivului să nu se modifice de la prima autentificare. Această măsură trebuie luată pentru a împiedica cazuri în care se adaugă noi date biometrice (amprenta nouă).

Deși autentificare prin senzori biometrici este mai rapidă și comodă, această nu ar trebui să înlocuiască în mod complet autentificare făcută la nivel de server. Ambele metode pot coexista în funcție de context.

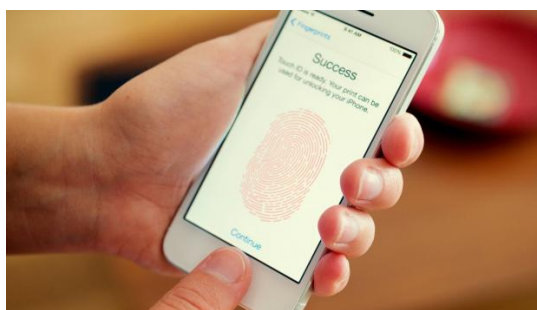


Figure 6: Autentificare prin senzor de amprentă

#### 2.1.4 Autentificare prin factori multipli

Autentificare prin factori multipli (MFA) este un sistem de securizare a autentificării prin impunerea a mai multor metode de verificare a identității unui utilizator.



Autentificare prin factori multipli combină mai multe metode independente de autentificare. Așa cum am văzut în capitolul anterior, autentificarea prin senzori biometrici și autentificarea prin credentiale lucrează cel mai bine împreună. Pe această idee, rolul autentificării prin factori multipli este acela de a crea un sistem greu de compromis în vederea asigurării siguranței și confidentialității datelor utilizatorului. Astfel dacă unu din componentele sistemului este compromis, atacatorul este oprit de restul barierelor. În cazul în care cineva are acces la credentialele unui utilizator și la dispozitivul sau mobil, atacatorul poate fi oprit prin folosirea senzorului de amprenta.

Un alt caz de utilizare al autentificării prin factori multipli îl reprezintă autentificarea în doi pași sau OTP (one time password). Rolul autentificării în doi pași este acela de a crea o barieră în plus în sistemul de securizare al autentificării prin creare de coduri/parole temporare unice.

După ce un utilizator se loghează folosind credențialele valide, un cod unic și temporar este generat și trimis utilizatorului prin diferite canale, de obicei prin SMS, email sau aplicații special făcute pentru generarea de coduri unice. Utilizatorul este apoi nevoit să introducă codul primit pentru a își confirma identitatea. Utilizarea sa nu se limitează doar la autentificare, ci poate fi folosită în mod general pentru a confirma identitatea persoanei. Un exemplu îl reprezintă aplicațiile financiare care atunci când se încearcă o plată, vor trimite un cod unic pentru a verifica identitatea persoanei care a inițiat acțiunea.

Deși folosirea autentificării prin doi pași este destul de comună în cadrul aplicațiilor mobile, această metodă prezintă și anumite vulnerabilități, mai ales când canalul de comunicare a parolei este prin SMS sau prin apel telefonic. SMS-urile pot fi interceptate și redirectionate, la fel și apelurile telefonice. În astfel de cazuri se poate limita valabilitatea codului primit la un interval scurt de timp (5-10 minute).

Utilizarea unui sistem de autentificare multiplu precum autentificare în doi pași este de altfel recomandată și de ENISA [7] într-un studiu făcut în vederea siguranței procesării datelor personale de către companii mari.

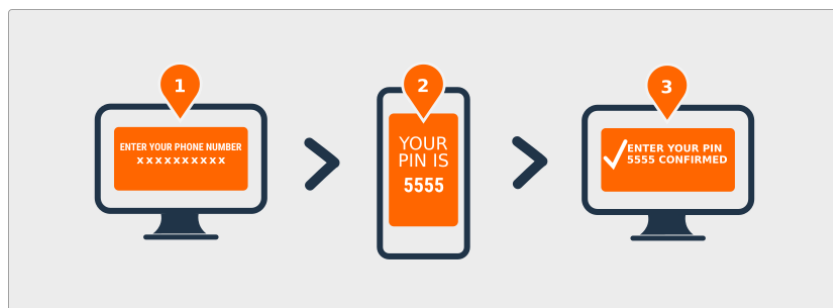


Figure 7: Autentificare în doi pași

## 2.2 Permisii

Permisunile sunt un aspect important în vederea păstrării confidențialității datelor utilizatorului. O aplicație poate cere o anumită permisiune în diferite cazuri, pentru a accesa date personale (contacte, mesaje) sau pentru a accesa anumite funcționalități și senzori (apeluri telefonice, camera, senzori biometrici).

În medie un dispozitiv mobil are instalate 95 de aplicații, fiecare aplicație având nevoie de 5 permisiuni [8]. Problematika permisiunilor este adesea ignorată și de utilizator și de dezvoltatorul aplicației. În trecut, pe dispozitivele cu sistem de operare Android, când o aplicație trebuia să determine SSID-ul rețelei curente nici o permisiune nu era necesară. Acest lucru putând duce la determinarea locației utilizatorului bazat pe numele și SSID-ul rețelei [9]. Spre exemplu dacă rețeaua s-ar numi "Gara Nord București", locația utilizatorului ar fi putut fi dezvăluită fără permisiunea lui. În versiunile noi de Android, determinarea SSID-ului se poate face doar dacă utilizatorul a dat consensul pentru folosirea locației sale.

În același timp, dezvoltatorul aplicației nu trebuie să abuzeze de permisiuni. Cererile directe către utilizator ar trebui să se limiteze la funcționalitățile aplicației. Spre exemplu, o aplicație de timp calculator nu ar avea nevoie de permisiunea pentru apeluri telefonice.

Pentru a combate astfel de cazuri, google a început dezvoltarea unui algoritm pentru determinarea dacă o aplicație folosește în mod eronat anumite permisiuni [10].

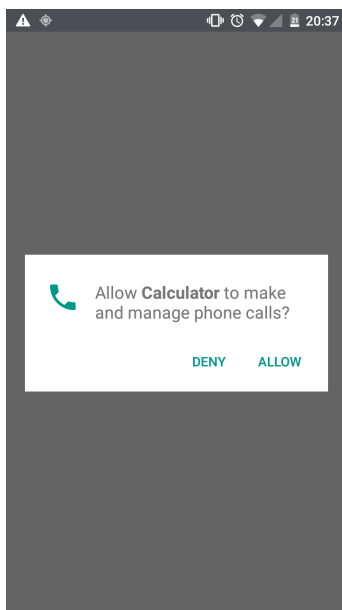


Figure 8: Abuzarea de permisiuni [11]

Pentru o gestiune corectă a permisiunilor se mai recomandă următoarele:

- Cererea unei anumite permisiuni să aibe loc doar atunci când este strict necesară. În cazul în care o aplicație depinde în mod permanent de o anumită permisiune (permisiunea de locație pentru aplicații de navigare), atunci cererea se poate face la deschiderea aplicației.
- Trebuie luat în considerare și diferitele versiuni ale sistemului de operare. Atât pe Android cât și pe iOS pot fi necesare diferite permisiuni pentru aceeași acțiune. Exemplu cu SSID amintit anterior.
- Folosirea unei singure permisiuni în loc de un întreg grup. De multe ori mai multe permisiuni sunt grupate pentru a facilita cererea lor. Dar în cazul în care doar un element din grup este folosit atunci este recomandat folosirea doar a elementului respectiv.
- Expunerea în mod clar a motivului necesității unei anumite permisiuni către utilizator.

## 2.3 Canale de comunicare

### 2.3.1 HTTP și HTTPS

Majoritatea aplicațiilor mobile se folosesc de unul sau mai multe servere pentru a își aduce date sau pentru a prelucra date preluate de la utilizator. Această practică este folosită pentru a evita stocarea de date pe dispozitivele utilizatorului având în vedere memoria limitată pe care o dețin. Din acest motiv este necesar folosirea unor protocoale de comunicare. Cele mai folosite protocoale de comunicare în ecosistemul mobil sunt HTTP și HTTPS.

Aceste protocoale de comunicare sunt un set de reguli care descriu modalitatea prin care datele sunt trimise și primite. În mediul mobil, HTTP și HTTPS sunt cele mai folosite protocoale pentru a trimite text, imagini și sunete.

HTTPS este varianta sigură a lui HTTP, pe tot parcursul comunicării, datele sunt criptate de la un capăt la altul. Deși HTTP este mai frecvent folosit, este recomandată folosirea protocolului HTTPS mai ales pentru aplicații care gestionează date sensibile.

Dezavantajul folosirii protocolului HTTPS îl reprezintă performanța. Criptare și decriptarea datelor transmise sunt operații costisitoare. Deși există o pierdere de performanță, există studii [12] care demonstrează că diferența de performanță este modestă, și încurajează folosirea protocolului mai sigur. Un alt studiu [13] arată că pe anumite sisteme de operare mobile, precum Android, rata de adopție pentru HTTPS este în urmă față de rata de adopție pe desktop.

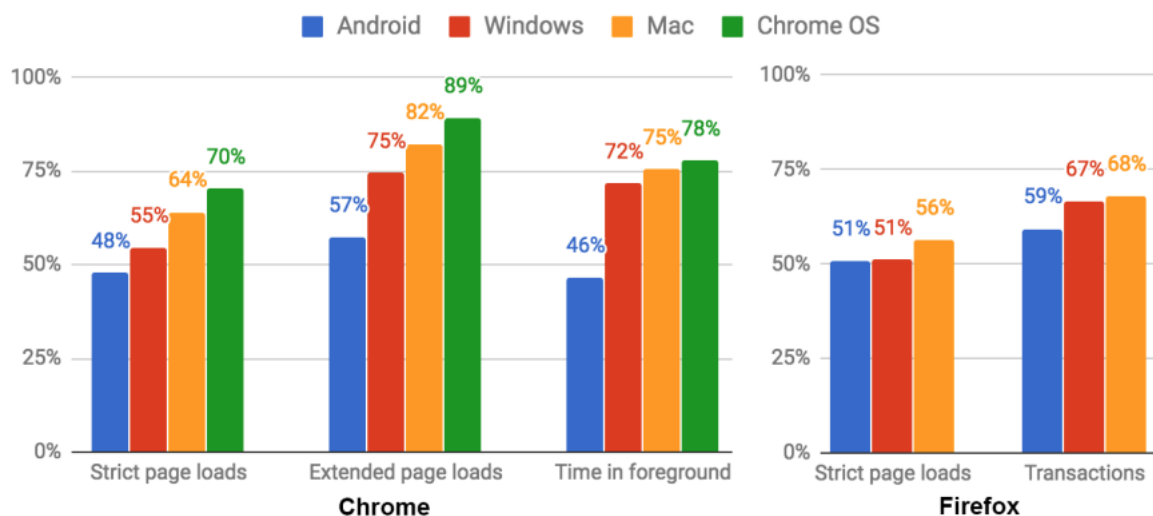


Figure 9: Procentul de utilizare HTTPS pe diferite sisteme de operare la sfarsitul unei saptamani din Februarie 2017 [13]

### 2.3.2 SMS

SMS (Short Message Service) este un serviciu folosit de majoritatea dispozitivelor mobile. Cazurile de utilizare ale serviciului variază de la simpla folosire pentru a comunica mesaje scurte, până la autentificare cu parolă unică. În 2010, 6.1 trilioane de mesaje au fost trimise cu o medie de 193.000 de SMS-uri pe secundă [14].

Din punct de vedere tehnic, SMS este un protocol de comunicare care permite schimbul de mesaj scurte. Un SMS poate fi format din 160 de caractere alfanumerice, mesajele mai mari de 160 de caractere sunt sparte în mai multe mesaje. Un mesaj trimis este mai întâi interceptat de SMSC (Short Message Service Center) care de cele mai multe ori este menținut de providerii de rețele telefonice. SMSC-ul trimite mai apoi mesajul către un alt SMSC (al receptorului) mesaj pe care în final îl trimite receptorului.

În ciuda popularității sale, comunicare prin SMS prezintă anumite vulnerabilități. Cel mai periculoasă vulnerabilitate este "SMS spoofing". Aceasta are loc când un atacator manipulează adresa mesajului pentru a impersona pe cineva. Aceste tipuri de atacuri pot fi prevenite prin verificarea datelor

emittătorului înainte ca mesajul să ajungă la receptor. O altă metodă de protejare, adoptată mai ales în cadrul autentificării prin 2 pași, este folosirea unui SMS gateway, servicii special dedicate pentru astfel de operații, dotate cu diverse măsuri de protecție.

### 2.3.3 WebSocket

Standardizat în 2011 în RFC 6455 [15], WebSocket este un protocol de comunicare bidirecțional bazându-se de fapt o conexiune de tip TCP.

Principalul avantaj pe care îl oferă protocolul WebSocket este facilitatea prin care se permite transferul de date în mod bidirecțional. În comparație cu protocolul HTTP, un server poate transmite date unui client fără ca acesta să fie făcut o cerere.

La fel ca HTTP, protocolul WebSocket (WS) este dublat de variată protecție WSS, oferind criptare de la un capăt la altul al comunicării.

Când vine vorba de aplicații mobile, WebSocket-urile sunt folosite predominant de aplicații care au nevoie de o comunicare de tip broadcast. Aplicațiile de mesagerie în grup precum WhatsApp folosesc WebSocket-uri pentru a notifica toți utilizatorii unui grup de mesaje noi primite.

Deși WebSocket rezolvă probleme de conectivitate, nu rezolvă și problemele de securitate [16]. vulnerabilități la nivelul acestui protocol variază de la simple interceptări ale datelor în rețea, atunci când se folosește varianta neprotejată a protocolului, până la vulnerabilități mai severe precum blocarea serviciului (DDos) [17]. Pentru a evita astfel de probleme este sugerată folosirea variantei protejate (wss) și limitarea conexiunilor sau verificarea conexiunilor când provin din aceeași sursă.

Fiind o tehnologie încă tânără, WebSocket încă nu este la fel de răspândit precum HTTP sau SMS, dar că orice sistem de comunicare, includerea lui într-o soluție soft necesită atenție sporită pentru a prevenii eventuale probleme de securitate.

## 2.4 Persistența datelor

### 2.4.1 Metode de persistare a datelor

Una din principalele atribuții a majoritatea aplicațiilor mobile este aceea de a gestiona și/sau stoca datele utilizatorului. Fie că vorbim de aplicații cu servicii web dedicate sau jocuri simple, toate aplicațiile au nevoie de o metodă pentru persistare datelor.

Deși modalitatea de persistare a datelor diferă în funcție de platforma (iOS sau Android), se pot extrage câteva caracteristici generale comune.

Dezvoltatorul aplicației trebuie să decidă unde și cum va stoca datele, în funcție de gradul lor de confidențialitate și tipul de dată. Folosirea în mod eronat a sistemelor oferite de platforma pe care se dezvoltă aplicația poate duce la expunerea de date sensibile.

Există mai multe metode prin care se pot salva datele și unde pot apărea vulnerabilități din punct de vedere al securității:

1. Fișiere Log, scopul lor, în mod normal, este acela de a păstra un jurnal al activității pentru o anumită aplicație, fiind ușor accesibile. Date sensibile pot fi expuse în mod involuntar prin astfel de fișiere (credentiale, token-uri, date primite din cereri HTML).
2. Baze de date locale SQL. Folosite pentru a păstra un volum mai mare de date. Pe ambele platforme există variate necriptate și criptate.
3. Fișiere folosite pentru setări (SharedPreferences și NSUserDefaults). Folosite pentru a stoca date de dimensiune mică cum ar fi valori pentru setări. La fel ca bazele de dată SQL, există variante criptate și necriptate. Trebuie menționat că atunci când fișierele de preferințe sunt folosite pentru a stoca date de autentificare (token-uri) este recomandată folosirea variantei criptate.
4. Memoria internă, sistemul de fișiere intern al dispozitivului poate fi folosit pentru a păstra date. De obicei se poate folosi pentru a păstra fișiere publice de tip multimedia, cum ar fi poze sau videoclipuri.
5. Memoria externă (doar pe Android), asemănătoare cu memoria internă, disponibilă prin folosirea de carturi SD sau alte extensii hardware.

Majoritatea metodelor enunțate anterior sunt protejate într-un fel sau altul de sistemul de operare. În cazul dispozitivelor mobile modificate (jail-break sau rooted), sistemele de protecție oferite de sistemul de operare ajung a fi compromise.

#### 2.4.2 Criptografie

Dupa cum am vazut pana acum, multe aspecte ale unei aplicatii mobile pot fi securizate prin folosirea de elemente native securizate, librării sau implementarii proprii. Toate acestea au la baza o caracteristica comuna, criptarea datelor.

După cum am văzut până acum, multe aspecte ale unei aplicații mobile pot fi securizate prin folosirea de elemente native securizate, librării sau implementarii proprii. Toate acestea au la baza o caracteristică comună, criptarea datelor.

Criptografia este studiul tehnicilor matematice legate de aspectele securității informațiilor, cum ar fi confidențialitatea, integritatea datelor, autentificarea entității și autentificarea originii datelor [18].

Problematica securității informației nu este una modernă, de a lungul istoriei au fost nevoie de diferite metode de securizare a informației, mai ales în timp de război. De obicei implica păstrarea datelor într-o manieră incopresibila. Pentru a decripta astfel de mesaje, se puteau folosi diferite tehnici de decodare.

Criptografia modernă se rezumă la algoritmi bazați pe teorie matematică, greu de spart datorită complexității și ipotezelor pe care se bazează. Practic astfel de algoritmi pot fi spărți dar necesită o putere de calcul foarte mare.

Deși există multe tehnici folosite în criptarea datelor, cea mai populară și folosită în zilele noastre este criptarea prin cheie publică (criptografie asimetrică), folosită de instituții guvernamentale, armata și corporații mari.

Criptografia asimetrică presupune folosirea a două chei, una pentru criptarea datelor (cheia publică) și una pentru decriptarea datelor (cheia privată). Fiecare receptor are o cheie privată unică pe care o folosește pentru a decripta datele. Emițătorul oferă cheia publică oricui, folosită pentru a cripta datele. Cheia publică și privată sunt de obicei într-o relație matematică dar calcularea lor nu este fezabilă.



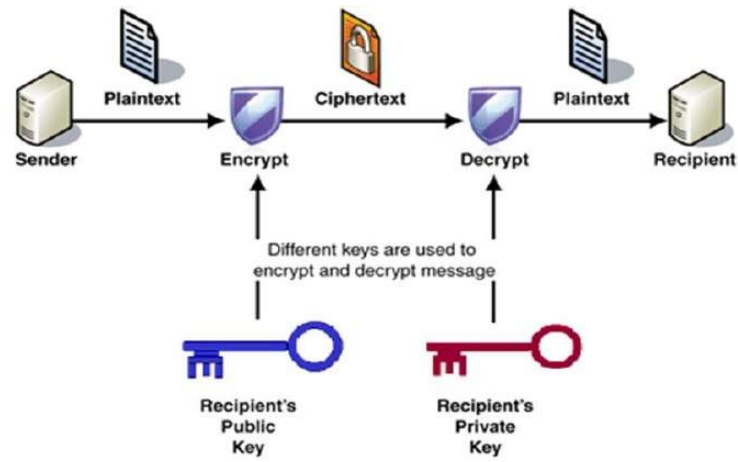


Figure 10: Criptografie Asimetrică [19]

RSA (Rivest–Shamir–Adleman) este cel mai folosit cripto sistem cu cheie publică. Relația matematică dintre cele două chei este securizată prin alegerea a două numere prime foarte mari care sunt păstrate secrete [20].

## 3 Medicarium

### 3.1 Analiza aplicației

#### 3.1.1 Problematika

”Mobile Health” (m-health) [21] este termenul folosit pentru a descrie utilizarea tehnologiilor mobile precum telefoanele pentru a sprijini și îmbunătăți sistemul de sănătate. Aplicațiile mobile au un potențial foarte mare când vine vorba de medicină, cazurile lor de utilizare variază de la simpla monitorizare a unor aspecte medicale până la comunicare între doctori, pacienți și instituții medicale.

În ultimii ani dispozitivele mobile au început să fie dotate cu din ce în ce mai mulți senzori pentru a oferi mai mult suport pentru astfel de aplicații. Creșterea în popularitate a adus ca urmare anumite reglementări. În iulie 2011, Administrația Statelor Unite pentru Alimente și Medicamente a emis un proiect de orientare privind reglementarea aplicațiilor medicale mobile [20]. Astfel se propune ca aplicațiile mobile medicale trebuie să gasească un echilibru între îmbunătățirea calității vieții utilizatorilor și respectarea siguranței și confidențialității.

Medicarium este o aplicație care își propune centralizarea istoricului medical al utilizatorilor săi. În România există deja un astfel de sistem prin ”Cardul de Sănătate”. Din păcate nu toate persoanele din România au primit astfel de carduri, mai mult de cât atât, viitorul acestui sistem nu este cert. O altă problemă a cardului de sănătate este faptul că utilitatea lui este limitată la sistemul de sănătate public din România.

Luând aceste probleme în calcul, Medicarium poate fi folosit oriunde, de oricine indiferent că vorbim de sistemul public sau private și indiferent de țară.

În prima fază Medicarium va fi folosit pentru a păstra istoricul medical al pacientului. Sunt stocate date generale ale pacientului (grupa de sânge, greutate, vârstă etc. . . ), cat si documente medicale (analize, teste).

### 3.1.2 Cazuri de utilizare

Aplicatia Medicarium permite urmatoarele functionalitati:

1. Înregistrare și verificare cont.
2. Autentificare prin factori multipli (date de logare, pin și senzori biomerici).
3. Stocarea și editarea datelor medicale generale ale pacientului.
4. Stocarea documentelor medicale. Utilizatorul poate adăuga noi documente folosind camera sau din galaria telefonului.
5. Modificarea vizibilității datelor în caz de urgență.
6. Mod de urgență care poate fi folosit de orice persoană pentru a vedea datele medicale pe care utilizatorul le-a setat în prealabil.

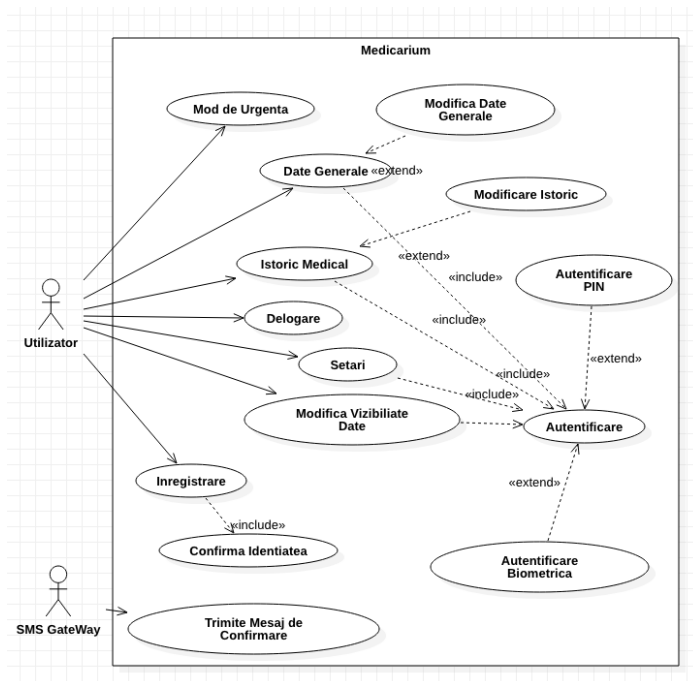


Figure 11: Diagrama Cazurilor de Utilizare

## 3.2 Proiectarea aplicației

### 3.2.1 Arhitectura

Solutia o sa fie compusa din 2 aplicatii mobile, clientul mobil propriu-zis si un "SMS Slave", o aplicatie separata folosita special pentru a trimite mesaje pentru autentificarea si verificarea utilizatorilor.

Clientul mobil este accesibil oricui pe cand aplicatia pentru mesaje este privata, fiind intretinuta impreuna cu serverele si baza de date.

La fel ca aplicatiile, avem doua server, un REST API care satisface cererile primite de clientii mobili si un SMS Gateway, care intermediaza comunicarea intre serverul REST si SMS Slave-ul.

Comunicarea intre servere se face prin HTTPS. Comunicarea intre SMS Gateway si SMS Slave se face prin WebSocket pentru a mentine un canal de comunicare bidirectional.

Server-ul REST comunica direct cu o baza de date nonrelationala de tip mongoDB.

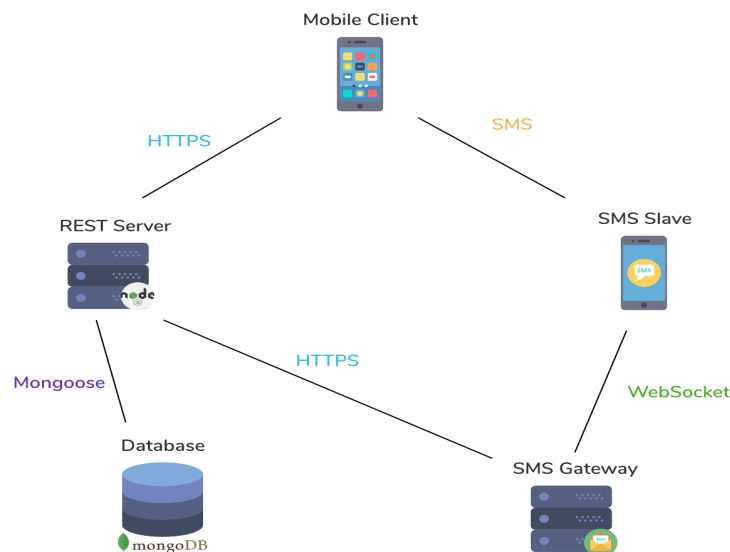


Figure 12: Diagrama de arhi

### 3.2.2 UML ceva???

## 3.3 Implementarea aplicației - Serverul și serviciile

### 3.3.1 Server REST

Representational State Transfer (REST) este stil arhitectural software care definește un set de constrângeri pentru crearea de servicii Web. Un serviciu Web este un server web construit pentru a satisface toate nevoile unui site sau unei aplicații [22].

Principala caracteristică a acestor tipuri de servicii îl reprezintă faptul care serverul nu stochează nici o stare a sesiunii clientului. Fiecare cerere conține toate informațiile necesare pentru a putea înțelege cererea. Cererile au loc în izolare și sunt independente, serverul nu se folosește de informații din alte cereri iar clientul este responsabil pentru trimiterea de orice dată e necesară pentru a obține răspunsul dorit.

Principalele avantaje ale unui serviciu REST sunt:

- Suport pentru diferite format de date (JSON, XML, text etc...)
- Performanță crescută și eficientă, serviciile REST folosesc puțină lățime de bandă
- Ușor de modificat, datorită unicității arhitecturii, componentele sunt izolate ușurând eventuale modificări
- Scalabilitate, fiind principalul motiv care a adus la adoptarea serviciilor REST [22]

În Medicarium, serverul REST este responsabil de a servi clienții mobili cu resurse de care au nevoie. Există o serie de rute la dispoziția clienților accesibile doar pe baza de Json Web Token (JWT).

Exemple de rute folosite în aplicație:

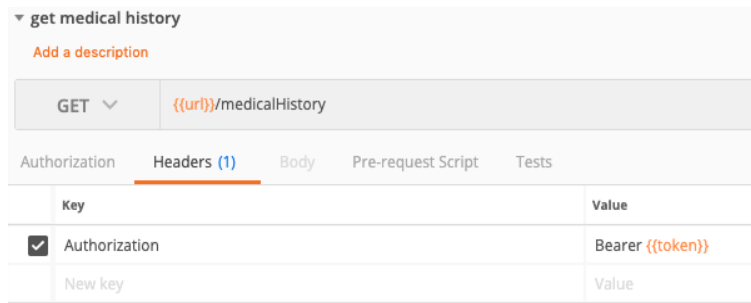


Figure 13: Exemplu de metoda GET cu JWT în antetul cererii

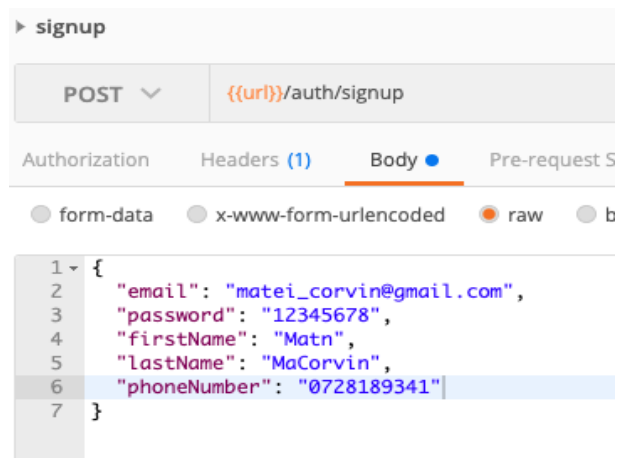


Figure 14: Exemplu de metoda POST cu JSON în corpul cererii



Figure 15: Exemplu de metoda DELETE cu mesaj de eroare

### 3.3.2 Node.js

Pentru implementarea serverului REST s-a folosit Node.js, un mediu de rulare care permite execuția de cod javascript în afară browser-ului.

Node.js este dublat de npm, un sistem de gestionarea a pachetelor care permite customizarea unui proiect Node.js cu diferite pachete.

Există numeroase avantaje atunci când se folosește Node.js pentru dezvoltarea unui server. Fiind javascript, serverul în sine este mai lejer și mai ușor de întreținut. Mai mult de cât atât, este și mult mai rapid, operațiile de I/O fiind foarte rapide. Un alt avantaj important îl reprezintă numeroase librării și pachete disponibile în npm.

Servicii mari precum Ebay, Netflix și PayPal [23], folosesc Node.js, iar popularitatea acestui stă doar să crească.

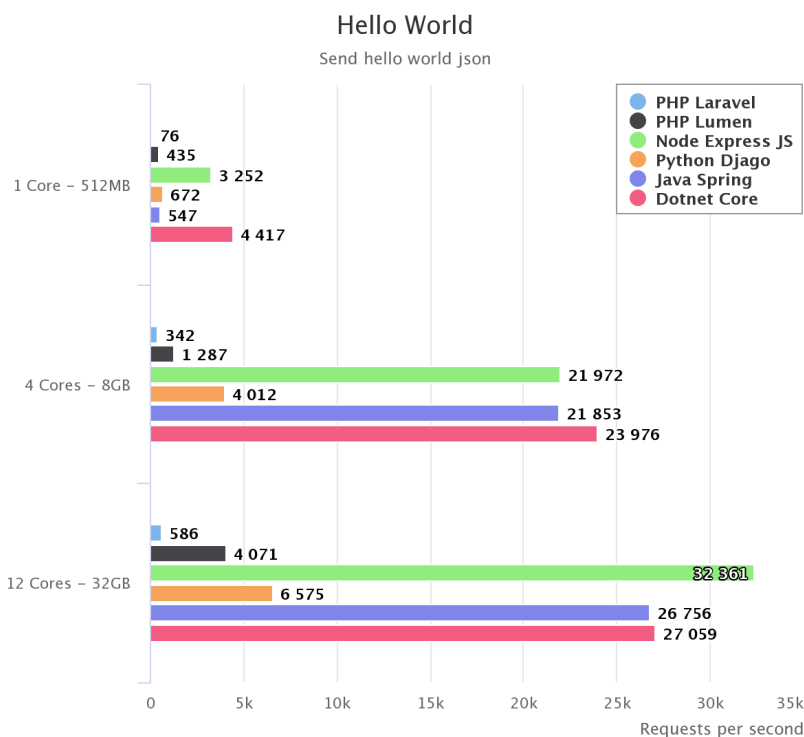


Figure 16: Performanță a diferitor framework-uri [24]

**3.3.3 MongoDB**

**3.3.4 Autentificare in doi pași**

**3.4 Implementarea aplicației - Clientul mobil**

**3.4.1 Android Jetpack**

**3.4.2 Kotlin**

**3.4.3 Autentificarea**

**3.4.4 Securitatea aplicației**

**3.4.5 Gestionarea permisiunilor**

**3.4.6 Gestionarea fișierelor**

**3.5 Testarea**

**4 Manual de utilizare**

**5 Concluzii**



## 6 Bibliografie

### Bibliografie

- [1] OWASP. *OWASP Top 10 2017*. URL: [https://www.owasp.org/images/7/72/OWASP%5C\\_Top%5C\\_10-2017%5C\\_%5C%28en%5C%29.pdf.pdf](https://www.owasp.org/images/7/72/OWASP%5C_Top%5C_10-2017%5C_%5C%28en%5C%29.pdf.pdf).
- [2] OWASP. *Top 10 Mobile 2016*. URL: [https://www.owasp.org/index.php/Mobile%5C\\_Top%5C\\_10%5C\\_2016-Top%5C\\_10](https://www.owasp.org/index.php/Mobile%5C_Top%5C_10%5C_2016-Top%5C_10).
- [3] *3 types of Authentication*. URL: <https://www.slideshare.net/awesomeadmin/secure-your-salesforce-org-with-twofactor-authentication>.
- [4] *RFC 7519 JWT*. URL: <https://tools.ietf.org/html/rfc7519>.
- [5] *JSON Web Token (JWT)*. URL: <https://tools.ietf.org/html/rfc7519>.
- [6] ENISA. *Smartphone Secure Development Guidelines*. 2017. URL: <https://www.enisa.europa.eu/publications/smartphone-secure-development-guidelines-2016>.
- [7] ENISA. *Guidelines for SMEs on the security of personal data processing*. 2017. URL: <https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing>.
- [8] Bin Liu et al. “Follow my recommendations: A personalized privacy assistant for mobile app permissions”. In: *Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016)*. 2016, pp. 27–41.
- [9] davx5. *Why does WiFi SSID restriction need the location permission?* URL: <https://www.davx5.com/faq/wifi-ssid-restriction-location-permission>.
- [10] Giles Hogben Martin Pelikan and Ulfar Erlingsson. *Identifying Intrusive Mobile Apps Using Peer Group Analysis*. URL: <https://security.googleblog.com/2017/07/identifying-intrusive-mobile-apps-using.html>.
- [11] Reddit Post. *Since when did a calculator need to make calls?* URL: [https://www.reddit.com/r/assholedesign/comments/8nlh3k/since\\_when\\_did\\_a\\_calculator\\_need\\_to\\_make\\_calls/](https://www.reddit.com/r/assholedesign/comments/8nlh3k/since_when_did_a_calculator_need_to_make_calls/).

- [12] Arthur Goldberg, Robert Buff, and Andrew Schmitt. “A comparison of HTTP and HTTPS performance”. In: *Computer Measurement Group, CMG98* 8 (1998).
- [13] Adrienne Porter Felt et al. “Measuring {HTTPS} Adoption on the Web”. In: *26th {USENIX} Security Symposium ({USENIX} Security 17)*. 2017, pp. 1323–1338.
- [14] “The rise of 3G”. In: URL: <http://www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf>.
- [15] Ian Fette and Alexey Melnikov. *The websocket protocol*. Tech. rep. 2011.
- [16] Jussi-Pekka Erkkilä. “Websocket security analysis”. In: *Aalto University School of Science* (2012), pp. 2–3.
- [17] *Testing WebSockets*. URL: [https://www.owasp.org/index.php/Testing\\_WebSockets\\_\(OTG-CLIENT-010\)](https://www.owasp.org/index.php/Testing_WebSockets_(OTG-CLIENT-010)).
- [18] Jonathan Katz et al. *Handbook of applied cryptography*. CRC press, 1996.
- [19] Tutorialspoint. *Public Key Encryption*. URL: [https://www.tutorialspoint.com/cryptography/public\\_key\\_encryption.htm](https://www.tutorialspoint.com/cryptography/public_key_encryption.htm).
- [20] Amy J Barton. “The regulation of mobile health applications”. In: *BMC medicine* 10.1 (2012), p. 46.
- [21] James G Kahn, Joshua S Yang, and James S Kahn. ““Mobile”health needs and opportunities in developing countries”. In: *Health Affairs* 29.2 (2010), pp. 252–258.
- [22] Mark Masse. *REST API Design Rulebook: Designing Consistent RESTful Web Service Interfaces.* ” O’Reilly Media, Inc.”, 2011.
- [23] Stefan Tilkov and Steve Vinoski. “Node.js: Using JavaScript to build high-performance network programs”. In: *IEEE Internet Computing* 14.6 (2010), pp. 80–83.
- [24] Mihai Cracan. *Web REST API Benchmark on a Real Life Application*. URL: <https://medium.com/@mihaigeorge.c/web-rest-api-benchmark-on-a-real-life-application-ebb743a5d7a3>.
- [25] Jakob Jonsson and Burt Kaliski. *Public-key cryptography standards (PKCS)# 1: RSA cryptography specifications version 2.1*. Tech. rep. 2003.