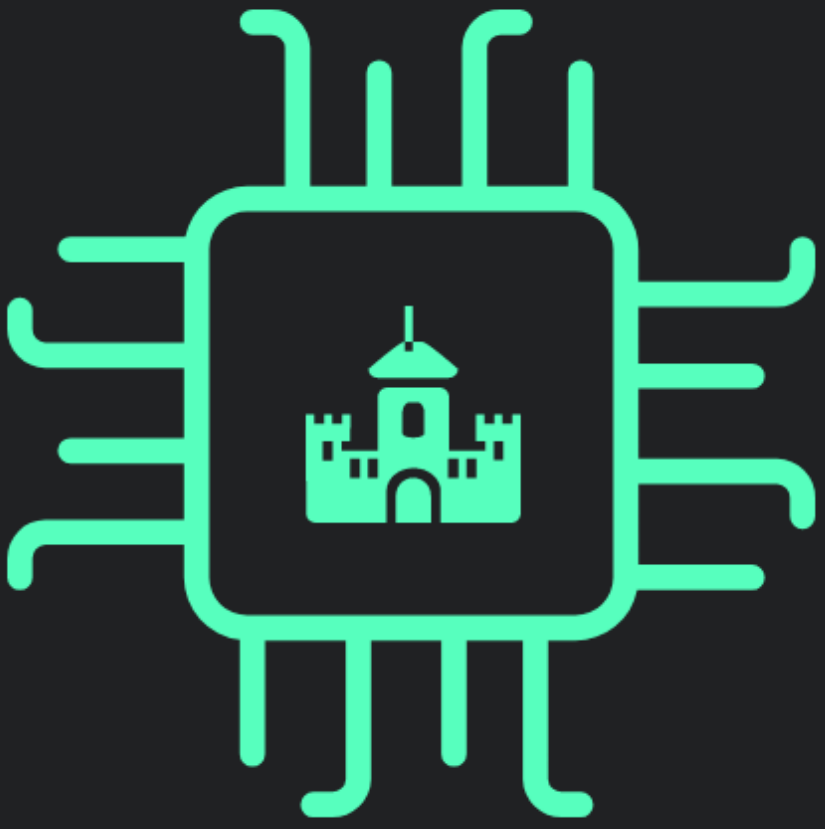
IBON ALONSO
MARIO ETXEBERRIA

KRIPTOFORT

ZURE JARDUEREN ERREGISTRO BAT ERAMANEZ COVID-ARI AURRE EGITEKO CAGSS: COVID ABISU GOIZTIARREKO SISTEMA SEGURUA

LAURO IKASTOLA 2022



Eskerrak
Gure proiektua sortu eta garatzeko prozesuan eman digun laguntza ezin baliotsuagoa dela eta, eskerrak eman nahi dizkiogu Amaia Perezi. Eskerrik asko, halaber, Liher Elgezabali, bere ideiekin aplikazioaren prototipatuan lagundu digulako. Azkenik, eskerrak eman nahi diogu Jon Hernandezi, aspektu tenkologikoarekin erlazionatutakoari buruz eman digun aholkuetatik.

Abstract
Pandemian zehar, covid-aren desarolloa kontrolatzeko aplikazio bat sortzeko hainbat saiakera egon dira. Hala ere, saiakera horiek ez dira oso emankorrak izan, erabiltzailearen kokapenaren zehaztasunik eza bezalako arrazoiengatik. Gure helburua da covid-ak eta oraindik izan ez direnen segurtasunak eragindako pertsonen esperientzia hobetzea, teknologia eta enkriptazioa erabiliz. Nahiko garrantzitsua iruditzen zaigu arlo horretan arakatzea, aplikazio gutxi saiatu baitira oraindik, eta bizitza asko salba ditzakeen proiektu bat da, behar bezala inplementatzen bada. Gu kriptografia eta horrekin lotutako guztia ikertzen hasi ginen, enkriptazio-metodoetatik hasi eta hautsi daitezkeen moduetaraino. Azken finean, zure kokapena erabiltzen duen aplikazio batek segurua izan behar du. Bestalde, prototipoak egiteko fasea hastean, "Radar COVID" bezalako aurreko proiektuak aztertuko ditugu. Asmatu egiten zutela eta gure aplikazioa hobetzeko huts egiten zutela ikertu genuen. Horri esker, gure ideia praktikan jartzeko modurik onena mugikorraren geolokalizazioa erabiltzea zela erabaki genuen, nahiko zehatza baitzen. Azkenik, gure ideiarekin bat datorren prototipo funtzional bat egitea lortu genuen.

AURKIBIDEA

1. Sarrera orokorra
2. Helburua
    a. Aplikazioa
3. Plangintza eta metodologia
    a. Funtzioak
    b. Funtzionamendua
    c. Segurtasuna
    d. Beste aplikazio batzuekiko alderaketa
    e. Adituarekin elkarrizketa
4. Emaitzak
5. Emaitzen eztabaida
6. Ondorioak
7. Bibliografia
8. Eskerrak

1. Sarrera orokorra

Teknologia gero eta leku gehiagotan dago, izan ere, azken urteetan ziztu bizian hedatu da gure bizitzak erabat aldatzen. Teknologia gure egunerokotasunaren parte bihurtu da, hain da bertakotua, non askotan ez baikara konturatzen hori nola iristen den gure eskuetara, zenbat pertsonak izan zuten guk baino lehenago eta zein den inpaktua. (Soziala, ekonomikoa, ingurumenekoa eta, bereziki, kulturala) gure bizitzei buruz duena.

Horrek guztiak, eta noski, teknologiaren munduan gertatzen diren aldaketa guztiak, aurrerapen guztiak, guri egokitu beharko litzaizkiguke. Faktore horiek guztiek ingurune izugarri eta arriskutsu batera garamatzate, eta defendatzeko sistemak behar ditugu, batez ere gure informazioa modu seguruan bidaliz leku batetik bestera.

Kriptografia edo informazio sentikorra enkriptatzeko artea eta zientzia, garai batean, gobernuaren, akademiaren eta militarren erresumen esklusiboa zen. Hala ere, azken aurrerapen teknologikoekin kriptografia egunerokotasunaren foku guztiak zulatzen hasi da. Zure mugikorretik bankura dagoen guztia kriptografiara doa, zure informazioa eta bizitza seguru mantentzeko.

Eta, zoritxarrez, kriptografiaren berezko konplexutasunak direla eta, askok uste dute hau hobea dela hacker-ak, multi-mila milioi dolarreko konglomeratuak eta NSA. Baina egiatik ezin zitekeen gehiago aldendu. Interneteko datu pertsonalen kopuru handia dela eta, inoiz baino garrantzitsuagoa da asmo txarrez gizabanakoengandik arrakastaz babesten ikastea.

2. Helburua

2019ko abenduaren 31n, Wuhanen detektatutako lehen pneumonia kasuak OMEri jakinarazi zitzaizkion. Aldi horretan, birusa ezezaguna zen oraindik. Kasuak abenduaren 12tik 29ra bitartean gertatzen dira, Wuhango osasun-agintarien arabera. Gure bizitza guztiak beti bezain arruntak izaten jarraitu zuten, 2020ko urtarrilaren 7an birus hori identifikatu zen arte, eta tira, ez dago kontatzeko askoz gehiago, historia oso ondo ezagutzen dugu.

Gure helburua jendeari covid-etik babesten laguntzea da aplikazio baten bidez, erabiltzaileen datuak babesteari garrantzi handia emanez. Egon zaren guneen erregistroa eramango duen aplikazio bat egin nahi dugu, gero datu horiek enkriptatu eta zerbitzari batera bidaltzeko, non erabiltzaile guztien datuak dauden, norekin eta non egon den jakin ahal izateko.

Sistema hau enpresa txiki eta ertainetara bideratuta egotea nahi dugu, jende gehiago dagoen lekuetan kontrola izatea oso zaila baita. Horrez gain, enpresa horiek, baliabide gutxiago dituztenez, zailtasun gehiago dituzte jarraipena egiteko. Baina dena laburbiltzen bada pertsona arruntei laguntzeko, birus horri errazago eta konplikazio gutxiagorekin aurre egin ahal izateko.

a. Aplikazioa

Gure helburua da kriptografikoki enkriptatutako aplikazio bat sortzea, kontagai-fasean covid-a uzkurtu duen norbaitekin egon bazara jakinarazteko. Aplikazio bat sortzea erabaki dugu, uste baitugu kutsatze asko prebenituko dituela kontaktuaren berri berehala ematerakoan. Bestalde, ziurtatu behar dugu aplikazioa eta haren datuak biziki enkriptatzen direla, ez baitugu nahi erabiltzaile baten kokapenen historiala okerreko eskuetan erortzea.

Aplikazio funtzionarioa honela: erabiltzaileak kokapena aktibatuta duen bitartean, aplikazioak aldizka erregistratuko du bere kokapena, bisitatzen dituen lekuen eta bisitatu dituzun orduen jarraipena egiteko. Covid-a hartuz gero, aplikazioak formulario bat irekiko du, eta erabiltzaileak sintomen hasiera-egunarekin eta aplikazioak zehaztu ezin dituen beste aldagai batzuekin bete beharko du. Ondoren, aplikazioak datu horiek erabiliko ditu fase infekziosoaren hasieran erabiltzailea non zegoen zehazteko, eta ordu berean leku berean 15 minutuz egon diren erabiltzaile guztiei jakinaraziko die.

Aplikazioak mapa bat izango du, mundu guztiarentzat erabilerraza izan dadin. Mapa honetan, zure azken lokazioak ikusiko dira, baita gehien erabiltzen dituzun lekuak ere. Mapa honi "etxea" edo "lana" bezalako kokapen batzuk gehitu ahal izango zaizkio, nabigatzeko errazagoa izan dadin eta erabiltzaileek lekuak azkar ezagutu ditzaten.

Arestian aipatutakoaz gain, aplikazioan bigarren mailako beste funtzio batzuk ere sartuko dira, hala nola doikuntzak eta kontua dituen menua. Horrez gain, aplikazioak beste funtzioren bat izan lezake, covid-ari buruzko azken berriak erakustea, esaterako.

3. Plangintza eta metodologia

Gure helburua, kontaktu berriren batek covid duenean abisatuko dizun aplikazio bat egitea da. Gailuaren kokapena zehaztuko duen eta datuak zerbitzari batean gordeko dituen gps-sitema bat erabiliko dugu. Atal honetan aplikazioak izango dituen funtzioak zehaztuko ditugu, nola sortuko dugun eta zein segurtasun-mota izango duen.

a. Funtzioak

Aplikazioaren funtzio nagusia izango da gps bidez zure kokapena zehaztea gailuaren kokapena erabiliz, eta beste erabiltzaile batzuenekin kontrastatzea, COVID-19a duen norbaiten kontaktuan edo leku berean egon zaren zehazteko. Horretarako, aplikazioak erabiltzailearen baimena beharko du bere kokapena erabiltzeko eta bigarren planoan exekutatzeko. Baimenak lortu ondoren. Plikazioak honela funtzionatuko du:

Lehenik eta behin, aplikazioak gailuaren kokapena lortzen du eta zerbitzari batean gordetzen du, lortu den orduarekin eta covid egoerarekin batera. Erabiltzaile batek covid-aren proban positibo eman duela jakinarazten duenean, zerbitzariek beren kokapenei buruzko informazioa kontrastatzen dute leku berean egon diren gainerako erabiltzaileekin. Pertsona bat infektatutako erabiltzailea baino hamabost minutu edo gehiago egon bada ligatzen, horren berri emango zaio.

Gainera, beste erabiltzaile batzuek birusa hartu dutela esan duten lekuak ere ikusi ahal izango dituzu. Mapan markatzaileak egongo dira, "Etxea" edo "lana" bezalako guneak markatu ahal izan ditzazun, datu-baseko informazioa oraindik ere zuzenagoa izan dadin. Funtzio horiez gain, aplikazioak leiho bat izango du covid-arekin lotutako albisteekin, gobernuak egiten dituen erregulazioekin egunean egon ahal izateko edo, besterik gabe, egoera ikusteko.

b. Funtzionamendua

Gure aplikazioaren funtzionamenduari dagokionez, telefonoak bidalitako gps seinalea koordenatu batzuetara itzultzea nahi dugu, ondoren telefonoak berak datu-base batera igo dezan, non pertsonen datuak alderatu ditzakegun. Informazio hori testu gisa konparatuko litzateke, eta, behin hori eginda, kode irekiko gps zerbitzu bat erabili nahi dugu, informazioa mapa batera itzultzeko, hori askoz ere erosoagoa baita ikusmenerako.

Garrantzitsua da aipatzea ez dugula erregistro-sistema konbentzionalik erabiliko, erabiltzailearen pribatutasuna babesteko. Erabiltzailearen anonimotasuna sustatzen duten zerbitzuek dagoeneko erabiltzen duten sistema da, kodeak erabiltzaileentzako identifikatzaile gisa erabiliz.

c. Segurtasuna

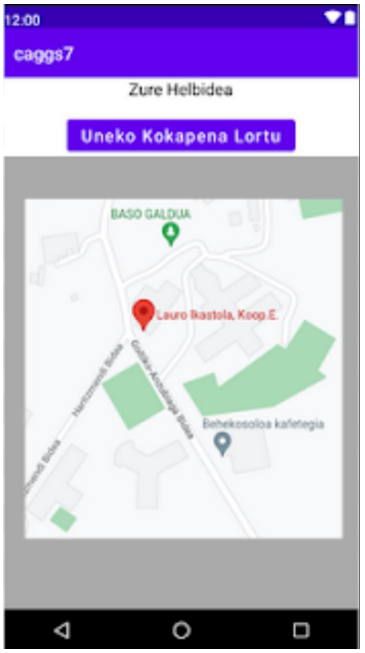
Segurtasunari dagokionez, aplikazioa denda ofizialen bidez deskargatuko da, inork ez dezan instalatzaile konprometiturik deskargatu. Aplikazioak ahalik eta datu gutxien eskatuko ditu, ahalik eta anonimo gehien erabili ahal izateko. Egia da hori nahiko zaila dela; izan ere, zure kokapena bidali behar da, erabiltzailearen pribatutasuna hausten duen zerbait bada ere. Horretaz gain, enkriptatze-metodo bat erabiliko dugu datuak datu-basera bidaltzeko. Horren ondorioz, koordenatuak ausazko zenbaki izatetik ausazko testu-zati izatera igaroko dira.

d. Beste aplikazio batzuekiko alderaketa

Ideia hori beste pertsona batzuek ere izan dute; horregatik, haien produktua gurearekin alderatuko dugu. Hain zuzen ere, alderatuko dugun aplikazioak "radar COVID" du izena, eta gai ekonomikoen eta transferentzia digitalaren ministerioak egiten du. Bi aplikazioen helburua berbera da, baina funtzionamendua nahiko desberdina da. Hasteko, aplikazioak hurbileko mugikorrak detektatzen ditu bluetooth erabiliz, eta gure aplikazioak, berriz, seinaleak bidaltzen ditu mugikorretik datu-base batera. Bluetooth sistema hau ez da batere eraginkorra aplikazioaren aipamenetan ikus daitekeen bezala, oso emaitza zehaztugabeak ematen baititu. Pribatutasunari dagokionez, aplikazioak, gureak bezala, ez du erabiltzailearen daturik jasotzen.

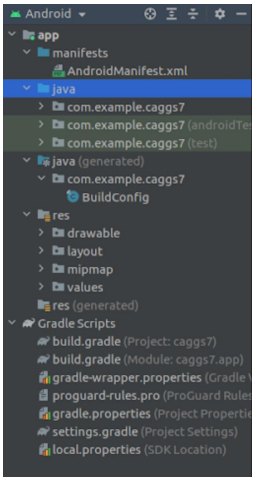
Laburbilduz, esan dezakegu zure aplikazioak erabiltzaileen pribatutasuna gehiago errespetatzen duela, baina ez dela hain zehatza. Hori ez da arazo bat, aplikazio hori Espainia osora bideratuta baitago, eta gurea, berriz, enpresa txiki eta ertainetara.

6. Emaitzak



Horretaz gain, noski, gure aplikazioa ere badago. Java programazio-sistemarekin funtzionatzen du android gailuetan. Hemen, ondoan, gure aplikazioaren azken emaitzaren argazki bat dago, eta, ikus daitekeenez, hiru zatitan banatuta dago: mapa, koordenatuak eta toki bakoitzeko covid-ari buruzko informazioa.

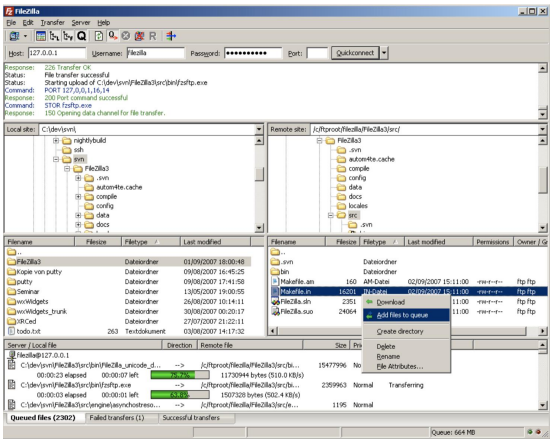
Koordenatuetarako, google play apia erabiltzen dugu. Aplikazioaren arabera, honek baimena emateko eskatzen dizu, hau da, aditzera ematen dizu zer egiten ari zaren baimenik gabe ez jarraitzeko. Koordenatuak ager daitezen, goian dagoen botoi urdinari eman behar zaio, eta klikatzean, "Luzera" eta "latitudea" dioen testua desagertu egingo da, eta zenbaki batzuk agertuko dira haren ordez. Datu hori bidaltzen zaio zerbitzuari, eta horren bidez funtzionatzen du aplikazioak.



Bigarren elementua mapa da, google maps aplikazioa erabiltzen duena, hau ere google taldeak garatua. Mapa hau erabiltzea erabaki dugu, google maps delako mapen zerbitzurik ezagunena eta erabiliena; gainera, oso zehatza da eta oso eguneratuta dago. Koordenatuen botoiak erakusten dizuna, baina gizakientzat ulergarriagoa dena.

Eta azkenik, lekuei buruzko informazioa dugu, gure datu-baseak tokian dagoen covid egoerari buruz dakiena, besterik ez. Hemen

agertzen den informazio guztia gure erabiltzaileek biltzen dute, eta, beraz, horien zehaztasuna gure erabiltzaileek gune horretan egiten duten jardueran oinarritzen da. Hau zerbitzarian dagoenaren idatzizko irudikapena da.



Zerbitzariari dagokionez, "Filezilla server" zerbitzua erabili dugu ftp zerbitzari bat sortzeko. Ubuntu sistema eragile batean funtzionatzen ari da, errendimendua handiagoa izan dadin.

7. Emaitzen eztabaida

Aukeratzeko orduan kontuan hartu ditugun irizpideak honako hauek dira: informazio gutxi abiadura handian zifratzea, memoria gutxi erabiltzea eta ahalik eta seguruena izatea. Irizpide horiei jarraiki, erabakia ez da zaila izan, literalki twofish delako enkriptatze-metodo irabazlea aipatutako eremu guztietan. Behin hori ikusita, algoritmoari buruz ikertu dugu, eta ez dugu erabili ezin izateko arrazoirik aurkitu; beraz, hori izango da proiekturako egokiena.

Azkenean, aplikazioak zehaztapen eraginkor batekin funtzionatzea lortu dugu, nahiz eta zaila izan. Aplikazioa lehen konparatutakoa baino eraginkorragoa da, radar covid, nfc teknologiarekin funtzionatzen duena.

8. Ondorioak

Laburbilduz, twofish da gure proiekturako etorkizun handiena duen enkriptatze-sistema. Ikertu ondoren, badirudi ez litzatekeela arazorik egon behar sistema hori gure aplikazioan erabiltzeko, eta horrek esan nahi du prest gaudela aplikazioa garatzen hasteko. Baina, noski, ezer egiten hasi aurretik, gure aurrerapen guztiak gaiari buruz benetan dakien norbaitekin kontsultatuko ditugu. Laburbilduz, gure sistema lehendik zegoena baino eraginkorragoa da, nahiz eta sistema informatiko sinpleagoak erabili.

7. Bibliografía y referencias

- “Criptografía.” *Wikipedia*, Wikimedia Foundation, 24 Dec. 2021, https://es.wikipedia.org/wiki/Criptograf%C3%ADa.
- GuilleVenDesarrollador de sistemas con más de 20 años de experiencia. Apasionado por transmitir conocimientos sobre tecnología., et al. “¿Qué Es La Criptografía?” *Tecnología + Informática*, 3 Jan. 2022, https://www.tecnologia-informatica.com/que-es-la-criptografia/.

- Brainshit. *Departamento De Matemática Aplicada a Las Tecnologías De La Información y Las Comunicaciones*, http://www.dma.fi.upm.es/recursos/aplicaciones/matematica_discreta/web/aritmetica_modular/criptografia.html.
- “Qué Es La Criptografía y Cuáles Son Sus Usos.” *VIU*, https://www.universidadviu.com/es/actualidad/nuestros-expertos/que-es-la-criptografia-y-cuales-son-sus-usos.
- “¿Qué Es Criptografía?” *NIC Argentina*, https://nic.ar/es/enterate/novedades/que-es-criptografia.
- Romero, Santiago. “¿Qué Es La Criptografía Avanzada?” *BBVA NOTICIAS*, BBVA, 20 Oct. 2020, https://www.bbva.com/es/que-es-la-criptografia-avanzada/.
- “Criptografía: Qué Es y Por Qué Deberías Usarla En Tu Teléfono Para Que No Te Espíen.” *BBC News Mundo*, BBC, https://www.bbc.com/mundo/noticias-50862657.
- por EALDE, Escrito, and Ealde. “Qué Es La Criptografía y Por Qué Es Útil En Ciberseguridad.” *EALDE Business School*, 29 June 2020, https://www.ealde.es/que-es-criptografia/.
- Hurtado, Javier Sáez. “Qué Es La Criptografía y Para Qué Sirve.” *Thinking for Innovation*, 21 Oct. 2021, https://www.iebschool.com/blog/que-es-la-criptografia-y-para-que-sirve-finanzas/.
- “Cómo Funciona La Criptografía.” *YouTube*, YouTube, 29 Apr. 2015, https://www.youtube.com/watch?v=Q8K311s7EiM.
- EaldeBusinesSchool. “Los Nuevos Retos En Ciberseguridad Y Privacidad De Los Datos.” *YouTube*, YouTube, 25 Sept. 2019, https://www.youtube.com/watch?v=JNVXzJhJ5uc.
- “¿Quã© Es Un Certificado Digital? : Certificados Digitales.” UPV, https://www.upv.es/contenidos/CD/info/711545normalc.html.

8. Agradecimientos

Gure proiektua sortu eta garatzeko prozesuan eman digun laguntza ezin baliotsuagoa dela eta, eskerrak eman nahi dizkiogu Amaia Perezi. Eskerrik asko, halaber, Liher Elgezabali, bere ideiekin aplikazioaren prototipatuan lagundu digulako. Azkenik, eskerrak eman nahi diogu Jon Hernandezi, aspektu tenkologikoarekin erlazionatutakoari buruz eman digun aholkuetatik.