Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Dean Črnigoj

Senzorski moduli NFC in varnost podatkov

magistrsko delo

študijski program druge stopnje
računalništvo in informatika

Mentor: doc. dr. Mira Trebar

Ljubljana, 2018

Avtorske pravice. Rezultati magistrskega dela so intelektualna lastnina avtorja in Fakultete za računalništvo in informatiko Univerze v Ljubljani. Za objavljanje ali izkoriščanje rezultatov magistrskega dela je potrebno pisno soglasje avtorja, Fakultete za računalništvo in informatiko ter mentorja.

©2018 Dean Črnigoj

Zahvala

Zahvaljujem se svoji mentorici doc. dr. Miri Trebar, za pomoč in vodstvo pri izdelavi magistrske naloge. Rad bi se zahvalil tudi svoji družini in punci Mirjani, ki so me spodbujali in stali ob strani v času študija.

Dean Črnigoj, 2018

Kazalo

Seznam uporabljenih kratic

kratica	angleško	slovensko
AES	Advanced Encryption Standard	simetrični kriptosistem
CSV	Comma Separated Values	podatki so v datoteki ločeni z vejico
DES	Data Encryption Standard	simetrični kriptosistem
ECMA	European Computer Manufacturers Association	standardizacijska organizacija za informacijske in komunikacijske sisteme
FIPS	Federal Information Processing Standards	ameriški standard za obdelavo informacij
FTP	File Transfer Protocol	protokol za prenos datotek
HTML	Hyper Text Markup Language	označevalni jezik za izdelavo spletnih strani
HTTP	Hyper Text Transfer Protocol	komunikacijski spletni protokol
HTTPS	Hyper Text Transfer Protocol Secure	varen komunikacijski spletni protokol
HSU	High Speed UART	serijska povezava z veliko hitrostjo

IDE	Integrated Development Environment	integrirano razvojno okolje
IEC	International Electrotechnical Commission	organizacija za elektrotehnične standarde
ISO	International Organization for Standardization	organizacija za standarde
IoT	Internet of Things	internet stvari
NDEF	NFC Data Exchange Format	izmejevalni format sporočil tehnologije NFC
NFC	Near Field Communication	tehnologija komunikacije kratkega dosega
MD	Message-Digest	zgoščevalni algoritem
PHP	Personal Home Page (PHP: Hypertext Preprocessor)	skriptni programski jezik
RFID	Radio-Frequency Identification	tehnologija radiofrekvenčne identifikacije
ROM	Read Only Memory	bralni pomnilnik
RTC	Real Time Clock	ura realnega časa
RSA	Rivest-Shamir-Adleman	kriptosistem z javnimi ključi
SPI	Serial Peripheral Interface	serijsko vodilo za komunikacijo med V/I elementi
SS-NFC	Sensor System-NFC	senzorski sistem NFC
TLS	Transport Layer Security	kriptografski omrežni protokol
WSN	Wireless Sensor Network	brezžično senzorsko omrežje

Povzetek

Naslov: Senzorski moduli NFC in varnost podatkov

Senzorski moduli in naprave za merjenje temperature, in pogosto tudi vlage, se dandanes nahajajo že v celotni prehranski verigi. Vendar je le teh še vedno premalo, oziroma niso v zadostni meri upoštevani pri zagotavljanju nadzora kakovosti živil, kar priča tudi podatek o količini zavržene hrane, še preden ta pride do trgovskih polic. Podatki o hladni verigi pogosto niso na voljo, ali pa je dostop omejen na lokalne uporabnike zaradi nezadostne varnosti. V magistrski nalogi je predstavljena rešitev za zajem senzorskih podatkov s tehnologijo komunikacije kratkega dosega (angl. Near Field Communication, NFC) in dodatno zaščito podatkov s šifriranjem AES. Implementirali smo avtonomno izvedbo senzorskega sistema NFC (SS-NFC). Omogoča branje podatkov z mobilnim telefonom ali pa jih modul NodeMCU posreduje na spletni strežnik. Vključuje različne načine delovanja z uporabo komunikacije Wi-Fi, lokalnim shranjevanjem senzorskih meritev ('On-line', 'Off-line'), šifriranjem podatkov in avtorizacijo uporabnika. SS-NFC smo analizirali s testiranjem temperature v hladni verigi in s preverjanjem senzorskih meritev temperature, vlage in svetlobe v hladilniku. S 3D tiskalnikom smo izdelali enostavno ogrodje prototipa za testiranje v realnem okolju.

Ključne besede

senzorski moduli, varnost, šifriranje, AES, NFC

Abstract

Title: NFC sensor modules and data security

Sensor modules and devices for measuring temperature, often also moisture, are nowadays included in almost every step in the food supply chain. However, these numbers are still too small, or not sufficiently taken into account in ensuring food quality control, which is also evident by the amount of food waste before it comes to shelves. The master's thesis presents a solution for capturing sensor data with Near Field Communication (NFC) technology and additional data protection with AES encryption. We implemented an autonomous NFC sensor system (SS-NFC) for use in the cold chain. Data is readable by mobile phone or uploaded to a server using NFC reader and NodeMCU. The system provides various modes of operation using Wi-Fi communication or local storage of sensor measurements ('On-line', 'Off-line'), data encryption and user authorization. SS-NFC was analysed by testing temperature in a cold chain and by evaluating the sensor measurements of temperature, humidity and light in the refrigerator. We made a simple SS-NFC prototype with 3D printer for easy testing in a real environment.

Keywords

sensor modules, security, encryption, AES, NFC

Poglavje 1

Uvod

Internet stvari (angl. Internet of Things, IoT) je hitro razvijajoče se področje povezovanja različnih naprav v internetnem omrežju. IoT je pravzaprav zelo veliko omrežje povezanih stvari in ljudi, ki zagotavlja zajemanje, izmenjavo in obdelavo podatkov. Hiter razvoj tehnologij omogoča, da se na številnih področjih uporablja tudi v povezavi s senzorskimi brezžičnimi sistemi. Vse več pozornosti je namenjeno varnosti in zasebnosti, saj je številčnost naprav in stalna povezljivost v internetno omrežje idealna za izkoriščanje raznih ranljivosti teh naprav.

IoT se vse bolj uveljavlja tudi v hladni verigi (opredeljeno v poglavju 2.3), saj senzorski moduli dandanes spremljajo že skoraj vsak korak v preskrbovalni verigi živilske industrije. Stalen nadzor je pomemben, saj se pogoji shranjevanja živila med skladiščenjem in transportom spreminjajo. Zagotoviti je potrebno spremljanje temperature, vlage in drugih zahtev za analizo, za shranjevanje ter predstavitev podatkov. Tu so ključni podatki o stanju živila, saj jih je mogoče pri nepooblaščenem dostopu enostavno prebrati in spreminjati. Na področju nadzora hladne verige obstajajo različne možnosti za izvedbo enostavnih in naprednih rešitev, ki vključujejo zaščito podatkov tudi že na nivoju zajema senzorskih meritev.

1.1 Opis problema in rešitve

V senzorskih sistemih je zaščiti podatkov še vedno posvečeno relativno malo pozornosti. Ker nismo našli primerne brezžične izvedbe s povezavo v internet z možnostjo zaščite podatkov na nivoju zajema meritev, ali pa ta ni bila zadostna, smo se odločili, da izdelamo lasten senzorski sistem. Realizirali smo ga z uporabo mikrokrmilnika, komunikacije kratkega dosega (angl. Near Field Communication, NFC) in namenskega senzorskega modula s senzorji za temperaturo, vlago in svetlobo. V izvedbi je zagotovljeno šifriranje podatkov tako na senzorskem modulu NFC, kakor tudi na oddaljenem spletnem strežniku. Implementirana je tudi varna povezava z uporabo varnega komunikacijskega spletnega protokola (angl. Hypertext Transport Protocol Secure, HTTPS). Za dodatno zaščito je na voljo avtorizacija uporabnikov s pametno kartico. Sistem omogoča prikaz podatkov na spletnem strežniku in izvoz v datoteko, kjer so podatki ločeni z vejico (angl. Comma Seperated Values, CSV) za dodatno analizo.

1.2 Prispevki magistrskega dela

Glavni prispevki magistrskega dela so:

- načrtovanje in razvoj brezžičnega senzorskega sistema NFC s povezavo v internetno omrežje,
- implementacija različnih načinov delovanja senzorskega sistema NFC,
- zagotavljanje varnosti senzorskih podatkov in avtorizacija uporabnikov,
- analiza in prikaz senzorskih podatkov in
- uporaba sistema za potrebe hladne verige.

1.3 Struktura dela

V drugem poglavju je opisano področje magistrskega dela, ki vključuje internet stvari, tehnologijo NFC, hladno verigo in osnove varnosti podatkov. Za vsakega od njih sta predstavljeni uporaba in obstoječe rešitve. V tretjem poglavju so opisani zasnova, potek načrtovanja in elementi senzorskega sistema NFC (SS-NFC). Nato je v četrtem poglavju podan razvoj SS-NFC, ki vsebuje razvojna okolja, orodja in spletni strežnik. V petem poglavju je opisano delovanje SS-NFC za različne načine delovanja. V šestem poglavju je opisana uporaba SS-NFC s potekom testiranja in eksperimentov ter analizo rezultatov. Povzetek rezultatov magistrskega dela s sklepnimi ugotovitvami se nahaja v sedmem poglavju.

Poglavje 2

Pregled področja

V magistrskem delu smo se pri načrtovanju in izdelavi senzorskega sistema NFC srečali s sistemi in tehnologijami, ki vključujejo nadzor okolja in zajem ter obdelavo podatkov pri skladiščenju in transportu živil. Raziskali in analizirali smo področja interneta stvari, tehnologije NFC, hladne verige in varnosti podatkov.

2.1 Internet stvari

Internet stvari povezuje veliko število različnih naprav v internetnem omrežju [18]. To niso samo računalniki in druge komunikacijske naprave, temveč so lahko aparati bele tehnike, različni vsadki in biočipi, senzorji v napravah, oblačilih, prevoznih sredstvih, itd. Zaradi hitrega razvoja tehnologij in cenenih naprav vključenih v IoT, je njihova razširjenost in množična uporaba že presegla število računalnikov in mobilnih naprav.

Razvoj tega področja vključuje pametne hiše, pametne avtomobile in mesta ter omogoča, da naprave komunicirajo med seboj brez posredovanja človeka ali spremenijo stanje z oddaljenim posredovanjem. V enem od primerov uporabe je predstavljeno, da si lahko nastavimo temperaturo ali prezračevanje doma na daljavo, npr. preko spleta [40].

Sprva varnosti posameznih naprav v IoT ni bilo posvečeno veliko pozorno-

sti, a ker so vse naprave povezane v internet in je zasnova relativno enostavna, jih je mogoče izkoristiti za razne napade, posledično pa onemogočiti njihovo delovanje [28]. Številčnost objav na to temo, predvsem v zadnjih letih potrjuje, da je varnost v IoT zelo pomembna. V primerjavi z internetom je omrežje naprav IoT manj varno, saj majhnost in enostavnost naprav predstavlja številne ranljivosti, predvsem na področju odkrivanja gesel in napadov za zavrnitev storitev (angl. Denial Of Service, DOS) [26]. Za zagotovitev varnosti v IoT, mora biti ta izvedena na vseh nivojih, od fizičnih plasti do servisnih aplikacij [29]. Razvite in predstavljene so bile različne rešitve, a so spremembe na področju tako velikih omrežij vprašljive in selitev poteka počasi [16].

2.2 Tehnologija NFC

Tehnologija NFC [19] je brezžična visokofrekvenčna komunikacija kratkega dosega med dvema napravama NFC. Deluje v frekvenčnem pasu 13,56 MHz, kateri je bil najprej uporabljen v tehnologiji radiofrekvenčne identifikacije (angl. Radio-Frequency Identification, RFID). Čeprav tehnologija RFID omogoča komunikacijo na razdalji nekaj metrov, je tehnologija NFC omejena na nekaj centimetrov. Trenutno je integracija NFC v mobilne naprave zelo razširjena, saj jih imajo uporabniki vedno pri sebi. Tehnologija NFC vnaša posebnosti v razvoju brezkontaktnih pametnih kartic, a je še vedno združljiva z njimi. Zasnovana je na standardu mednarodne organizacije ISO 18092 (angl. International Organization for Standardization). Podpira obstoječe kartice in značke zasnovane na standardu ISO 14443, standardu Sony FeliCa in še druge kartice v tehnologiji NFC [31]. Na fizičnem nivoju omogoča dva načina delovanja in sicer:

- Pasivni način: inicialna naprava omogoča nosilno polje z frekvenco 13,56 MHz. Ciljna naprava odgovori z modulacijo obstoječega polja, pri čemer jo to polje tudi napaja. V tem načinu je omogočena kompatibilnost z obstoječimi karticami zasnovanimi na standardu ISO 14443

ali Sony FeliCa. Razdalje delovanja so do 10 cm, prenos podatkov pa je lahko 106, 212 ali 424 Kbit/s.

- Aktivni način: inicialna in ciljna naprava komunicirata z izmenjujočim generiranjem lastnega polja. V tem načinu potrebujeta obe napravi izvor napajanja. Razdalje v tem načinu so do 20 cm, hitrosti pa so lahko nad 1 Mbit/s. Za preprečevanje trkov podatkov naprava izključi lastno radio-frekvenčno polje, medtem ko čaka na podatke.

2.2.1 Uporaba

Trije glavni primeri uporabe so:

- Branje/Pisanje: v tem primeru bralnik NFC bere brez-kontaktne pametne kartice. Odvisno od tipa kartice se lahko uporabi zaznavanje več kartic. Bralnik NFC lahko bere ali pa spreminja podatke na kartici.
- Emulacija kartice: v tem načinu se bralnik NFC obnaša kot brez-kontaktna kartica. Glede na to, da se pametna kartica emulira, se lahko bralnik NFC uporabi za emulacijo različnih tipov kartic.
- P2P način: ta način delovanja je specifičen za tehnologijo NFC. Vzpostavi se obojestranska povezava za komunikacijo med dvema aktivnima napravama NFC.

Obstajajo številne rešitve in načini uporabe in sicer vstopnice, javni transport, mobilno plačevanje, pametni plakati, značke izdelkov in mnoge druge. Na področju zdravstva so že leta 2011 naredili raziskavo, v kateri so merili učinkovitost in delovanje srčnega spodbujevalnika [34]. Predstavili so metode senzorskega modula NFC, uporabo bralnika NFC, ter povezavo na oddaljeni strežnik in branje z mobilnim telefonom.

2.2.2 Varnost

Ker je tehnologija NFC splošno razširjena in je vgrajena v skoraj vsak mobilni telefon, je varnost pomembna za končnega uporabnika. Če pomislimo še to,

da vedno več naprav omogoča plačevanje z uporabo tehnologije NFC, je ta še bolj zanimiva za potencialne napadalce, saj lahko z izrabo ranljivosti kaj hitro pridobijo finančne koristi [19].

Ko govorimo o varnosti NFC, jo razdelimo na več različnih področij in sicer:

- varnost značk NFC,
- varnost pametnih kartic NFC,
- varnost bralnikov in ostalih naprav NFC,
- varnost komunikacije NFC.

Varnost značk NFC

Značke NFC (angl. NFC Tags) so pasivne značke za enkratno uporabo pri označevanju proizvodov, tiskanju vstopnic za predstave, smučarskih kart in podobno. Zaradi svoje enostavnosti in majhnosti je tudi manjši poudarek na varnosti. V začetku so značke uporabljale enostavne kriptografske algoritme, kateri so se z leti nadgrajevali. Pomembno je, da vedno uporabljamo novejše različice ali pa se pozanimamo o varnosti uporabljenih. Velik problem predstavlja tudi kloniranje značk, a novejše že imajo popravke na tem področju.

Varnost pametnih kartic NFC

Pametne kartice NFC so podobno kot značke NFC majhnih oblik in se ponavadi uporabljajo za plačevanje raznih storitev. Tem je posvečeno več varnostnih elementov in tudi vsaka kartica vsebuje namenski mikroprocesor, a vselej je pomembno, da se uporablja novejšo različico. Napadi so zahtevnejši in vsebujejo razhroščevanje mikroprocesorja ali pa poizkušajo z raznimi napadi stranskih kanalov tako, da opazuje kako so se karakteristike pametne kartice spremenile ob izmenjavi podatkov v komunikaciji NFC.

Varnost bralnikov NFC

Bralniki NFC vsebujejo kritične informacije, in velikokrat so le ti uničeni ali ukradeni, saj lahko napadalci iz njih pridobijo kriptografske ključe ali pa le te uporabijo za učenje o uporabljeni komunikaciji ali protokolih. Prav tako lahko napadalci bralnike NFC zamenjajo s svojimi in posnemajo legitimno uporabo. Pred uporabo se je dobro prepričati, da je ohišje bralnika NFC nepoškodovano. Pogosto uporabljamo tudi mobilno napravo, ki omogoča uporabo tehnologije NFC, zato je pomembno, da z njo ustrezno ravnamo in je ne izpostavljamo nepooblaščenim osebam. Izkoristijo lahko še neodkrite pomanjkljivosti v operacijskem sistemu in tako dostopajo do naše komunikacije NFC.

Varnost komunikacije NFC

Čeprav je razdalja pri komunikaciji z NFC omejena na nekaj centimetrov, nam to še ne zagotavlja varne komunikacije. Nekateri tipi napadov so bili opisani in predstavljeni že leta 2006 [24]. Napade delimo na več segmentov [19]:

- **Prisluškovanje (angl. Eavesdropping).** Nepooblaščena oseba preko anten prisluškuje komunikaciji med legitimnimi napravami. Zaradi narave brezžične komunikacije je ta napad med najresnejšimi grožnjami. Primer odprtokodne naprave, s katero je mogoče prisluškovati pasivnim in aktivnim komunikacijam NFC, je Proxmarkov instrument [14].

- **Spreminjanje podatkov (angl. Data modification).** Napadalec poizkuša spremeniti, ali izbrisati pomembne podatke, tako da prestreže komunikacijo med dvema napravama NFC in jih zamenja z drugimi ali sploh ne pošlje naprej.

- **Vnos podatkov (angl. Data insertion).** Napadalec poizkuša vnesti dodatne podatke v komunikacijo NFC. To je mogoče izvesti v primeru, ko prejemnik dolgo časa čaka na odgovor.

- **Napad s posrednikom (angl. Man-In-the-Middle Attack).** Napad zahteva prestrezanje komunikacije in spremembo le te, pri kateri legitimni uporabnik ne zasledi, da je prišlo do napada.

- **Napad med prenosom (angl. Relay Attack).** Kartice ISO 14443 so ranljive na napad med prenosom. En od primerov je predstavljen z napadom med prenosom podatkov tako, da sta uporabljeni dve namensko izdelani napravi NFC [23].

- **Napad s ponovitvijo (angl. Replay Attack).** V tem primeru je s prisluškovanjem zajet signal komunikacije in nato uporabljen za komuniciranje z naslednjim uporabnikom.

2.3 Hladna veriga

Na področju prehrane, zdravstva in farmacije se pogosto srečamo s hladno verigo. Potrošniki se vsakodnevno srečujemo z njo, zato jo lahko za področje živil predstavimo z naslednjo definicijo, ki je povzeta po nacionalnem inštitutu za javno zdravje [12]:

"Hladna veriga pomeni vzdrževanje predpisane, dovolj nizke temperature živila, da ohranimo varnost in čim boljšo kakovost živila v celotni živilski verigi; od proizvodnje, prevoza, shranjevanja in razdeljevanja do porabe pri končnem potrošniku.

V današnji, moderni družbi, sta zamrzovanje in hlajenje živil pogosto uporabljeni metodi konzerviranja hitro pokvarljivih živil. Proizvodnja zamrznjenih in hlajenih živil je ena izmed najhitreje rastočih panog v živilski industriji, med drugim tudi zaradi časovne stiske posameznika v vsakdanjem življenju. V dobi globalizacije nekatera živila potujejo preko celega planeta, preden pridejo do mize potrošnika.

Zahtevane temperaturne pogoje, ki jih na označbi navaja proizvajalec živil, je treba zagotavljati na vseh stopnjah živilsko-prehranske verige, v katero je kot zadnji člen vključen tudi potrošnik. Vzdrževanje dovolj nizke temperature

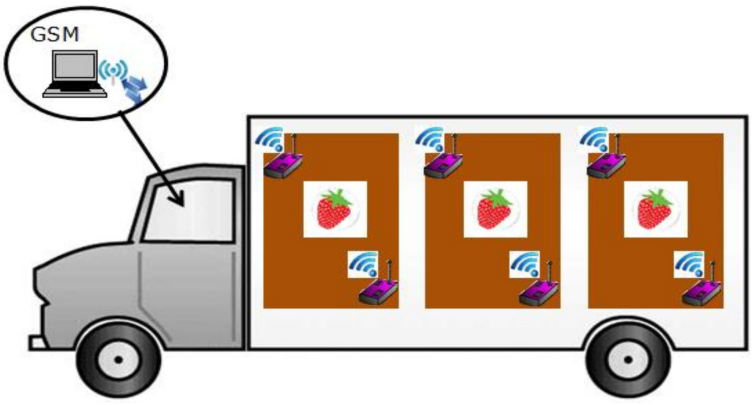
je ključni preventivni ukrep, ki preprečuje rast in preživetje mikroorganizmov v živilu in ki poleg varnosti zagotavlja tudi kakovost živila.

Odstopanje od zahtevanega temperaturnega režima lahko privede do okužb in zastrupitev z živili ter sproži proces kvarjenja živil."

Ker je vedno večja potreba po nadzoru živil preko oddaljenih centrov, se v hladni verigi uporabljajo namenska brezžična senzorska omrežja (angl. Wireless sensor network, WSN).

2.3.1 Primeri uporabe

Hladna veriga je zelo pomembna in se zelo pogosto uporablja v živilski industriji, ker se lahko temperatura okolja spreminja in predvsem v transportu precej razlikuje od predpisane [33]. Ena od rešitev je predstavljena v hladni verigi z brezžičnim senzorskim omrežjem in z uporabo tehnologije RFID v primerjavi z ZigBee [38]. Drug primer navaja rešitev z uporabo tehnologije Bluetooth, kjer razvijalci izdelajo lasten sistem z uporabo sistema Arduino in dodatnih senzorjev [41]. Slika 2.1 prikazuje izvedbo brezžičnega senzorskega sistema za nadzor hladne verige v transportu [32].



Slika 2.1: Primer uporabe sistema [32].

Uporaba naprednih tehnologij je v hladni verigi pomembna za varnost živil. Ocenjujejo, da bi npr. zmanjšanje količin odpadnih živil za 5% v Av-

straliji privedlo do prihranka milijarde dolarjev. Prav tako obstajajo analize, da bi pri nadzorovanem uravnavanju hlajenja živil omogočilo prihranke do 12 milijonov dolarjev [10]. Še dodatne temperaturne zahteve so specificirane v farmaciji in zdravstvu, saj morajo biti nekatera zdravila in cepiva hranjena v strogo določenem temperaturnem območju, v celotni verigi od proizvodnega procesa do končne uporabe [37].

2.3.2 Varnost podatkov v hladni verigi

Varnost je v hladni verigi pomembna zaradi nepooblaščenih dostopov do občutljivih senzorskih podatkov. Prav tako je pomembna zaščita in avtentičnost podatkov na vseh nivojih komunikacije [29]. Zato je potrebno podatke zaščititi že na nivoju zajema senzorskih meritev. Tako podatki lahko ohranijo svojo avtentičnost v naslednjih nivojih. Pomembno je zagotoviti zaščito nepooblaščenega dostopa ter onemogočanju storitve kot tudi ponarejanja podatkov.

Pri razvoju varnosti na tem področju prispeva že razvit protokol Safe-ATQ za varno komunikacijo v hladni verigi [30]. Specifikacija sicer ne določa kakšen kriptografski algoritem uporabimo, omogoča pa preverjanje integritete sporočila z uporabo zastarele zgoščevalne funkcije MD5. Za uporabo tega protokola bi bilo potrebno vključiti novejše pristope, lahko pa predstavlja izhodišče pri načrtovanju novih senzorskih sistemov.

Enega od primerov uporabe senzorskega sistema predstavlja rešitev z uporabo modula WebTag [21]. Sistem uporablja zaščito podatkov samo v smislu avtorizacije na vgrajenem spletnem strežniku modula. Varna uporaba WSN omrežij je predstavljena tudi na področju kmetijstva [17]. Opisana je uporaba zapletenega, a varnega načina avtorizacije uporabnikov in dostopa do podatkov različnih senzorjev. Rešitev je namenjena za specifično področje in zahtevnejšo infrastrukturo ter točno specificirano uporabo senzorjev.

2.4 Varnost podatkov

Varnost podatkov zagotovimo z uporabo varnega kanala za prenos podatkov, uporabo kriptografije in avtorizacije ter drugimi načini. Najbolje je, če uporabljamo kombinacijo le-teh. Za posamezne primere uporabe je smiselno izbrati različne stopnje varnosti in tudi če se zdi, da dodatna varnost ni potrebna, previdnost ni odveč. Najpogosteje je uporabljena zaščita z uporabniškim imenom in geslom, katera omogoči uporabnikom dostop do podatkov.

Ker obstajajo številni napadi na tehnologijo NFC in pri prenosu podatkov v internetno omrežje, je pomembna še dodatna zaščita z uporabo varne povezave, avtorizacije s pametnimi karticami in vključitvijo kriptografije.

2.4.1 Avtorizacija

Avtorizacija uporabnike loči po načinu dostopa do podatkov. V nekaterih primerih lahko brez avtorizacije preberemo vse podatke, le-teh pa ne smemo spreminjati. V našem primeru brez avtorizacije ni mogoče dostopati do podatkov oziroma le teh posredovati v spletni strežnik.

Doslej je bilo sredstvo avtorizacije navaden ključ vrat, sedaj pa mnogo pogosteje uporabljamo za avtorizacijo prav pametne kartice in ključe, kateri najpogosteje uporabljata tehnologijo NFC. Veliko je tudi govora o dvostopenjski avtorizaciji v kombinaciji z različnimi primeri uporabe [25]. Tudi v našem primeru smo za avtorizacijo uporabili pametno kartico NFC in obstoječ bralnik v sistemu.

2.4.2 Kriptografija

Kriptografija je veda o varni komunikaciji, kjer se osnovne podatke oziroma čistopis spremeni v tajnopis z različnimi kriptografskimi algoritmi. V osnovi poznamo štiri različne tipe [35, 39]:

- Klasična kriptografija - zamenjalne (pomične, afine, Vigenere, Hill...) in permutacijske šifre predstavljajo osnovne kriptografske pristope, ki

segajo daleč v zgodovino varne komunikacije in se uporabljajo tudi še danes.

- Simetrični kriptosistemi – npr. DES, 3DES in AES. Simetrični kriptosistemi uporabljajo enak ključ za šifriranje in dešifriranje. Imenujemo jih bločni kriptosistemi, ker operirajo nad bloki enakih velikosti. Poznamo pa tudi tokovne kriptosisteme, kateri operirajo nad biti z uporabo tokovnih ključev. Med njimi sta najbolj poznana RC4 in SEAL, sedaj pa se v večji meri uporabljata Salsa20 ter ChaCha.

- Asimetrični kriptosistemi – npr. RSA, ElGamal, DSA ter algoritmi, ki temeljijo na eliptičnih krivuljah. Uporabljajo različne ključe, tako imenovane zasebne in javne. Z uporabo teh kriptosistemov je omogočeno zagotavljanje zasebnosti in pristnosti digitalnih podatkov, saj se kombinacija zasebnih in javnih ključev uporabi za šifriranje in podpis poslanih podatkov.

- Zgoščevalne funkcije – družine funkcij SHA, BLAKE in RIPEMD. Uporabljajo se za preverjanje integritete sporočila v kombinaciji z drugimi kriptosistemi.

Uporaba kriptosistema je torej odvisna od uporabe in zahtev komunikacijskega kanala. V naslednjem poglavju je podrobno opisan algoritem AES, ker je uporabljen v magistrski nalogi.

Algoritem AES

Ameriški nacionalni inštitut za standarde in tehnologijo je leta 1997 objavil razpis za nov simetričen kriptosistem. Le tega je poimenoval Advanced Encryption Standard (AES) [11]. Med prispelimi rešitvami so izbrali algoritem Rijndael, ki je postal leta 2001 nov standard in je nadomestil kriptosistem DES. AES [20] je iterativna šifra, ki deluje nad bloki fiksne dolžine 128 bitov. Različne dolžine ključev pa omogočajo uporabo več kombinacij krogov (angl. cycles). Tako je potrebnih 10 krogov za 128-bitni, 12 krogov za 192-bitni in

14 krogov za 256-bitni ključ. Trenutno algoritem AES velja za varnega in se ga lahko uporabi tudi za avtentikacijo v sistemu RFID [22]. Tako kot vsi blokovni šifrirni algoritmi tudi AES podpira različne načine:

- `Electronic Codebook (ECB)` - Rezultat enakega čistopisa je vedno enak tajnopis AES, ne potrebuje inicializacijskega vektorja in je deterministično.
- `Cipher Block Chaining (CBC)` - Zahteva uporabo kriptografsko varnega naključnega števila (inicializacijskega vektorja), le ta se uporabi z operatorjem XOR na čistopisu in šifrira z AES. Naslednji blok uporabi tajnopis prejšnega bloka za operacijo XOR s čistopisom.
- `Propagating Cipher Block Chaining (PCBC)` - Operacije so podobne načinu CBC, le da v naslednjem koraku uporabi XOR čistopisa in tajnopisa prejšnega bloka.
- `Cipher Feedback (CFB)` - V prvem koraku se šifrira naključni inicializacijski vektor z AES, tajnopis pa dobimo tako, da rezultat AES z operatorjem XOR uporabimo na čistopisu. Naslednji blok uporabi tajnopis prejšnega bloka namesto inicializacijskega vektorja.
- `Output Feedback (OFB)` - Operacije so podobne načinu CFB, le da se v naslednjem koraku uporabi rezultat AES šifrirane operacije (pred XOR).
- `Counter (CTR)` - V prvem koraku se šifrira število katero se lahko uporabi samo enkrat (angl. Number Only Once, NOUNCE), ter števec z AES, tajnopis pa dobimo tako, da rezultat AES z operatorjem XOR uporabimo na čistopisu. Naslednji blok uporabi enak način, le da se števec poveča. Izmed vseh načinov je to edini poleg ECB, kateri se lahko paralelizira v šifriranju in dešifriranju ter omogoča naključni dostop do blokov. Ob vsakem novem bloku se števec poveča, na začetku je lahko 0 ali pa kakšno drugo število.

Slika 2.2 prikazuje rezultat šifriranja bitne slike (a) z načinom ECB (b) in ostalimi. V drugih načinih bi dobili sliko šuma (c), saj inicializacijski vektor ter naslednji koraki poskrbijo, da je v enaki barvi rezultat drugačen. Izbor načina je zelo pomemben, še posebno če se podatki podvajajo.

(a) Originalna slika **(b)** ECB način **(c)** CBC ali drugi načini

Slika 2.2: Primer šifriranja: (a) Originalna slika, (b) Šifriranje z ECB načinom, (c) Šifriranje s CBC in drugimi načini[1].

[1]Pridobljeno 4.5.2018 iz spletnega naslova: `https://twitter.com/CTZN5/status/885485617366396928`.

Varna povezava s spletnim strežnikom

Če hočemo dostopati do spletne strani, potrebujemo njen spletni naslov. Določen je s protokolom za prenos podatkov HTTP (angl. HyperText Transfer Protocol) ali pa HTTPS (angl. HyperText Transfer Protocol Secure). HTTP ni varen način povezovanja in podatki, ki se pošiljajo na spletno stran, se lahko prestrežejo. Tudi HTTPS v določenih primerih ni varen, saj se lahko deli strani še vedno posredujejo preko nezaščitenega kanala HTTP ali pa stran in njen certifikat ni med zaupanja vrednimi. O tem nas obvesti brskalnik, ko dostopamo, ali posredujemo podatke preko nezaščitenega kanala. HTTPS uporablja kriptografski protokol TLS (angl. Transport Layer Security). Za varnost in integriteto sporočil je poskrbljeno v samem protokolu, prav tako pa se uporabljajo javni in zasebni ključi za zagotavljanje identitete spletne strani. HTTPS način se smatra za varen način povezovanja in njegova uporaba hitro raste.

Poglavje 3

Zasnova in načrtovanje SS-NFC

Izdelava senzorskega sistema NFC (SS-NFC) je potekala vnaprej zastavljenih ciljih, ki so bili opredeljeni in so vključevali enostavno zasnovo in načrtovanje modularne rešitve za zajem meritev temperature, relativne vlage in svetlobe. Opisali smo tudi module, ki so bili uporabljeni za izdelavo in povezave med njimi tekom načrtovanja.

3.1 Ideja

Ideja o brezžičnem senzorskem sistemu ni nova in je bila uporabljena pred tehnologijo NFC. Z razvojem tehnologije NFC pa poleg prednosti obstajajo tudi pomanjkljivosti, saj so podatki na voljo vsakomur, ki ima fizični dostop do naprave. Odločili smo se za razvoj senzorskega sistema NFC in določili cilje, kateri bodo ohranili prvotni namen njegove uporabe in odpravili morebitne pomanjkljivosti, ki jih prinaša tehnologija NFC.

Primarni cilj magistrskega dela je razvoj in implementacija SS-NFC z brezžično povezavo v internetno omrežje. Zasnovan je kot samostojna naprava s senzorji temperature, vlage in svetlobe. Omogočal bo spremljanje in nadzor živil v hladni verigi. Vključeval bo različne načine delovanja, analizo in shranjevanje podatkov lokalno ali pa s sprotnim pošiljanjem na strežnik.

Pomemben prispevek predstavlja tudi zaščita podatkov in preprečevanje

dostopa nepooblaščenim osebam. Obstoječe rešitve običajno nimajo posebne zaščite v senzorskih modulih, ali pa je vključena samo v omejenem obsegu. V ta namen smo zasnovali ustrezno avtorizacijo uporabnika ter šifriranje podatkov.

3.2 Zahteve

Pred načrtovanjem SS-NFC smo definirali zahteve oziroma funkcionalnosti, ki se skladajo z idejno zasnovo in smo jih upoštevali tako v fazi načrtovanja in razvoja. Zahteve so naslednje:

- zajem senzorskih podatkov za potrebe hladne verige (temperatura, vlaga in svetloba),
- uporaba tehnologije NFC in brezžične komunikacije Wi-Fi,
- shranjevanje podatkov na strežnik, obdelava in prikaz v spletni aplikaciji,
- izvoz podatkov (datoteka .csv in slike grafov v datotekah .png, .jpg, .pdf ter .svg),
- uporaba več senzorskih modulov v sistemu,
- različni načini delovanja sistema:
  - 'On-line' – meritve se sproti pošiljajo na strežnik,
  - 'Off-line' – meritve se shranjujejo na modulu s senzorji,
  - zaznavanje nepričakovanih dogodkov,
  - obveščanje in predstavitev podatkov,
- avtorizacija uporabnikov,
- preprečevanje dostopa nepooblaščenim uporabnikom s šifriranjem podatkov,

- konfiguracijo sistema prek spletne strani (način delovanja, način zaščite, interval zajema) in
- cenovno ugoden sistem.

3.3 Načrtovanje SS-NFC

V povezavi s postavljenimi zahtevami za izvedbo SS-NFC potrebujemo naslednjo strojno in programsko opremo:

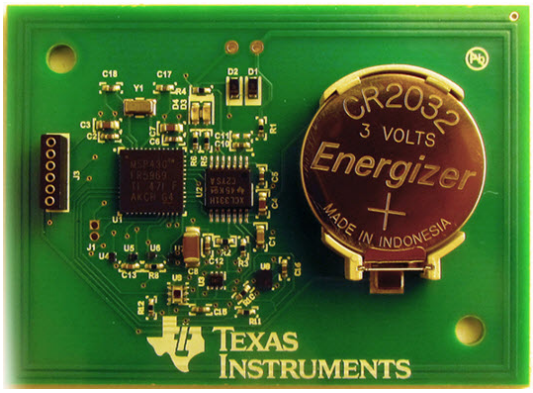
- mikrokrmilnik,
- podporo uporabi tehnologij NFC in Wi-Fi,
- modul NFC s senzorji temperature, vlage in svetlobe,
- spletni strežnik za shranjevanje in prikazovanje rezultatov meritev.

Najprej smo razmišljali o mikrokrmilniku Arduino, ker je zelo razširjen med manjšimi sistemi IoT. Za realizacijo celotnega sistema, bi morali dodati modul Wi-Fi, modul NFC in posamezne senzorje. Odločili smo se poiskati primernejšo rešitev, ker sistem Arduino ni bil najbolj primeren in cenovno najbolj ugoden, predvsem zaradi cene dodatnih modulov, kateri bi bili potrebni za realizacijo sistema.

Z zamenjavo mikrokrmilnika Arduino z NodeMCU, kateri je cenovno ugodnejši, smo zadostili osnovnim potrebam, saj le ta že vsebuje vgrajen modul Wi-Fi. Poleg mikrokrmilnika smo potrebovali še modul NFC, namenske senzorje pa smo nadomestili s senzorskim modulom TIDA-00524, kateri vsebuje tehnologijo NFC in podpira šifriranje podatkov. Z izbiro dodatnega senzorskega modula smo tako zagotovili, da lahko izvajamo več meritev hkrati, čeprav imamo na voljo samo en mikrokrmilnik. Izbrana rešitev je cenovno ugodnejša, poleg tega pa omogoča branje senzorskih podatkov tudi z mobilnim telefonom.

3.3.1 TIDA-00524

TIDA-00524 [9] je senzorski modul NFC, ki deluje kot naprava za shranjevanje senzorskih podatkov (angl. Multi-sensor Data Logger) z zelo nizko porabo energije proizvajalca Texas Instruments (slika 3.1).



Slika 3.1: TIDA-00524 [9].

Specifikacije:

- modul je manjši od velikosti kreditne kartice;
- življenjska doba baterije je 5 let;
- vsebuje 3 senzorje: temperatura (T), svetloba (E), vlaga (RH);
- komunikacija je skladna z NFC Forum 4 tipa B;
- 3 KB pomnilnika za shranjevanje sporočil NDEF;
- 64 KB pomnilnika za program in meritve, od tega je za meritve na voljo 46 KB pomnilnika;
- vsebuje vgrajen modul ure realnega časa (angl. real time clock, RTC);
- omogoča uporabo enega ali kombinacije več senzorjev;

- omogoča nastavljanje različnih parametrov preko protokola NFC;
- ob izgubi napetosti ohrani prejšnje vrednosti meritev, katere so shranjene v pomnilniku;
- uporablja mikrokrmilnik MSP430, kateri omogoča uporabo šifriranja AES;
- omogoča spreminjanje programa preko orodja MSP-FET [5].

Uporaba

Modul vsebuje osnovno različico programa, katero proizvajalec imenuje »DEMO Mode«. S stališča funkcionalnosti zadostuje potrebam zapisovanja in branja senzorskih podatkov. Za potrebe magistrskega dela bomo zasnovali nov program ter ga nadgradili z varnostjo podatkov ter drugimi funkcijami.

Za izpis podatkov potrebujemo bralnik NFC, kateri omogoča delovanje v skladu z zahtevami NFC Forum 4 tipa B. Najlažje je podatke prebrati z mobilnim telefonom in aplikacijo NFC Tools [7]. Slika 3.2 prikazuje osnovni izpis senzorskega sistema TIDA-00524, ter navodila za uporabo le tega. Zajem senzorskih podatkov je zapisan v prvi vrstici (datum in čas, T, E, RH). Če je od zadnjega brisanja podatkov preteklo več intervalov, je teh vrstic več, paziti je potrebno tudi na pravočasno brisanje, saj se same ne pobrišejo in modul samo dodaja vrstice od zgoraj navzdol. Začetek vrstice predstavlja datum in uro izvedbe meritve (če je ta pravilno nastavljen), naprej pa so predstavljene meritve izbranih senzorjev. Modul ima v pomnilniku shranjenih največ 1076 meritev, če uporabljamo vse tri senzorje. Pri različnih intervalih zajema lahko modul shrani podatke za več dni ali tednov. Tabela 3.1 prikazuje podatke o številu meritev in časovnem obdobju v številu dni, če so uporabljeni vsi trije senzorji ob različnih intervalih.

Konfiguriranje modula

Po prebranih navodilih vidimo, da je potrebno pred uporabo modul nastaviti. S tekstovnim izmenjevalnim formatom NFC (angl. NFC Data Exchange

```
[03/20/18 13:08]  26.9 C | 005 lx | 55% RH

TI's Datalogger Demo!

Default Settings:
    Mode: Temperature Only (F)
    Time: 12:00:00 AM
    Date: 01/01/15
    Polling Interval: 10 Minutes
    Default State: Stopped

Control Commands
    ST - Start
    SP - Stop
    CD - Clear Data
    RE - Reset

Config Commands
    TI hh:mm:ss - Set Time
    DA mm/dd/yy - Date
    PI xxx - Set Polling Interval (minutes)
    TM x - Temp Mode: 'F' or 'C'
    MO x - Set Mode (0-3)
        0: Temperature
        1: Temperature and Light
        2: Temperature and Humidity
        3: Temperature, Light, and Humidity
```

Slika 3.2: Primer izpisa TIDA-00524 v »DEMO Mode«.

Format, NDEF), nato pošljemo različne ukaze. Uporabljeni so:

- Kontrolni: začetek (`ST`) in konec (`SP`) zajema meritev, brisanje podatkov (`CD`) in ponastavitev modula na privzete nastavitve (`RE`).
- Konfiguracijski:
  - `TM C` ali `TM F`: nastavitev temperature v Celsius ali Fahrenheit.
  - `MO X`: sprememba načina pri uporabi razpoložljivih senzorjev.
  - `TI 14:00:00`: nastavi čas.
  - `DA 03/12/18`: nastavi datum.

Interval zajema (minuta)	Število meritev	Število dni
1	1076	0,75
10	1008	7
15	1056	11
30	1056	22
60	1056	44

Tabela 3.1: Časovna obdobja in število meritev senzorjev glede na dolžino intervala zajema.

– `PI 010`: nastavi interval zajema podatkov na 10 minut.

V primeru izgube stika ali izpraznjene baterije se v modulu TIDA-00254 shrani spodnje sporočilo. Ob zamenjavi baterije moramo čas ponovno nastaviti, ter po potrebi pobrisati podatke in ponovno poslati ukaz za začetek zajema podatkov `ST`.

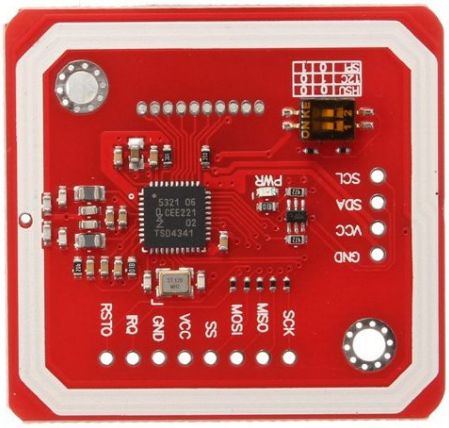
```
Power was interrupted!
Time and Date have been reset.
Current state:  Stopped
```

3.3.2 PN532 NFC Module V3

PN532 [13] je bralnik NFC, proizvajalca NXP semiconductors (slika 3.3). Omogoča povezovanje z različnimi napravami NFC, ter različne načine fiksno ožičene komunikacije. Ta modul smo v izvedbi sistema izbrali zato, ker ima podporo standarda ISO/IEC 14443B, katero potrebujemo za uspešno komunikacijo z modulom TIDA-00524.

Specifikacije:

- podpira branje, pisanje v standardih ISO/IEC 14443A, FeliCa, ISO/IEC 14443B;



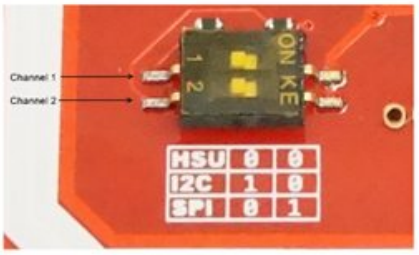
Slika 3.3: Modul NFC [13].

- podpira emulacijo kartic MIFARE Classic 1k in MIFARE Classic 4k / FeliCa;
- podpira komunikacijo ISO 18092, ECMA 340 Peer to Peer;
- podpira komunikacije kot so dvo žični protokol (angl. Inter-Integrated Circuit, I^2C), serijsko vodilo za V/I elemente (angl. Serial Peripheral Interface Bus, SPI) in serijsko povezavo z veliko hitrostjo (angl. High Speed UART, HSU);
- omogoča prenos podatkov NFC s hitrostjo do 424 bit/s;
- omogoča delovanje v napetostnem območju med 3,3 V in 5 V;
- manjši od velikosti kreditne kartice.

Konfiguriranje modula

Izbiro komunikacije je potrebno nastaviti s pomočjo dveh stikal prikazanih na sliki 3.4. V našem sistemu smo uporabili komunikacijo I^2C.

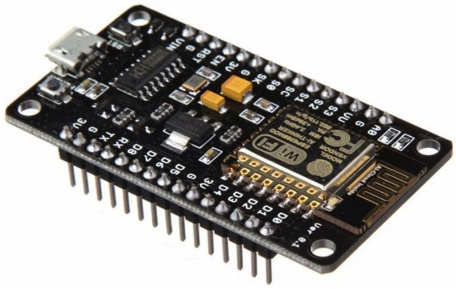
Prvo stikalo smo nastavili na »1«, drugega pa smo pustili na privzeti vrednosti »0«. Ob uporabi te različice komunikacije smo morali dodati dva »Pull Up« upora in sicer vrednosti 10 kΩ.



Slika 3.4: Stikalo bralnika NFC [13].

3.3.3 NodeMCU

NodeMCU [8] je razvojna ploščica IoT, katera je izpeljanka samostojnega modula Wi-Fi z uporabo mikrokrmilnika ESP8266 (slika 3.5). Ploščica že vsebuje podporo odjemalca Wi-Fi, prav tako pa je sedaj tudi kompatibilna z okoljem Arduino, tako da je lažji razvoj. Za potrebe magistrskega dela smo izbrali modul zaradi nizke cene, ter že vgrajene podpore Wi-Fi.



Slika 3.5: Modul NodeMCU [8].

Specifikacije:

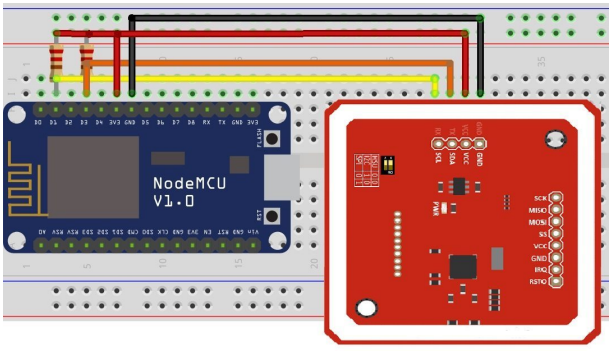
- mikrokrmilnik ESP8266, 80MHz;
- 128 kB bralno-pisalnega pomnilnika (angl, Random-access memory, RAM), 4MB bralnega pomnilnika (angl. Read-Only Memory, ROM);
- podpora Wi-Fi;

- 12 prostih vhodno izhodnih povezav (angl. general-purpose input/output, GPIO);
- podpora Arduino integriranega razvojnega okolja (angl. integrated development environment, IDE);
- napajanje 5V, micro univerzalno serijsko vodilo (angl, universal serial bus, USB) ali prek žične povezave;
- delovanje na 3,3V, prav tako vse povezave;
- 2 vgrajeni Led diodi;
- strojna podpora SPI.

3.3.4 Povezava in komunikacija modulov

Povezava modula NodeMCU z modulom NFC

Povezavo med NodeMCU ter modulom NFC smo najprej poizkušali izvesti s pomočjo povezave SPI, a nam ta ni delovala. Zato smo preverili delovanje z I^2C. Na začetku je bila povezava zelo nestabilna. S spremembo programske kode v knjižnicah ter dodanima dvema uporoma 10 kΩ se je povezava izkazala za stabilno. Slika 3.6 prikazuje žično povezavo NodeMCU z modulom NFC.



Slika 3.6: Žična povezava modula NodeMCU z modulom NFC [13].

Povezava modula NFC s TIDA-00524

Za vzpostavitev povezave NFC z modulom TIDA-00524 smo morali prenesti okolje Arduino IDE ter knjižnice za modul NFC. Knjižnice so izdelane za branje kartic in emulacijo NFC tipa A. Zato smo dodali različne metode in spremembe, da je NFC bralnik prebral kartice tipa B. Sprva smo morali definirati konstanto, katera je omogočala bralniku NFC zaznavanje kartic tipa B.

```
#define PN532_ISO14443B (0x03)
```

Le to smo uporabili v spremenjeni metodi `readPassiveTargetID`, katera je bila potrebna zaradi različnih prebranih parametrov ob zaznavanju modula TIDA-00524.

Komunikacija NFC forum 4 Ker različica NFC forum 4 za branje sporočil NDEF uporablja svoj standard in podpore tem karticam ni bilo, smo morali le tega posebej integrirati v Arduino okolje. V specifikaciji [6] so podrobno opisani ukazi in ustrezni postopki, katere smo potrebovali za branje sporočil NDEF. Za vse klice ukazov smo uporabili metodo `inDataExchange`, katera bralniku NFC sporoča, kateri ukaz bomo sporočili naprej. Ob vsakem ukazu nam bralnik sporoči ali je bil ukaz pravilno izveden s sporočilom 0x90 0x00, ter rezultatom pred tem sporočilom.

Pred vsakim branjem sporočila NDEF je potrebno izvesti določeno zaporedje ukazov:

1. `NDEF Tag Application select (00 A4 04 00 07 D2 76 00 00 85 01 01 00)` - izberi aplikacijo značke NDEF.

2. `Capability Container select (00 A4 00 0C 02 E1 03)` – v našem primeru ni obvezna.

3. `ReadBinary data from CC file (00 B0 00 00 0F)` – neobvezna.

4. `NDEF Select command (00 A4 00 0C 02 E1 04)` - izberi sporočilno datoteko NDEF (`E1 04`).

5. `NDEF ReadBinary (00 B0 00 00 02)` - preberi samo dolžino sporočila NDEF (2 bajta).

Preostanek sporočila NDEF nato preberemo z ukazom `NDEF ReadBinary`. Ker je lahko dolžina sporočila daljša od dolžine katero lahko preberemo z ukazom, le tega uporabimo večkrat in podamo odmik v datoteki. Vsako sporočilo ima na začetku, poleg dolžine še tip sporočila, jezik v katerem je sporočilo ter kontrolne bite. V našem primeru je zato prvi odmik do začetka sporočila 12 bajtov, tako da je naslednji ukaz `NDEF ReadBinary (00 B0 00 0C 14)`. Prva dva bajta (`0x00 0xB0`) v ukazu pomenita vrsto ukaza. Sledi odmik (`0x00 0x0C`) dolžine dveh bajtov, ter dolžina prebranega sporočila (`0x14`), kar je v našem primeru 20 bajtov.

Za sporočanje kontrolnih ali konfiguracijskih ukazov modula TIDA-00524 uporabimo ukaz `NDEF Update command`. Za pošiljanje ukazov moramo le tega pretvoriti v sporočilo NDEF, kar pomeni da za sporočilo 2 bajtov porabimo 9 bajtov dolgo sporočilo NDEF. Spodaj je naveden primer za pošiljanje ukaza za začetek zajema senzorskih podatkov (`ST`):

```
NDEF Update command (00 D6 00 00 09 C1 01 00 00 00 02 54 53 54)
```

Prva dva bajta (`0x00 0xD6`) v ukazu pomenita vrsto ukaza. Sledi dolžina celotnega sporočila (`0x00 0x00 0x09`) ki znaša 9 bajtov. Z nekaj odmika sledi dolžina notranjega sporočila (`0x02`), ki znaša 2 bajta. Nato sledi vrsta sporočila (`0x54`), katera pomeni da gre za tekstovno sporočilo. Na koncu je podan še zapis ukaza (`0x53 0x54`), kateri ustreza "ST", če uporabimo standardno ASCII tabelo.

Vzpostavljanje povezave z omrežjem Wi-Fi

Ker je povezljivost Wi-Fi že vgrajena v modul NodeMCU je povezovanje z omrežjem enostavno. V inicializaciji določimo, da se modul obnaša kot odjemalec, ter definiramo v katero omrežje naj se poveže in njegovo geslo.

```
WiFi.mode(WIFI_STA);
WiFiMulti.addAP("ime_SSID", "geslo");
```

Ko je vzpostavljena komunikacija z internetnim omrežjem preverimo ali se je modul uspešno povezal na Wi-Fi omrežje z:

```
If(WiFiMulti.run() != WL_CONNECTED)
```

Po morebitnem večkratnem preverjanju uporabimo zahtevo spletnega komunikacijskega protokola (HTTP), v kateri podamo spletni naslov, ter atribute v zahtevi POST, kateri se posredujejo na spletni strežnik:

```
HTTPClient http
http.begin(url_naslov);
int httpCode = http.POST(POST_s);
```

Le ta nam ob uspešnem, vrne kodo 200, ob neuspešnem pa kodo za komunikacijo HTTP (401 - neavtoriziran naslov, 404 - naslova ni mogoče najti, 500 - napaka spletnega strežnika ali drugi).

Poglavje 4

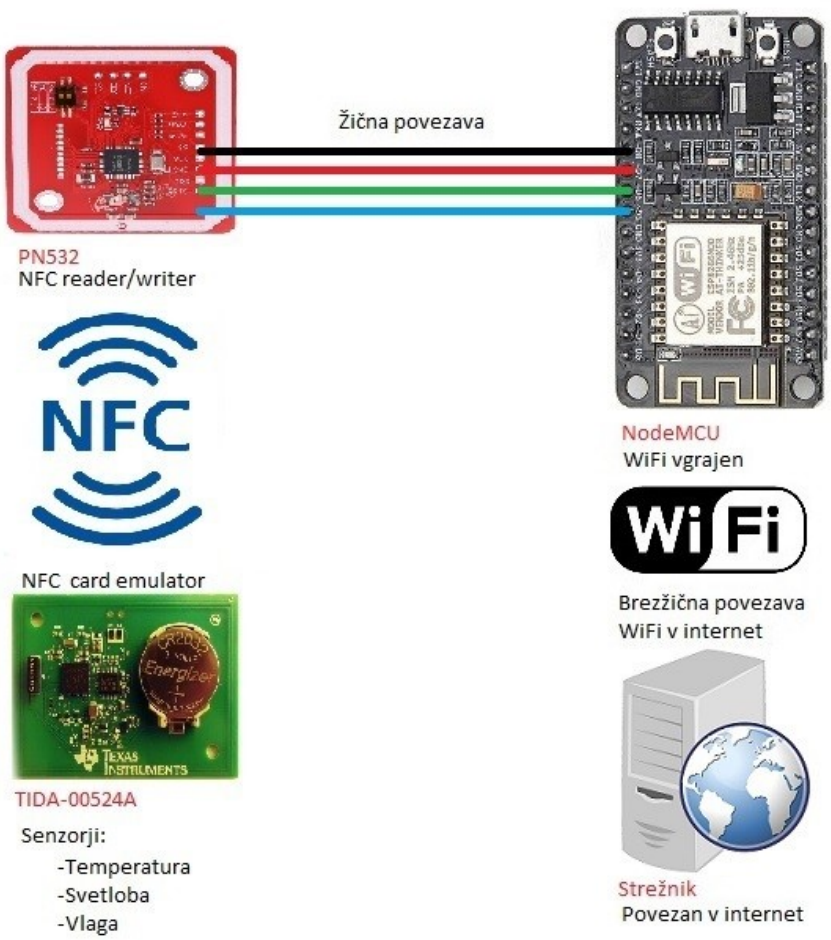
Razvoj SS-NFC

V poglavju o razvoju senzorskega sistema NFC smo najprej opisali arhitekturo sistema in podrobno delovanje spletnega strežnika. Spoznali smo se z okolji in orodji, ki smo jih potrebovali za razvoj SS-NFC ter predstavili prototip sistema.

4.1 Arhitektura

Med razvojem senzorskega sistema NFC so se nekatere funkcionalnosti dodajale in dopolnjevale. Slika 4.1 prikazuje arhitekturo SS-NFC s fiksnimi ali brezžičnimi povezavami elementov, ki so bili opisani v poglavju 3.

Prva različica sistema je vključevala branje modula TIDA-00524 in posredovanje podatkov v spletni strežnik. Naslednje variante programske kode so omogočale branje spremenjenih različic modula TIDA-00524 v povezavi s predstavljenimi funkcionalnostmi in uporabo kartice NFC za avtorizacijo uporabe modula TIDA-00524. Nato se je začel vzporedni razvoj različice brez šifriranja podatkov in različice s šifriranjem podatkov. Ko sta bili obe različici izpopolnjeni, smo izvedli migracijo v eno samo različico, katera je podpirala branje parametrov iz spletne strani. Spletno stran smo nadgradili in omogočili spreminjanje različnih načinov delovanja.



Slika 4.1: Arhitektura senzorskega sistema.

4.2 Spletni strežnik

Za spletni strežnik smo sprva uporabili namenski strežnik z operacijskim sistemom Ubuntu[1], ter spletnim strežnikom Apache[2]. Za podatkovno bazo

[1]Operacijski sistem Ubuntu, dostopen na `https://www.ubuntu.com/`.(pridobljeno 6.9.2018)

[2]Spletni strežnik Apache, dostopen na `https://httpd.apache.org/`.(pridobljeno 6.9.2018)

smo izbrali MySQL[3]. Spletna stran je izdelana v jeziku PHP, za prikazovanje grafov je uporabljen modul Highcharts[4]. Ker je konfiguracija omogočala samo povezave HTTP, smo programsko kodo PHP z enakimi funkcionalnostmi preselili na brezplačni strežnik s HTTPS podporo. Spletna stran je dosegljiva na naslovu `https://dc9932.000webhostapp.com/`.

4.2.1 Posredovanje podatkov v spletni strežnik

Za posredovanje senzorskih podatkov iz modulov je v programu uporabljena metoda POST, katera posreduje podatke na spletni strežnik. Sistem podpira povezave HTTP in HTTPS, a je sledeča varnejša zato uporabljamo povezavo s HTTPS.

Surovi podatki

Spletni naslov za posredovanje podatkov je enak spletnemu naslovu za prikaz podatkov, le da vsebuje še dodatno pot: `/api/put/measurement.php`, le ta pa zahteva več parametrov:

- `key` (parameter v katerem je posredovan javni ključ modula TIDA-00524 (namesto parametra Id));
- `temperature` (temperatura);
- `humidity` (vlaga);
- `light` (svetloba);
- `datetime` (datum in čas zadnje meritve v prvi vrstici);
- `pastS` (meritev je bila opravljena x sekund nazaj) (opcijsko).

[3]Strežnik podatkovne baze MySQL, dostopen na `https://www.mysql.com/`.(pridobljeno 6.9.2018)

[4]Modul Highcharts, dostopen na `https://www.highcharts.com/`..(pridobljeno 6.9.2018)

Primer posredovanih parametrov: `key`=hash&`temperature`=24.3 &`humidity`=38&`light`=022&`datetime`=3/20/18 13:28

Ob uspešnem vnosu v podatkovno bazo in prikazu na spletno stran strežnik vrne naslednji odgovor:

```
[HTTP(S)] POST...  code:  200
{status:"ok", "value":"0"}
```

Šifrirani podatki

V načinu s šifriranjem podatkov je naslov spremenjen, saj se posredujejo drugačni podatki. Naslov za posredovanje šifriranih podatkov je: `/api/put/measurementE.php`, le ta pa sprejme parametre:

- `key` (parameter v katerem je posredovan javni ključ modula TIDA-00524 (namesto parametra Id));
- `valuesE` (šifrirani podatki senzorjev);
- `datetimeE` (šifriran zadnji datum);
- `iveE` (inicializacijski vektor);
- `pastS` (meritev je bila opravljena x sekund nazaj) (opcijsko).

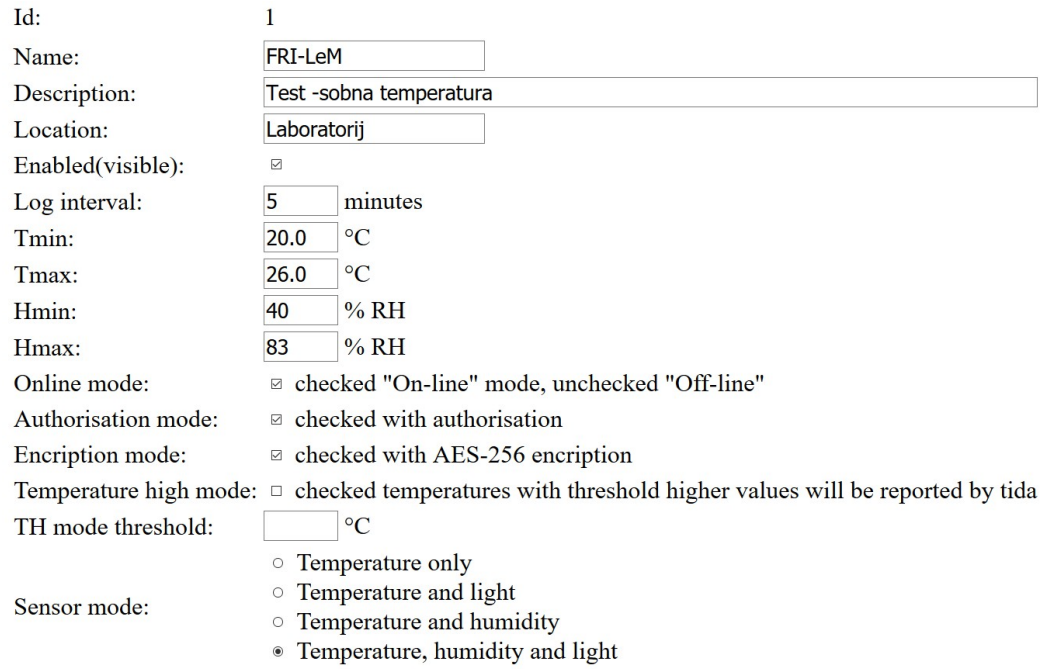
4.2.2 Nastavitve parametrov

Če se v spletno stran prijavimo z administratorskim računom, lahko spreminjamo določene parametre, urejamo obstoječe in dodajamo nove module TIDA-00524, shranjujemo datoteke CSV na strežnik, ter brišemo stare senzorske podatke iz podatkovne baze (slika 4.2).

Slika 4.3 prikazuje podstran, katera omogoča nastavljanje parametrov za posamezen modul TIDA-00524. Spreminjamo lahko ime, opis in lokacijo testa. Prikaz vrednosti v grafu lahko za določen modul TIDA-00524 skrijemo,

Slika 4.2: Prikaz vseh modulov TIDA-00524 v podatkovni bazi in njihovo urejanje.

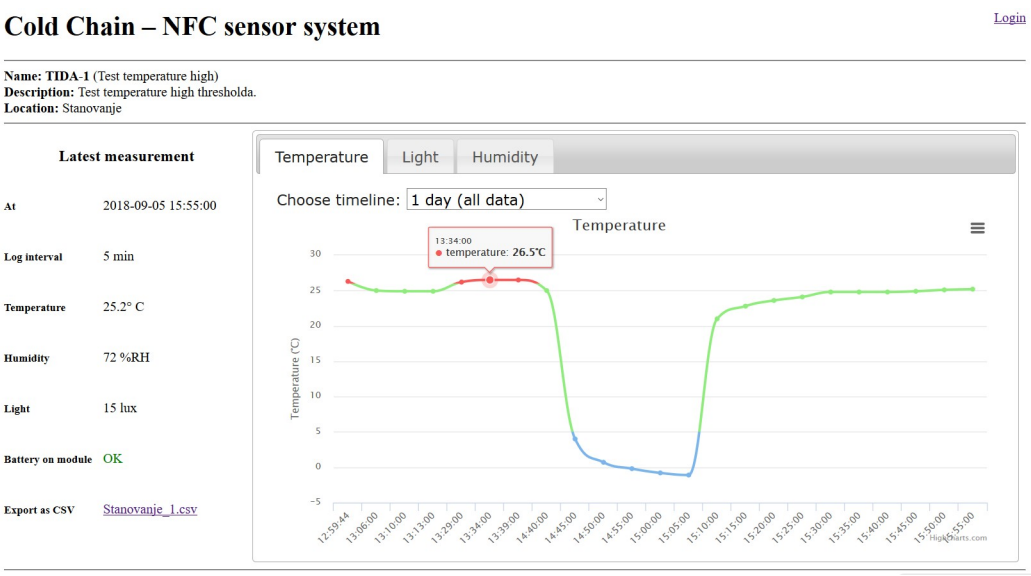
če ni označen parameter Enabled. Predvideno območje vrednosti za temperature nastavimo v poljih Tmin, Tmax, Hmin, Hmax. Kot parametre modula TIDA-00524 pa lahko nastavimo interval zajema podatkov, 'On-line' ali 'Off-line' način, način z avtorizacijo ter način s šifriranjem podatkov. Upravljamo lahko tudi s kombinacijo senzorjev in tako izberemo 4 različne načine zajema podatkov.



Slika 4.3: Nastavitev parametrov za modul Id = 1.

4.2.3 Prikaz podatkov

Na spletni strani so prikazani podatki o testu z nastavljenimi parametri, podatki o zadnji meritvi in grafom senzorskih podatkov za posamezen modul TIDA-00524. Omogočen je različen časovni prikaz podatkov in sicer za dan (vsi podatki), dan (povprečna vrednost na uro), teden (povprečna vrednost na uro), mesec (povprečna vrednost na dan), 3 mesece (povprečna vrednost na dan) ter leto (povprečna vrednost na teden). Prav tako vsak graf ločeno prikazuje meritve temperature, vlage in svetlobe. Vrednosti v predvidenem območju so prikazane z zeleno barvo, previsoke vrednosti so prikazane z rdečo barvo, prenizke pa z modro barvo. Slika 4.4 prikazuje izgled spletne strani z grafom enega modula.



Slika 4.4: Izgled spletne strani.

Spletna stran omogoča izvoz podatkov v datoteko. Shranjene vrednosti so ločene z vejico (angl. comma-separated values, CSV), da lahko podatke uporabimo v lastnih analizah in drugačnih predstavitvah. V levem spodnjem kotu (slika 4.4) s klikom podatke izvozimo v datoteko katera ima ime po lokaciji ter identifikaciji modula TIDA-00524. Ob koncu vsakega testa ali

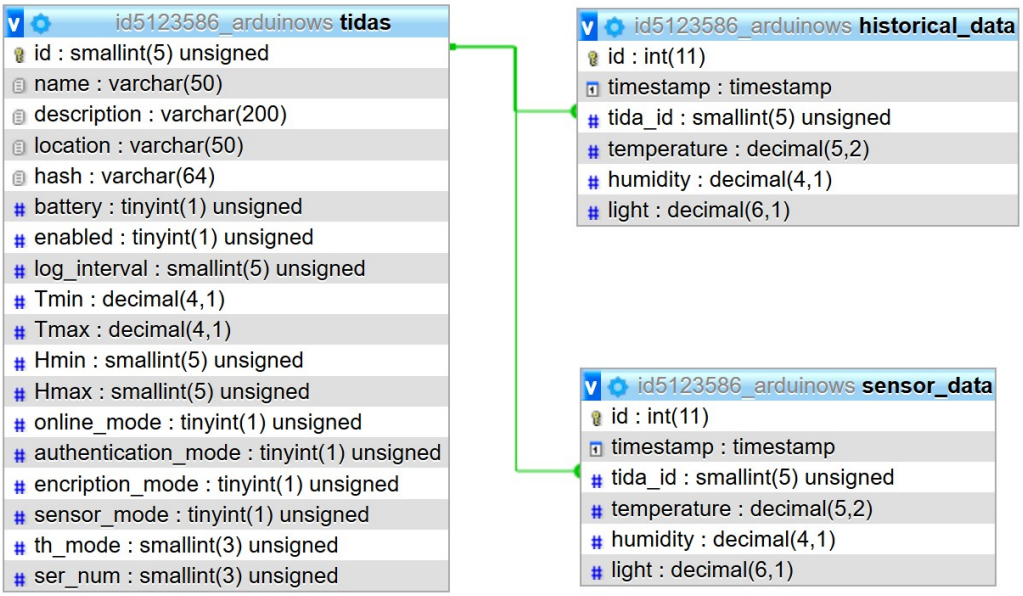
ob brisanju podatkov je priporočljivo podatke izvoziti ali pa jih shraniti na strežnik. Slika 4.5 prikazuje vsebino izvožene datoteke CSV.

```
#,Title,"Test luči v hladilniku"
#,Description,"Interval 1 minuta, bomo videli če zaznamo luč"
#,Location,Hladilnik
#,Dataloger,1
#,LogInterval(s),60
#,StartDate,2018-05-30,14:33:00
#,EndDate,2018-05-30,23:28:00
#,Measurements,536#
date,time,temperature,light,humidity
2018-05-30,14:33:00,26.80,29.0,64.0
2018-05-30,14:34:00,21.50,0.0,43.0
```

Slika 4.5: Primer vsebine datoteke CSV.

4.2.4 Podatkovna baza

Spletna stran uporablja enostavno podatkovno bazo za shranjevanje senzorskih meritev (slika 4.6). V tabeli `tidas` je shranjen trenuten opis testa, nastavitve modula TIDA-00524, mejne vrednosti temperature in vlage ter način zaščite podatkov. V drugih dveh pa so shranjeni senzorski podatki. Ko senzorske podatke odstranimo z administratorskim računom, se ti le premaknejo iz tabele `sensor_data` v drugo tabelo `historical_data`, tako da so še vedno na voljo, če jih slučajno potrebujemo in po potrebi izvozimo v datoteko CSV.



Slika 4.6: Struktura podatkovne baze spletne strani.

4.3 Razvojna okolja in orodja

4.3.1 Arduino IDE

Arduino IDE [1] je odprtokodno razvojno okolje primarno namenjeno za razvojne plošče Arduino. Zaradi modularnosti in odprtega dostopa so podprte tudi druge plošče in moduli. Orodje je napisano v Javi in podpira operacijske sisteme Windows, Linux ter MacOS. Izvira iz okolij Processing in Wiring, ter podpira programiranje v programskem jeziku C in C++. Projekti so imenovani skice in vsak projekt vsebuje vsaj funkciji setup() in loop(). Okolje smo uporabili za programiranje modula NodeMCU.

4.3.2 Code Composer Studio

Code composer studio [2] je primarno razvojno okolje za mikroprocesorje podjetja Texas Instruments. Trenutna različica 8.0 podpira operacijske sisteme Windows, Linux x64 ter MacOS. Osnova orodja je odprtokodno orodje

Eclipse, katero je spremenjeno in ustreza zahtevam mikroprocesorjev. Omogoča tudi razhroščevanje JTAG ali 'Spy-Bi-Wire' s pomočjo lastnih namenskih razhroščevalnikov. Okolje smo uporabili za programiranje modula TIDA-00524.

4.3.3 Adobe Dreamweaver

Adobe Dreamweaver [3] je plačljiv program za razvoj spletnih strani in podpira različne spletne tehnologije in operacijska sistema Windows ter MacOS. Dreamweaver uporabnikom omogoča predogled spletne strani v lokalno nameščenih spletnih brskalnikih. Tako kot drugi programi za urejanje kode HTML ureja datoteke na lokalni ravni, nato pa jih naloži/posodobi na oddaljenem spletnem strežniku z uporabo protokolov FTP, SFTP, ali WebDAV. Trenutna različica 18.1 podpira razvoj na več zaslonih, ter omogoča Subversion (SVN), in git sistem za nadzor različic. Program smo uporabili za razvoj spletne strani.

4.3.4 MSP-FET

MSP-FET [5] je namensko orodje za prenos programa v mikrokrmilnike tipa MSP430. Preko 14 žičnega konektorja omogoča prenos preko standardnega JTAG vmesnika ali pa protokola 'Spy-Bi-Wire'. V računalnik se priklopi prek USB vodila in podpira Code composer studio, IAR Embedded Workbench ter GCC - Open Source Compiler for MSP Microcontrollers razvojna okolja za prenos programa. V tej nalogi smo uporabili starejšo različico orodja in sicer MSP-FET430UIF[5].

[5]Orodje za programiranje in razhroščevanje sistemov MSP430, dostopno na `http://www.ti.com/tool/MSP-FET430UIF` (pridobljeno 6.9.2018)

4.4 Prototip SS-NFC

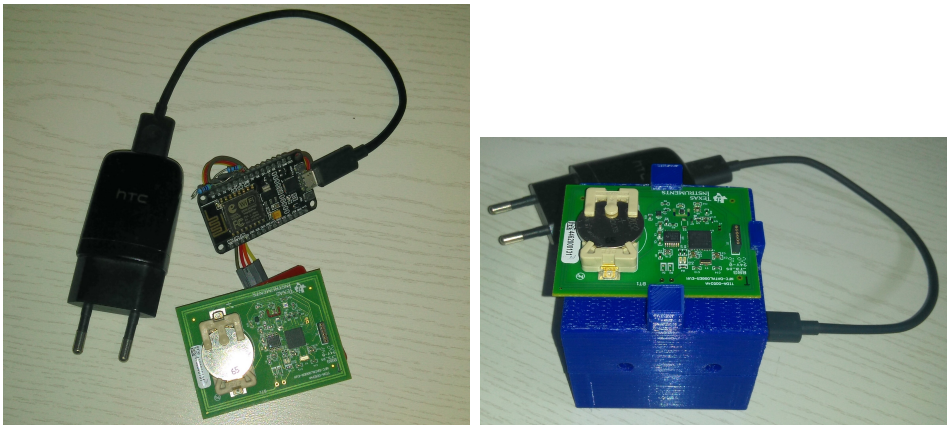
Za izdelavo prototipa senzorskega sistema NFC smo imeli 49,2 EUR stroškov[6]. Tabela 4.1 prikazuje posamezne stroške prototipa SS-NFC.

Modul/ Material	**Cena (EUR)**
TIDA-00524	25
NodeMCU	11
PN532 NFC Module V3 in 2-krat MIFARE Classic	13
2-krat Upor 10 kΩ	0,2

Tabela 4.1: Stroški prototipa SS-NFC.

Za SS-NFC smo se odločili izdelati namensko ohišje, da bi bila uporaba lažja in bolj estetska. Zaradi dostopnosti storitve tiskanja v 3D, smo se odločili izdelati načrt, ter ohišje natisnili. V načrtu smo predvideli morebitno segrevanje bralnika NFC in NodeMCU. Ohišje smo oblikovali tako, da zrak kroži in minimalno ali skoraj nič ne vpliva na meritve senzorskega modula TIDA-00524, katerega smo namestili na vrh ohišja, tako da je izpostavljen direktni svetlobi ter posledično realni temperaturi in vlagi. Načrt vsebuje dva dela in sicer zgornji in spodnji del, ki sta shranjena v datoteki stl. Prototip SS-NFC je prikazan na sliki 4.7 a) brez ohišja in na sliki 4.7 b) z ohišjem.

[6]Cene so bile pridobljene 7.9.2018 v spletnih trgovinah `www.ti.com/tool/TIDA-00524`, `https://www.arissi.eu/` in `https://www.conrad.si` in ne vključujejo morebitnih stroškov dostave.



(a) Brez namenskega ohišja **(b)** Z namenskim ohišjem

Slika 4.7: Prototip senzorskega sistema NFC.

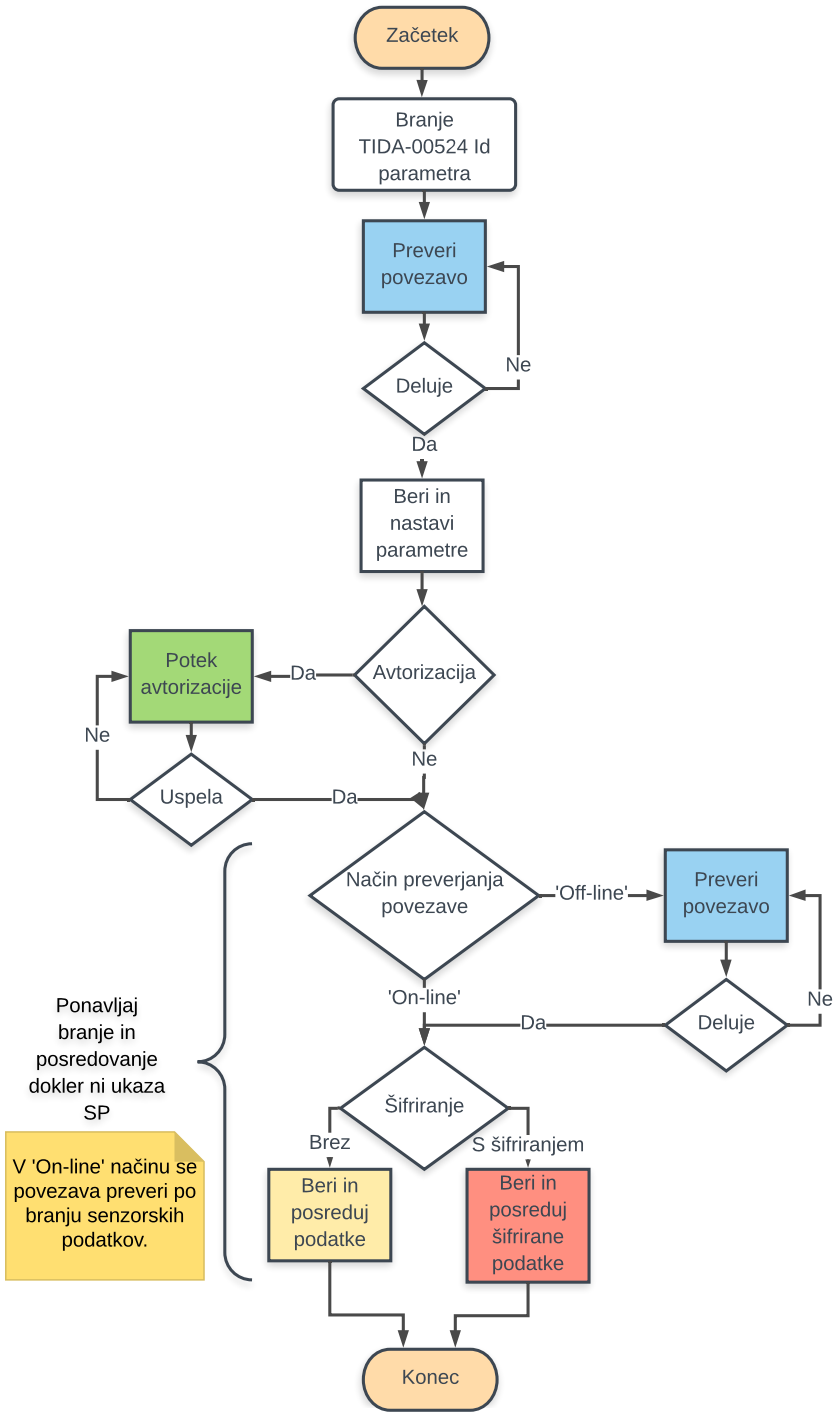
Poglavje 5

Delovanje SS-NFC

Senzorski sistem-NFC (SS-NFC) omogoča več različnih načinov delovanja, odvisno od dostopnosti povezave Wi-Fi ter načina zaščite podatkov in avtorizacije uporabnika. Načini delovanja so 'On-line' in 'Off-line' način, način z avtorizacijo, način brez in s šifriranjem podatkov ter način z branjem vrednosti odstopanj. Lahko so uporabljeni posamezno ali pa se dopolnjujejo, na primer lahko uporabimo na enem modulu TIDA-00524 način z avtorizacijo in šifriranjem podatkov v 'Off-line' načinu delovanja. Način delovanja se prebere iz spletne strani po pridobitvi parametra Id modula TIDA-00524. Prav tako se načini delovanja znova preberejo, ko sistem zazna drugačen parameter Id. Postopek izbire delovanja sistema je prikazan na sliki 5.1.

SS-NFC omogoča zaznavanje prazne baterije na modulu TIDA-00524, saj smo po nekaj izpraznjenih baterijah ugotovili kako se ob prazni bateriji prekine komunikacija. Zato smo v programu dodali obveščanje na določenemu modulu tako, da se ob zaznavi prazne baterije v serijsko konzolo Arduino izpiše prikazano sporočilo ter podatek posreduje v spletni strežnik.

```
Tag B present
Retry older tag(Battery low)
[HTTP(S)] POST...  code:  200
{status:"ok", "value":"0"}
```



Slika 5.1: Delovanje SS-NFC po priključitvi na električno napajanje, kateremu sledi preverjanje povezave z nastavljenim omrežjem Wi-Fi, branje parametrov in izbira načina delovanja.

SS-NFC omogoča zaznavanje sporočil »Power was interrupted!« ter »Memory full!« in ob zaznavi le te preskoči in prebere podatke kateri sledijo. Ugotovil bo tudi napačno nastavitev datuma in časa na modulu TIDA-00524. V takem primeru bo s pomočjo prebranih podatkov spletnega strežnika nato le tega pravilno nastavil. Primer sporočila, ki se izpiše v serijsko konzolo Arduino ob popravljanju časa na modulu TIDA-00524, je podan v naslednji obliki.

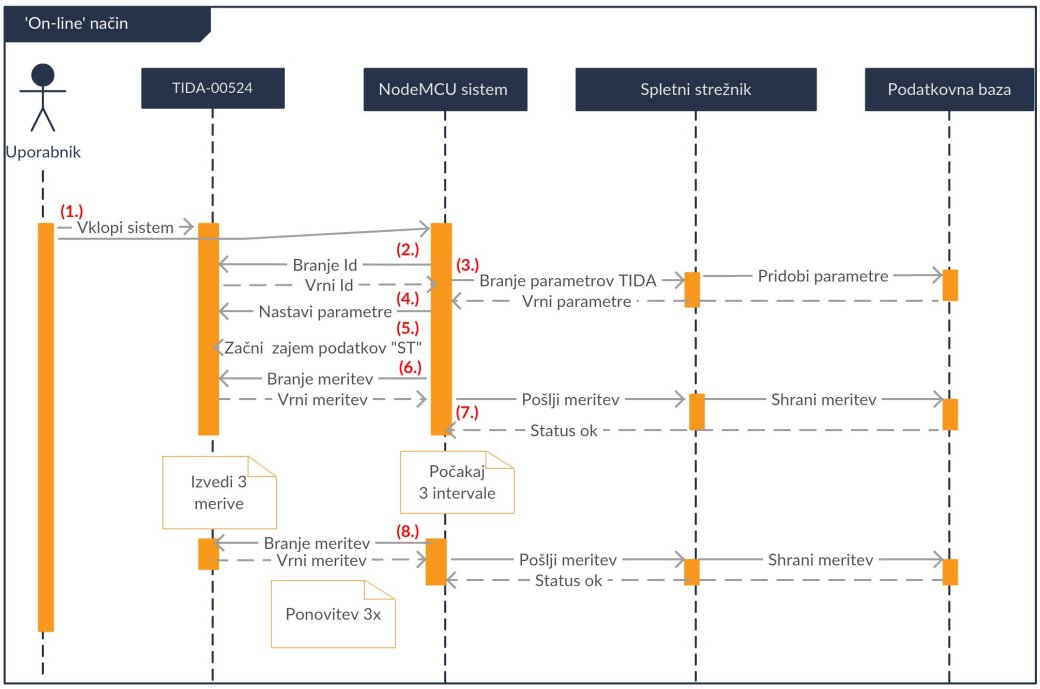
```
[HTTP(S)] POST...  code:  200
{Correct Timestamp:"05-29-18 14:38"}
Corrected time on TIDA!
```

Za lažje spremljanje stanja sistema je na modulu NodeMCU omogočena luč LED, katera utripne ob vsakem novem koraku povezave NFC, vzpostavljanju povezave Wi-Fi, ter povezovanju na spletno stran. Ob avtorizaciji utripata izmenično dve luči LED, ko pa NodeMCU prebere senzorske podatke in je v čakanju na naslednji senzorski interval, se luč LED ugasne. V primeru težave zaznavanja bralnika NFC luč LED utripa z višjo hitrostjo.

5.1 'On-line' način

'On-line' način delovanja sistema se uporabi takrat, ko imamo povezavo Wi-Fi vedno omogočeno. Modul NodeMCU prebere vse senzorske podatke, ter le te posreduje v spletni strežnik. V primeru, da po branju modula TIDA-00525 le ta ne vsebuje senzorskih podatkov, pošlje ukaz »ST« (začni zajemanje podatkov). Ob uspešnem vnosu na spletni strežnik, se v modulu NodeMCU nastavi zamik za trikratnik intervala senzorskega modula. Na ta način nam ni potrebno vedno spremljati kdaj bo nov podatek na voljo in ob naslednjem branju modula NodeMCU istočasno prebere 3 podatke naenkrat. Po uspešnem branju ter vnosu na spletni strežnik pošlje ukaz »CD«, da se pobrišejo prebrani podatki in se sprosti prostor na modulu TIDA-00524. Če povezava Wi-Fi zaradi prekinitve ni na voljo, je možnih več poizkusov

vzpostavitve povezave Wi-Fi, tako da ob morebitni neuspeli povezavi in že prebranem podatku, le tega ne izgubimo in zavržemo. Če po več poskusih povezava še vedno ni na voljo, se nastavi zamik za interval zajema podatkov in se podatek prebere znova. Slika 5.2 prikazuje 'On-line' način delovanja.



Slika 5.2: 'On-line' način delovanja SS-NFC.

1. Vklop sistema (modul TIDA-00524, modul NodeMCU).
2. Branje parametra Id na modulu TIDA-00524.
3. Preverjanje povezave in branje parametrov na spletnem strežniku.
4. Nastavljanje parametrov na NodeMCU in modulu TIDA-00524.
5. Začni z zajemom podatkov (Pošlji ukaz ST modulu TIDA-00524).
6. Preberi prvo meritev in jo posreduj v podatkovno bazo.
7. Podatek je pravilno shranjen, počakaj 3 intervale meritev.

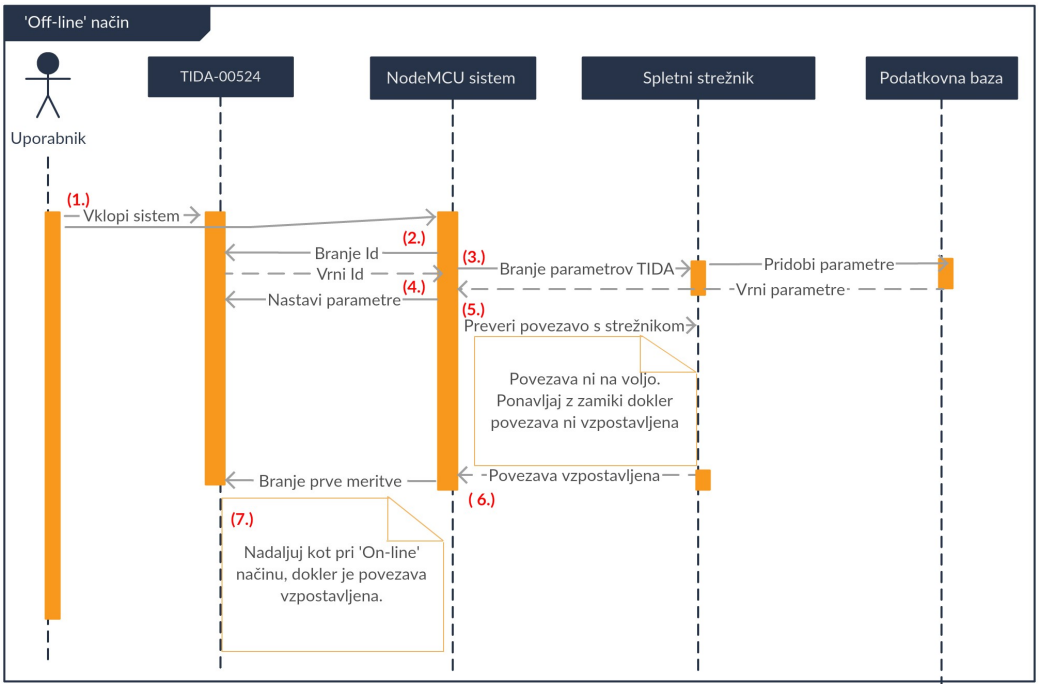
8. Preberi 3 meritve ter pošlji strežniku za shranjevanje v podatkovno bazo. Ponavljaj ta korak do izklopa sistema.

5.2 'Off-line' način

'Off-line' način bere modul TIDA-00524 na enak način, le da po prejetih parametrih najprej preveri ali je brezžično omrežje na voljo. Spodnje sporočilo v serijski konzoli Arduino prikazuje primer, ko brezžično omrežje ni na voljo, modul NodeMCU ne opravi nobenega branja ter tako prihrani nepotrebno komunikacijo z modulom TIDA-00524. Preverjanje o dosegljivosti omrežja se na začetku preverja na 5 sekund, kasneje pa se čas preverjanja podaljša. Medtem lahko TIDA-00524 shranjuje senzorske podatke v svoj pomnilnik. Ko je brezžično omrežje Wi-Fi na voljo, začne z branjem ter posredovanjem podatkov. Slika 5.3 prikazuje 'Off-line' način delovanja.

```
Wifi not connected, no reading.
Delay for 5000 msec.
```

1. Vklop sistema (modul TIDA-00524, modul NodeMCU).
2. Branje parametra Id na modulu TIDA-00524.
3. Preverjanje povezave in branje parametrov na spletnem strežniku.
4. Nastavljanje parametrov na NodeMCU in modulu TIDA-00524.
5. Preveri povezavo s spletnim strežnikom.
6. Povezava je vzpostavljena. Preberi prvo meritev.
7. Nadaljuj kot pri 'On-line' načinu delovanja.



Slika 5.3: 'Off-line' način delovanja SS-NFC.

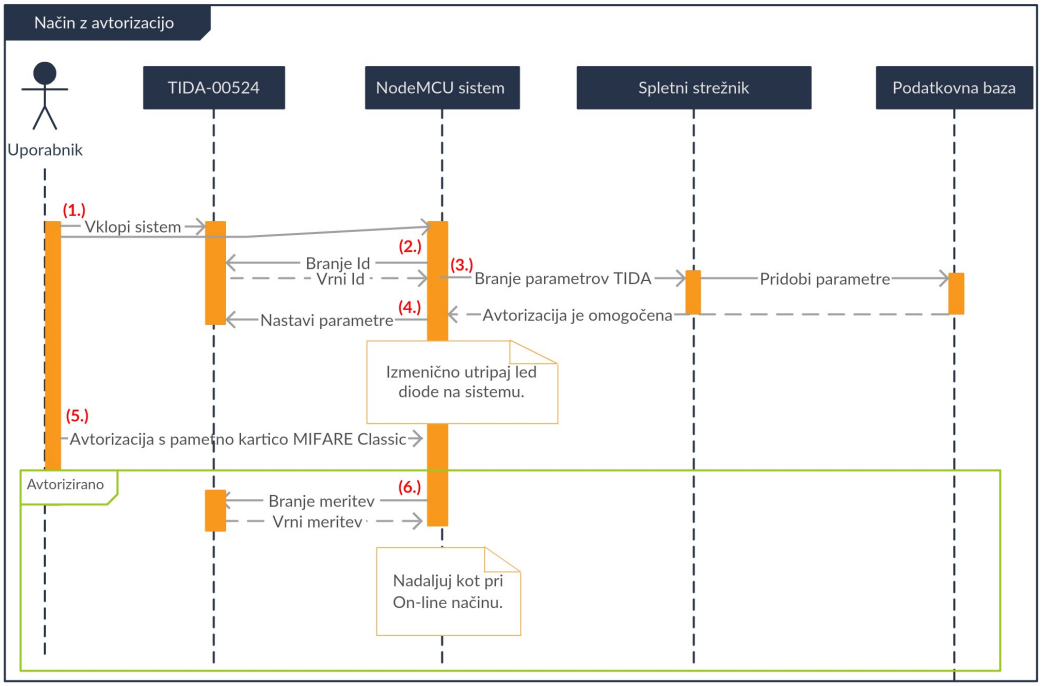
5.3 Način z avtorizacijo

Na sistemu je omogočena avtorizacija s pametno kartico MIFARE Classic [4]. Če je na modulu NodeMCU omogočena avtorizacija, se branje modula TIDA-00524 začne po uspešni avtorizaciji. Na kartici je zapisan tudi parameter Id modula TIDA-00524 tako, da je ta način mogoče uporabiti tudi za branje več modulov hkrati. Spodnje sporočilo v serijski konzoli Arduino prikazuje primer uspešno avtoriziranega uporabnika ter nato branje podatkov.

```
Authorisation neeeded, put your Id card next to NFC reader!
Reading api key....
Authorisation succeeded!  Delay for 5000 msec.

Scan a TIDA00524
```

Slika 5.4 prikazuje način z avtorizacijo.



Slika 5.4: Delovanje SS-NFC v načinu z avtorizacijo.

1. Vklop sistema (modul TIDA-00524, modul NodeMCU).
2. Branje parametra Id na modulu TIDA-00524.
3. Preverjanje povezave in branje parametrov na spletnem strežniku.
4. Nastavljanje parametrov na NodeMCU in modulu TIDA-00524 (Avtorizacija je omogočena).
5. Ponavljaj preverjanje dokler uporabnik ni avtoriziran. Čakaj na prebrano vsebino pametne kartice. Ko je vsebina potrjena, nadaljuj s postopkom.
6. Preberi prvo meritev in jo vstavi v podatkovno bazo. Nato nadaljuj kot pri 'On-line' načinu.

5.4 Način brez šifriranja

Način brez šifriranja podatkov je privzet način komunikacije z modulom NodeMCU. Način komunikacije je podoben že privzetemu načinu TIDA-00524, le da smo izpustili nekatere znake, ter omogočili izpis vedno enake dolžine. Na tak način smo prihranili približno 15% prostora za dodatne meritve. Primer izpisa podatkov v načinu brez šifriranja podatkov.

(blok0) `[06/10/18 11:05]025.0C|00057lx|52%RH` (37 bajtov),
(blok1) `[06/10/18 10:55]024.0C|00254lx|46%RH` (37 bajtov).

5.5 Način s šifriranjem

Šifriranje podatkov izvajamo na modulu TIDA-00524, saj so le tako podatki zaščiteni pred raznimi napadi NFC. Uporabljamo koprocesor AES, kateri potrebuje za šifriranje bloka dolžne 16 bajtov 167 procesorskih ciklov. Za dolžino smo izbrali 256 bitni ključ, podatke pa smo skrajšali tako, da je v enem bloku čas meritve, v drugem pa meritev. Ker so podatki šifrirani, ter brez ključa neberljivi, smo spremenili program TIDA-00524. Izpis vključuje samo zadnji datum meritve, ostali pa so pozneje s pomočjo NodeMCU in spletnega strežnika izračunani iz odmika meritev. Tako prihranimo na prostoru in lahko dodatno shranimo še približno 50% več meritev. Tabela 5.1 prikazuje zapis treh meritev pred šifriranjem podatkov.

Blok	Vsebina	Dolžina	Pomen
0	`[06/10/18 10:55]`	16 bajtov	Datum zadnje meritve.
1	`024.0C00254lx46%`	16 bajtov	Meritev 1, T = 24 °C.
2	`024.3C0003211x50%`	16 bajtov	Meritev 2, T = 24,3 °C.
3	`024.2C0002211x51%`	16 bajtov	Meritev 3, T = 24,2 °C.

Tabela 5.1: Čistopis treh meritev v načinu s šifriranjem.

Modul NodeMCU s pomočjo bralnika NFC prebere šifrirane bloke, ter jih posreduje na spletni strežnik. Le te dodatno kodira z algoritmom Base64 [27], ker je to enostaven prenos binarnih podatkov na spletni strežnik. Prav tako smo Base64 spremenili v algoritem base64url, saj so se nekateri znaki še vedno nepravilno prenesli. Dekodiranje iz Base64 ter nato dešifriranje AES se izvede na spletnem strežniku. Prav tako se tam podatki interpretirajo v meritve temperature, vlage in svetlobe.

Šifriranje podatkov

Ključ dolžine 256 bitov se generira s pomočjo psevdogeneratorja števil na modulu TIDA-00524 ob zajemu vsake meritve. Tako ključ ni nikjer shranjen in ga je posledično težje odkriti s branjem RAM/ROM modula. Ključ se razlikuje na vsakem modulu TIDA-00524 in je odvisen od parametra Id ter serijske številke modula TIDA-00524. Enak psevdogenerator števil se uporabi na spletnem strežniku za generiranje ključa ob dešifriranju sporočila. Psevdokoda generiranja ključa je naslednja:

Algorithm 1 Psevdokoda generiranja ključa

```
1: i ←0
2: Id ←getTIDA00524Id()
3: Serial ←getTIDA00524Serial()
4: seed2(Id XOR Serial) {inicializiraj seme}
5: repeat
6:     kljuc[i] ← random2() {naključno število}
7:     i ← i + 1
8: until i ≥ dolzina_kljuca
```

Modul TIDA-00524 podpira štiri različne načine šifriranja:

- `ECB` - register AESACTL0 nastavimo na konstanto AESCM__ECB,
- `CBC` - register AESACTL0 nastavimo na konstanto AESCM__CBC,
- `CFB` - register AESACTL0 nastavimo na konstanto AESCM__CFB,

- `OFB` - register AESACTL0 nastavimo na konstanto AESCM__OFB.

Izbrali smo način `OFB`, saj je izmed zgoraj omenjenih najbolj primeren, še posebej kadar hočemo ohraniti majhen prenos podatkov med moduli. Način `ECB` nam ne ustreza, saj je deterministično, podatki se velikokrat ponavljajo in bi to lahko privedlo do odkritja podatkov s testiranjem v enakem laboratorijskem okolju. Pri načinu `CBC` bi bilo potrebno poleg vsake meritve pošiljati še unikaten in predvsem nepredvidljiv inicializacijski vektor.

Ker modul TIDA-00524 ne podpira načina `CTR` in smo želeli uporabiti inicializacijski vektor ter števec zaradi velikosti podatkov, smo to dosegli tako da v vsakem bloku podatkov definiramo drugi števec. Tako se način `OFB` ali `CFB` obnaša tako kot `CTR` in lahko namesto celotnega inicializacijskega vektorja uporabimo skrajšanega skupaj s števcem [35].

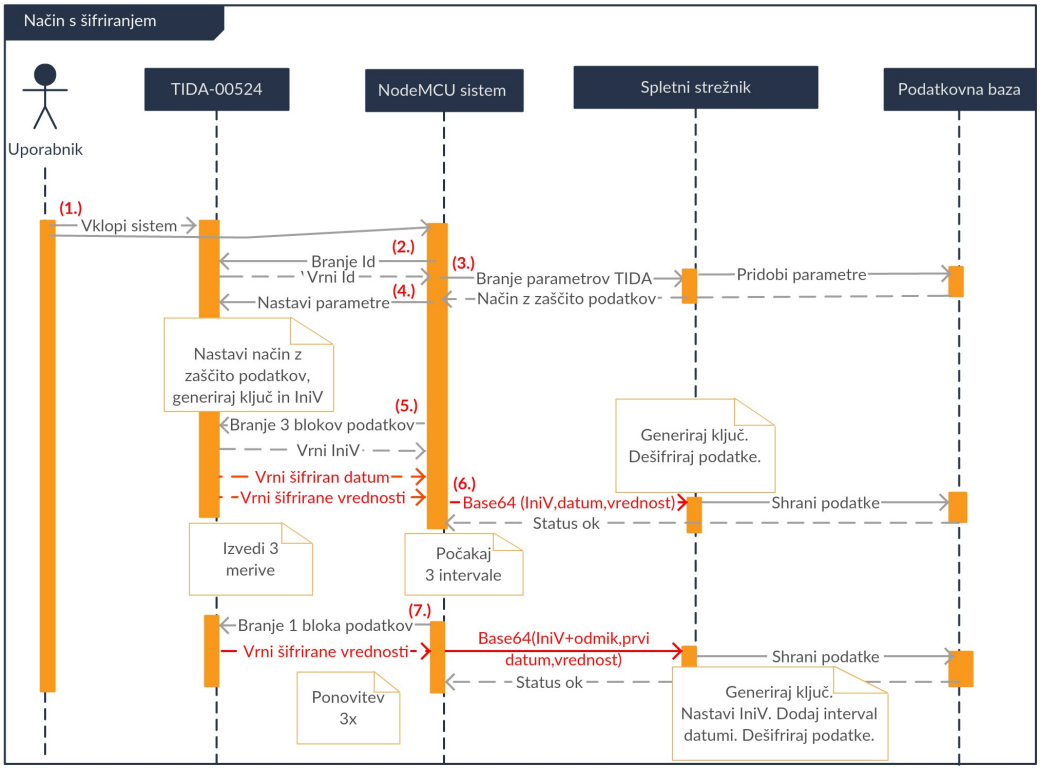
Inicializacijski vektor (IniV) se generira vsakič, ko se modul TIDA-00524 zažene, ali ko se števec ponastavi (doseže vrh). Na naključnost inicializacijskega vektorja vplivajo različni faktorji, od datuma, do meritev. Psevdokoda prikazuje primer generiranja inicializacijskega vektorja.

Algorithm 2 Psevdokoda generiranja inicializacijskega vektorja

```
1: i ←0
2: repeat
3:    if i = 2 then
4:       seed2(temp.0) {inicializiraj seme glede na decimalko temperature}
5:    else if i = 5 then
6:       seed2(humidity) {inicializiraj seme glede vlažnost}
7:    else if i = 7 then
8:       seed2(time) {inicializiraj seme glede na minuto}
9:    end if
10:   IniV[i] ← random2() {naključno število}
11:   i ← i + 1
12: until i ≥ (dolzina_IniV − 3)
```

Zadnja dva bajta sta rezervirana za števec, ki se spreminja z vsakim blokom. Modul NodeMCU prebere incializacijski vektor samo enkrat, naslednje

pa spletni strežnik izračuna glede na to kateri blok je bil zaporedoma prebran. Slika 5.5 prikazuje delovanje v načinu s šifriranjem podatkov.



Slika 5.5: Delovanje SS-NFC v načinu s šifriranjem podatkov.

1. Vklop sistema (modul TIDA-00524, modul NodeMCU).
2. Branje parametra Id na modulu TIDA-00524.
3. Preverjanje povezave in branje parametrov na spletnem strežniku.
4. Nastavljanje parametrov na NodeMCU in TIDA-00524 modulu (Šifriranje podatkov je omogočeno). Prav tako se na modulu TIDA-00524 generirata ključ in IniV.
5. Preberi 3 bloke podatkov (48 bajtov). Ti so IniV, datum in podatki meritev (vsak po 16 bajtov). Datum in podatki so šifrirani.

6. Dodatno kodiraj podatke z Base64 in jih posreduj na strežnik. Odkodiranje in odšifriranje se nato izvede na spletnem strežniku. Počakaj 3 intervale meritev.

7. Preberi samo 1 blok podatkov. Ti so šifrirani podatki meritev. Datum in IniV izračunaj iz odmika vrednosti prebranih ob prvi meritvi. Ponovi 3 krat, ter počakaj 3 intervale.

5.6 Način z branjem vrednosti odstopanj

V tem načinu delovanja se zabeležijo samo meritve, katere so nad določeno mejo podane temperature. Vrednosti nastavimo na spletni strani v Edit parameters (slika 4.3 - parameter `Temperature high mode` za omogočanje in `TH mode threshold` za preseženo vrednost). Interval zajema podatkov ostane nespremenjen, le vrednosti se v modulu TIDA-00524 ne shranijo, če te ne presegajo dovoljenih nastavitev. Modul NodeMCU v tem primeru po prebranem praznem modulu TIDA-00524 le temu ne pošlje ukaza za začetek zajema podatkov, ampak le zapiše, da v tem intervalu vrednosti niso bile presežene. Spodnje sporočilo se izpiše v serijski konzoli v primeru, ko NodeMCU ne prebere nobene presežene vrednosti v tem načinu delovanja.

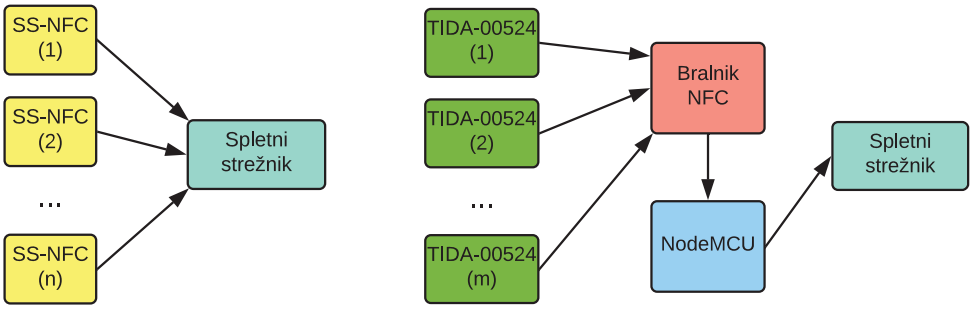
```
Tag B present
No data this period.  Values are in lower temperature state.
```

5.7 Vozlišča senzorskih sistemov ali modulov

Obstajata dva načina komunikacije s strežnikom v primeru uporabe večjega števila SS-NFC ali modulov TIDA-00524. Uporaba dveh ali več senzorskih sistemov NFC (SS-NFC), tako da vsak pošilja podatke o svojem modulu TIDA-00524, je prikazan na sliki 5.6 (a). Sestavili smo dva kompleta, tako da lahko pošiljamo spletnemu strežniku meritve istočasno z uporabo dveh

SS-NFC. V tem primeru lahko uporabimo 'On-line' način delovanja in se tako podatki sproti prenašajo na spletni strežnik.

Obstaja pa še način, v katerem branje poteka izmenično in je prikazan na sliki 5.6 (b). Tako lahko SS-NFC prebere en modul TIDA-00524, pošlje podatke spletnemu strežniku in nato še drugega, ter tretjega itd. V tem primeru se uporabi v TIDA-00524 zapisan Id, kateri v programu NodeMCU s pomočjo tabele preslika le tega v pravilni javni ključ. Drug način pa je branje javnega ključa s pomočjo avtorizacije opisane v poglavju 5.3. V tem načinu je smiselno uporabiti 'Off-line' način delovanja, saj se podatki prenašajo izmenično.



(a) Spletni strežnik komunicira z n SS-NFC.

(b) SS-NFC komunicira z m moduli TIDA-00524 in podatke pošlje spletnemu strežniku.

Slika 5.6: Različna vozlišča senzorskih sistemov.

Poglavje 6

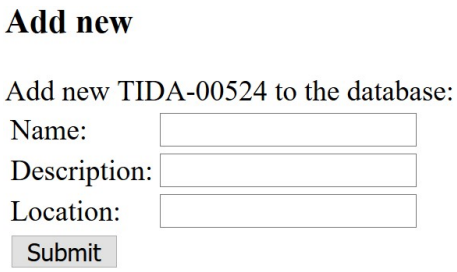
Uporaba SS-NFC

Senzorski sistem NFC zahteva zaradi različnih načinov delovanja več korakov pred začetkom zajemanja senzorskih meritev. V sistem je potrebno morebiti dodati nov modul TIDA-00524 ali pa le tega ponovno konfigurirati za drugačen način uporabe. Postopek in izvedba sta opisana pred izvedbo testov SS-NFC in dveh eksperimentov hladne verige.

6.1 Inicializacija

Senzorski sistem NFC (SS-NFC) je potrebno pred vsako uporabo pripraviti za zajem novih meritev. Postopek poimenujemo inicializacija. Če imamo nov modul TIDA-00524, ga moramo najprej dodati v podatkovno bazo, da dobi unikatno oznako Id. To izvedemo tako, da se na strežniku prijavimo z administratorskim računom in vpišemo ime, opis in lokacijo (slika 6.1). Modul TIDA-00524 nato sprogramiramo z orodjem MSP-FET [5] in nastavimo Id, ki mu je bil dodeljen. V primeru spremembe omrežja Wi-Fi, spremenimo tudi geslo in ime omrežja v programu mikrokrmilnika NodeMCU.

Če smo modul TIDA-00524 že prej uporabljali, samo spremenimo parametre na spletni strani z uporabo povezave `Edit TIDA parameters` (slika 4.3). Pred začetkom novega testa prejšnje podatke najprej shranimo v datoteko CSV in izbrišemo (slika 4.2). Ob prvem branju modula TIDA-00524 se para-



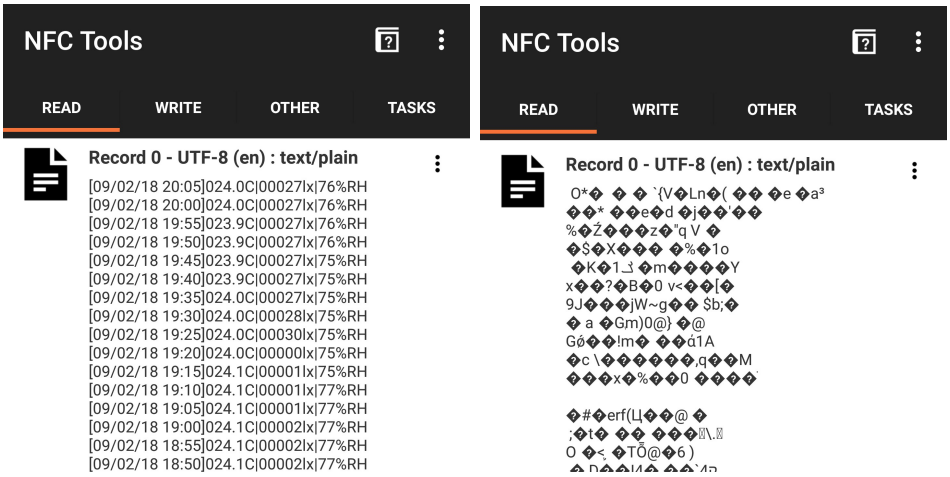
Slika 6.1: Dodajanje novega modula TIDA-00524 v podatkovno bazo.

metri preberejo ter ustrezno nastavijo. Če uporabljamo način brez avtorizacije, se začne zajem senzorskih meritev in ob prvi meritvi tudi nastavljanje pravega časa na modulu TIDA-00524. V primeru avtorizacije se izvede branje parametra Id s kartico NFC in zajem senzorskih podatkov se prične po uspešnem preverjanju.

6.2 Primeri uporabe

SS-NFC je primarno namenjen uporabi v hladni verigi za nadzor temperature in vlage različnih živil ter proizvodov. Obstajajo pa še druga področja uporabe, lahko ga definiramo tudi kot vremensko postajo, napravo za zaznavanje svetlobe in tako dalje. Različni načini omogočajo delovanje v različnih okoljih in situacijah. Prav tako ga lahko uporabimo brez stalne omrežne napetosti, saj modul TIDA-00524 deluje z baterijo in omogoča zajem podatkov in shranjevanje v internem pomnilniku več dni brez branja sistema. Meritve so v načinu brez šifriranja podatkov na voljo tudi za ogled z mobilnim telefonom in namensko aplikacijo za branje kartic NFC [7] (slika 6.2). Tako lahko meritve pregledujemo tudi na sami lokaciji, če internetno omrežje ni na voljo.

Na spletni strani so predstavljene trenutne vrednosti senzorjev, ali shranjene meritve za določeno časovno obdobje. Omogočen je tudi izvoz podatkov v datoteki CSV za nadaljnjo analizo (slika 4.5). Na voljo je tudi opcija v kateri lahko starejše meritve shranimo na strežnik in potem nakna-



(a) Brez šifriranja. **(b)** S šifriranjem.

Slika 6.2: Del zaslona mobilnega telefona pri branju senzorskih podatkov z aplikacijo NFC Tools [7] v načinu brez šifriranja in s šifriranjem.

dno prenesemo v datoteki CSV. Nastavitve mejnih vrednosti nam omogočajo jasen pregled o odstopajočih vrednostih senzorjev, da so le te na grafu jasno označene (slika 4.4).

Uporabo načina z avtorizacijo predlagamo za okolja, kjer je pomembno, da se uporabnika pred vsakim zajemanjem in posredovanjem podatkov na spletni strežnik preveri. Kot primer naj navedemo skladišče, kjer obstaja možnost, da se senzorski moduli namestijo na napačne lokacije, ki niso usklajene z zapisom v spletni aplikaciji.

Način s šifriranjem podatkov predlagamo za uporabo v okoljih, kjer je pomembna varnost podatkov, predvsem v farmaciji ali pa za izdelke z večjo vrednostjo, kjer je pomembna diskretnost in onemogočena manipulacija s podatki.

'On-line' način je primeren za stalen nadzor v hladni verigi. Senzorski sistem namestimo v hladilnico, katera ima na voljo omrežje Wi-Fi. Podatki se lahko v tem primeru preverjajo oddaljeno, preko spletne strani.

'Off-line' način lahko uporabimo v transportu, kjer ni na voljo stalnega

omrežja Wi-Fi. Ko transport prispe na cilj, sistem ob zaznavi omrežja Wi-Fi avtomatično posodobi senzorske podatke, kateri so bili zajeti tekom transporta.

Način s branjem vrednosti odstopanj uporabimo tam, kjer so pomembne samo presežene vrednosti in nam je pomembno, da prihranimo pri shranjevanju rezultatov. Tukaj lahko izpostavimo primer celotne hladne verige, kjer je kot presežena vrednost nastavljena vrednost temperature, katere izdelek ne sme prekoračiti. Če ni preseženih vrednosti, je bil izdelek shranjen v zahtevanih pogojih, v nasprotnem primeru pa nam modul sporoči čas preseženih vrednosti in kakšne so te bile.

Shranjevanje meritev

V primerjavi s privzeto različico programa TIDA-00524 (opisano v tabeli 3.1), lahko v pomnilniku za predstavljeno izvedbo shranimo več meritev, še posebej, če uporabimo način s šifriranjem podatkov. V načinu brez šifriranja podatkov lahko shranimo 1250 meritev, kar predstavlja 15% izboljšavo, v primeru da uporabljamo šifriranje podatkov pa 2719 meritev, kar zagotavlja 150% izboljšavo v shranjevanju meritev. Tabela 6.1 prikazuje primerjavo števila dni merjenja podatkov ob uporabi treh senzorjev. Pri izbiri ostalih kombinacij senzorjev bi v primeru prvotne različice lahko shranili več meritev [9], pri uporabi v SS-NFC pa smo v programu poenotili izpis in kombinacija uporabljenih senzorjev ne vpliva na število shranjenih meritev.

Interval zajema (v minutah)	Začetna različica (v dnevih)	Brez šifriranja (v dnevih)	S šifriranjem (v dnevih)
1	0,75	0,87	1,89
10	7	8	18
15	11	13	28
30	22	26	56
60	44	52	113

Tabela 6.1: Primerjava števila dni hranjenja meritev glede na interval zajema v različnih načinih delovanja in začetno različico programa modula TIDA-00524.

6.3 Testiranje senzorjev

V fazi razvoja SS-NFC smo testiranje in preverjanje funkcionalnosti izvajali v sobi. Mejnih vrednosti meritev nismo dosegli pri uporabi vseh različnih senzorjev.

Temperature so bile od 15°C do 30°C stopinj, zato smo za doseg nižjih temperatur modul postavili v hladilnik in zamrzovalnik. Ugotovili smo, da modul TIDA-00524 deluje tudi pod temperaturo minus 17 °C, a je zaradi visoke vlage v zamrzovalniku potrebna uporaba neprodušne embalaže.

Za primere relativne vlage smo v hladilniku zlahka dosegli mejno vrednost 99 % RH, za nižje vrednosti pa smo morali modul TIDA-00524 postaviti nad radiator.

Pri svetlobi smo v stanovanju težko dosegli vrednost preko 140 lx. Ko smo modul TIDA-00524 uporabili zunaj v sončnem vremenu, je ta dosegla mejno vrednost 16535 lx.

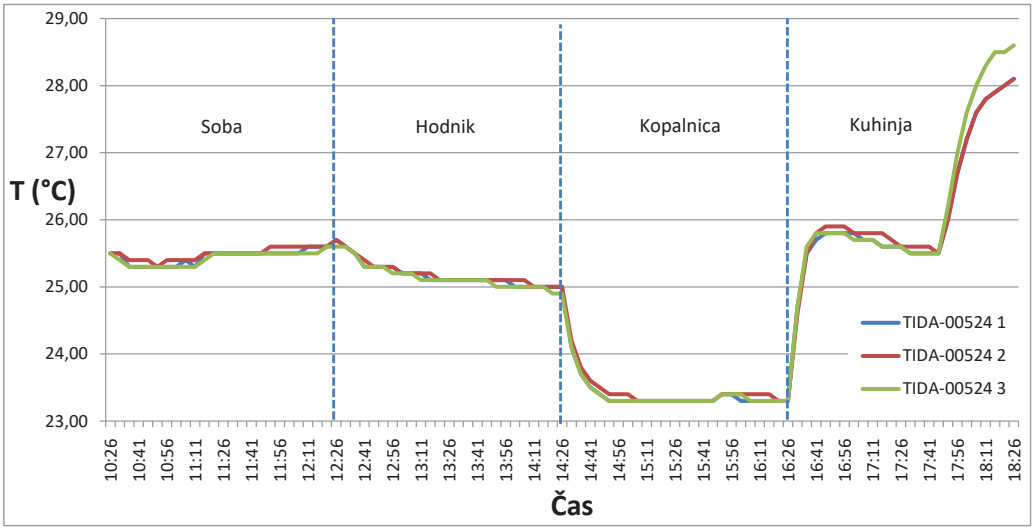
6.3.1 Primerjava delovanja senzorskih modulov

Za preverjanje odstopanja posameznih meritev senzorjev smo tri module TIDA-00524 postavili enega zraven drugega ter tako zagotovili, da imajo

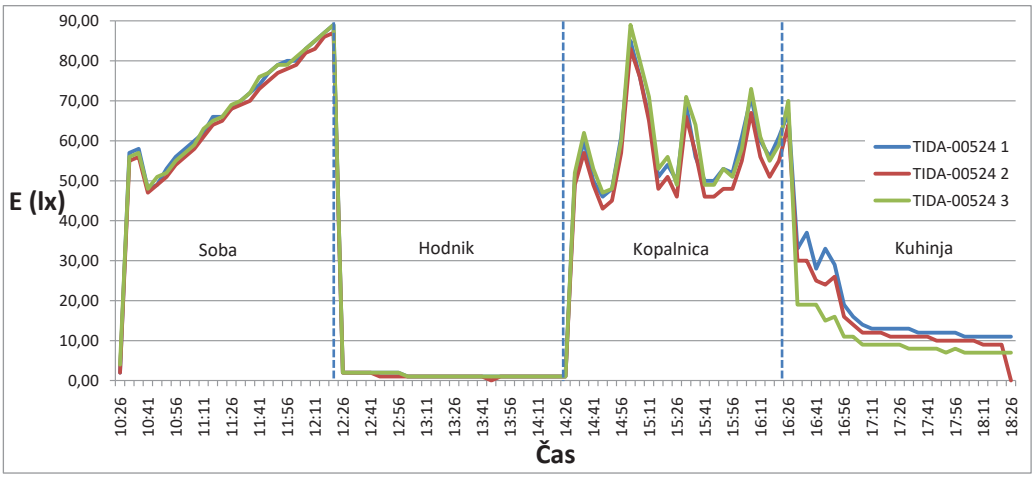
enake pogoje pri izvedbi testa (slika 6.3). Delovali so v 'Off-line' načinu, interval zajema podatkov je bil 5 minut. Test smo izvajali 8 ur, od 10:26 do 18:26. Moduli so bili po 2 uri v sobi, na hodniku, kopalnici ter nazadnje v kuhinji.

Slika 6.3: Postavitev modulov TIDA-00524 za analizo senzorskih meritev.

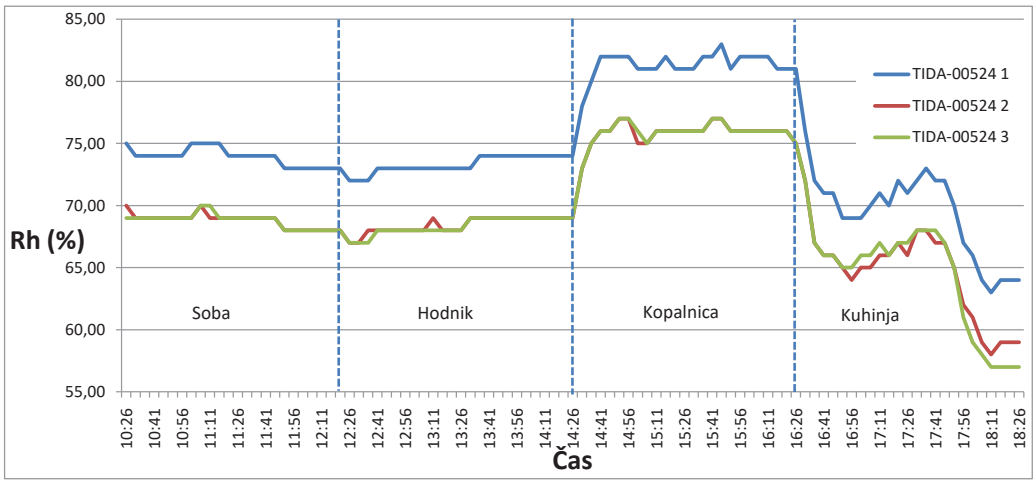
Podatke vseh treh modulov smo nato prebrali z uporabo SS-NFC in jih analizirali. Slike 6.4, 6.5 in 6.6 prikazujejo posamezne meritve za temperaturo, svetlobo in relativno vlago.



Slika 6.4: Primerjava meritev temperature.



Slika 6.5: Primerjava meritev osvetljenosti.



Slika 6.6: Primerjava meritev relativne vlažnosti.

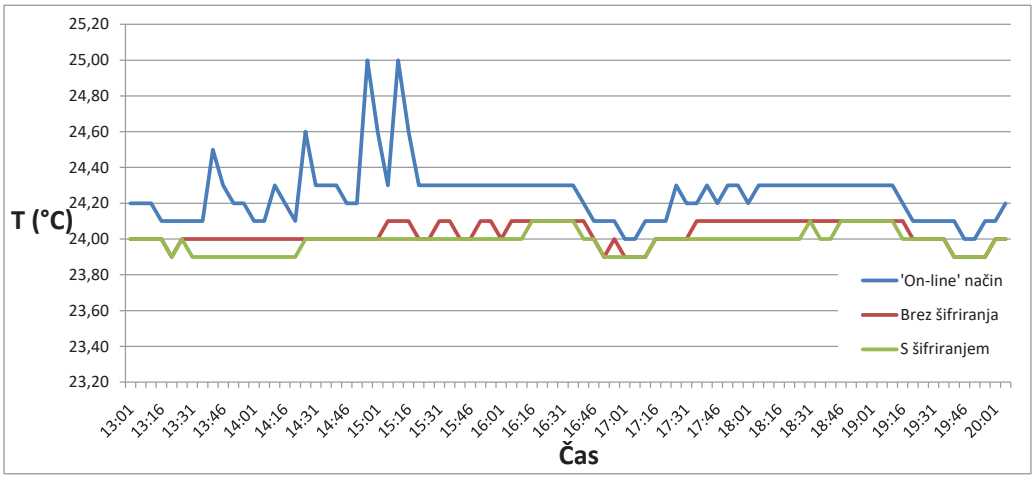
Rezultati testov pri primerjavi meritev med moduli TIDA-00524 so pokazali največje odstopanje, 0.5 °C v temperaturi, 6 % v vlagi, ter 15 lx v svetlobi. Še največje odstopanje se prikaže pri modulu TIDA-00524 1 in sicer v relativni vlagi v primerjavi z drugi moduli. Tabela 6.2 prikazuje povprečni (Srv) in standardni odklon (Std) meritev med posameznimi moduli TIDA-00524.

Modul	T(Δ°C)		E(Δlx)		RH(Δ%)	
	Srv	Std	Srv	Std	Srv	Std
TIDA-00524 1	0,0453	0,0595	1,8608	2,4138	5,103	0,35
TIDA-00524 2	0,0628	0,0666	1,6288	1,7082	2,5051	0,2612
TIDA-00524 3	0,069	0,118	2,1907	2,8952	2,5979	0,03828

Tabela 6.2: Povprečni odklon meritev in standardni odklon med moduli TIDA-00524.

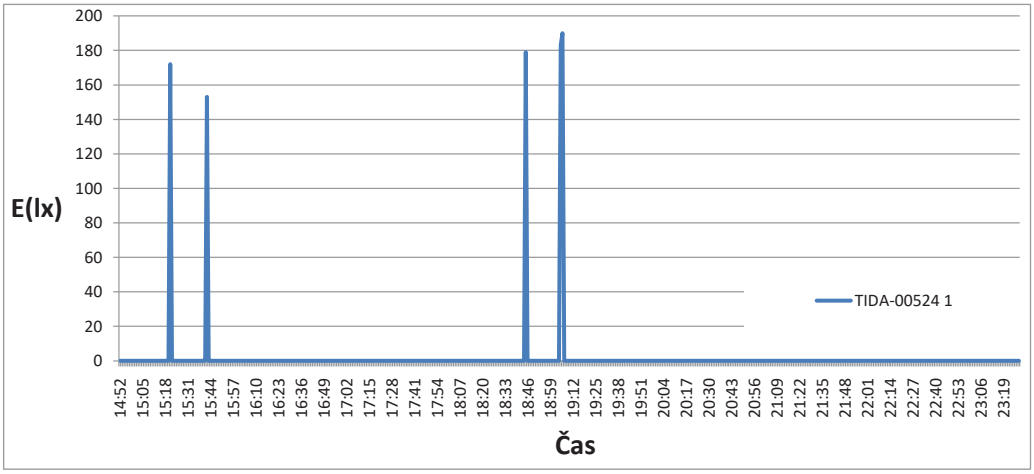
6.3.2 Primerjava različnih načinov delovanja

Ker omogoča SS-NFC različne načine delovanja, bi lahko pričakovali kakšna odstopanja v zajemu meritev. Zanimala nas je predvsem temperatura, saj lahko šifriranje ali pa 'On-line' način dodatno obremenita modul TIDA-00524 in posledično povzročita povišanje temperature. Testirali smo v sobi s tremi moduli TIDA-00524. Prvi je bil v 'On-line' načinu in je bil pozicioniran nad bralnikom NFC, drugi je bil v 'Off-line' načinu brez šifriranja ter postavljen zraven prvega, tretji pa v 'Off-line' načinu s šifriranjem. Interval zajema podatkov je bil nastavljen na 5 minut, testirali smo 7 ur. Ker je bil prvi modul v 'On-line' načinu, v tem testu senzorjev nismo premikali. Slika 6.7 prikazuje temperaturo v različnih načinih delovanja. V meritvah opazimo manjše odstopanje modula v 'On-line' načinu verjetno zato, ker je bil modul malo dvignjen zaradi bralnika NFC.



Slika 6.7: Primerjava temperature v različnih načinih delovanja.

Senzor za svetlobo smo testirali z namenom zaznavanja prižganih luči. V tem primeru smo ugotavljali kdaj je odprt hladilnik. Slika 6.8 prikazuje vrednosti osvetljenosti hladilnika. Interval zajema podatkov je nastavljen na najmanjšo vrednost in sicer 1 minuto. Test smo izvajali od 14:52 do 23:28.



Slika 6.8: Meritve zaznave svetlobe v hladilniku.

Na sliki vidimo, da je bil hladilnik 4-krat odprt. Pri zadnji meritvi je interval širši, ker smo pustili vrata dalj časa odprta. Če smo vrata hladilnika odprli za kratek čas in se v tem času meritev ni zabeležila, le ta ni prikazana v zaznavi.

6.4 Hladna veriga

Za prikaz uporabe SS-NFC v hladni verigi smo module uporabili v dveh različnih eksperimentih in se poskušali približati pogojem v realni uporabi. Najprej smo izmerili in analizirali temperature shranjevanja v prostoru in hladilnici za izračun dobe uporabnosti mesa, nato pa smo preverjali senzorske meritve v hladilniku pri shranjevanju kupljenih živil.

Eksperiment 1

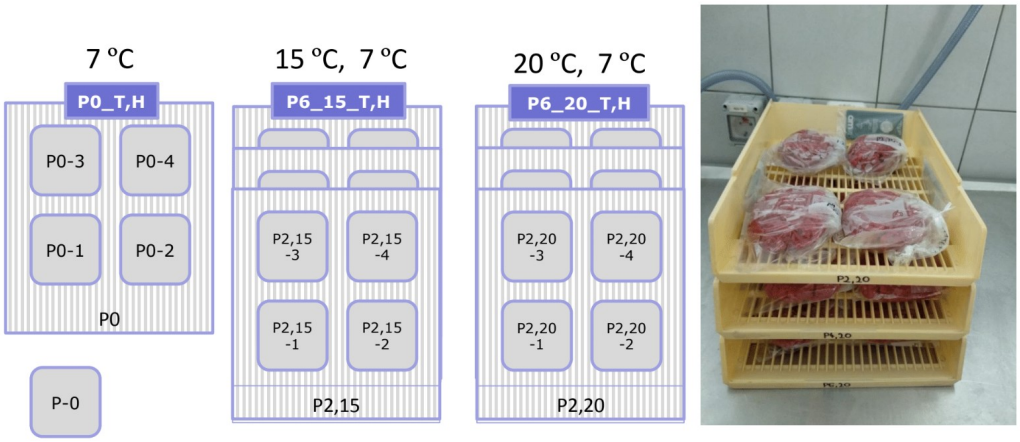
Za hitro pokvarljiva živila, kot so meso in različni mesni izdelki, je potrebno pred uporabo zagotavljati ustrezno temperaturo (hraniti pri temperaturi od x °C do y °C) in preveriti koliko časa je živilo uporabno (porabiti do: Datum). Tabela 6.3 vsebuje podatke o izvedbi eksperimenta. Uporabljeni so bili trije moduli TIDA-00524 in postavljeni na mrežne podstavke s paketi mletega govejega mesa (slika 6.9). Z njimi smo merili temperature pod različnimi pogoji hranjenja (P0_T,H je bil s paketi postavljen takoj v hladilnico na temperaturo 7 °C, P6_15_T,H je bil 6 ur na sobni temperaturi 15 °C ter nato postavljen v hladilnico, P6_20_T,H je bil 6 ur na sobni temperaturi 20 °C ter nato postavljen v hladilnico).

Hladna veriga: mleto meso	Podatki
obdobje - začetek in konec	21.5.2018, 8:55 - 24.5.2018, 11:00
lokacija	Biotehniška fakulteta: hladilnica, laboratorij
način delovanja	'Off-line', brez avtorizacije in šifriranja
moduli TIDA-00524	P0_T,H; P6_15_T,H; P6_20_T,H
interval zajema meritev	7 min

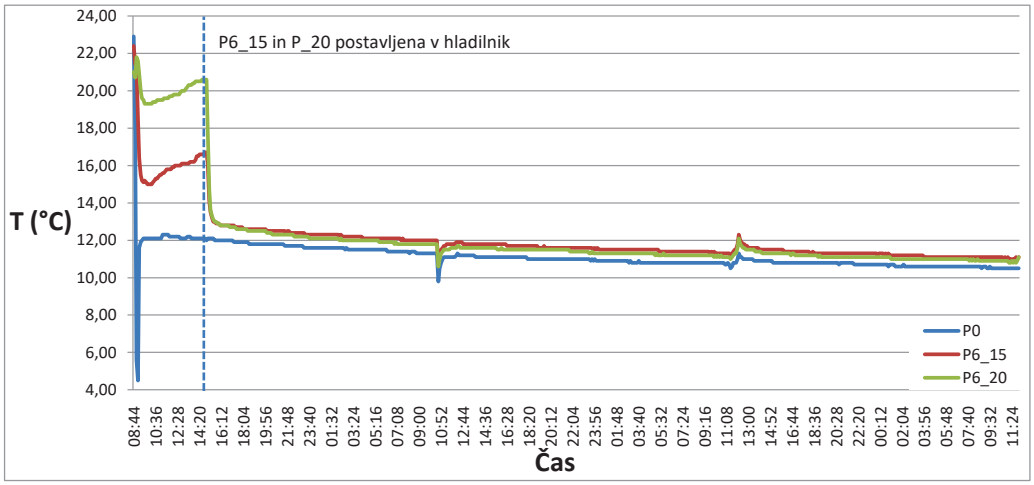
Tabela 6.3: Hladna veriga – analiza pogojev hranjenja mletega govejega mesa (temperatura, vlaga).

Za analizo dobe uporabnosti so nas zanimale predvsem temperaturne spremembe v odvisnosti od časa hranjenja (slika 6.10). Prvih šest ur so

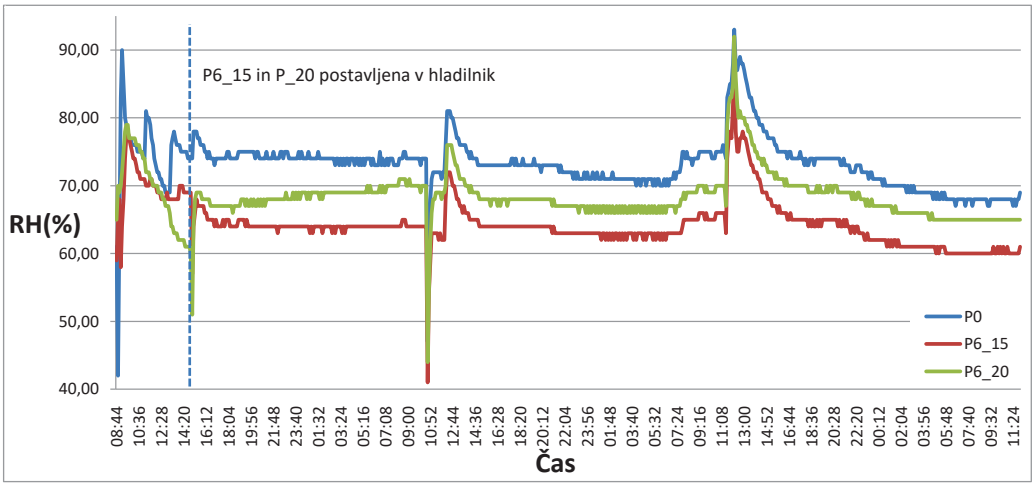
podatki povezani z lokacijo paketov, nato pa so zelo podobni. Razlike so majhne in so povezane z mestom postavitve v hladilnici. V tem času so se v dopoldanskih urah pojavila odstopanja, enkrat se je temperatura znižala, drugič pa se je zvišala. Zanimiv je podatek, da izmerjena temperatura v hladilniku ni bila 7 °C, kot je bilo nastavljeno, ampak je bila v času testiranja med 12 °C in 11 °C. Slika 6.11 prikazuje izmerjeno relativno vlago treh modulov, kjer so razlike in odstopanja v primeru neznanih dogodkov dosti večja. Razloge za takšne rezultate bi lahko iskali v delovanju hladilnice, odpiranju in zapiranju vrat ter v prinašanju ali odnašanju živil iz prostora.



Slika 6.9: Prikaz lokacije modulov TIDA-00524 v eksperimentu.



Slika 6.10: Rezultati temperature v eksperimentu 1.



Slika 6.11: Rezultati relativne vlage v eksperimentu 1.

Eksperiment 2

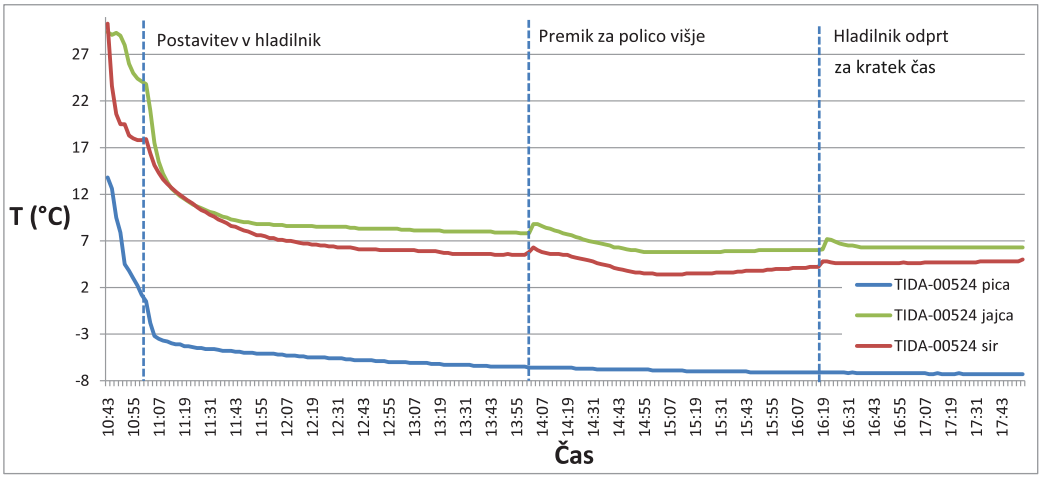
Za eksperiment 2 smo izvedli preverjanje hladne verige v transportu, od nakupa v trgovini, do shranjevanja živil v hladilniku (Tabela 6.4). Primerjali smo meritve treh različnih živil glede na postavitev v hladilniku in sicer jajca, sir gorgonzola ter zmrznjeno pico. Jajca so bila v trgovini na navadni trgovski polici ter smo jih kasneje ohladili. Za shranjevanje je navedeno naj le te shranjujemo na hladnem. Sir je bil v trgovini v hladilniku in smo ga po nakupu in prihodu domov postavili v hladilnik. Shranjevanje je bilo določeno v hladilniku in sicer do 7°C. Pica je bila v trgovini v zamrzovalniku in smo jo po prihodu v stanovanje postavili v zamrzovalnik. V eksperimentu smo uporabili kombiniran vgradni hladilnik s prostornino 120 litrov. Jajca smo v eksperimentu postavili na začetku v spodnji predal, sir pa na spodnjo polico nad njim. Slika 6.12 prikazuje module TIDA-00524 postavljene v embalaže izdelkov ob nakupu. Slika 6.13 prikazuje izmerjene temperature, slika 6.14 pa relativno vlago. Svetloba je bila večino časa konstantna 0 lx, razen na začetku eksperimenta v avtomobilu ter ob odpiranju hladilnika. Po treh urah v hladilniku smo živila premaknili za eno polico višje k zamrzovalniku.

Hladna veriga: shranjevanje kupljenih živil	Podatki
obdobje - začetek in konec	23.8.2018, 10:43 - 17:59
lokacija	avto, stanovanje: hladilnik
način	'Off-line', brez avtorizacije in šifriranja
moduli TIDA-00524	pica, sir, jajca
interval zajema meritev	2 min

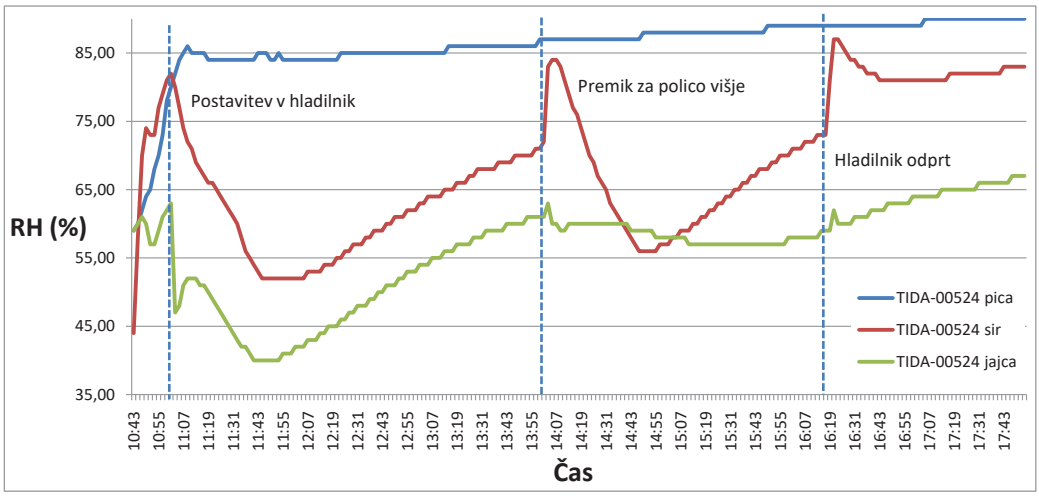
Tabela 6.4: Hladna veriga – analiza pogojev živil od nakupa do hladilnika (temperatura, vlaga).

(a) TIDA-00524 - pica **(b)** TIDA-00524 - sir **(c)** TIDA-00524 - jajca

Slika 6.12: Modula TIDA-00524 v/na embalažah izdelkov.



Slika 6.13: Temperatura v eksperimentu 2.



Slika 6.14: Relativna vlaga v eksperimentu 2.

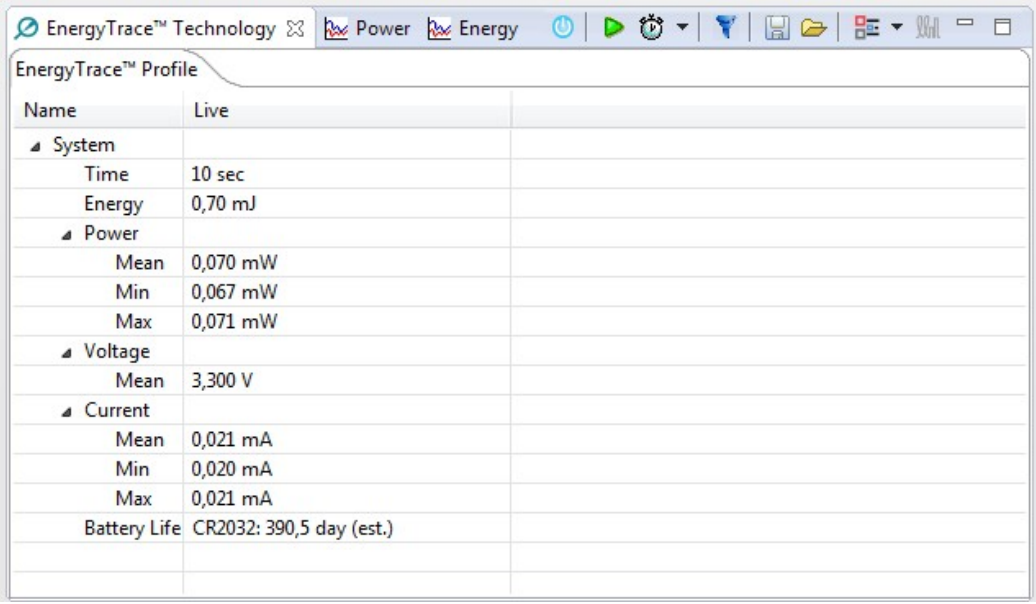
6.5 Analiza rezultatov

Življenjska doba baterije

Proizvajalec modula TIDA-00524 [15] predvideva pet let delovanja z uporabo ene baterije CR20132 ob avtonomni uporabi in branju podatkov s pametnim telefonom. S testiranjem smo ugotovili, da te navedbe veljajo samo za zajemanje podatkov, saj se je ob testiranju komunikacije NFC baterija hitro izpraznila (približno 1 teden). Program na modulu NodeMCU smo zato spremenili tako, da se komunikacija izvede vsak večkratnik intervala zajemanja podatkov. Prav tako smo v 'Off-line' načinu omogočili branje šele po zaznavanju omrežja Wi-Fi. Z dodatnimi optimizacijami smo tako dosegli, da bi po naši oceni modul TIDA-00524 uporabimo brez težav tudi en mesec ali več.

Za dodatno analizo porabe energije uporabljajo mikrokrmilniki družine MSP430 tehnologijo EnergyTrace™. Ta funkcija omogoča realen prikaz porabe energije ter prikaže v katerem stanju varčne porabe se nahaja mikrokrmilnik. Slika 6.15 prikazuje okno za sporočanje podatkov o porabi energije med razhroščevanjem. Ker je za uporabo tehnologije zahtevano orodje MSP-FET in smo pri izdelavi uporabljali starejšo verzijo nam ta tehnologija za

spremljanje porabe na modulu TIDA-00524 ni bila na voljo.



Slika 6.15: Okno v Code Composer Studio, kateri prikazuje informacije EnergyTrace™.

Za ugotavljanje porabe baterije smo v načinu delovanja s šifriranjem in brez zato uporabili drug pristop. Ugotovili smo, da v načinu s šifriranjem mikrokrmilnik potrebuje 4200 več ukazov za zapis podatkov v NDEF sporočilo. Vsi ukazi so izvedeni v normalnem načinu delovanja mikrokrmilnika pri povprečni porabi 100 µA/MHz [9]. Za baterijo pa smo uporabili standardno kapaciteto 220 mAh (CR2032). Izračunali smo koliko bi vplivala uporaba šifriranja na kapaciteto baterije modula TIDA-00524 v petletnem obdobju z nastavitvijo zajema podatkov na 10 minut (6.1). Ugotovili smo, da je šifriranje zanemarljivo. Poraba je bistveno večja pri komunikaciji NFC.

$$\frac{\frac{0{,}1\ \text{mA} * 4200(ukazov)}{1\ \text{MHz} * 3600(ura)} * 6 * 24 * 365 * 5}{220\ \text{mA}h} = 0,0139\% \tag{6.1}$$

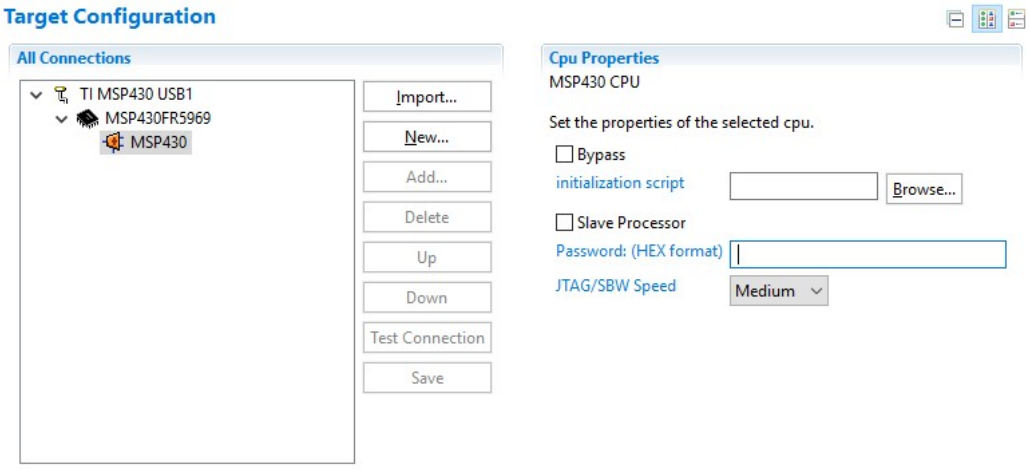
Varnostna analiza

Varnost senzorskega sistema je primarno namenjena preprečevanju ponarejanja ali prirejanja senzorskih podatkov. Z uporabo senzorjev svetlobe ali

vlage lahko ugotovimo ali je kdo nepooblaščeno dostopal do modula in dodatno analiziramo ali so podatki pristni.

Ker sistem ne podpira izmenjevanja ključa za šifriranje, obstaja možnost ponareditve programa TIDA-00524 z uporabo enakega parametra Id. To smo poskušali izboljšati z uporabo serijske številke modula TIDA-00524 in jo uporabili kot dodatni parameter za ključ, ker je drugačna za vsak modul in je ni možno spreminjati. Ob prvi uporabi šifriranja modula TIDA-00524 se ta prenese na spletni strežnik in se v naslednjih komunikacijah uporabi za generiranje ključa. To nam omogoča, da bi bili ob spremenjeni serijski številki za enak parameter Id podatki zavrnjeni oziroma neberljivi.

Za dodatno zaščito programske kode modula TIDA-00524, se priporoča uporaba metod za zaščito modulov mikrokrmilnikov MSP430 [36]. Primer slike 6.16 prikazuje zaščito programske kode z geslom.



Slika 6.16: Zaščita programske kode modula TIDA-00524 z geslom.

Poglavje 7

Sklepne ugotovitve

V magistrskem delu smo raziskali in analizirali področje senzorskih modulov in varnosti. Predstavili smo različne načine šifriranja s poudarkom na tistih, ki so primerni za našo izvedbo na modulu TIDA-00524. Opisali smo idejno zasnovo in potek načrtovanja senzorskega sistema. Posamezne elemente smo podrobno opisali in podali potek razvoja sistema. Definirali smo različne načine delovanja sistema in predstavili izvedbo prototipa z namenskim ohišjem. Zaključili smo s testiranjem in opisali primere uporabe sistema ter podali izsledke analize.

Cilj magistrskega dela je bil izdelati senzorski sistem NFC, kateri bi vključeval ustrezen nivo varnosti in bi omogočal sprotno pošiljanje podatkov o meritvah temperature, vlage in svetlobe na strežnik. Pri tem smo želeli, da vključuje šifriranje senzorskih podatkov in po potrebi avtorizacijo uporabnikov. Za razliko od obstoječih rešitev je v magistrskem delu pomemben poudarek na varnosti in istočasno omogoča različne načine delovanja.

Senzorski sistem NFC že zagotavlja vse funkcionalnosti, katere smo si zadali ob načrtovanju, vendar pa še vedno obstajajo določene možnosti izboljšav. S stališča uporabe bi lahko dodali različico sistema, v katerem deluje sistem NFC samostojno z uporabo baterij. Za ta način bi morali spremeniti program NodeMCU, tako da bi uporabljal manj energije z uporabo funkcij globokega spanja. Spletni strani bi lahko dodali funkcional-

nost RESTful APIja, tako bi lahko uporabniki implementirali lastne grafe ter načine obveščanja o nepričakovanih spremembah ali dogodkih pri zaznavanju napačnih ali neustreznih meritev. Na spletni strani bi lahko dodali obveščanje o preseženih vrednostih prek e-pošte ali kakega drugega protokola. Izdelali bi lahko namensko aplikacijo za mobilne telefone, katera bi podpirala branje šifriranih senzorskih podatkov.

Literatura

[1] Arduino ide. Dostopno na: https://www.arduino.cc/en/Main/Software (pridobljeno 6. 3. 2018).

[2] Code composer studio. Dostopno na: http://www.ti.com/tool/CCSTUDIO (pridobljeno 6. 3. 2018).

[3] Adobe dreamweaver. Dostopno na: https://www.adobe.com/si/products/dreamweaver.html (pridobljeno 23. 7. 2018).

[4] Nxp semiconductors, mifare classic family. Dostopno na: https://www.mifare.net/en/products/chip-card-ics/mifare-classic/ (pridobljeno 17. 5. 2018).

[5] Msp mcu programmer and debugger. Dostopno na: http://www.ti.com/tool/MSP-FET (pridobljeno 21. 8. 2018).

[6] Nfc forum - type 4 tag operation specification. Dostopno na: http://apps4android.org/nfc-specifications/NFCForum-TS-Type-4-Tag_2.0.pdf (2011, pridobljeno 22. 12. 2017), .

[7] Nfc tools. Dostopno na: https://play.google.com/store/apps/details?id=com.wakdev.wdnfc(Android), https://itunes.apple.com/us/app/nfc-tools/id1252962749(iPhone) (pridobljeno 9. 8. 2018), .

[8] Nodemcu - an open-source firmware based on esp8266 wifi-soc. Dostopno na: http://nodemcu.com/index_en.html (pridobljeno 17. 5. 2018).

[9] Ultralow power multi-sensor data logger with nfc interface reference design. Dostopno na: http://www.ti.com/tool/TIDA-00524 (2015, pridobljeno 16. 11. 2017).

[10] Australian alliance for energy productivity : Optimizing the food cold chain. Dostopno na: https://www.airah.org.au/Content_Files/Industryresearch/05-17-A2EP_Cold_Chain_Report.pdf (2017, pridobljeno 23. 1. 2018).

[11] Specification for the advanced encryption standard. Dostopno na: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf (2001, pridobljeno 17. 5. 2018).

[12] Nijz - hladna veriga za zagotavljanje varnosti živil. Dostopno na: http://www.nijz.si/sl/hladna-veriga-za-zagotavljanje-varnosti-zivil (pridobljeno 17. 5. 2018).

[13] Pn532 nfc rfid module user guide. Dostopno na: https://dangerousthings.com/wp-content/uploads/PN532_Manual_V3-1.pdf (2013, pridobljeno 16. 11. 2017).

[14] Radio frequency identification tool. Dostopno na: http://www.proxmark.org/ (pridobljeno 3. 8. 2018).

[15] Ultralow power multi-sensor data logger with nfc interface reference design. Dostopno na: http://www.ti.com/lit/ug/tidu821/tidu821.pdf (2015, pridobljeno 16. 11. 2017).

[16] F. A. Alaba, M. Othman, I. A. T. Hashem in F. Alotaibi. Internet of things security: A survey. *Journal of Network and Computer Applications*, 88(Supplement C):10–28, 2017. ISSN 1084-8045.

[17] R. Ali, A. K. Pal, S. Kumari, M. Karuppiah in M. Conti. A secure user authentication and key-agreement scheme using wireless sensor networks

for agriculture monitoring. *Future Generation Computer Systems*, 84: 200–215, 2018. ISSN 0167-739X.

[18] L. Atzori, A. Iera in G. Morabito. The internet of things: A survey. *Computer networks*, 54(15):2787–2805, 2010.

[19] V. Coskun, K. Ok in B. Ozdenizci. *Near field communication (NFC): From theory to practice*. John Wiley & Sons, 2011. ISBN 1-119-97109-2.

[20] J. Daemen in V. Rijmen. *The design of Rijndael: AES-the advanced encryption standard*. Springer Science & Business Media, 2013. ISBN 978-3-662-04722-4.

[21] J. J. Echevarria, J. Ruiz-de Garibay, J. Legarda, M. Álvarez, A. Ayerbe in J. I. Vazquez. Webtag: Web browsing into sensor tags over nfc. *Sensors*, 12(7):8675–8690, 2012. ISSN 1424-8220.

[22] M. Feldhofer, S. Dominikus in J. Wolkerstorfer. Strong authentication for rfid systems using the aes algorithm. V *International Workshop on Cryptographic Hardware and Embedded Systems*, str. 357–370. Springer, 2004.

[23] G. Hancke. A practical relay attack on iso 14443 proximity cards. Dostopno na: `http://www.rfidblog.org.uk/hancke-rfidrelay.pdf` (pridobljeno 21. 8. 2018).

[24] E. Haselsteiner in K. Breitfuß. Security in near field communication (nfc). V *Workshop on RFID security*, str. 12–14, 2006.

[25] W. A. Hufstetler, M. J. H. Ramos in S. Wang. Nfc unlock: Secure two-factor computer authentication using nfc. V *2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, str. 507–510, Okt 2017.

[26] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu in D. Qiu. Security of the internet of things: perspectives and challenges. *Wireless Networks*, 20 (8):2481–2501, Nov 2014.

[27] S. Josefsson. The base16, base32, and base64 data encodings. Dostopno na: `https://tools.ietf.org/html/rfc4648` (2006, pridobljeno 17. 5. 2018).

[28] S. Li in D. X. Li. *Securing the Internet of Things*. Elsevier Science, 2017. ISBN 9780128045053.

[29] S. Li, T. Tryfonas in H. Li. The internet of things: a security point of view. *Internet Research*, 26(2):337–359, 2016.

[30] D. Linhua, W. Jiuru in L. Li. Privacy-preserving temperature query protocol in cold-chain logistics. V *7th International Conference on Intelligent Human-Machine Systems and Cybernetics*, Vol. 1, str. 113–116, Avg 2015.

[31] G. Madlmayr, C. Kantner in T. Grechenig. Near field communication. V *Secure Smart Embedded Devices, Platforms and Applications*, str. 351–367, New York, NY, 2014. Springer New York.

[32] R. B. Melis. *New techniques and methods for cold chain monitoring and tracking in perishable products*. PhD thesis, Universidad Politécnica de Madrid, 2016.

[33] R. B. Melis, U. M. Carthy, L. Ruiz-Garcia, J. Garcia-Hierro in J. R. Villalba. New trends in cold chain monitoring applications - a review. *Food Control*, 86(Supplement C):170–182, 2018. ISSN 0956-7135.

[34] C. A. Opperman in G. P. Hancke. A generic nfc-enabled measurement system for remote monitoring and control of client-side equipment. V *2011 Third International Workshop on Near Field Communication*, str. 44–49, Feb 2011.

[35] C. Paar in J. Pelzl. *Understanding cryptography: a textbook for students and practitioners*. Springer Science & Business Media, 2009. ISBN 978-3642041006.

[36] K. Pier. Msp code protection features. Dostopno na: `http://www.ti.com/lit/an/slaa685/slaa685.pdf` (2015, pridobljeno 7. 9. 2018).

[37] C. M. Reddy, S. Malliyala, Y. Naresh, H. Raghunandan in H. Jinadatharaya. Good cold chain management practices. *Journal of Pharmacy Research*, 10:5043–5047, 2012.

[38] T. Sánchez López, D. C. Ranasinghe, M. Harrison in D. McFarlane. Adding sense to the internet of things. *Personal and Ubiquitous Computing*, 16(3):291–308, Mar 2012. ISSN 1617-4917.

[39] D. R. Stinson. *Cryptography: theory and practice*. CRC press, 3 edition, 2006. ISBN 1-58488-508-4.

[40] M. Wang, G. Zhang, C. Zhang, J. Zhang in C. Li. An iot-based appliance control system for smart homes. V *2013 Fourth International Conference on Intelligent Control and Information Processing (ICICIP)*, str. 744–747, Jun 2013.

[41] J. Zhang, L. Chen, X. Tang in Q. Gao. A remote monitoring system for cold chain logistics by means of social networks. *Open Cybernetics & Systemics Journal*, 9:888–893, 2015.