STREDNÁ PRIEMYSELNÁ ŠKOLA ELEKTROTECHNICKÁ

**Návrh a implementácia inteligentného IoT domu**

**ročníkový projekt**

**MARTIN LÁSZLÓ**

**2.D**

**Vedúci projektu: Ing. Dominik Zatkalík, PhD.**

2024

Obsah

1 Úvod do IoT 4

1.1 História IoT 4

1.1.1 Počiatok 21. Storočia 5

2 Ako fungujú IoT technológie 6

2.1 Senzory a zariadenia 6

2.1.1 Konektivita 6

2.1.2 Spracovanie dát 6

2.1.3 Užívateľské rozhranie 6

3 IoT aplikácie 7

3.1 Spotrebiteľský sektor 7

3.2 Zdravotníctvo 7

3.3 Inteligentné mestá 7

3.4 Poľnohospodárstvo 8

3.5 Priemyselná automatizácia 8

3.6 Smart autá 8

4 Návrh a implementácia IoT domu 9

4.1 Implementácia IoT 9

4.1.1 Konfigurácia bezdrôtového routera IoT siete 10

4.1.2 Konfigurácia RADIUS servera 10

4.2 Finalizácia a verifikácia produktu 12

5 Záver 14

Zoznam použitej literatúry 15

Anotácia

IoT sa stáva súčasťou našej každodennej reality, kde nás obklopuje všade okolo. Skoro každá domácnosť využíva tieto technológie a ich zavádzaním do vládnych štruktúr sa stávajú neoddeliteľnou súčasťou moderného života. Táto práca sa zaoberá návrhom a realizáciou inteligentného domu prostredníctvom Internetu vecí (IoT). Prvá časť poskytuje teoretický prehľad IoT, zahŕňajúci bezpečnostné aspekty, históriu, využitie a úvodný koncept. Ďalej sa diskutuje o nasadení a praktickom využití. Druhá časť sa zameriava na praktickú stránku projektu, kde sa využíva Cisco Packet Tracer na návrh siete pre IoT dom. Táto implementácia zahŕňa integráciu rôznych IoT zariadení a senzorov, s dôrazom na zabezpečenie komunikácie a súkromia dát. Cieľom práce je demonštrovať proces navrhovania a implementácie inteligentného domu pomocou IoT technológií s dôrazom na bezpečnosť a efektívnosť.

**Annotation**

The IoT is becoming part of our everyday reality, surrounding us everywhere. Almost every household utilizes these technologies, and their integration into governmental structures is becoming an inseparable part of modern life. This work focuses on the design and implementation of a smart home through the Internet of Things (IoT). The first part provides a theoretical overview of IoT, covering security aspects, history, usage, and introductory concepts. Further discussions revolve around deployment and practical application. The second part delves into the practical aspect of the project, utilizing Cisco Packet Tracer to design a network for the IoT home. This implementation includes integrating various IoT devices and sensors, with a focus on ensuring communication security and data privacy. The aim of the work is to demonstrate the process of designing and implementing a smart home using IoT technologies with an emphasis on security and efficiency.

1. Úvod do IoT

Termín IoT alebo Internet vecí sa vzťahuje na kolektívnu sieť pripojených zariadení a technológiu, ktorá umožňuje komunikáciu medzi zariadeniami a cloudom, ako aj medzi samotnými zariadeniami. Vďaka nástupu lacných počítačových čipov a telekomunikácií s vysokou priepustnosťou máme teraz miliardy zariadení pripojených na internet. To znamená, že bežné zariadenia ako zubné kefky, vysávače, autá a stroje môžu pomocou senzorov zbierať údaje a inteligentne reagovať na používateľov. Internet vecí integruje bežné "veci" s internetom. Celý priemysel vznikol so zameraním na naplnenie našich domovov, podnikov a kancelárií zariadeniami IoT. Tieto inteligentné objekty môžu automaticky prenášať údaje do a z internetu. Všetky tieto "neviditeľné výpočtové zariadenia" a s nimi súvisiaca technológia sa spoločne označujú ako Internet vecí. Zariadenia IoT sú typicky vybavené technológiou ako senzory a softvér a môžu zahŕňať mechanické a digitálne stroje a spotrebné predmety. Stále viac organizácií v rôznych odvetviach využíva IoT na efektívnejšie fungovanie, poskytovanie vylepšenej zákazníckej služby, zlepšovanie rozhodovania a zvyšovanie hodnoty podniku. S IoT je možné prenášať údaje cez sieť bez potreby interakcií človek-na-človeka alebo človek-na-počítač. Vec v internete vecí môže byť človek s implantovaným monitorom srdca, automobil s vstavanými senzormi, ktoré upozorňujú vodiča na nízky tlak v pneumatikách, alebo akýkoľvek iný prírodný alebo umelý objekt, ktorý možno priradiť adresu internetového protokolu a je schopný prenášať údaje cez sieť.

* 1. História IoT

Koncept Internetu vecí (IoT) sa prvýkrát oficiálne spomenul v roku 1999, keď Kevin Ashton, spoluzakladateľ Auto-ID Centra na Massachusettskom technologickom inštitúte (MIT), predstavil túto myšlienku v prezentácii pre spoločnosť Procter & Gamble (P&G). Chcel upriamiť pozornosť vrcholového manažmentu P&G na technológiu rádiového identifikačného označenia (RFID), a preto nazval svoju prezentáciu "Internet vecí", aby zahrnul nový trend z roku 1999: internet. Taktiež v roku 1999 vyšla kniha profesora MIT Neila Gershenfelda s názvom "Keď veci začnú premýšľať", ktorá síce nepoužila presný termín "Internet vecí", ale poskytla jasnú predstavu o budúcnosti IoT. IoT sa vyvinulo z bezdrôtových technológií, mikroelektromechanických systémov, mikroslužieb a internetu. Táto konvergencia pomohla zrútiť múry medzi operačnou technológiou a informačnou technológiou, čo umožnilo analyzovať neštruktúrované údaje generované strojmi na získanie poznatkov pre zlepšenie procesov. Hoci Kevin Ashton bol prvý, kto zmienil IoT, myšlienka pripojených zariadení existovala už od 70. rokov minulého storočia. Prvé internetové zariadenie bol napríklad automat na kolu na Carnegie Mellon University. Programátori cez internet mohli skontrolovať stav automatu a zistiť, či ich čaká studený nápoj, ak sa rozhodnú pre cestu k automatu. IoT sa vyvinulo z komunikácie M2M (stroj ku stroju), pri ktorej sa stroje pripájajú k sebe cez sieť bez ľudskej interakcie. M2M sa týka pripojenia zariadenia do cloudu, jeho správy a získavania údajov. Rozvíjajúc M2M na vyššiu úroveň, IoT je senzorová sieť miliárd inteligentných zariadení, ktoré pripájajú ľudí, počítačové systémy a iné aplikácie na zber a zdieľanie údajov.

* + 1. Počiatok 21. Storočia

Na začiatku 21. storočia sa koncept IoT ekosystému stal významným, najmä keď čínska vláda označila IoT za strategickú prioritu v jej päťročnom pláne. Medzi rokmi 2010 a 2019 sa IoT výrazne rozšírilo medzi spotrebiteľmi, keď ľudia stále viac využívali pripojené zariadenia, ako sú smartfóny a smart televízory, ktoré komunikovali cez jednu sieť. Ďalším dôležitým komponentom pri vytváraní funkčného IoT bola udalosť z júna 2012, keď sa hlavní poskytovatelia internetových služieb a webové spoločnosti dohodli na zvýšení adresného priestoru na globálnom Internete aktiváciou protokolu IPV6 pre svoje služby a produkty. V roku 2020 sa počet IoT zariadení aj naďalej zvyšoval, pričom mobilné IoT fungovalo na 2G, 3G, 4G a 5G. V roku 2023 zbierali a zdieľali miliardy pripojených zariadení údaje pre spotrebiteľov a priemysel.

Tab. 1 Porovnanie medzi aktívnymi zariadeniami bez IoT a IoT od roku 2015

|  |  |  |  |
| --- | --- | --- | --- |
| **Rok** | **Zariadenia bez IoT** | **IoT Zariadenia** | **% Zariadení IoT** |
|  |
| **2015** | *9,7 miliárd* | *3,6 miliárd* | *27%* |  |
|  |
| **2016** | *9,8 miliárd* | *4,6 miliárd* | *31,9%* |  |
|  |
| **2017** | *9,9 miliárd* | *6,1 miliárd* | *38,1%* |  |
|  |
| **2018** | *9,9 miliárd* | *8 miliárd* | *44,7%* |  |
|  |
| **2019** | *10 miliárd* | *10 miliárd* | *50%* |  |
|  |

1. Ako fungujú IoT technológie

Kompletný IoT systém integruje štyri odlišné komponenty: senzory/zariadenia, konektivitu, spracovanie údajov a užívateľské rozhranie. Nižšie stručne vysvetlím každý komponent a jeho úlohu.

* 1. Senzory a zariadenia

Kompletný IoT systém integruje štyri odlišné komponenty, pričom senzory a zariadenia hrajú kľúčovú úlohu. Senzory alebo zariadenia zbierajú údaje zo svojho okolia, či už ide o teplotu, tlak alebo dokonca videozáznamy. Je dôležité poznamenať, že v tejto fáze sa údaje získavajú prostredníctvom rôznych typov senzorov, ktoré môžu byť samostatné alebo sú súčasťou multifunkčných zariadení.

* + 1. Konektivita

Po zbere údajov senzory a zariadenia potrebujú spôsob, ako tieto údaje preniesť do cloudu. To sa uskutočňuje prostredníctvom rôznych metód konektivity, ako sú mobilné siete, WiFi, Bluetooth alebo satelitné spojenie. Každá metóda má svoje výhody a nevýhody, ale cieľom je dostať údaje do cloudu bezpečne a spoľahlivo.

* + 1. Spracovanie dát

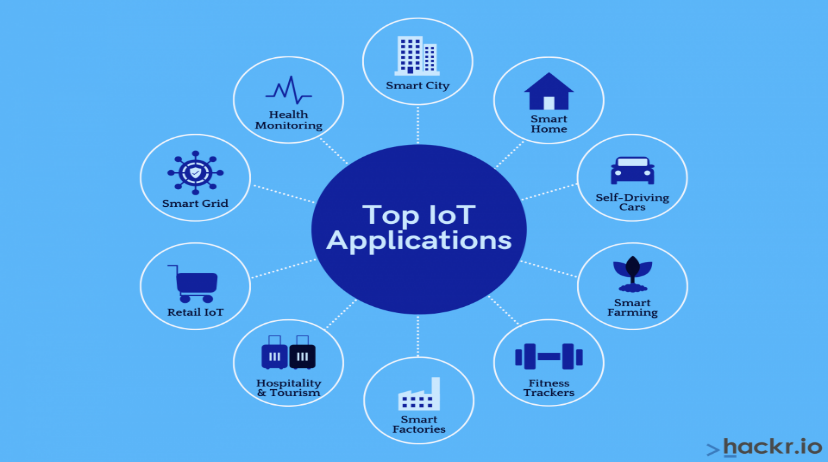
Keď sa údaje dostanú do cloudu, nasleduje ich spracovanie softvérom. Tento softvér môže vykonávať rôzne úlohy, od jednoduchého kontrolovania údajov na ich kompletnú analýzu. To zahŕňa aj identifikáciu anomálií, ako sú príliš vysoké teploty alebo detekcia nežiaducich osôb.

* + 1. Užívateľské rozhranie

Nakoniec, informácie zo spracovaných údajov sú poskytnuté užívateľovi cez užívateľské rozhranie. To môže zahŕňať rôzne formy komunikácie, ako sú e-maily, textové správy alebo notifikácie. Užívateľ tiež môže mať možnosť aktívne ovplyvňovať systém prostredníctvom rozhrania, napríklad vzdialene upravovať nastavenia alebo sledovať živé videonahrávky. Zároveň môže systém automaticky reagovať na určité udalosti bez priameho zásahu užívateľa. To znamená, že IoT systém môže sledovať prostredie a vykonávať príslušné akcie na základe definovaných pravidiel bez potreby manuálneho zásahu.

1. IoT aplikácie

Internet vecí (IoT) ponúka široké spektrum aplikácií, ktoré zasahujú do rôznych oblastí, vrátane spotrebiteľského sektora, podnikania, výroby a IIoT. Tieto aplikácie majú významný vplyv na rôzne vertikály, vrátane automobilového priemyslu, telekomunikácií a energetiky. Môžeme povedať, že sa svet IoT veľmi rýchlo rozvíja a rastie. Toto sú tie najpopulárnejšie a najčastejšie aplikácie IoT.



Obr. 1 Typy IoT aplikácii

* 1. Spotrebiteľský sektor

V IoT spotrebiteľskom segmente sa objavujú inteligentné domácnosti, ktoré zahŕňajú termostaty, spotrebiče a pripojené kúrenie, osvetlenie a elektroniku, ovládané cez počítače a smartfóny. Wearable zariadenia sú vybavené senzormi a softvérom na zbieranie a analýzu údajov používateľov, čo uľahčuje život. Tieto zariadenia sa využívajú aj v oblasti verejnej bezpečnosti, napríklad zlepšujú reakčné časy záchranárov alebo monitorujú vitálne funkcie pracovníkov na nebezpečných miestach. Trend inteligentných domov rastie celosvetovo.

* 1. Zdravotníctvo

IoT aplikácie transformujú zdravotnícke systémy na wellness systémy, zlepšujúc výkon, presnosť a dostupnosť zariadení. Zhromažďujú údaje ako krvný tlak, hladinu cukru v krvi a EKG a umožňujú pacientom kontaktovať lekárov cez smart mobilné aplikácie.

* 1. Inteligentné mestá

Inteligentné mestá využívajú technológie na poskytovanie služieb, ktoré zahŕňajú zlepšenie dopravy a sociálnych služieb, podporu stability a dávajú hlas svojim občanom. IoT aplikácie pomáhajú v oblasti riadenia vody, kontroly odpadov a zvládania núdzových situácií.

* 1. Poľnohospodárstvo

S rastúcim obyvateľstvom do roku 2050, ktoré sa odhaduje na 10 miliárd ľudí, poľnohospodárstvo musí využiť technológie na zlepšenie výnosov. IoT aplikácie v poľnohospodárstve umožňujú monitorovanie skleníkov a automatizáciu zavlažovacích systémov.

* 1. Priemyselná automatizácia

Priemyselná automatizácia je oblasť, kde kvalita výrobkov zohráva kľúčovú úlohu pre väčší návratnosť investícií. IoT sa využíva v monitorovaní toku produktov, digitalizácii tovární, riadení skladov, bezpečnosti a logistike, optimalizácii dodávateľských reťazcov a kontrole kvality.

* 1. Smart autá

Pripojené autá, nazývané aj vozidlá s internetovým pripojením, majú senzory a komunikačné technológie na výmenu údajov s inými zariadeniami. Sú pripojené k verejnej sieti aj k špeciálnym automobilovým sieťam, umožňujúc funkcie ako diaľková diagnostika a aktualizácie softvéru cez vzduch.

Graf. 1 Celosvetové výdavky (€) za IoT technológie v miliardách

1. Návrh a implementácia IoT domu

Návrh a implementácia inteligentného IoT domu začína výberom vhodnej platformy a nástrojov, ktoré umožnia efektívne a spoľahlivé spravovanie a monitorovanie domácich zariadení. Cieľom je vytvoriť inteligentný dom, ktorý bude nielen pohodlný a efektívny, ale aj bezpečný a spoľahlivý. Ako prvý krok sme sa rozhodoli využiť aplikáciu Cisco Packet Tracer, ktorá poskytuje prostredie na simuláciu siete IoT zariadení. Po vytvorení nového projektu sme sa pustilo do navrhovania inteligentného domu, pričom ako východiskový bod sme použili plán mojej chaty. Tento plán nám poskytuje základnú štruktúru a prehľad o existujúcich miestnostiach a ich vzájomných pomeroch či veľkostiach. Následne sme použili dostupné IoT technológie v aplikácii ako napríklad riadenie osvetlenia, kúrenia, alebo monitorovanie energetického spotrebu. Na kresbu plánu domu sme použili v aplikácii dostupnú paletu základných geometrických tvarov. Týmto umožníme presný prehľad miestností, tvaru a rozloženia. Nakoniec sme pridali do každej miestnosti text s označením ako „Obývačka“ či „Spálňa“.

* 1. Implementácia IoT

Po úvodnom návrhu nasleduje fáza implementácie, kde budeme postupne integrovať jednotlivé IoT zariadenia a senzory do IoT siete. Pri implementácii budeme klásť dôraz na zabezpečenie komunikácie medzi zariadeniami a centrálnym riadiacim systémom, aby bola zachovaná bezpečnosť a súkromie mojich domácich údajov. Takto sa začína cesta k vytvoreniu inteligentného IoT domu, ktorý prinesie do môjho každodenného života nové možnosti a vylepšenia v oblasti pohodlia, efektivity a bezpečnosti. Rozhodol som sa, že sieť rozložím na dve časti. Jedna bude prepájať IoT technológie medzi sebou a druhá bude domáca sieť, ktorá bude prepájať telefón, počítače a iné zariadenia. Začneme s prípravou IoT siete. Keďže dnešné moderné siete fungujú bezdrôtovo tak aj naša sieť bude fungovať bezdrôtovo. Packet Tracer nám túto vec umožňuje vo veľkom rozsahu s možnosťou detailnej konfigurácie. Ako druhé budeme potrebovať server, ktorý bude spravovať tieto IoT zariadenia, prístup k nim a ich zabezpečenie pomocou protokolu RADIUS. Aby sme mohli spravovať server ako administrátor, pridám laptop. Nakoniec pridáme switch. Switch bude prepájať server s laptopom a routerom. Dokončíme to prepojením servera, laptopu a routera do switchu priamym ethernetovým káblom. Teraz sme pripravený nakonfigurovať jednotlivé zariadenia.

* + 1. Konfigurácia bezdrôtového routera IoT siete

Použijeme teda dostupný bezdrôtový router WRT300N. V konfigurácii prejdeme do položky pre nastavenie bezdrôtovej site. Prvú položku „SSID“ resp. názov siete som si nastavil na IoT. Na mene nezáleží a môžeme si zvoliť ľubovolné. Pre autentifikáciu cez server sme si vybrali WPA2. To nám odomkne položku pre nastavenie prístupu RADIUS servera. Keďže sme si vybrali IP adresu 192.172.12.1 ako default gateway tak sme sa rozhodoli dať serveru adresu 192.172.12.10 a heslo sme si vybrali cisco123. Následne sme prešli do nastavenia samotného routera v GUI. Nastavili sme routeru ako som už spomínal IP adresu 192.172.12.1 a masku podsiete 255.255.255.0. Aby sme nemuseli pridávať IoT zariadeniam IP adresu manuálne, použijeme na to DHCP protokol. Zariadenia pripojené k tejto sieti si vyžiadajú IP adresu od servera podľa zoznamu dostupných adries. Týmto si uľahčíme veľa práce. Nastavenie dokončíme pridaním bezdrôtového zabezpečenia. Pre zabezpečenie siete pomocou RADIUS servera sa používa WPA2-Enterprise protokol. Siete ako WPA2-Personal umožňujú mať iba jedno heslo, zatiaľ čo WPA2-Enterprise nám umožňuje nastaviť heslo pre každé zariadenie zvlášť. Týmto si zvýšime bezpečnosť. Pre šifrovanie dát a informácií zvolíme najpoužívanejší protokol AES. Týmto sme dokončili nastavenie samotného routera a môžeme prejsť na ďalší krok.

* + 1. Konfigurácia RADIUS servera

IoT aplikácie, správanie a prístup bude spravovať lokálny RADIUS Server. RADIUS servery prijímajú požiadavky na pripojenie používateľov, autentifikujú používateľa a potom vrátia konfiguračné informácie potrebné pre zariadenie klienta, aby poskytlo službu používateľovi. Využíva protokol RADIUS (Remote Authentication Dial-In User Service). Komunikácia medzi klientom a serverom prebieha pomocou protokolu UDP (User Datagram Protocol). Prijíma požiadavky o pripojenie od klientov, autentifikuje používateľov a vráti konfiguračné informácie klientovi, aby mohol poskytnúť službu používateľovi. UDP sa často používa tam, kde je dôležitá rýchlosť a efektívnosť prenosu dát, ale nie je potrebná spoľahlivosť doručenia. UDP neposkytuje mechanizmy na zabezpečenie doručenia správ, kontrolu toku alebo obnovu spojenia, čo znamená, že nie je vhodný pre aplikácie, ktoré vyžadujú spoľahlivé doručenie dát. V tomto prípade na spoľahlivosti nezáleží. Server vyhľadáva používateľov v databáze a ak sa používateľ nájde a heslo je správne, server poskytne prístupové parametre. Je dôležité spomenúť, že RADIUS protokol je typ AAA protokolu. AAA znamená autentifikácia, autorizácia a účtovanie. Autentifikácia zahŕňa overovanie autenticity používateľských alebo zariadení identít. Autorizácia zahŕňa udelenie oprávnení na čítanie, aktualizáciu konfiguračných súborov alebo vykonávanie programov a účtovanie zahŕňa meranie využitia zdrojov používateľa alebo zariadenia v autentifikovanej relácii. Serveru priradím statickú IPv4 adresu. Už pri nastavovaní routeru sme zadali, že IP adresa RADIUS servera bude 192.172.12.10. To znamená, že nastavíme túto statickú IP adresu priamo v serveri. Maska podsiete a default gateway bude rovnaká ako sme zadali v routeri. Týmto je RADIUS server pripojený k sieti. Aby sme registrovali IoT zariadenia a používateľov do siete a aby sme dokázali manažovať tieto zariadenia použijeme na to spomenutý AAA protokol. Začneme vytvorením prístupu pre klienta do systému. Meno klienta si zvolíme ľubovoľne, teda IoT. Keďže sme nastavili IP adresu routera na 192.172.12.1 tak aj adresa klienta bude rovnaká. Heslo bude „cisco123“ a typ serveru nastavíme na „Radius“. Klienta máme úspešne pridaného do systému. Môžeme pridať aj ďalších ale pre tentokrát bude stačiť jeden prístup. Ako ďalšie musíme pridať a registrovať všetky IoT, ktoré chceme mať pripojené k sieti. Cez „User Setup“ v nastaveniach AAA protokolu môžeme pridať meno a heslo. Popridávali sme všetky IoT zariadenia ručne. Meno a heslo sme nastavili rovnaké ako napr. „BedroomLight1“ meno je aj heslo. V sekcii IoT nám už stačí len zapnúť registračný server a nastavenia protokolov RADIUS servera máme hotové.

Posledným krokom bude pripojiť každé IoT zariadenie a registrovať ho v sieti. Dokážeme to tým, že v každom IoT zariadení zapneme DHCP protokol pre priradenie automatickej IP adresy, následne prejdeme do nastavení IoT a v sekcii nastavenia servera pre IoT zvolíme „IoT Server“. Bude si to po nás pýtať tri parametre. Jeden bude IP adresa IoT serveru, ktorá bude 192.172.12.10, druhý bude meno používateľa, čo bude „IoT“ a potom heslo, ktoré sme nastavili na „cisco123“. V bezdrôtovom nastavení vložíme názov IoT siete, ktorý sme si vybrali. Pre autentifikáciu zvolíme WPA2, kde následne vložíme registračné údaje, ktoré sme vytvorili pre IoT zariadenie v RADIUS serveri. To znamená meno klienta a heslo. Ešte pred dokončením si overíme či ú všetky parametre správne zadané. Častokrát sa stáva, že sa zariadenie so sieťou nespojí. Keď sme všetko skontrolovali a je to správne, môžeme prejsť na finálny krok.

* 1. Finalizácia a verifikácia produktu

Predtým než náš produkt môže byť prezentovaný verejnosti, musíme skontrolovať a overiť pripojenie do siete, či zariadenia pracujú a fungujú správne. Začneme teda s pripojením administračného laptopu pre náš IoT server. Na laptope si otvoríme príkazový riadok a zadáme IP adresu nášho serveru. Mnohokrát spomínané, naša IP adresa je 192.172.12.10. Pre overenie pripojenia zadáme príkaz:

ping 192.172.12.10

Ak sme zadali údaje a príkaz správne, malo by nám vypísať toto:

Pinging 192.172.12.10 with 32 bytes of data:

Reply from 192.172.12.10: bytes=32 time<1ms TTL=128

Reply from 192.172.12.10: bytes=32 time<1ms TTL=128

Reply from 192.172.12.10: bytes=32 time<1ms TTL=128

Reply from 192.172.12.10: bytes=32 time<1ms TTL=128

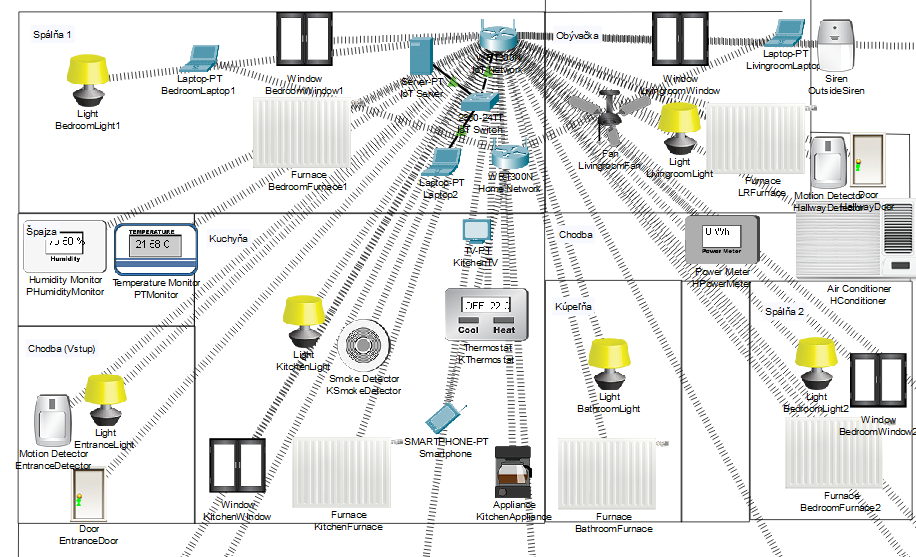
Ping statistics for 192.172.12.10:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

Výsledok nám ukazuje, že všetky zaslané dátové pakety boli úspešne odoslané, prijaté a vrátené späť. Ak sme však dostali iný výsledok, pravdepodobne sme dostali niekde chybu a mali by sme skontrolovať nastavenia siete, laptopu a serveru. Teraz môžeme skontrolovať pripojenie servera k sieti. Otvoríme si opäť príkazový riadok a zadáme ten samý príkaz len tentokrát použijeme IP adresu siete, teda 192.172.12.1. Ak dostaneme rovnakú odpoveď od IP adresy siete tak sme úspešne overili pripojenie. Opäť ak došlo k inej odpovedi, máme to pravdepodobne zle a treba skontrolovať nastavenia. Teraz overme či sa dokážeme cez administračný laptop pripojiť a registrovať na registračnú stránku bežiacu na IoT serveri. V laptope si otvoríme webový prehliadač. Naša webová stránka bude IP adresa RADIUS Servera. Vložíme adresu 192.172.12.10 a dáme vyhľadať. To nás presmeruje na lokálnu stránku panelu pripojených IoT zariadení. Prvé sa musíme registrovať. Registrujeme počítač pod prihlasovacími údajmi klienta, ktorého sme si vytvorili v protokole AAA. Meno si dáme ako „IoT“ a heslo „cisco123“. Hneď ako klikneme na vytvoriť, prejdeme naspäť na prihlásenie a zadáme tie samé údaje. Ak sme všetko urobili správne tak nás to nasmeruje na panel všetkých pripojených IoT zariadení. Ak funguje všetko správne uvidíme tam všetky prihlásené IoT zariadenia. Tu môžeme meniť správanie sa IoT zariadení. Napríklad svetlu môžeme zmeniť status na zapnutý, slabé svetlo a silné svetlo. Pri okne môžeme ho otvárať a zatvárať. Teraz keď nám úspešne naša IoT sieť funguje, tak nám stačí už vytvoriť domácu sieť, kde sa vedia všetky ostatné zariadenia pripojiť a komunikovať. Vytvorením separátnej domácej siete tak zvýšime bezpečnosť, jednoduchosť prístupu a v prípade výpadku jednej zo sietí, nám zostane tá druhá fungovať. Použijeme ten samý bezdrôtový router ako pri vytváraní IoT siete. Tentokrát bude nastavovanie siete veľmi jednoduché. Použijeme už prednastavené hodnoty routera ako je IP adresa routera 192.168.0.1. Zapneme DHCP server, čo nám umožní automatické priradenie IP adries. Dáme si rozsah dostupných adries 50 a masku podsiete 255.255.255.0. Zabezpečenie siete použijeme klasický protokol pre domáce siete, teda WPA2-PSK, ktorý je najpoužívanejší protokol v domácich sieťach a v malých firmách. Tento protokol si po nás bude pýtať aby sme nastavili heslo pre prihlasovanie sa do tejto siete. Názov siete bude „Home“ a heslo „home\_123“. Nakoniec už len stačí aby zariadenia si nastavili názov siete a heslo rovnaké ako sme nastavili domácej sieti, vypnúť ich, vymeniť im module z ethernet drôtového pripojenia na modul pre bezdrôtové pripojenie a naspäť ich zapnúť. Overiť spojenie týchto zariadení môžeme opäť cez terminál pomocou príkazu ping. Týmto sme dokončili nastavenie domácej siete a zariadenia sa vedia úspešne pripojiť k tejto sieti a voľna IP adresa je im pridelená. Týmto je náš produkt hotový a môžeme ho prezentovať.



Obr. 2 Výsledok zapojenia siete zariadení v IoT sieti vo vnútri domu

1. Záver

V našej rozsiahlej práci sme sa s veľkou starostlivosťou a zanietením venovali komplexnému procesu návrhu a implementácie inteligentného domu, ktorý je poháňaný revolučnou technológiou IoT. Od samotných základov IoT sme postupovali k praktickému uskutočneniu projektu v simulovanom prostredí Cisco Packet Tracer. Naším zámerom nebola iba teoretická diskusia, ale konkrétny a aplikovateľný výstup, čo sme dosiahli vytvorením zdokonalenej siete a premenou obyčajnej chaty na sofistikovaný inteligentný dom. S nasadením rôznych IoT zariadení a senzorov sme vytvorili rozsiahlu sieť, ktorá je schopná nielen monitorovať, ale aj riadiť rôzne aspekty domáceho prostredia. Dôrazne sme zdôraznili kľúčový význam zabezpečenia komunikácie a ochrany súkromia údajov v tejto novodobej realite. V priebehu našej práce sme sa zameriavali nielen na technické aspekty, ale aj na bezpečnostné hľadiská a súkromie užívateľov, čím sme demonštrovali náš záväzok k integrite a dôveryhodnosti nášho projektu. Cieľom našej práce bolo nielen vytvoriť statický model inteligentného domu, ale aj predstaviť proces navrhovania a implementácie so zameraním na bezpečnosť a efektívnosť. Výsledkom nášho úsilia je funkčný model inteligentného domu, ktorý výrazne zvyšuje pohodlie, efektívnosť a bezpečnosť života jeho obyvateľov. Významným prínosom nášho projektu je aj fakt, že integrácia IoT technológií do domáceho prostredia otvára dvere k novým možnostiam automatizácie a monitorovania, čo pozitívne ovplyvňuje životný štýl užívateľov. Napriek úspešnej realizácii projektu vidíme stále priestor na ďalšie vylepšenia a rozšírenie funkcií. V budúcnosti plánujeme rozšíriť sortiment dostupných IoT zariadení a senzorov, implementovať pokročilejšie algoritmy na spracovanie údajov a ďalšie bezpečnostné opatrenia na ochranu súkromia používateľov, ako napríklad lepšie nastavenie firewallu, či zvýšená automatizácia. Zhodnotenie všetkých získaných dát a informácií jasne ukazuje, že s rastúcim vývojom IoT technológií a ich širším prijatím sa inteligentné domy stanú ešte dôležitejšou súčasťou našej každodennej reality. Svet sa neustále posúva vpred a je evidentné, že budúcnosť bude silne ovplyvnená touto inovatívnou technológiou. Smelo môžeme predpokladať, že čoskoro budeme žiť v dobe, kedy bude náš svet úplne ovládaný IoT, čo prinesie so sebou nové výzvy, ale aj nekonečné možnosti pre ďalší rozvoj a zlepšenie ľudského života.

Zoznam použitej literatúry

1. ASHTARI, Hossein. Spiceworks - What Is User Datagram Protocol (UDP)? Definition, Working, Applications, and Best Practices for 2022. [online]. Aktualizované: 17. August 2022 [cit. 2024-4-10]. Dostupné na internete: <<https://www.spiceworks.com/tech/networking/articles/user-datagram-protocol-udp/>>
2. BEZOS, Jeff. Amazon AWS – What is IoT?. [online]. [cit. 2024-3-15]. Dostupné na internete: <<https://aws.amazon.com/what-is/iot/>>
3. FOOTE, Keith D. Data Versity – History of IoT. [online]. 2022 [cit. 2024-3-15]. Dostupné na internete: <<https://www.dataversity.net/brief-history-internet-things/>>
4. GRILLIS, Alexander S. TechTarget – IoT. [online]. Aktualizované: August 2023 [cit. 2024-3-15]. Dostupné na internete: < <https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT>>
5. HOWARTH, Josh. Exploding Topics - 80+ Amazing IoT Statistics (2024-2030). [online]. Aktualizované: 15. Apríl 2024. [cit. 2024-4-23]. Dostupné na internete: <<https://explodingtopics.com/blog/iot-stats>>
6. JAISWAL, Sonoo. Javatpoint – Internet of Things Applications. [online]. [cit. 2024-4-3]. Dostupné na internete: <<https://www.javatpoint.com/internet-of-things-applications>>
7. KAUSHIK, Vikas. ReadWrite - Understanding the Internet of Things (IoT) and its Impact on Our Lives. [online]. Aktualizované: 18.7.2023 [cit. 2024-3-16]. Dostupné na internete: <<https://readwrite.com/understanding-the-internet-of-things-iot-and-its-impact-on-our-lives/>>
8. MCCLELLAND, Calum. Medium – IoT History Explained. [online]. 2016 Aktualizované: 20. November 2017 [cit. 2024-3-15]. Dostupné na internete: <<https://medium.com/iotforall/iot-explained-how-does-an-iot-system-actually-work-e90e2c435fe7>>
9. ROBBINS, Chuck. Cisco – Examine how the RADIUS works. [online]. 2001 Aktualizované: 26. Január 2024 [cit. 2024-4-10]. Dostupné na internete: <<https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html>>
10. SHAH, Sakshyam. Teleport – What is AAA Security?. [online]. 2022 [cit. 2024-4-10]. Dostupné na internete: <<https://goteleport.com/blog/aaa-security-protcols-for-network-access/>>
11. TINAIKAR, Ranjit. Ness – IoT Is Everywhere. [online]. [cit. 2024-3-16]. Dostupné na internete: <<https://www.ness.com/iot-is-everywhere-how-iot-is-changing-our-daily-lives>>
12. VAILSHERY SUJAY, Lionel. Statista - Internet of Things (IoT) spending worldwide. [online]. 2023 Aktualizované: 13. Február 2024. [cit. 2024-4-11]. Dostupné na internete: <<https://www.statista.com/statistics/668996/worldwide-expenditures-for-the-internet-of-things/>>
13. YADAV, Aakash. Hackr.io - Top 10 IoT Applications in 2024. [online]. 2022 [cit. 2024-4-20]. Dostupné na internete: <<https://hackr.io/blog/top-10-iot-applications>>