УДК 004

Б.Сопілка, магістр гр. КН-22М-2
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ МЕРЕЖНОГО КЕРУВАННЯ ПОМЕШКАННЯМИ З ВИКОРИСТАННЯМ ПРОТОКОЛУ MODBUS/RTU

У статті розроблено програмне забезпечення, яке призначено для системи мережного керування помешканнями з використанням протоколу Modbus/RTU. Метою розробки є дослідження та програмна реалізація системи мережного керування помешканнями з використанням протоколу Modbus/RTU. Об'єктом дослідження є процес мережного керування помешканнями з використанням протоколу Modbus/RTU. Предметом дослідження є методи мережного керування помешканнями з використанням протоколу Modbus/RTU. Методи дослідження базуються на методах Інтернету речей, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи мережного керування помешканнями з використанням протоколу Modbus/RTU. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

Постановка проблеми. Останнім часом в Україні розвивається будівництво будинків, оснащених системами інтелектуального керування. В Україні, як і в усьому світі, самими популярними об'єктами для впровадження інтелектуальних технологій є комерційна нерухомість (торгові центри, офісні будинки, банки, готелі), державні будинки (вокзали, аеропорти, спортивні й культурні установи), а також об'єкти домашньої автоматизації. У сучасних будинках, насичених інженерним устаткуванням, системи автоматизації й керування виконують функції забезпечення інженерної безпеки експлуатації будинку, інтеграції інженерних систем і, в остаточному підсумку, визначають рівень стійкості функціонування всього об'єкта.

Ідея автоматизації й об'єднання різних систем керування в рамках однієї інтелектуальної системи стимулювала класифікацію об'єктів по двох сегментах:

– автоматизація будинків (Building Automation) – такі об'єкти називають інтелектуальним будинком;

– автоматизація житла (Home Automation) – ці об'єкти звичайно називають системою «Мережне керування помешканнями з використанням протоколу Modbus/RTU».

Автоматизація будинків спрямована, насамперед, на економію ресурсів і зниження експлуатаційних витрат. Автоматизовані системи для житлових будинків мають на увазі створення затишку, комфорту й зручності для його мешканців.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-20] було виявлено певні прогалини у забезпеченні системи мережного керування помешканнями з використанням протоколу Modbus/RTU.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи мережного керування помешканнями з використанням протоколу Modbus/RTU.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем мережного керування помешканнями з використанням протоколу Modbus/RTU.

– Дослідження системи мережного керування помешканнями з використанням протоколу Modbus/RTU.

– Програмна реалізація системи мережного керування помешканнями з використанням протоколу Modbus/RTU.

Об'єктом дослідження є процес мережного керування помешканнями з використанням протоколу Modbus/RTU.

Предметом дослідження є методи мережного керування помешканнями з використанням протоколу Modbus/RTU.

Методи дослідження базуються на методах Інтернету речей, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Забезпечення ефективної роботи локальної мережі «Розумний дім» вимагає вирішення цілого комплексу завдань:

1. Гетерогенність системи: суміщення декількох технологій передачі даних (протоколів).

Отже, система повинна підтримувати декілька технологій передачі даних, тим самим стаючи більш універсальною.

2. Мультидистанційність: управління системою та отримання інформації про її діяльність за допомогою різних каналів передачі даних (SMS сервіс, Інтернет, ПК).

Необхідність отримання інформації про стан будинку, яку надає локальна система «Розумний дім» може бути необхідна в будь-який момент, так само як і необхідність управління системою. Тому актуальним є не лише управління системою з домашнього ПК, що розташований у даній будівлі, а й за допомогою Інтернет чи мобільного зв'язку.

3. Ієрархічність прав користування системою: система розробляється як багатокористувацька, тож доцільним є функція розподілення прав/ролей для користувачів.

Доступ до системи можуть мати декілька користувачів. Це доцільно і для офісних будівель (можуть бути наявні ролі охоронця, прибиральниці, робітника тощо) і для житлових квартир (батьки, дитина). Різні користувачі, що мають доступ до системи можуть мати різні ролі та наділені відповідними праи.

Отже, метою розроблюваної системи є підвищення ефективності та зручності дистанційного та локального управління системою автоматичного контролю параметрів мережі «Розумний дім», розподілення прав/ролей багатокористувацької системи.

Загальна схема роботи розроблюваної системи така:

– центральний мікроконтроллер (або комп'ютер) приймає сигнали від командних пристроїв;

– потім передає ці сигнали виконавчим модулів і систем в будинку;

– виконавчі модулі та системи отримують команди по електромережі, по інфрачервоному або радіоканалу;

– включають або вимикають відповідні пристрої: освітлення, систему охорони, кондиціювання повітря, опалення, подачу води тощо.

Для забезпечення контролю людиною дій системи «Розумний дім» існують такі засоби управління як сенсорні панелі, вимикачі і кнопкові панелі, пульти дистанційного управління, персональний комп'ютер (ПК) тощо. В результаті аналізу існуючих засобів управління з ціллю розвитку та вдосконалення їх щодо розв'язання задач, які булі вказані, обрано ПК.

В ході розробки моделі програмного забезпечення системи визначено основні вимоги до системи:

– підтримка декількох каналів передачі даних від центрального мікроконтролера (GSM, USB, COM, TCP/IP);

– підтримка протоколів передачі даних та команд користувача (Internet, SMTP, POP3, GSM(SMS), TCP/IP);

– авторизація та автентифікація користувачів;

– можливість одночасної роботи з однією системою багатьох користувачів з динамічними рівнями доступу (за допомогою різних протоколів);

– можливість швидкого налагодження системи під окрему систему датчиків та керуючих пристроїв, можливість модифікації схеми.

Проблема одночасної підтримки різних каналів даних вирішена за допомогою використання паралельних потоків. Це значно покращує швидкодію отримання даних, адже програма проводить не послідовне опитування каналів передачі даних на наявність нових повідомлень від центрального контролера, або окремого датчика, а паралельну перевірку каналів. Звичайно, використовувати даний метод краще на ПК на основі багатоядерних процесорів, щоб повністю оцінити всі переваги швидкодії паралельних потоків.

Для вирішення проблеми одночасної роботи з протоколами передачі даних (команд користувача) було використано аналогічний метод. Користувач може завчасно налаштувати ті протоколи, які він буде використовувати та система переходить у стан очікування у паралельних потоках на команду користувача для подальшої їх обробки.

Ієрархічність прав користування системою забезпеченно окремим модулем, за допомогою якого виконується аутентифікація та авторизація користувачів системи. У розроблюваній системі виділено 3 основні групи користувачів: адміністратор (фахівець, що здійснює налагоджування системи), головний користувач (адміністратор серед користувачів) та користувачі з динамічним рівнем доступу.

Розробка структурної схеми

Система "Мережне керування помешканнями з використанням протоколу Modbus/RTU" – це комплекс інтелектуальної автоматики, який керує абсолютно всіма інженерними системами сучасної будівлі, будь то квартира, будинок або офіс. Основні завдання системи "Мережне керування помешканнями з використанням протоколу Modbus/RTU" – це комфорт і безпека. Система управління "Мережне керування помешканнями з використанням протоколу Modbus/RTU" дозволяє централізовано встановлювати – освітлення, температуру, вологість, доступ і безпеку.

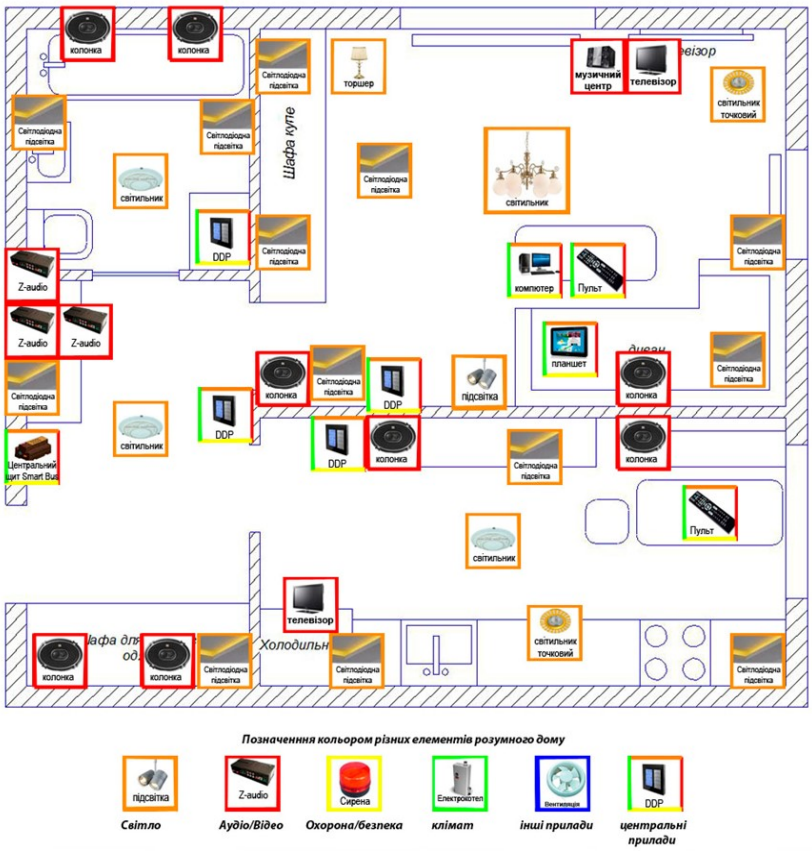

Рисунок 1 – Структура схема системи

Автоматизація «розумного дому» є одним із найкращих варіантів використання технології IoT, оскільки ринок B2C для пристроїв IoT стрімко зріс за останні роки. Цей прискорений інтерес до рішень для розумного дому частково викликаний тим, що через COVID-19 люди почали проводити більше часу вдома та хочуть зробити свої домівки затишнішими та зручнішими.

Розвиток автоматизації розумного будинку: важливість надійних технологій IoT

Наразі клієнти B2C обережно вибирають свого індивідуального партнера з домашньої автоматизації через часті випадки, коли компанії з Інтернету речей раптово припиняють свою діяльність, як це сталося з виробником Інтернету речей Insteon. Керівникам не вдалося продати компанію, і в квітні 2022 року Insteon покинула ринок, навіть не попередивши своїх клієнтів. Через це багато людей мали пристрої IoT, які більше не підтримувалися.

Технології IoT зазвичай включають апаратні та програмні компоненти. У цьому розділі ми зосередимося на розробці додатків домашньої автоматизації для ефективного керування пристроями Інтернету речей. Лише за допомогою правильного поєднання апаратного та програмного забезпечення IoT ви зможете надавати виняткові послуги своїм клієнтам. Розробка безпечних і безперебійно функціонуючих технологій IoT може допомогти вам легше знаходити надійних інвесторів і залучати нових клієнтів.

Але починаючи розробку рішення для розумного будинку, ви можете зіткнутися з багатьма проблемами. Давайте обговоримо, як вирішити хоча б деякі з них.

Як подолати загальні виклики впровадження технологій розумного будинку

Незважаючи на зростаючий ринок B2C IoT, багато людей все ще не готові прийняти системи домашньої автоматизації. У цьому розділі ми обговорюємо загальні проблеми, які заважають користувачам використовувати технології Інтернету речей і вимагають додаткових зусиль і інвестицій від постачальників послуг Інтернету речей.

Високі витрати на впровадження. Коли мова заходить про IoT, це завжди стосується вартості. Коли ми думаємо про рішення для розумного будинку, ми зазвичай уявляємо собі великий футуристичний будинок. Багато людей вважають, що розумні будинки – це ідея майбутнього і що лише багаті можуть дозволити собі технології розумного будинку. Проте ринок IoT розвивався роками, і більшість пристроїв IoT для домашнього використання не коштують цілого стану. Ключовим моментом є розробка простих у навігації та безперебійного функціонування інтелектуальних домашніх систем, щоб виправдати їх вартість для ваших клієнтів. Люди охоче інвестують у високоякісні пристрої IoT, які можуть полегшити їм життя.

Незрозуміле значення. Встановлення пристроїв IoT може здатися радше розвагою, ніж необхідністю. Є пристрої IoT, які використовуються лише для розваг, але є також досить зручні пристрої, які можуть забезпечити безпеку вашого дому, наприклад, коли ви відсутні. Ваше завдання як постачальника послуг IoT полягає в тому, щоб ви надавали цінність своїм клієнтам. Тому під час програмування «розумного будинку» дуже важливо збагатити своє рішення широким і корисним набором функціональних можливостей і постійно вивчати відгуки клієнтів.

Відсутність взаємодії. Незалежно від того, скільки пристроїв IoT у вас є, якщо вони не спілкуються один з одним і ви не можете керувати ними з центрального концентратора, вони не будуть корисними. Важливо надати сучасним клієнтам централізовану платформу управління IoT, яка може служити центром для всіх підключених побутових пристроїв і створювати відчуття інтегрованої та повноцінної системи розумного дому.

Питання безпеки та конфіденційності. Пристрої та рішення IoT часто можуть бути скомпрометовані, якщо вони не захищені належним чином. Користувачі обережно довіряють свої будинки партнерам IoT, які не можуть довести безпеку своїх рішень. Далі в цьому розділі ми обговоримо, як забезпечити безпеку програмного забезпечення IoT. В першу чергу йдеться про налаштування безпечного життєвого циклу розробки програмного забезпечення (S-SDLC) під час розробки програм для iOS або Android для домашньої

автоматизації. Також важливо, щоб рішення Інтернету речей відповідали міжнародним і місцевим актам і нормам із захисту даних, як-от GDPR у Європі.

Різні групи користувачів можуть мати різні причини відмови від впровадження технологій IoT. Вивчіть свою цільову аудиторію та вирішуйте її критичні виклики.

Розглянувши проблеми впровадження розумного дому, тепер ми можемо обговорити випадки використання та функціональні можливості програмних рішень для розумного дому.

Розробка додатків для розумного дому: варіанти використання та функціональні можливості

Функціональні можливості, які ви можете включити у своє програмне рішення IoT, залежать від типу та кількості підтримуваних пристроїв IoT. Незалежно від того, чи є ви виробником пристроїв Інтернету речей чи постачальником програмного забезпечення для Інтернету речей, вам потрібно буде створити програмне забезпечення, яке зможе задовольнити більшість потреб ваших кінцевих клієнтів. Ви можете створити розумний домашній продукт, який може стати системою управління будинком для великого набору пристроїв IoT.

Безпека

Безпека часто є основною причиною, чому клієнти вибирають пристрої IoT. Спостереження за вашим будинком на відстані є однією з переваг рішень IoT. Наприклад, IoT-компанія Netatmo надає користувачам розумні камери спостереження та дверні дзвінки. Netatmo Smart Video Doorbell дозволяє користувачам бачити своїх відвідувачів і розмовляти з ними віддалено.

Netatmo також дозволяє клієнтам керувати всіма своїми пристроями безпеки за допомогою єдиного мобільного додатку, а також отримувати сповіщення в режимі реального часу у разі будь-яких підозрілих дій у будинку або поблизу нього. Віддалений домашній моніторинг варто включити в будь-яке програмне рішення IoT.

Автоматизація домашніх справ

Ще одним популярним варіантом використання пристроїв IoT є автоматизація домашніх справ, що може заощадити багато часу. Існує багато побутової техніки і навіть цілі системи розумного дому, які можуть виконувати домашні справи.

Наприклад, духовка June – це розумна духовка з кількома функціями, якими можна дистанційно керувати з мобільного додатку. Користувачі можуть дистанційно розігрівати свої страви або дивитися відео в прямому ефірі, як вони готуються. Духова шафа має камеру з механізмом розпізнавання їжі, тому, коли їжу поміщають у духовку June, вона визначає, що готується, і пропонує найкращий режим для приготування. Крім того, програма надсилає сповіщення, коли їжа готова.

Іншим прикладом є програма Bosch Home Connect, яка дозволяє клієнтам контролювати всі свої розумні побутові прилади Bosch. Насправді інші виробники, зокрема Siemens, Gaggenau та NEFF, мають подібні програми. Додаток Bosch особливо корисний для керування цілим набором кухонної техніки, щоб спростити процеси приготування та прибирання. Додаток також є чудовим помічником, оскільки пропонує широкий вибір статей та рецептів для спрощення домашніх справ.

Контроль клімату та енергоспоживання

Контроль температури, вологості та якості повітря вдома також вважається важливими функціями домашньої автоматизації. Такі компанії, як Nest і Ecobee, пропонують розумні термостати, які дозволяють регулювати температуру вдома. Ecobee також має функцію eco+, за допомогою якої клієнти можуть попередньо нагрівати та охолоджувати свої домівки перед приходом, підвищуючи енергоефективність. Перегляньте також наш нещодавній проект stromee, створене нами програмне забезпечення для ефективного моніторингу споживання енергії, яке дозволяє користувачам стати більш екологічними, а також заощадити гроші на рахунках за електроенергію.

Пристрої Ecobee не мають власного програмного забезпечення, а підключаються до звичайних рішень, таких як Amazon Alexa, Apple HomeKit і Google Assistant, щоб

забезпечити домашню автоматизацію iOS і Android. Однак використання цих рішень домашньої автоматизації призведе до меншої гнучкості для користувачів і може не дозволити їм отримати доступ до повного потенціалу вашого пристрою. Наприклад, користувачі можуть не мати змоги переглядати історичні графіки температури вдома за певний час.

Розваги

Використання пристроїв IoT для розваг важливо для багатьох клієнтів, особливо для зайнятих сімей з дітьми. Програмні рішення, такі як Roomie Remote, допомагають клієнтам контролювати свої аудіо- та відеосистеми. Використовуючи Roomie Remote, користувачі можуть переглядати аудіо, відео та інші медіа на своєму Apple TV за допомогою жестів або голосу. Крім розважальних функцій, Roomie Remote допомагає користувачам контролювати інші пристрої, такі як термостати, камери спостереження та освітлення.

У наступних розділах ми обговоримо, як створити масштабоване, безпечне та привабливе програмне забезпечення для домашньої автоматизації.

Як побудувати систему розумного будинку

Існує багато виробників пристроїв IoT. Причому у користувачів часто є кілька пристроїв від різних виробників. Їм може бути незручно використовувати окремий мобільний додаток або веб-платформу для кожного пристрою. Набагато простіше, коли всі пристрої IoT підключені, спілкуються один з одним за допомогою єдиного протоколу зв'язку та керуються ними через централізовану платформу IoT.

У попередній статті ми розглянули основні аспекти віддаленого керування Інтернетом речей для мереж великих пристроїв. Ви можете прочитати цю статтю, якщо плануєте надавати свої послуги IoT не лише клієнтам B2C, але й великим підприємствам.

У цьому розділі ми обговорюємо три аспекти розробки системи управління розумним будинком:

– Налаштування хмарного середовища для збору та зберігання даних IoT

– Забезпечення безпеки програмного забезпечення IoT відповідно до галузевих стандартів

– Увімкнення аналізу та візуалізації даних IoT

Хмарна обробка та зберігання даних IoT

Забезпечення належного агрегування, обробки та зберігання даних IoT є важливим елементом у створенні систем управління IoT. Оскільки дані IoT є неструктурованими та часто генеруються в реальному часі, необхідно створити відповідне хмарне середовище. Кілька сервісів AWS, як-от AWS IoT Core та AWS IoT Device Management, дозволяють підключати стільки пристроїв IoT до хмари, скільки необхідно. Ви також можете розглянути нашу статтю про обробку даних у реальному часі, щоб отримати більше інформації про керування даними в реальному часі.

Найбільш підходящим сервісом для зберігання даних IoT є відро Amazon S3 або озеро даних. Озера даних можуть зберігати величезні обсяги неструктурованих даних. У нашому детальному посібнику зі сховищ даних ми обговорюємо, чим озеро даних відрізняється від інших систем зберігання даних, і розповідаємо про його переваги для підприємств.

Щоб навести вам приклад успішного запуску системи IoT у хмарі, ми обрали виробника електроніки Belkin, який почав випускати набір пристроїв для автоматизації розумного будинку. Оскільки кількість розумних домашніх пристроїв і клієнтів зростала, керівництво Belkin зрозуміло, що локальна архітектура компанії IoT не може впоратися з навантаженням, тому вони вирішили перейти на хмарну архітектуру. Результати цього рішення були вражаючими:

Життєвий цикл розробки програмного забезпечення (SDLC) був скорочений більш ніж на 40 відсотків, з 12 місяців до 6,5 місяців.

Компанія заощадила від 30 до 40 відсотків на операційних витратах

Для RAKwireless, виробника пристроїв IoT, ми створили масштабоване рішення IoT за допомогою сервісів AWS IoT Core та AWS Lambda. Завдяки нашому рішенню RAKwireless

вдалося скоротити час, витрачений на налаштування та обслуговування мережі IoT, і тепер вона готова надавати свої послуги набагато більшій кількості підприємств.

Хмарні обчислення можуть бути правильним вибором для розробки вашої платформи управління IoT, якщо ви очікуєте, що ваша компанія буде масштабуватися. Як ми бачили з Belkin, хмарні рішення також скорочують тривалість SDLC і допомагають оптимізувати ваші інвестиції в розробку програмного забезпечення IoT. Насправді серед постачальників послуг Інтернету речей зростає тенденція переносити свою інфраструктуру в хмару. Отже, якщо ви тільки виходите на ринок Інтернету речей, варто створити надійну хмарну інфраструктуру з самого початку, щоб уникнути майбутніх труднощів із хмарною міграцією.

Як зробити програму домашньої автоматизації максимально безпечною

У цьому розділі ми наголошували на тому, що вам слід звернути увагу на розробку максимально безпечної системи розумного дому. Нікому не буде приємно дізнатися, що його камеру спостереження зламали, і тепер будь-хто може проникнути в їхній будинок непоміченим. Щоб випускати безпечні продукти IoT, важливо дотримуватися принципів безпеки на всіх етапах SDLC.

Крім того, може бути корисним дотримуватися певного набору галузевих стандартів, наприклад, архітектури безпеки платформи (PSA).

Відповідно до PSA розробник розумного дому має виконати чотири важливі кроки для розробки безпечного програмного забезпечення IoT.

Аналізуйте. Під час цього кроку команда розробників програмного забезпечення повинна скласти список вимог безпеки за допомогою методів моделювання загроз і виявлення вразливостей.

Архітектор. Цей крок вимагає розробки архітектури безпеки, яка відповідає вимогам PSA та десяти цілям безпеки PSA.

Реалізувати. Наступним кроком є створення програмного забезпечення з архітектурою безпеки та забезпечення безпеки апаратного забезпечення. Також важливо встановити безпечний зв’язок між пристроями IoT і програмними рішеннями.

Сертифікувати. Отримання сертифікату PSA в кінцевому підсумку пов’язане з безпекою технологій IoT. Захист вашої мережі IoT відповідно до стандартів PSA пропонує не лише додатковий захист, але й слугує перевагою продажу, доводячи вашим клієнтам, що ви дбаєте про якість своїх послуг.

Рішення IoT складаються з апаратних і програмних компонентів, і засоби контролю безпеки для них відрізняються. Насправді не існує універсального підходу до безпеки для систем Інтернету речей, тому необхідно налаштувати елементи керування безпекою для кожного апаратного та програмного продукту.

Засоби безпеки для апаратного забезпечення IoT

Безпечне завантаження. Це процес перевірки мікропрограми пристрою IoT за допомогою криптографічних хеш-алгоритмів. Щоб забезпечити Secure Boot, пристрій запрограмовано на ключі безпеки та підписи.

Корінь довіри. Для середовища Secure Boot також потрібен Root of Trust, набір ідентифікаційних і криптографічних ключів, вбудованих в обладнання IoT. Корінь довіри зазвичай вважається серцем пристрою IoT.

Автентифікація пристрою. Кожен пристрій у мережі IoT повинен пройти процедуру автентифікації перед підключенням до шлюзу, щоб переконатися, що він не зламаний і йому можна довіряти.

Алгоритми шифрування. Щоб забезпечити високий рівень безпеки системи IoT, ви можете використовувати комбінацію симетричних і асиметричних алгоритмів шифрування. Наприклад, асиметричний алгоритм RSA і симетричний алгоритм Blowfish можуть бути добре реалізовані в апаратному забезпеченні IoT завдяки низькому енергоспоживанню.

Шифрування точка-точка. Дуже важливо шифрувати дані з моменту їх захоплення пристроєм Інтернету речей, доки ці дані не досягнуть точки дешифрування, наприклад шлюзу Інтернету речей або хмарного середовища.

Засоби безпеки для програмного забезпечення IoT

Безпека маршрутизації. Шифрування та хешування таблиць маршрутизації з даними, що зберігаються в маршрутизаторі, а також підтримка багатошляхової маршрутизації даних допомагають покращити безпеку даних IoT і підвищити відмовостійкість мережі IoT.

Захист даних користувача. Щоб уникнути несанкціонованого доступу до системи та забезпечити конфіденційність даних користувача, ви повинні встановити механізми автентифікації та перевірки особи у своєму програмному забезпеченні IoT.

Списки контролю доступу (ACL). Ще одним корисним рішенням для захисту додатків IoT є створення списків керування доступом (ACL), які містять політики та вказівки щодо дозволів для того, хто може отримати доступ до мережі IoT. Списки керування доступом можуть надавати доступ до системи або блокувати її для внутрішніх і зовнішніх користувачів системи.

Брандмауери. Додатковим заходом безпеки є встановлення брандмауерів. Це рішення використовується для блокування несанкціонованого доступу та спроб журналювання, якщо механізми автентифікації та ACL вийшли з ладу або зламані.

Програми захисту. Антивірусні та антишпигунські програми можуть бути додатковим заходом безпеки, який може врятувати систему IoT від потенційних зловмисних атак.

Наведений вище список елементів керування безпекою можна змінювати залежно від потреб кожного конкретного проекту IoT. Крім усіх засобів контролю безпеки, ви та ваша команда розробників програмного забезпечення повинні регулярно проводити сесії з оцінки ризиків і довірчого управління.

Аналітика та візуалізація даних IoT

Пропонувати послуги аналізу та візуалізації даних IoT необов’язково, але це може дати вам конкурентну перевагу. Однак такі послуги можуть вимагати більше зусиль від вашої команди розробників програмного забезпечення, оскільки звичайні інструменти бізнес-аналітики та аналітики можуть не підтримувати аналіз даних IoT через неструктурований характер даних IoT.

У цьому випадку ми віддаємо перевагу сервісу AWS IoT Analytics. Він автоматизує всі етапи аналізу даних IoT. Цей сервіс також підключається до Amazon QuickSight, який дозволяє візуалізувати дані за допомогою алгоритмів машинного навчання. Неструктуровані дані IoT надходять у необробленому форматі та можуть мати прогалини та помилкові показання, а AWS IoT Analytics очищає дані перед виконанням подальшого аналізу.

Ключові переваги служб аналізу даних IoT:

– Дані IoT не просто збираються, але й генерують уявлення та допомагають клієнтам краще побачити відчутну цінність їх мережі IoT.

– Збагачення аналізу даних IoT даними із зовнішніх джерел, наприклад прогнозів погоди, може допомогти клієнтам передбачити, як регулювати температуру вдома.

– Функціонал аналізу даних IoT також може дозволити клієнтам підвищити ефективність свого дому, бачачи закономірності в продуктивності домашніх пристроїв.

Останнім аспектом розробки програмного забезпечення для розумного дому є унікальний дизайн UI/UX, який може або привернути клієнтів, або відштовхнути їх.

UI/UX дизайн у розробці домашньої автоматизації

Користувачі очікують вдосконаленого дизайну інтерфейсу користувача/UX від рішень автоматизації розумного будинку. Завантажуючи нову цифрову банківську програму зі свого традиційного банку, користувачі можуть пробачити певні недоліки дизайну, якщо програма виконує важливі банківські послуги. Але коли мова йде про програмне забезпечення для розумного дому, користувачі очікують чогось іншого та футуристичного. У той же час вони очікують, що додаток буде зручним і корисним.

Важливим аспектом, який відрізняє дизайн домашньої автоматизації IoT від проектування інших рішень, є прямий зв’язок між цифровим і фізичним світами. Розробникам потрібно знайти способи зробити так, щоб програмне забезпечення IoT полегшувало використання фізичних пристроїв IoT, а не викликало плутанину.

Скевоморфний дизайн більше не є варіантом, але принаймні невелика схожість між цифровим і фізичним світом IoT повинна бути збережена.

Наприклад, у додатку, який ми розробили для нашого клієнта, дизайнери відобразили термостат так, як він виглядає у фізичному світі, щоб користувачі інтуїтивно зрозуміли, як збільшити або зменшити температуру в своєму домі. І, природно, вони вирішили позначити функцію управління світлом за допомогою лампочки.

Ми підготували кілька порад, які допоможуть вам створити належний дизайн інтерфейсу користувача/користувача користувача для програмного забезпечення IoT:

– Включіть чітку адаптацію користувача. Налаштування середовища IoT може бути проблемою для нетехнічних користувачів, тому ваше завдання – зробити їхню подорож максимально зрозумілою та простою. Ви можете включити захоплюючі аудіо- та візуальні елементи в дизайн вашої системи домашньої автоматизації, які направлятимуть користувачів через процес адаптації.

– Зробіть свій дизайн інклюзивним. Якщо припустити, що ви хочете надати свої продукти IoT якомога більшій кількості людей, вам потрібен інклюзивний дизайн. Наприклад, дуже важливо зробити ваше програмне забезпечення зрозумілим для людей із вадами зору або глухими.

– Додайте інтерактивні чат-боти для вирішення проблем. Щоб зменшити рівень розчарування користувачів, коли вони стикаються з проблемами своїх розумних домашніх пристроїв, ви можете створити інтерактивний чат-бот, який легко знайти. Приділяти особливу увагу розробці функцій усунення несправностей має вирішальне значення для програмного забезпечення IoT, оскільки простого екрана з інструкціями у звичайному тексті або просто кнопки для запиту підтримки може бути недостатньо.

– Вибирайте футуристичні кольори, форми та шрифти. Пристрої IoT асоціюються з технологіями майбутнього, тому було б чудово, щоб ваше програмне забезпечення виглядало футуристично, як ми зробили з додатком ConnectHome.

Поєднання технологій хмарних обчислень, належного контролю безпеки та привабливого дизайну UI/UX може допомогти вам розробити надійне програмне забезпечення IoT. Але обов’язково зосередьтеся також на апаратних компонентах, щоб ваші клієнти могли якомога плавніше поєднувати фізичний і цифровий світи. Обов’язково довірте свій IoT-проект надійному та досвідченому партнеру з розробки програмного забезпечення, який має продуктове мислення.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів мережного керування помешканнями з використанням протоколу Modbus/RTU. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем мережного керування помешканнями з використанням протоколу Modbus/RTU; Досліджена система мережного керування помешканнями з використанням протоколу Modbus/RTU; На основі отриманих результатів досліджень створена програмна реалізація системи мережного керування помешканнями з використанням протоколу Modbus/RTU. Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання мережного керування помешканнями з використанням протоколу Modbus/RTU. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». Advanced Information Systems, 2023, 7(2), pp. 49-56.
2. Kuznetsov, O., Kuznetsova, Y., Smirnov, O., Kostenko, O., Zvieriev, V. «Evaluating Hashing Algorithms in the

Age of ASIC Resistance». CEUR Workshop Proceedings, 2023, 3628, pp. 93-105.
3. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchev, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
4. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». Lecture Notes on Data Engineering and Communications Technologies, 2023, 178, pp. 208–223.
5. Smirnova, T., Gnatyuk, S., Yudin, O., Sydorenko, V., Polozhentsev, A., «The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems». CEUR Workshop Proceedings Volume 3156, 2022, Pages 390-399.
6. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools». Communications in Computer and Information Science, 2021, vol 1486. Springer, Cham. pp 169-184.
7. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
8. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346.
9. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
10. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.
11. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». CEUR Workshop Proceedings Volume 2616, 2020, Pages 125-136.
12. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379.
13. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.
14. Smirnov O. Kuznetsov A., Zaicenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.
15. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
16. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.
17. Smirnov, O., Odarchenko, R., Abakumova, A., Usik, P., Kundyz, M., «QoE optimization technique for media delivery in 5G networks». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019. P.597-601.
18. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». CEUR Workshop Proceedings, Vol 2588, P. 90-106, 2019.
19. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation Properties», 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019/ Lviv, Ukraine, 2-6 July, 2019, P. 395-399.
20. Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 353-358.
21. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 347-352.
22. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», CEUR Workshop Proceedings Volume 2353, CEUR Workshop Proceedings 2019, Pages 618-629.
23. Smirnov A.A., Kuznetsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», Telecommunications and Radio Engineering. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78.