ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до бакалаврської роботи
на тему:

«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ПОБУДОВИ ЗАХИЩЕНОЇ СЕНСОРНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ ОБЛАДНАННЯ RASPBERRY PI»

Виконала студентка 4 курсу, групи БСД-43
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Іваненко П.О.
(прізвище та ініціали)
Керівник Довженко Н.М.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ-2023

ВСТУП

Актуальність дослідження. В нинішню цифрову епоху сенсорні мережі все частіше використовуються в різних сферах, таких як охорона здоров'я, моніторинг навколишнього середовища, промислова автоматизація, розумні будинки та кібербезпека. Системи розподілених датчиків здатні контролювати, збирати дані з широкого діапазону фізичних умов і умов навколишнього середовища, виявляти зловмисників, відстежувати переміщення і надавати сповіщення у реальному часі у разі підозрілої активності.

Raspberry Pi є важливими у сфері кібербезпеки завдяки своїй універсальності та низькій вартості, що робить його привабливим інструментом як для професіоналів, так і для любителів. Є багато шляхів використання цього обладнання у сфері кібербезпеки. Raspberry Pi можна використовувати як портативну платформу для проведення тестування на проникнення та оцінки вразливостей або створення інструментів моніторингу безпеки мережі, таких як системи виявлення вторгнень (IDS), системи аналізу мережевого трафіку (NTA) і honeypots. Також, Raspberry Pi є гарним прикладом збору та аналізу даних розвідки про загрози з різних джерел, таких як розвідка з відкритим кодом (OSINT) і моніторинг даркнету.

Дослідження такої важливої теми, як сенсорні мережі на базі Raspberry Pi може сприяти підвищенню безпеки, покращенню ефективності та надійності та сприянню їх широкому використанню.

Об'єкт дослідження — сенсорна мережа.

Предмет дослідження — побудова захищеної сенсорної мережі з використанням обладнання Raspberry Pi.

Мета роботи — розробка рекомендацій щодо створення захищеної сенсорної мережі за допомогою Raspberry Pi.

Завдання бакалаврської роботи:

— дослідити поняття сенсорна мережа, її компоненти та архітектуру;

— проаналізувати поширені види атак на сенсорні мережі та знайти шляхи їх мінімізації;

— розглянути історію Raspberry Pi, його протоколи безпеки та проаналізувати механізми безпеки;

— розробити рекомендації щодо побудови захищеної сенсорної мережі з використанням Raspberry Pi.

Методи дослідження – опрацювання технічної літератури за даною темою, аналіз експлуатаційної документації інструментів, проведення експлуатації інструментів.

Практичне значення одержаних результатів: рекомендації щодо побудови захищеної сенсорної мережі з використанням Raspberry Pi можуть бути використані у сфері забезпечення кібербезпеки у персональних та корпоративних інформаційних системах.

1 АНАЛІЗ ОСОБЛИВОСТЕЙ ФУНКЦІОНУВАННЯ СЕНСОРНИХ МЕРЕЖ

1.1 Огляд сенсорних мереж

Сенсорна мережа — це група взаємопов’язаних сенсорних пристроїв, які призначені для збору даних із навколишнього середовища, їх обробки та передачі в центральне місце для подальшого аналізу чи дії. Основною метою сенсорної мережі є моніторинг і збір даних про фізичні або екологічні умови території [1].

Сенсорні мережі складаються з різноманітних компонентів, які разом збирають і обробляють дані з фізичного світу. Ці компоненти можна розділити на три основні категорії: сенсорні пристрої, комунікаційні модулі та обчислювальні вузли.

Датчики. Датчики використовуються бездротовими сенсорними вузлами для збору даних із середовища. Це апаратні пристрої, які виробляють вимірну реакцію на зміну фізичного стану, наприклад температури чи тиску. Датчики вимірюють фізичні дані параметра, що підлягає моніторингу, і мають певні характеристики, такі як точність, чутливість тощо. Безперервний аналоговий сигнал, створений датчиками, оцифровується аналого-цифровим перетворювачем і надсилається до контролерів для подальшої обробки. Деякі датчики містять необхідну електроніку для перетворення необроблених сигналів у показання, які можна отримати через цифрове з’єднання (наприклад, I2C, SPI), а багато з них перетворюють в одиниці, наприклад °C. Більшість сенсорних вузлів мають малі розміри, споживають мало енергії, працюють у високих об’ємних щільностях, автономні та працюють без нагляду, а також адаптуються до навколишнього середовища. Оскільки бездротові сенсорні вузли, як правило, є дуже маленькими електронними пристроями, їх можна обладнати лише обмеженим джерелом живлення менше ніж 0,5-2 ампер-години та 1,2-3,7 вольт.

Датчики поділяються на три категорії: пасивні, всенаправлені датчики; пасивні, вузькопроменеві датчики; і активні датчики.

Пасивні датчики сприймають дані без фактичного маніпулювання навколишнім середовищем шляхом активного зондування. Вони мають автономне живлення; тобто енергія потрібна тільки для посилення їх аналогового сигналу.

Активні датчики активно досліджують навколишнє середовище, наприклад, ехолот або радар, і їм потрібна постійна енергія від джерела живлення.

Вузькопроменеві датчики мають чітко визначене поняття напрямку вимірювання, подібно до камери. Всенаправлені датчики не мають поняття напрямку, задіяного у своїх вимірюваннях.

Більшість теоретичних робіт щодо бездротових мереж передбачає використання пасивних всенаправлених датчиків. Кожен сенсорний вузол має певну зону охоплення, для якої він може надійно та точно повідомляти про конкретну величину, яку він спостерігає. Декілька джерел споживання енергії в датчиках: дискретизація сигналу та перетворення фізичних сигналів в електричні, формування сигналу та аналого-цифрове перетворення.

Деякі з часто використовуваних сенсорних пристроїв у сенсорних мережах включають:

Датчики температури: ці датчики використовуються для вимірювання температури навколишнього середовища.

Датчики вологості: ці датчики використовуються для вимірювання вологості навколишнього середовища.

Датчики світла: ці датчики використовуються для вимірювання інтенсивності світла в навколишньому середовищі.

Акселерометри: ці датчики використовуються для вимірювання прискорення об’єктів у навколишньому середовищі.

Камери: ці датчики використовуються для захоплення візуальної інформації про навколишнє середовище.

Мікрофони: ці датчики використовуються для захоплення звукової інформації про навколишнє середовище.

Процесор. Процесор є мозком сенсорної мережі. Він відповідає за обробку даних, зібраних датчиками, і прийняття рішень на основі цих даних. Процесори

можуть бути вбудовані в самі датчики або розташовані в центральному концентраторі, залежно від програми.

Процесор також може виконувати об’єднання даних, що передбачає об’єднання даних від кількох датчиків для підвищення точності вимірювань. Алгоритми злиття даних розроблені для усунення помилок, зменшення шуму та підвищення надійності мережі датчиків.

Комунікація. Комунікація є важливим компонентом сенсорної мережі. Це дозволяє датчикам передавати дані на інші пристрої в мережі або на центральний сервер або хмарну платформу. Бездротовий зв’язок є найпоширенішою формою зв’язку в сенсорних мережах, оскільки він більш гнучкий і економічно ефективний, ніж дротовий зв’язок.

Бездротовий зв’язок може бути досягнутий за допомогою різних технологій, таких як Wi-Fi, Bluetooth, Zigbee та LoRaWAN. Кожна технологія має свої переваги та недоліки, і вибір технології залежить від застосування.

Джерело живлення. Джерело живлення є ще одним важливим компонентом сенсорної мережі. Датчики зазвичай є малопотужними пристроями, призначеними для роботи від батареї або невеликого джерела живлення. Джерело живлення має бути надійним і довговічним, оскільки заміна батарей або підзарядка датчиків може бути дорогим і трудомістким [2].

Для сенсорних мереж доступні різні варіанти живлення, наприклад сонячна енергія, збір енергії та довговічні батареї. Вибір джерела живлення залежить від застосування та розташування датчиків.

1.2 Архітектура сенсорних мереж

У сенсорній мережі зв’язок має вирішальне значення, оскільки очікується, що вузли будуть передавати дані на центральний вузол або базову станцію. Стек протоколів у сенсорній мережі визначає правила та процедури, які вузли використовують для зв’язку один з одним.

Стек протоколів у сенсорній мережі можна розділити на п’ять рівнів, а саме фізичний рівень, канальний рівень, мережевий рівень, транспортний рівень і прикладний рівень.

Фізичний рівень. Фізичний рівень є найнижчим рівнем у стеку протоколів і відповідає за передачу бітів через фізичне середовище. Цей рівень відповідає за вибір частоти, генерацію несучої частоти, виявлення сигналу, модуляцію та шифрування даних. IEEE 802.15.4 пропонується як типовий для низьких швидкісних окремих областей і бездротових сенсорних мереж із низькою вартістю, енергоспоживанням, щільністю, дальністю зв’язку для покращення терміну служби батареї. CSMA/CA використовується для підтримки зіркоподібної та однорангової топології. Існує декілька версій IEEE 802.15.4.V.

Основні переваги використання такого типу архітектури в сенсорних мережах полягають у тому, що кожен вузол просто передбачає передачу на меншу відстань із низькою потужністю до сусідніх вузлів, через що споживання електроенергії є низьким порівняно з іншими видами архітектури сенсорної мережі. Цей тип мережі є масштабованим, а також має високу відмовостійкість.

Канальний рівень. Канальний рівень відповідає за надійну передачу даних між вузлами. Він відповідає за виявлення та виправлення помилок у даних, які передаються через фізичний носій. Канальний рівень також забезпечує механізм для синхронізації вузлів, керування потоком і адресації. У сенсорній мережі вузли використовують різні протоколи канального рівня, такі як ZigBee, Bluetooth Low Energy (BLE) і IEEE 802.15.4.

Канальний рівень розділений на два підрівні: підрівень керування логічним зв’язком (LLC) і підрівень керування доступом до середовища (MAC). Підрівень LLC забезпечує загальний інтерфейс для протоколів вищого рівня, тоді як підрівень MAC керує доступом до фізичного середовища.

Підрівень керування доступом до медіа (MAC): Підрівень MAC відповідає за керування доступом до фізичного середовища. Він відповідає за те, щоб кілька вузлів могли отримати доступ до фізичного середовища, не викликаючи зіткнень. Підрівень MAC використовує різні методи для керування доступом до фізичного

середовища, такі як множинний доступ з розділенням часу (TDMA), множинний доступ з розділенням частот (FDMA) і множинний доступ з визначенням несучої з виявленням колізій (CSMA/CD).

Підрівень Logical Link Control (LLC): Підрівень LLC забезпечує загальний інтерфейс для протоколів вищого рівня. Він відповідає за керування передачею даних між підрівнем MAC і мережевим рівнем. Підрівень LLC забезпечує механізми виявлення та виправлення помилок, щоб забезпечити точне передавання та отримання даних. Підрівень LLC також забезпечує механізми керування потоком для керування передачею даних між підрівнем MAC і мережевим рівнем.

Мережевий рівень. Мережевий рівень відповідає за маршрутизацію даних між вузлами сенсорної мережі. Він забезпечує механізм для пошуку найкращого шляху між вузлами та гарантує, що дані доставляються до призначеного пункту призначення. Мережевий рівень також забезпечує механізм контролю перевантажень і управління якістю обслуговування (QoS). У сенсорній мережі вузли використовують різні протоколи мережевого рівня, такі як Ad-hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR) і Destination-Sequenced Distance-Vector (DSDV) [3].

Мережевий рівень забезпечує механізм адресації вузлів у мережі. Кожному вузлу призначається унікальна адреса, яка використовується для його ідентифікації в мережі. У сенсорних мережах найбільш часто використовуваною схемою адресації є 16-розрядна адреса IEEE.

Мережевий рівень відповідає за маршрутизацію пакетів даних від вихідного вузла до вузла призначення. У сенсорних мережах використовуються різні протоколи маршрутизації залежно від топології мережі та конкретних вимог до мережі.

В ієрархічній маршрутизації вузли організовані в ієрархію, де вузли вищого рівня відповідають за маршрутизацію пакетів даних між вузлами нижчого рівня. Це зменшує накладні витрати, пов’язані з маршрутизацією у великих мережах, і покращує масштабованість мережі.

У маршрутизації на основі розташування вузли використовують своє фізичне розташування для визначення оптимального маршруту для пакетів даних. Це зменшує накладні витрати, пов'язані з обслуговуванням таблиць маршрутизації, і підвищує ефективність мережі.

Мережевий рівень забезпечує механізми контролю перевантаження, щоб забезпечити ефективну роботу мережі в умовах інтенсивного трафіку. У сенсорних мережах найбільш часто використовуваним механізмом контролю перевантаження є механізм керування на основі швидкості. У цьому механізмі вузли в мережі відстежують швидкість трафіку та відповідно регулюють швидкість передачі, щоб уникнути перевантаження.

Мережевий рівень забезпечує механізми якості обслуговування, щоб гарантувати, що мережа відповідає конкретним вимогам програми. У механізмі пріоритетів пакетам даних призначається пріоритет на основі їх важливості, а вузли в мережі визначають пріоритет передачі пакетів даних на основі їх пріоритету.

Транспортний рівень. Транспортний рівень у сенсорних мережах відповідає за забезпечення надійної наскрізної передачі даних між вузлами джерела та призначення. Це важливий рівень, який відіграє вирішальну роль у забезпеченні своєчасної та ефективної доставки даних від вузлів датчиків до базової станції [3].

Функції транспортного рівня в сенсорних мережах:

Сегментація: транспортний рівень у сенсорних мережах сегментує дані на менші одиниці для передачі. Ця сегментація допомагає оптимізувати використання мережевих ресурсів, таких як пропускна здатність, енергія та пам’ять.

Контроль помилок: транспортний рівень у сенсорних мережах забезпечує механізми контролю помилок для забезпечення надійної передачі даних. Це включає механізми виявлення та виправлення помилок, які допомагають виявляти та виправляти помилки, які можуть виникнути під час передачі даних.

Контроль потоку: транспортний рівень у сенсорних мережах забезпечує механізми керування потоком, які регулюють швидкість передачі даних. Це

допомагає запобігти перевантаженню мережі та гарантує, що дані передаються зі швидкістю, яку можуть обробити приймальні вузли.

Контроль перевантаження: транспортний рівень у сенсорних мережах забезпечує механізми контролю перевантаження, які керують потоком даних, щоб запобігти перевантаженню мережі. Це допомагає підтримувати оптимальну продуктивність мережі та гарантує, що дані передаються своєчасно та ефективно.

Прикладний рівень. Прикладний рівень є найвищим рівнем у стеку протоколів і відповідає за реалізацію конкретних прикладних протоколів. Він забезпечує механізм для вузлів для спілкування один з одним на основі типу програми, що використовується. У сенсорній мережі вузли використовують різні протоколи прикладного рівня, такі як Constrained Application Protocol (CoAP), Message Queuing Telemetry Transport (MQTT) і Advanced Message Queuing Protocol (AMQP).

Основною функцією прикладного рівня є збір даних із сенсорної мережі. Збір даних передбачає отримання даних з різних датчиків у мережі та передачу їх користувачеві. У сенсорних мережах використовуються різні протоколи збору даних залежно від характеру даних, що збираються, і конкретних вимог програми

У деяких програмах необхідно агрегувати дані з кількох датчиків, щоб отримати значущу інформацію. Агрегація даних передбачає об’єднання даних з кількох датчиків для формування більш повної картини середовища, що контролюється. Протоколи агрегації даних використовуються для забезпечення ефективного й точного збору та обробки даних

Об’єднання даних – це техніка, яка передбачає об’єднання даних із кількох джерел для підвищення точності та надійності даних. У сенсорних мережах об’єднання даних використовується для об’єднання даних із кількох датчиків для забезпечення більш точного представлення середовища, що контролюється. Залежно від конкретних вимог програми використовуються різні методи об’єднання даних.

Після того, як дані зібрані, узагальнені та об’єднані, їх потрібно поширити користувачеві. Протоколи поширення даних використовуються для передачі

даних від сенсорної мережі до користувача. Ці протоколи можуть включати механізми для стиснення даних, шифрування та виправлення помилок для забезпечення ефективної та безпечної передачі даних.

У деяких програмах необхідно виявляти певні події в середовищі, яке контролюється. Протоколи виявлення подій використовуються для моніторингу даних, зібраних із датчиків, і ідентифікації подій, які відповідають певним критеріям. Ці протоколи можуть включати алгоритми для розпізнавання образів і виявлення аномалій.

Локалізація — це процес визначення фізичного розташування датчика в мережі. Протоколи локалізації використовуються для визначення розташування датчиків у мережі та надання цієї інформації користувачеві. Цю інформацію можна використовувати для відстеження руху об’єктів або для надання послуг на основі визначення місцезнаходження.

У сенсорних мережах управління енергією є критичним аспектом прикладного рівня. Протоколи управління енергією використовуються для оптимізації споживання енергії датчиками в мережі. Ці протоколи можуть включати механізми керування живленням, циклічність роботи та збір енергії.

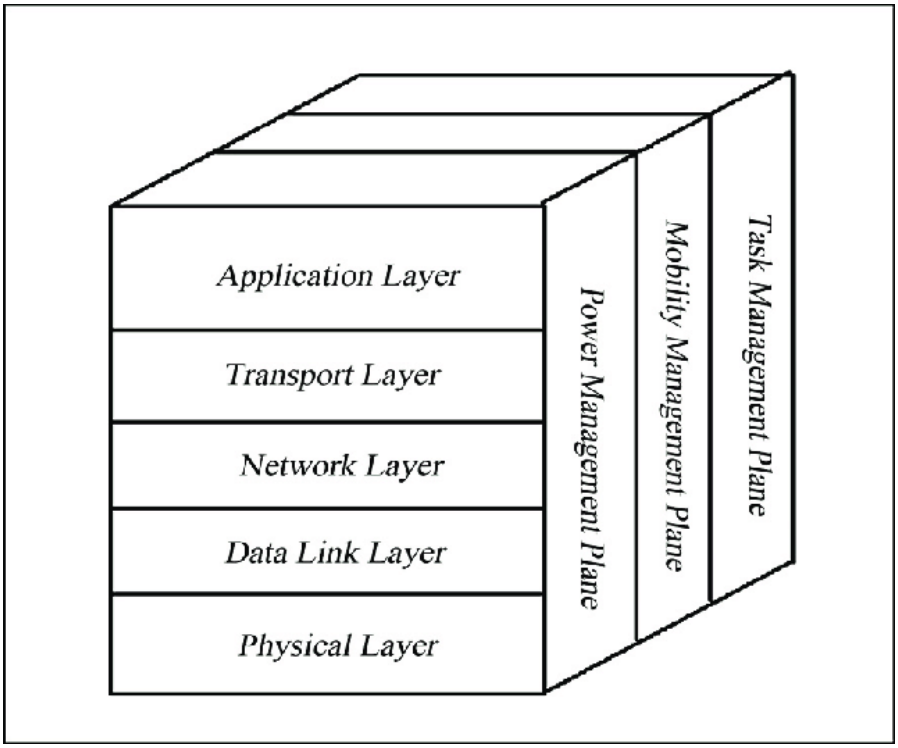

Рис. 1.1. Стек протоколів в сенсорних мережах

1.3 Безпека сенсорних мереж

Сенсорні мережі все частіше використовуються в різноманітних програмах, таких як промислові системи керування, розумні будинки та моніторинг навколишнього середовища. Однак через бездротову природу та розподілену архітектуру ці мережі вразливі до широкого спектру загроз безпеці.

Сенсорні мережі складаються з великої кількості невеликих пристроїв, які називаються сенсорними вузлами, які відповідають за визначення навколишнього середовища та передачу даних на центральний вузол або базову станцію. Ці вузли зазвичай малопотужні та мають обмежені обчислювальні можливості, що робить їх уразливими до таких різних атак.

Питання безпеки в сенсорних мережах залежать від необхідності знати, що ми збираємося захищати. Є чотири цілі безпеки в сенсорних мережах: конфіденційність, цілісність, автентифікація та доступність.

Конфіденційність — це можливість приховувати повідомлення від пасивного зловмисника, коли повідомлення, передане через сенсорні мережі, залишається конфіденційним.

Цілісність означає здатність підтвердити, що повідомлення не було підроблено, змінено чи змінено, поки воно було в мережі.

Автентифікація повинна знати, чи повідомлення надійшли з вузла, з якого вони нібито походять, щоб визначити надійність походження повідомлення.

Доступність визначає, чи має вузол можливість використовувати ресурси, а мережа доступна для передачі повідомлень.

Атаки на сенсорні мережі можна розділити на два типи: пасивні та активні атаки. Пасивні атаки не передбачають будь-яких змін даних або мережевих операцій, а натомість зосереджені на перехопленні даних або аналізі трафіку. Активні атаки, з іншого боку, передбачають модифікацію або введення даних у мережу, і вони можуть завдати значної шкоди мережі датчиків [4].

Атаки на відмову в обслуговуванні. Атаки на відмову в обслуговуванні (DoS) є поширеним типом кібератак, які можуть мати руйнівний вплив на

сенсорні мережі. У сенсорній мережі атаки DoS можуть бути особливо шкідливими, оскільки вони можуть порушити нормальну роботу мережі та поставити під загрозу точність і надійність зібраних даних.

DoS-атаки включають заповнення мережі великим обсягом трафіку або запитів, перевантаження мережі та її переставання відповідати. Це може призвести до ряду проблем, таких як низька продуктивність, простої мережі та неможливість збору або передачі даних. Нижче наведено деякі поширені типи DoS-атак, які можуть відбуватися в сенсорних мережах.

Атаки на виснаження ресурсів: під час атак на виснаження ресурсів зловмисник надсилає велику кількість запитів до вузла датчика або мережі, що призводить до того, що вузол або мережа вичерпують такі ресурси, як цикли ЦП, пам’ять або пропускна здатність. Це може призвести до того, що вузол або мережа перестануть відповідати й не зможуть обробляти запити.

Атаки маршрутизації: під час атак маршрутизації зловмисник маніпулює протоколами маршрутизації, що використовуються в мережі, щоб перенаправляти трафік до певного вузла, внаслідок чого вузол перевантажується та не може обробити трафік. Це може призвести до простою мережі або втрати даних.

Атаки затоплення: атаки затоплення передбачають надсилання великої кількості запитів або пакетів у мережу, що спричиняє її перевантаження та нездатність обробляти законний трафік. Це може призвести до того, що мережа перестане відповідати або втратити дані.

Розподілені DoS-атаки: розподілені DoS-атаки (DDoS) включають кілька зловмисників, які переповнюють мережу запитами або трафіком із кількох джерел, що ускладнює ідентифікацію джерела атаки та пом’якшення її. Це може призвести до простою мережі, втрати даних або крадіжки конфіденційної інформації.

Щоб запобігти DoS-атакам у сенсорних мережах, можна впровадити різні заходи безпеки. До них належать:

Системи виявлення вторгнень. Системи виявлення вторгнень можна використовувати для моніторингу мережевого трафіку та виявлення будь-якої ненормальної поведінки чи шаблонів трафіку, які можуть вказувати на атаку DoS.

Фільтрування трафіку: фільтрацію трафіку можна використовувати для фільтрації зловмисного трафіку та запобігання його потраплянню в мережу, зменшуючи вплив атак DoS.

Балансування навантаження: балансування навантаження можна використовувати для рівномірного розподілу трафіку в мережі, запобігаючи перевантаженню будь-якого окремого вузла та зменшуючи вплив DoS-атак.

Резервування: Резервування можна використовувати для того, щоб кілька вузлів у мережі могли виконувати однакові функції, зменшуючи вплив атак DoS на окремі вузли.

Сегментація мережі: Сегментація мережі може бути використана для відділення критичних частин мережі від менш критичних частин, зменшуючи вплив DoS-атак на критичні системи.

Атаки глушіння. Атаки з перешкодами – це тип кібератак, який може серйозно вплинути на продуктивність сенсорних мереж. У сенсорній мережі атаки з перешкодами включають навмисну передачу радіочастотних сигналів, щоб порушити або заблокувати передачу законних даних між вузлами або від вузлів до базової станції. Ці атаки можуть перешкодити належному функціонуванню сенсорних мереж і призвести до втрати або неточної передачі критичних даних [4].

Існує два основних типи атак глушіння: безперервне глушіння та вибіркове глушіння.

Безперервне глушіння: під час атаки безперервного глушіння зловмисник постійно випромінює радіочастотні сигнали на тій самій частоті, що й мережа датчиків, що призводить до перешкод і порушує нормальний зв’язок між вузлами мережі.

Вибіркове глушіння: під час атаки вибіркового глушіння зловмисник випромінює сигнали лише на частотах, які використовує цільовий вузол, що

призводить до порушення зв’язку між вузлом і базовою станцією. Цей тип нападу складніше виявити, оскільки він не є постійним.

Для здійснення атаки з перешкодами зловмисник може використовувати різні методи, наприклад:

Передача високої потужності: зловмисник може використовувати передавач високої потужності, щоб наповнювати цільову частоту сигналами, перевищуючи законні сигнали та спричиняючи збій мережі.

Перемикання частоти: зловмисник може використовувати техніку стрибкоподібного перемикання частоти, щоб постійно перемикатися між частотами та передавати сигнали, щоб порушити роботу мережі.

Оманливі перешкоди: зловмисник може використовувати оманливі перешкоди, які включають випромінювання сигналів, які імітують законні сигнали, викликаючи плутанину серед вузлів і порушуючи роботу мережі.

Реактивні перешкоди: зловмисник може використовувати реактивні перешкоди, які включають моніторинг мережі та передачу сигналів лише тоді, коли виявлено законний трафік. Це ускладнює виявлення та пом’якшення атаки.

Щоб запобігти атакам глушіння у сенсорних мережах, можна впровадити різні заходи безпеки, зокрема:

Стрибкова зміна частоти: сенсорні мережі можуть використовувати методи стрибкової зміни частоти, щоб часто змінювати частоти, що використовуються для зв’язку, що ускладнює зловмиснику блокування мережі.

Технологія розширеного спектру: сенсорні мережі можуть використовувати технологію розширеного спектру, яка поширює сигнал у ширшому частотному діапазоні, що ускладнює зловмиснику блокування мережі.

Шифрування: шифрування можна використовувати для захисту зв’язку між вузлами в мережі, що ускладнює зловмиснику розшифровку зв’язку та виконання атаки з перешкодами.

Контроль потужності: Контроль потужності можна використовувати для регулювання потужності передачі вузлів, ускладнюючи зловмисникам подолання законних сигналів.

Атаки компрометації вузлів. Атаки на компрометацію вузлів у сенсорних мережах передбачають компрометацію зловмисником одного чи кількох вузлів у мережі, щоб отримати доступ до конфіденційної інформації, маніпулювати даними або порушити нормальну роботу мережі. Ці атаки можуть мати серйозні наслідки, оскільки можуть поставити під загрозу цілісність і конфіденційність даних, що передаються в мережі.

Фізичний компрометація: зловмисник отримує фізичний доступ до вузла та встановлює шкідливе програмне або апаратне забезпечення, що дозволяє зловмиснику отримати контроль над вузлом і даними, які ним передаються.

Віддалений компрометація: зловмисник використовує вразливі місця в мережевих протоколах або програмах, запущених на вузлі, щоб отримати віддалений доступ до вузла та його даних.

Соціальна інженерія: зловмисник може обманом змусити користувача встановити шкідливе програмне забезпечення на вузлі або розкрити конфіденційну інформацію.

Після того, як вузол скомпрометовано, зловмисник може виконувати різні шкідливі дії, зокрема:

Маніпулювання даними: зловмисник може змінити або видалити дані, передані скомпрометованим вузлом, що може призвести до неправильного аналізу даних або прийняття рішень.

Крадіжка даних: зловмисник може викрасти конфіденційні дані, передані скомпрометованим вузлом, що може призвести до компрометації конфіденційної інформації.

Відмова в обслуговуванні: зловмисник може використовувати скомпрометований вузол, щоб заповнити мережу трафіком або заблокувати законний трафік, що призведе до порушення нормальної роботи мережі.

Щоб запобігти атакам компрометації вузлів у сенсорних мережах, можна застосувати кілька заходів безпеки, зокрема:

Контроль доступу: механізми контролю доступу можуть бути реалізовані для обмеження доступу до вузлів і даних, що ними передаються.

Автентифікація: вузли можуть бути автентифіковані за допомогою цифрових сертифікатів або інших механізмів, щоб гарантувати, що лише авторизовані вузли можуть спілкуватися один з одним.

Шифрування: шифрування можна використовувати для захисту зв’язку між вузлами в мережі, гарантуючи, що дані, що передаються між вузлами, є конфіденційними та не можуть бути перехоплені зловмисниками.

Виявлення вторгнень: системи виявлення вторгнень можна використовувати для виявлення та реагування на атаки компрометації вузла.

Атаки червоточини. Атаки червоточини в сенсорних мережах — це тип кібератак, під час яких зловмисник створює ярлик або прямий тунель між двома віддаленими вузлами в мережі, перехоплюючи пакети в одному місці, а потім пересилаючи їх в інше місце, минаючи проміжні вузли. Це створює червоточину або ярлик у мережі, яким зловмисник може скористатися для подальших атак на мережу.

Атаки через червоточину особливо складно виявити та запобігти в сенсорних мережах, оскільки вони можуть бути здійснені шляхом скомпрометації лише двох вузлів у мережі, що ускладнює виявлення атаки традиційними механізмами безпеки.

Внутрішньорегіональна атака через червоточину: у цьому типі атаки зловмисник захоплює пакети з одного місця в мережі та тунелює їх до іншого місця в тому самому регіоні. Цього можна досягти за допомогою високошвидкісного бездротового з’єднання між двома вузлами або фізичним переміщенням вузлів ближче один до одного.

Міжрегіональна атака через червоточину: у цьому типі атаки зловмисник захоплює пакети з одного місця в мережі та тунелює їх до іншого місця в іншому регіоні. Цього можна досягти за допомогою високошвидкісного бездротового або дротового з’єднання між двома регіонами.

Перехоплення даних: зловмисник може перехоплювати та маніпулювати даними, що передаються між двома регіонами, порушуючи цілісність і конфіденційність даних.

Затоплення даних: зловмисник може заповнити мережу трафіком, перевантаживши мережу та спричинивши її збій.

Відмова в обслуговуванні: зловмисник може використовувати червоточину для здійснення атаки на відмову в обслуговуванні, блокуючи законний трафік і порушуючи нормальну роботу мережі.

Щоб запобігти атакам через червоточину в сенсорних мережах, можна застосувати кілька заходів безпеки, зокрема:

Протоколи безпечної маршрутизації: протоколи безпечної маршрутизації можна використовувати для виявлення та запобігання атакам через червоточину в мережі.

Перевірка сусідів: вузли можуть перевіряти ідентичність своїх сусідів, обмінюючись маркерами автентифікації або сертифікатами, гарантуючи, що в мережу включено лише законні вузли.

Радіочастотний аналіз. Радіочастотний аналіз можна використовувати для виявлення та визначення місцезнаходження червоточини в мережі.

Синхронізація часу: Синхронізацію часу можна використовувати для виявлення та запобігання атак через червоточину, оскільки затримку, спричинену червоточиною, можна виявити шляхом порівняння позначок часу переданих пакетів.

Атаки Сибілу. Атаки Сибілу – це тип кібератак, під час якого зловмисник створює кілька підроблених ідентифікаторів або «вузлів Сибіл», щоб отримати контроль над мережею. Під час атаки Сибілу зловмисник може використовувати ці фальшиві ідентифікаційні дані, щоб заповнити мережу трафіком, маніпулювати даними, що передаються мережею, або порушити нормальну роботу мережі.

Атаки Сибілу особливо складно виявити та запобігти в сенсорних мережах, оскільки вузли мережі зазвичай мають обмежені ресурси та не мають достатньої потужності для виконання складних криптографічних операцій.

Реплікація вузла: зловмисник створює кілька підроблених вузлів, кожен з яких має унікальний ідентифікатор, і впроваджує їх у мережу.

Крадіжка особистих даних: зловмисник викрадає ідентифікаційні дані законного вузла в мережі та використовує їх для створення кількох підроблених вузлів.

Змова: зловмисник вступає в змову з кількома законними вузлами в мережі, щоб створити велику кількість підроблених вузлів.

Після створення вузлів Сиблу зловмисник може виконувати різні шкідливі дії, зокрема:

Маніпулювання даними: зловмисник може маніпулювати даними, які передаються вузлами Сибілу, що може призвести до неправильного аналізу даних або прийняття рішень.

Відмова в обслуговуванні: зловмисник може використовувати вузли Сибілу, щоб заповнити мережу трафіком або заблокувати законний трафік, що призведе до порушення нормальної роботи мережі.

Атаки на репутацію: зловмисник може використовувати вузли Сибілу, щоб штучно підвищити свою репутацію в мережі, надаючи їм несправедливу перевагу над іншими вузлами в мережі.

Щоб запобігти атакам Сибілу у сенсорних мережах, можна застосувати декілька заходів безпеки, зокрема:

Захищена реєстрація вузла: можна реалізувати процес реєстрації захищеного вузла, щоб гарантувати, що лише законним вузлам дозволено приєднуватися до мережі.

Управління довірою на основі репутації: систему управління довірою на основі репутації можна використовувати для виявлення та запобігання атакам Сибілу у мережі.

Фізична автентифікація: механізми фізичної автентифікації, такі як маркери автентифікації на основі апаратного забезпечення, можна використовувати для запобігання атакам крадіжки особистих даних.

Розбиття мережі: розділення мережі можна використовувати для ізоляції вузлів Сибілу в окремій мережі, запобігаючи їхньому впливу на нормальну роботу мережі [4].

1.4 Особливості побудови сенсорних мереж із використанням Raspberry Pi

Сенсорні мережі — це група взаємопов'язаних датчиків, які збирають і передають дані в центральне розташування для аналізу й обробки. Raspberry Pi — це універсальний одноплатний комп'ютер, який можна використовувати для створення сенсорної мережі, підключивши до нього кілька датчиків і запрограмувавши його для збору, обробки та передачі даних

Сенсорна мережа з Raspberry Pi також може використовуватися для програм кібербезпеки. Ось кілька способів використання сенсорної мережі на базі Raspberry Pi для кібербезпеки:

Моніторинг мережі: Raspberry Pi можна використовувати для створення системи моніторингу мережі, яка фіксує та аналізує мережевий трафік з метою безпеки. Підключивши Raspberry Pi до мережі, він може перехоплювати пакети та аналізувати їх за допомогою програмних засобів, таких як Wireshark або tcpdump. Це може допомогти виявити потенційні загрози безпеці, наприклад зловмисне програмне забезпечення або підозрілу активність.

Налаштування системи мониторингу мережі з сенсорною мережею за допомогою Raspberry Pi:

Відповідні датчики: залежно від типу мережі, яку треба контролювати, потрібно буде вибрати відповідні датчики. Наприклад, якщо контролювати температуру та вологість – знадобляться датчики температури та вологості.

Підключення датчиків до Raspberry Pi: залежно від типу датчика може знадобитися використання додаткового апаратного забезпечення, наприклад аналого-цифрового перетворювача (АЦП).

Встановлення необхідного програмного забезпечення: потрібно встановити програмне забезпечення на Raspberry Pi, яке зчитує дані датчиків і передає їх на центральний сервер. Існує багато доступних варіантів програмного забезпечення, наприклад Node-RED, Python і MQTT.

Налаштування мережі датчиків: потрібно налаштувати мережу датчиків, щоб дані датчиків передавалися на центральний сервер. Це можна зробити за допомогою різних бездротових протоколів, таких як Wi-Fi, Bluetooth або Zigbee.

Налаштування центрального серверу. Необхідно налаштувати центральний сервер, який отримуватиме та оброблятиме дані датчиків. Залежно від вимог може знадобитися використовувати базу даних для зберігання даних датчиків і інформаційну панель для відображення даних.

Перевірка системи: коли все буде налаштовано, потрібно перевірити систему, щоб переконатися, що дані датчиків передаються правильно, а центральний сервер правильно отримує й обробляє дані.

Виявлення вторгнень: Raspberry Pi можна використовувати для створення системи виявлення вторгнень, яка відстежує мережевий трафік на наявність ознак несанкціонованого доступу. Підключивши Raspberry Pi до мережі та використовуючи спеціалізоване програмне забезпечення, як-от Snort або Bro, він може виявляти та попереджати про підозрілу активність, як-от сканування портів, атаки грубої сили та інші загрози безпеці.

Налаштування системи виявлення вторгнень за допомогою Raspberry Pi і сенсорної мережі:

Необхідно визначити датчики, які вам потрібні: на ринку доступно багато типів датчиків, наприклад датчики руху, датчики тиску, датчики температури та багато інших. Ви повинні вибрати датчики на основі ваших потреб і середовища, в якому ви хочете встановити систему.

Налаштування Raspberry Pi: можна використовувати будь-яку модель Raspberry Pi, але для кращої продуктивності рекомендується використовувати останню. Інсталяція останньої версії ОС Raspbian на Raspberry Pi з підключенням до Інтернету.

Встановлення необхідного програмного забезпечення: наприклад Python, Flask і бібліотеку GPIO для взаємодії датчиків із Raspberry Pi.

Підключення датчиків до Raspberry Pi.

Код для читання даних датчика: код Python для читання даних датчика за допомогою бібліотеки GPIO.

Алгоритм виявлення вторгнення. Наприклад, якщо датчик руху виявляє рух, коли там нікого не повинно бути, він може викликати сповіщення.

Налаштування системи сповіщень: система сповіщень, яка сповіщатиме про виявлення вторгнення. Можна використовувати електронну пошту, SMS або будь-який інший спосіб.

Перевірка системи. Необхідно ретельно перевірити систему, щоб переконатися, що вона працює належним чином і може точно виявляти вторгнення.

Фізична безпека: Raspberry Pi можна використовувати для створення системи фізичної безпеки, яка контролює фізичне середовище на предмет несанкціонованого доступу. Підключивши до Raspberry Pi такі датчики, як детектори руху, датчики дверей і камери, він може виявити будь-яку підозрілу активність і попередити про неї [5].

Контроль доступу: Raspberry Pi можна використовувати для створення системи контролю доступу, яка обмежує доступ до мережі або фізичного простору. Підключивши такі датчики, як клавіатури, зчитувачі RFID або біометричні датчики, до Raspberry Pi можна перевірити особу користувача та надати або заборонити доступ на основі попередньо визначених правил.

Тестування безпеки: Raspberry Pi можна використовувати як тестову платформу для оцінки безпеки. Встановивши на Raspberry Pi спеціалізоване програмне забезпечення, наприклад Kali Linux або Metasploit, його можна використовувати для перевірки безпеки мереж, пристроїв і програм.

Загалом, сенсорна мережа на базі Raspberry Pi може бути потужним інструментом для програм кібербезпеки. Завдяки низькій вартості, універсальності та простоті використання Raspberry Pi можна використовувати для створення налаштованих рішень безпеки для широкого спектру програм.

Висновки до першого розділу

Проведено аналіз сенсорних мереж, їх компоненти, архітектура, безпека та особливості побудови.

Досліджено, що сенсорні мережі захоплююча галузь технологій, яка швидко розвивається, і вона може революціонізувати широкий спектр галузей. Однією з ключових переваг сенсорних мереж є їх здатність збирати та передавати дані в режимі реального часу. Проте сенсорні мережі також створюють низку проблем, зокрема проблеми, пов’язані з конфіденційністю та безпекою даних, а також занепокоєння щодо впливу цих мереж на навколишнє середовище та суспільство в цілому.

Розглянуто, як саме побудувати сенсорну мережу з Raspberry Pi, підключити датчики, встановити програмне забезпечення, налаштувати та встановити сервер.

2 ДОСЛІДЖЕННЯ ЗАГРОЗ БЕЗПЕЦІ СЕНСОРНИХ МЕРЕЖ ІЗ ВИКОРИСТАННЯМ RASPBERRY PI

2.1 Історія розвитку Raspberry Pi

Raspberry Pi – це серія однобічних комп'ютерів, розроблених Фондом Raspberry Pi у Великобританії. Розробка Raspberry Pi розпочалася в 2006 році, коли група комп'ютерних вчених на чолі з Ебеном Аптон помітила зниження додатків для інформатики серед студентів.

Перше покоління Raspberry Pi Model B було випущено в лютому 2012 року, а потім простіша і дешевша Model A.

У 2014 році Фонд випустив плату з покращеним дизайном Raspberry Pi Model B+. Ці плати першого покоління оснащені процесорами ARM11, розміром приблизно з кредитну картку та представляють стандартний основний форм-фактор. Покращені моделі A+ і B були випущені протягом року. «Обчислювальний модуль» був випущений у квітні 2014 року для вбудованих програм.

Raspberry Pi 2 був випущений у лютому 2015 року і спочатку мав 900 МГц 32-бітний чотирьохядерний процесор ARM Cortex-A7 з 1 ГБ оперативної пам'яті. Версія 1.2 мала 64-розрядний чотирьохядерний процесор ARM Cortex-A53 з тактовою частотою 900 МГц (такий самий, що й у Raspberry Pi 3 Model B, але зі зниженою частотою до 900 МГц).

Raspberry Pi 3 Model B була випущена в лютому 2016 року з 64-розрядним чотирьохядерним процесором ARM Cortex-A53 з тактовою частотою 1,2 ГГц, вбудованим Wi-Fi 802.11n, можливостями завантаження Bluetooth і USB.

У День Пі 2018 року була представлена модель Raspberry Pi 3 Model B+ із швидшим процесором 1,4 ГГц, утричі швидшим гігабітним Ethernet (пропускна здатність обмежена приблизно 300 Мбіт/с внутрішнім з'єднанням USB 2.0) і 2,4/5 ГГц. дводіапазонний Wi-Fi 802.11ac (100 Мбіт/с). Інші функції включають

живлення через Ethernet (PoE) (з додатковим PoE HAT), завантаження через USB і мережеве завантаження (SD-карта більше не потрібна).

Raspberry Pi 4 Model B була випущена в червні 2019 рокутз 64-розрядним чотирьохядерним процесором ARM Cortex-A72 з частотою 1,5 ГГц, вбудованим Wi-Fi 802.11ac, Bluetooth 5, повним гігабітним Ethernet (пропускна здатність не обмежена), два порти USB 2.0, два порти USB 3.0, 1–8 ГБ оперативної пам’яті та підтримка двох моніторів через пару портів micro HDMI (HDMI Type D) для роздільної здатності до 4K. Від версії з 1 ГБ оперативної пам’яті відмовилися, а ціни на версію 2 ГБ були знижені. Версія на 8 ГБ має перероблену друковану плату. Pi 4 також живиться через порт USB-C, що дає змогу подавати додаткове живлення на подальшу периферію, якщо використовується з відповідним блоком живлення. Але Pi може працювати лише від 5 вольт, а не від 9 чи 12 вольт, як інші міні-комп’ютери цього класу. Початкова плата Raspberry Pi 4 має недолік конструкції, через який USB-кабелі сторонніх виробників, які використовуються в Apple MacBook, неправильно ідентифікують її та відмовляються подавати живлення. Компанія Tom's Hardware протестувала 14 різних кабелів і виявила, що 11 з них вмикали та живили Pi без проблем. Недолік дизайну було виправлено у версії 1.2 плати, випущеній наприкінці 2019 року. У середині 2021 року з’явилися моделі Pi 4 B з покращеним Broadcom BCM2711C0. Зараз виробник використовує цей чіп для Pi 4 B і Pi 400. Однак тактова частота Pi 4 B не була збільшена на заводі [6].

Raspberry Pi 400 був випущений у листопаді 2020 року. Сучасний зразок клавіатурного комп’ютера, він має 4 ГБ оперативної пам’яті LPDDR4 на спеціальній платі, створеній на основі існуючої Raspberry Pi 4, у поєднанні з клавіатурою в одному корпусі. Корпус був створений на основі клавіатури Raspberry Pi. Надійне рішення для охолодження (тобто широка металева пластина) і оновлений імпульсний блок живлення дозволяють процесору Broadcom BCM2711C0 Raspberry Pi 400 працювати на частоті 1,8 ГГц, що на 20% швидше, ніж Raspberry Pi 4, на якому він працює.

Raspberry Pi Zero з меншим розміром і обмеженими можливостями вводу/виводу (I/O) і загального введення/виводу (GPIO) був випущений у листопаді 2015 року за 5 доларів США. На рис. 1.1 представлений Raspberry Pi Zero.

16 травня 2016 року була випущена Raspberry Pi Zero v1.3, яка додала роз'єм для камери.

28 лютого 2017 року був випущений Raspberry Pi Zero W, версія Zero з можливостями Wi-Fi і Bluetooth, за 10 доларів США.

12 січня 2018 року була представлена Raspberry Pi Zero WH, версія Zero W із попередньо розпаяними роз'ємами GPIO.

28 жовтня 2021 року був випущений Raspberry Pi Zero 2 W, версія Zero W із системою в пакеті (SiP), розроблена Raspberry Pi і заснована на Raspberry Pi 3. На відміну від старих моделей Zero, Pi Zero 2 W підтримує 64-розрядний процесор. Ціна близько 15 доларів США [7].

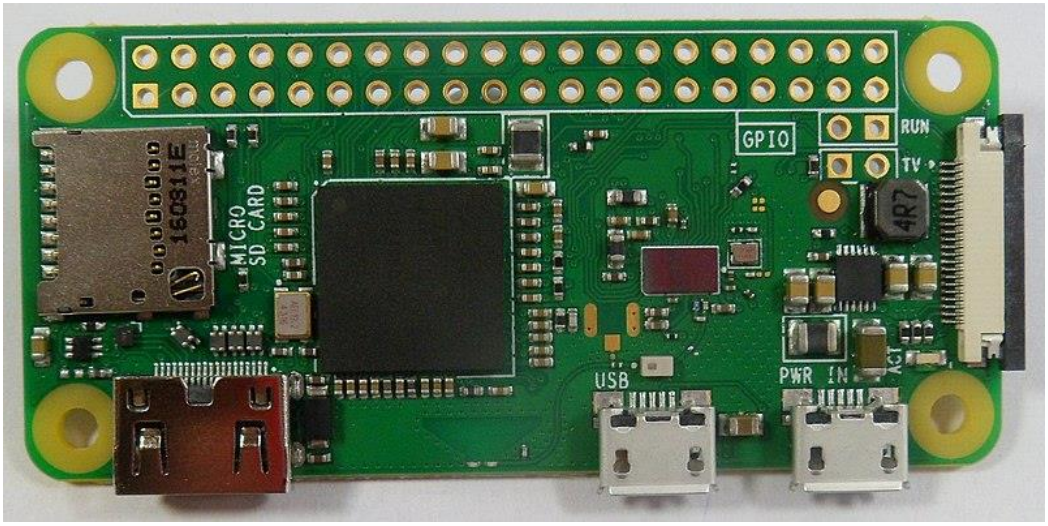

Рис. 2.1. Raspberry Pi Zero

Raspberry Pi Pico був випущений у січні 2021 року за роздрібною ціною 4 долари. Це була перша плата Raspberry Pi на основі одного чіпа мікроконтролера; RP2040, розроблений Raspberry Pi у Великобританії. Pico має 264 КБ оперативної пам'яті та 2 МБ флеш-пам'яті. Його можна програмувати на C, C++, Assembly, MicroPython, CircuitPython і Rust. Raspberry Pi Foundation співпрацює з Adafruit,

Pimoroni, Arduino та SparkFun для створення аксесуарів для Raspberry Pi Pico та багатьох інших плат на основі RP2040 Silicon Platform. Замість того, щоб виконувати роль комп'ютера загального призначення (як інші в діапазоні), він призначений для фізичних обчислень, подібних за концепцією до Arduino.

30 червня 2022 року був випущений Raspberry Pi Pico W, версія Pico з підтримкою Wi-Fi 802.11n, за 6 доларів США. Бездротовий чіп CYW43439 у Pico W також підтримує Bluetooth, але ця функція не була активована під час запуску. На рис. 2.2 представлена Raspberry Pi Pico [7].

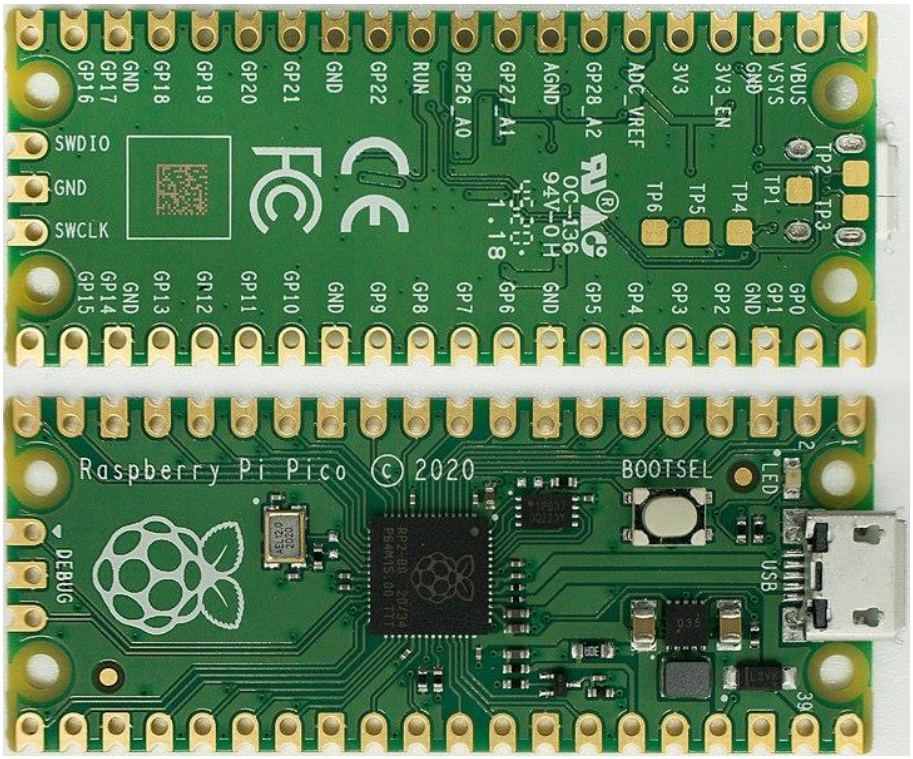

Рис. 2.2. Raspberry Pi Pico

Технологія Raspberry Pi датчиків дозволяє комп'ютеру взаємодіяти зі своїм середовищем та фіксувати дані, використовуючи різні типи датчиків. Деякі особливості технології Raspberry Pi датчиків:

Сумісність: Сенсори Raspberry Pi сумісні з різними типами датчиків, таких як температура, вологість, світло, звук, рух, тиск та датчики газу.

Простота використання: Технологія Raspberry Pi Sensors проста у використанні навіть для початківців, оскільки датчики можна легко підключити до шпильок GPIO Raspberry Pi.

Збір даних у режимі реального часу: Технологія Raspberry PI Sensors дозволяє отримати збору даних у режимі реального часу, що дозволяє користувачам контролювати та аналізувати дані з датчиків у режимі реального часу.

Низьке споживання електроенергії: Технологія Raspberry Pi Sensors використовує низьку потужність, що робить її ідеальною для проектів IoT (Internet of Things), які вимагають від датчиків працювати протягом тривалого періоду.

Налаштування: Технологія Raspberry Pi Sensors налаштована, що дозволяє користувачам змінювати програмне забезпечення та обладнання для задоволення їх конкретних вимог.

Універсальність: Технологія Raspberry Pi Sensors є універсальною, що робить її придатною для широкого спектру застосувань, таких як автоматизація домашньої роботи, моніторинг навколишнього середовища та промисловий контроль.

Програмне забезпечення з відкритим кодом: Технологія Raspberry Pi Sensors використовує програмне забезпечення з відкритим кодом, що дозволяє користувачам отримувати доступ до великої спільноти розробників та ресурсів.

2.2 Протоколи безпеки

У сучасному світі протоколи відіграють вирішальну роль, оскільки вони визначають набір правил і процедур для зв’язку між пристроями, що забезпечує безперебійний і надійний обмін даними. Без протоколів пристрої можуть не мати змоги ефективно спілкуватися, що призводить до помилок, втрати даних та інших проблем.

У випадку Raspberry Pi протоколи особливо важливі, оскільки вони часто використовуються для створення проектів, які потребують зв’язку з різними датчиками, контролерами та іншими пристроями. Ці пристрої можуть використовувати різні протоколи та інтерфейси, тому для Raspberry Pi важливо

підтримувати широкий спектр протоколів, щоб забезпечити сумісність з різними апаратними компонентами.

SSH. SSH, також відомий як Secure Shell або Secure Socket Shell, — це мережевий протокол, який надає користувачам, особливо системним адміністраторам, безпечний спосіб доступу до комп'ютера через незахищену мережу.

SSH також відноситься до набору утиліт, які реалізують протокол SSH. Secure Shell забезпечує надійну автентифікацію за допомогою пароля та автентифікацію за відкритим ключем, а також зашифрований обмін даними між двома комп'ютерами, які підключаються через відкриту мережу, наприклад Інтернет.

Крім забезпечення надійного шифрування, SSH широко використовується мережевими адміністраторами для віддаленого керування системами та програмами, дозволяючи їм входити в інший комп'ютер через мережу, виконувати команди та переміщувати файли з одного комп'ютера на інший.

SSH відноситься як до протоколу криптографічної мережі, так і до набору утиліт, які реалізують цей протокол. SSH використовує клієнт-серверну модель, з'єднуючи клієнтську програму Secure Shell, де відображається сеанс, із сервером SSH, де виконується сеанс. Реалізації SSH часто включають підтримку протоколів додатків, які використовуються для емуляції терміналу або передачі файлів.

SSH також можна використовувати для створення безпечних тунелів для інших протоколів додатків, наприклад, для безпечного віддаленого запуску графічних сеансів X Window System. Сервер SSH за замовчуванням прослуховує порт 22 стандартного протоколу керування передачею (TCP).

Secure Shell було створено для заміни незахищеної емуляції терміналу або програм входу, таких як Telnet, rlogin (віддалений вхід) і rsh (віддалена оболонка). SSH забезпечує ті самі функції – вхід у систему та запуск термінальних сеансів на віддалених системах. SSH також замінює програми передачі файлів, такі як протокол передачі файлів (FTP) і rcp (віддалене копіювання).

Основним використанням SSH є підключення до віддаленого хосту для термінального сеансу. Форма цієї команди така:

ssh UserName@SSHserver.example.com

Ця команда змусить клієнт спробувати підключитися до сервера під назвою server.example.com, використовуючи ідентифікатор користувача UserName. Якщо це перше встановлення з'єднання між локальним хостом і сервером, користувачеві буде запропоновано ввести відбиток відкритого ключа віддаленого хоста та підключитися, незважаючи на те, що попереднього з'єднання не було:

The authenticity of host 'sample.ssh.com' cannot be established.

DSA key fingerprint is 01:23:45:67:89:ab:cd:ef:ff:fe:dc:ba:98:76:54:32:10.

Are you sure you want to continue connecting (yes/no)?

Відповідь «так» на запит призведе до продовження сеансу, а ключ хоста збережеться у файлі unknown_hosts локальної системи. Це прихований файл, який за замовчуванням зберігається у прихованому каталозі під назвою /.ssh/known_hosts у домашньому каталозі користувача. Після того, як ключ хоста буде збережено у файлі unknown_hosts, клієнтська система може знову підключатися безпосередньо до цього сервера без потреби в будь-яких погодженнях; ключ хоста автентифікує з'єднання [6].

Функції, які підтримує SSH, включають наступне:

— безпечний віддалений доступ до мережевих систем або пристроїв із підтримкою SSH для користувачів, а також автоматизованих процесів;

— безпечні та інтерактивні сеанси передачі файлів;

— автоматизована та безпечна передача файлів;

— безпечна видача команд на віддалених пристроях або системах;

— безпечне управління компонентами мережевої інфраструктури.

SSH — це безпечний спосіб віддаленого доступу до інтерфейсу командного рядка Raspberry Pi. Цей протокол дозволяє входити в Raspberry Pi з іншого комп'ютера та виконувати команди так, ніби ви фізично присутні біля Pi.

VNC. Віртуальні мережеві обчислення (VNC) — це графічна система спільного використання робочого столу, яка дозволяє віддалено керувати

робочим середовищем іншого комп'ютера через мережеве з'єднання. Він забезпечує спосіб доступу та взаємодії з робочим середовищем віддаленого комп'ютера так, ніби користувач фізично сидить перед комп'ютером.

Система VNC складається з двох компонентів: сервера VNC і засобу перегляду VNC. Сервер VNC працює на комп'ютері, до якого користувач хоче отримати віддалений доступ, а програма перегляду VNC працює на комп'ютері, який користувач використовує для доступу до віддаленого комп'ютера. Програма перегляду VNC зв'язується з сервером VNC через мережеве з'єднання, дозволяючи переглядати робоче середовище віддаленого комп'ютера та керувати ним.

Одна з ключових переваг VNC полягає в тому, що він дозволяє отримати віддалений доступ до середовища графічного робочого столу комп'ютера, навіть якщо до комп'ютера не під'єднано монітор чи клавіатуру. Це може бути корисним для таких завдань, як віддалене адміністрування, усунення несправностей або розробка програмного забезпечення.

VNC — це кросплатформна система, що означає, що її можна використовувати для доступу та керування робочими середовищами в широкому діапазоні операційних систем, включаючи Windows, macOS і Linux. VNC також легко налаштовується з параметрами налаштування роздільної здатності, глибини кольору та інших параметрів для оптимізації продуктивності на основі ваших конкретних потреб і умов мережі.

Raspberry Pi підтримує VNC, що означає, що ви можете використовувати VNC для віддаленого доступу до робочого середовища вашого Raspberry Pi з іншого комп'ютера.

Щоб використовувати VNC із Raspberry Pi, потрібно спочатку встановити сервер VNC на Pi. Доступно кілька варіантів серверів VNC, включаючи RealVNC і TightVNC.

1. Інсталювання серверу VNC на Raspberry Pi. Можна зробити це за допомогою терміналу, ввівши таку команду:

sudo apt-get install tightvncserver

2. Запуск серверу VNC на Raspberry Pi, ввівши таку команду в терміналі: *vncserver :1*

3. Коли сервер VNC запускається вперше, зазвичай запропоновано створити пароль. Цей пароль знадобиться, коли користувач віддалено підключаєтесь до Raspberry Pi за допомогою VNC.

4. На віддаленому комп'ютері необхідно завантажити та інсталювати програму перегляду VNC. RealVNC Viewer і TightVNC Viewer є двома популярними варіантами.

5. Необіхдно відкрити програму перегляду VNC і ввести IP-адресу Raspberry Pi разом із номером порту (зазвичай: 1). Також повинно ввести пароль, який користувач створив раніше.

6. Необхідно натиснути «Підключитися», щоб установити віддалене підключення до робочого середовища Raspberry Pi. Тепер можна переглядати середовище робочого столу Raspberry Pi і взаємодіяти з ним так, ніби користувач сидить перед Pi.

VNC — це зручний спосіб віддаленого доступу до робочого середовища Raspberry Pi, який може бути корисним для різноманітних завдань, таких як програмування, налагодження та моніторинг.

FTP. Термін «протокол передачі файлів» (FTP) відноситься до процесу, який включає передачу файлів між пристроями через мережу. Процес працює, коли одна сторона дозволяє іншій надсилати або отримувати файли через Інтернет. Спочатку він використовувався як спосіб для користувачів спілкуватися та обмінюватися інформацією між двома фізичними пристроями, а тепер широко використовується для зберігання файлів у хмарі, яка зазвичай є безпечним місцем, яке зберігається віддалено.

Протокол передачі файлів дозволяє окремим особам і компаніям обмінюватися електронними файлами з іншими, не перебуваючи в одному просторі. Це можна зробити за допомогою FTP-клієнта або через хмару. Незалежно від варіанту, обом сторонам потрібне робоче підключення до Інтернету [6].

Більшість веб-браузерів постачаються з клієнтами FTP, які дозволяють користувачам передавати файли зі свого комп’ютера на сервер і навпаки. Деякі користувачі можуть захотіти використовувати FTP-клієнт третьої сторони, оскільки багато з них пропонують додаткові функції. Приклади FTP-клієнтів, які можна завантажити безкоштовно, включають FileZilla Client, FTP Voyager, WinSCP, CoffeeCup Free FTP і Core FTP.

Багато людей використовували FTP раніше, навіть не підозрюючи про це. Якщо ви коли-небудь завантажували файл із веб-сторінки, ви використовували FTP. Першим кроком є вхід, який може відбуватися автоматично або шляхом введення імені користувача та пароля вручну. FTP також вимагатиме доступу до FTP-сервера через певний номер порту. Після того, як ви отримаєте доступ до FTP-сервера через FTP-клієнт, ви можете передавати файли. Не всі загальнодоступні FTP-сервери вимагають входу, оскільки деякі сервери дозволяють отримати до них анонімний доступ.

Як зазначалося вище, FTP спочатку був розроблений як спосіб надсилання та отримання файлів між двома фізичними комп’ютерами. Але зі змінами в технології користувачі можуть виконувати передачу файлів через хмару. Використання хмари дозволяє здійснювати перекази зручно та безпечно (що може захистити окремих осіб і компанії від витоку даних) і за відносно низьку вартість.

Щоб використовувати FTP із Raspberry Pi, потрібно буде встановити FTP-сервер на Pi. Доступно кілька варіантів FTP-сервера, зокрема ProFTPD і vsftpd.

1. Інсталювання FTP-серверу на Raspberry Pi. Можна зробити це за допомогою терміналу, ввівши таку команду:

sudo apt-get install proftpd

2. Налаштування FTP-серверу, відредагувавши файл конфігурації. Можна зробити це за допомогою такої команди:

sudo nano /etc/proftpd/proftpd.conf

3. У файлі конфігурації потрібно буде встановити наступні параметри:

ServerName "FTP Server"

ServerType standalone

DefaultRoot /home/pi

Ці налаштування налаштовують сервер FTP на використання домашнього каталогу Pi як кореневого каталогу за замовчуванням.

4. Необхідно зберегти файл конфігурації та перезапустити FTP-сервер, ввівши таку команду:

sudo service proftpd restart

5. На віддаленому комп'ютері необхідно завантажити та інсталювати клієнтську програму FTP. FileZilla — популярний FTP-клієнт, доступний для Windows, Mac і Linux.

6. Необхідно відкрити клієнтську програму FTP і ввести IP-адресу Raspberry Pi, а також ім'я користувача та пароль, які використовуєте для входу в Pi.

7. Після підключення до FTP-сервера Raspberry Pi можна передавати файли між комп'ютером і Pi, перетягуючи файли між двома розташуваннями.

FTP — це корисний спосіб передачі файлів між Raspberry Pi та іншими комп'ютерами в мережі. Це може бути особливо корисним для передачі великих файлів, таких як мультимедійні файли або сховища коду.

MQTT. MQTT (Message Queuing Telemetry Transport) – це легкий протокол обміну повідомленнями, який зазвичай використовується в програмах Інтернету речей (IoT). Це дозволяє пристроям спілкуватися один з одним у моделі публікації-підписки, де пристрої можуть публікувати повідомлення брокеру, а інші пристрої можуть підписуватися на ці повідомлення.

MQTT означає Message Queuing Telemetry Transport. Це надзвичайно простий і легкий протокол обміну повідомленнями (підписка та публікація), розроблений для обмежених пристроїв і мереж із високою затримкою, низькою пропускною здатністю або ненадійними мережами. Його принципи розробки спрямовані на зменшення пропускної здатності мережі та вимог до ресурсів пристроїв і забезпечення безпеки постачання. Крім того, ці принципи є перевагами для пристроїв M2M (машина-машина) або IoT, оскільки продуктивність акумулятора та пропускна здатність дуже важливі.

За допомогою MQ Telemetry Transport пристрої IoT з обмеженими ресурсами можуть надсилати або публікувати інформацію на певну тему на сервер, який діє як брокер повідомлень MQTT. Потім брокер передає інформацію тим клієнтам, які раніше підписалися на тему клієнта. Для людини тема виглядає як ієрархічний шлях до файлу. Клієнти можуть підписатися на певний рівень ієрархії теми або використовувати символ підстановки, щоб підписатися на кілька рівнів.

Протокол MQTT є хорошим вибором для бездротових мереж, які мають різну затримку через випадкові обмеження пропускної здатності або ненадійні з'єднання. Якщо з'єднання від клієнта, який підписався, до брокера переривається, брокер буферизує повідомлення та надсилає їх абоненту, коли абонент повертається в режим онлайн. Якщо з'єднання від Клієнта публікації до Посередника розривається без сповіщення, Посередник може роз'єднатися та надіслати Підписнику кешоване повідомлення з інструкціями від Видавця.

Брокер MQTT є центром кожного протоколу публікації/підписки. Залежно від реалізації, брокер може керувати до тисячі одночасно підключених клієнтів MQTT. Брокер відповідає за отримання всіх повідомлень, фільтрацію повідомлень, визначення того, хто підписався на кожне повідомлення, і надсилання повідомлення цим підписаним клієнтам. Брокер також проводить сеанси всіх постійних клієнтів, включаючи підписки та пропущені повідомлення. Ще одним завданням Брокера є аутентифікація та авторизація клієнтів. Зазвичай брокер є розширюваним, що полегшує спеціальну автентифікацію, авторизацію та інтеграцію з серверними системами. Інтеграція особливо важлива, оскільки Брокер часто є компонентом, який безпосередньо доступний в Інтернеті, обслуговує багато клієнтів і повинен пересилати повідомлення до систем аналізу та обробки нижче. Коротше кажучи, Брокер є центральним центром, через який має проходити кожне повідомлення. Тому важливо, щоб ваш брокер мав високу масштабованість, міг бути інтегрований у внутрішні системи, його було легко контролювати та, звісно, був безвідмовним [7].

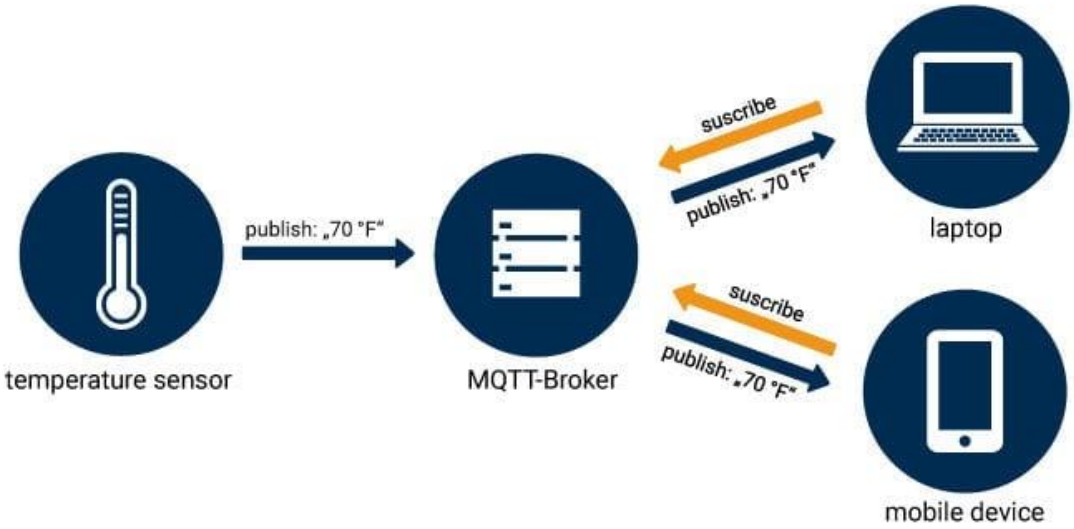

Рис. 2.3. Структура MQTT

Raspberry Pi підтримує MQTT, що означає, що можна використовувати MQTT для забезпечення зв’язку між Raspberry Pi та іншими пристроями в системі IoT.

1. Встановлення брокеру MQTT на Raspberry Pi. Mosquitto — популярний брокер MQTT з відкритим кодом, який можна встановити за допомогою такої команди в терміналі:

sudo apt-get install mosquitto mosquitto-clients

2. Запуск служби Mosquitto:

sudo systemctl start mosquitto

3. Необхідно написати сценарій Python, який використовує бібліотеку paho-mqtt для публікації та підписки на повідомлення MQTT. Приклад сценарію, який публікує повідомлення та підписується на тему:

```
import paho.mqtt.client as mqtt
def on_connect(client, userdata, flags, rc):
 print("Connected with result code "+str(rc))
        client.subscribe("test/topic")
def on_message(client, userdata, msg):
        print(msg.topic+" "+str(msg.payload))
client = mqtt.Client()
```

client.on_connect = on_connect

client.on_message = on_message

client.connect("localhost", 1883, 60)

client.publish("test/topic", "Hello, world!")

client.loop_forever()

4. Запуск сценарію Python на Raspberry Pi:

python script.py

5. На іншому пристрої необхідно підписатися на ту саму тему за допомогою клієнта MQTT. Для цього можна використовувати клієнт командного рядка Mosquitto:

mosquitto_sub -h localhost -t "test/topic"

6. Можна побачити повідомлення «Hello, world!» , яке відображається на терміналі передплатного пристрою.

MQTT — це потужний інструмент для забезпечення зв’язку між пристроями в системі IoT, а підтримка MQTT Raspberry Pi робить його популярним вибором для проектів IoT.

2.3 Механізми безпеки сенсорних мереж Raspberry Pi

Механізми безпеки сенсорної мережі розроблені для захисту сенсорної мережі від різних типів атак, включаючи компрометацію вузлів, аналіз трафіку, підслуховування та атаки на відмову в обслуговуванні (DoS).

Види механізмів безпеки. Підсистема безпеки — це механізм, який використовується для встановлення безпечного зв’язку між пристроями всередині мережі. Механізм безпеки вищого рівня, такий як криптографія, використовується для захисту інформації від викрадення неавторизованими користувачами. «Криптографія має дві основні операції: шифрування та дешифрування» [8]. Шифрування даних — це процес, у якому вся інформація кодується за допомогою алгоритму шифрування. Дешифрування даних — це процес, у якому авторизований користувач отримує дані від відправника та розшифровує їх у

вихідну інформацію за допомогою ключа шифрування. Система ключів шифрування використовує два типи ключів: відкритий ключ і закритий ключ. Відкритий ключ використовується відправником, де всі дані, надіслані від цього користувача, шифруються за допомогою цього ключа. Одержувачі використовують власний закритий ключ, щоб розшифрувати дані до вихідної інформації. Ця система ідеально підходить для запобігання злому інформації, оскільки лише одержувач знає закритий ключ, і одержувач може переконатися, що дані надходять від початкового відправника. Недоліком цього механізму є те, що для шифрування та дешифрування даних потрібен час, що збільшує час обробки.

Іншим типом механізму захисту є брандмауер. На відміну від криптографії, «Брандмауер — це пристрій, який забезпечує застосування політик безпеки на межі між двома або більше мережами». Функція брандмауера полягає в тому, щоб контролювати доступ до всіх даних, що надходять у комп'ютерну систему. Будь-які шкідливі дані будуть виявлені та заблоковані [8].

Secure Shell (SSH). Secure Shell (SSH) — це командний інтерфейс і протокол на основі UNIX для безпечного доступу до віддаленого комп'ютера. SSH розташований на прикладному рівні моделі OSI. SSH відноситься до програми або протоколу, який дозволяє користувачеві входити до іншого комп'ютера в мережі. Користувач може виконувати команди на віддаленій системі та копіювати файли в іншу систему. SSH використовується мережевими адміністраторами для віддаленого керування різними типами серверів. SSH має надійні методи автентифікації та здатність безпечно спілкуватися через незахищені мережі. За допомогою SSH будь-який вид автентифікації, включаючи автентифікацію за паролем, повністю зашифрований. Однак, коли дозволено вхід на основі пароля, зловмисники можуть неодноразово намагатися отримати доступ до сервера. Користувачі можуть вимкнути автентифікацію на основі пароля, налаштувавши автентифікацію за ключем SSH. Ключі SSH зазвичай містять більше бітів даних, ніж паролі, тому зловмисник може виконати набагато більше комбінацій». Більшість алгоритмів ключів SSH вважаються недоступними для сучасного

комп'ютерного обладнання через те, що виконання всіх можливих збігів займає багато часу». Щоб запустити SSH у Kali Linux, необхідрно ввести команду «service --status-all» на терміналі. Це перевіряє встановлення SSH на Kali Linux. «service sshstart» і «service ssh status», щоб запустити SSH і перевірити стан роботи. Запуск SSH і зміна файли конфігурації, перейшовши безпосередньо до каталогу SSH, ввівши «cd /etc/ssh», а потім необхідно написати «nanosshd_config» у наступному рядку. Ці команди відображають файл GNU sshd_config, показаний на малюнку 2.4 [9].

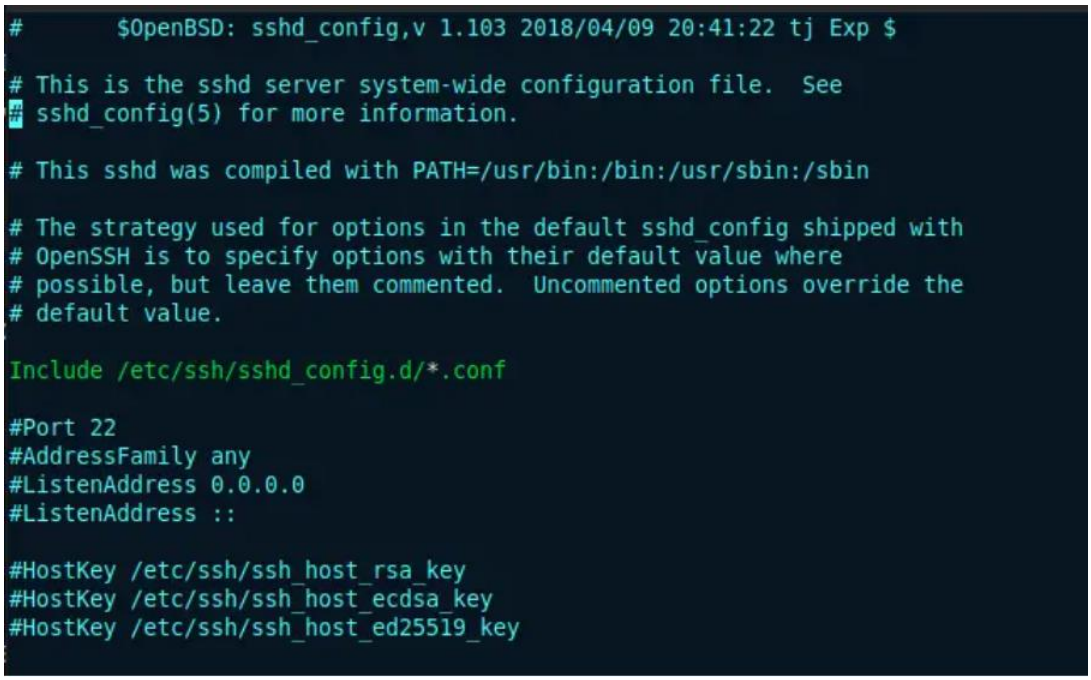

Рис. 2.4. Редагування sshd_config

Користувач може змінити номер порту в діапазоні від 0 до 65535. Стандартним портом встановлено значення 22, як показано на рис.2.4, але рекомендується змінити порт для посилення безпеки. Необхідно перезапустити SSH, ввівши «service ssh restart». Це застосує налаштування та перезапустить SSH. Потрібна пара ключів RSA для SSH. Команда "ssh-keygen-t rsa" відобразить опцію для користувача, щоб зберегти ключ у певному місці та парольну фразу, налаштовану користувачем. Користувач може просто використати надані значення за замовчуванням і пропустити пароль. Після встановлення параметра

користувач побачить згенеровані криптографічні ключі, як показано на рис.2.5 [9].

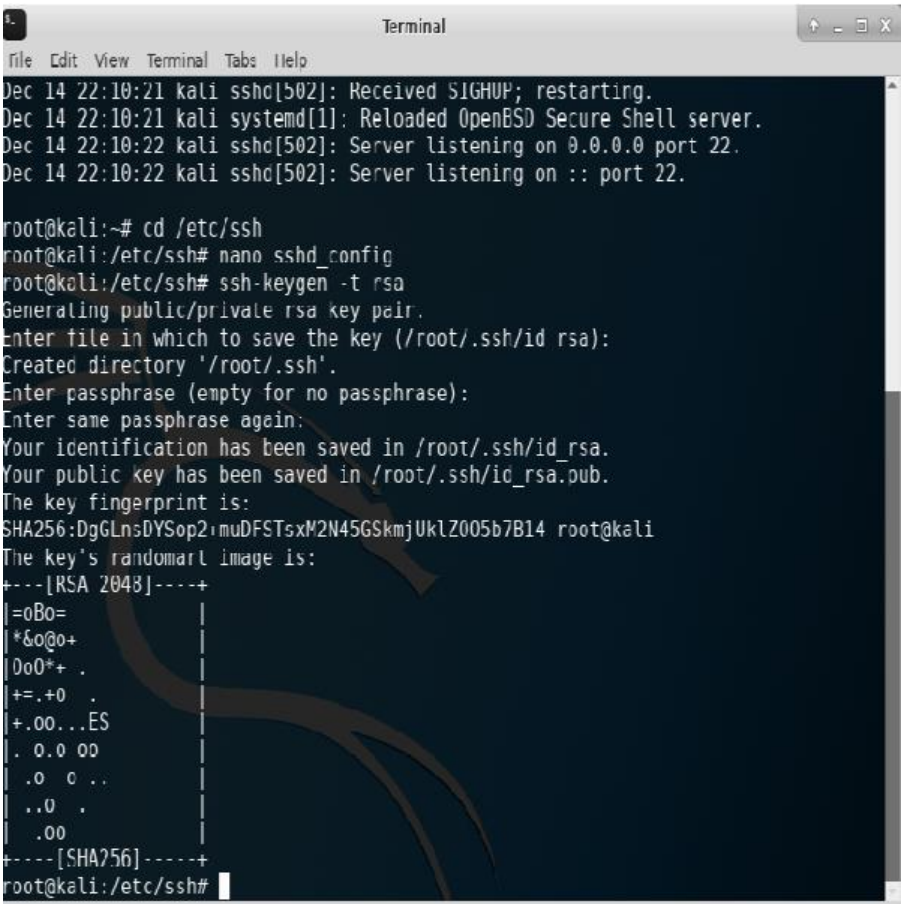

Рис. 2.5. Генерація ключів SSH

Безпечне агрегування даних. Агрегація даних — це технологія, яка використовується в системі сенсорної мережі для зменшення споживання батареї шляхом надсилання меншої кількості зайвих необроблених даних, зібраних датчиками. Під час агрегації даних необроблені дані, зібрані датчиками, будуть об’єднані або видалені, щоб зменшити кількість повторюваних даних. Буде менше обробки даних через агрегацію – це різко зменшує обсяг завдань обробки та передачі для центрального процесора. Безпечне агрегування даних стосується додавання безпечного аспекту під час агрегації даних. Наприклад, у системі сенсорної мережі багато вузлів датчика підключено до окремого центрального контролера. Кожен контролер аналізує та обробляє необроблені дані. Для хакерів, які намагаються викрасти дані, що передаються через мережу, легко отримати контроль над одним контролером і надіслати неправдиві дані головному

контролеру. Як показано на рис.2.6., концепція безпечного агрегування даних полягає в тому, що лише центральний контролер буде зберігати інформацію та спілкуватися з усіма вузлами. Для інших контролерів, які підключаються безпосередньо до датчика, вони можуть надсилати дані лише на центральний контролер і не мають права зберігати дані та спілкуватися з іншими вузлами.

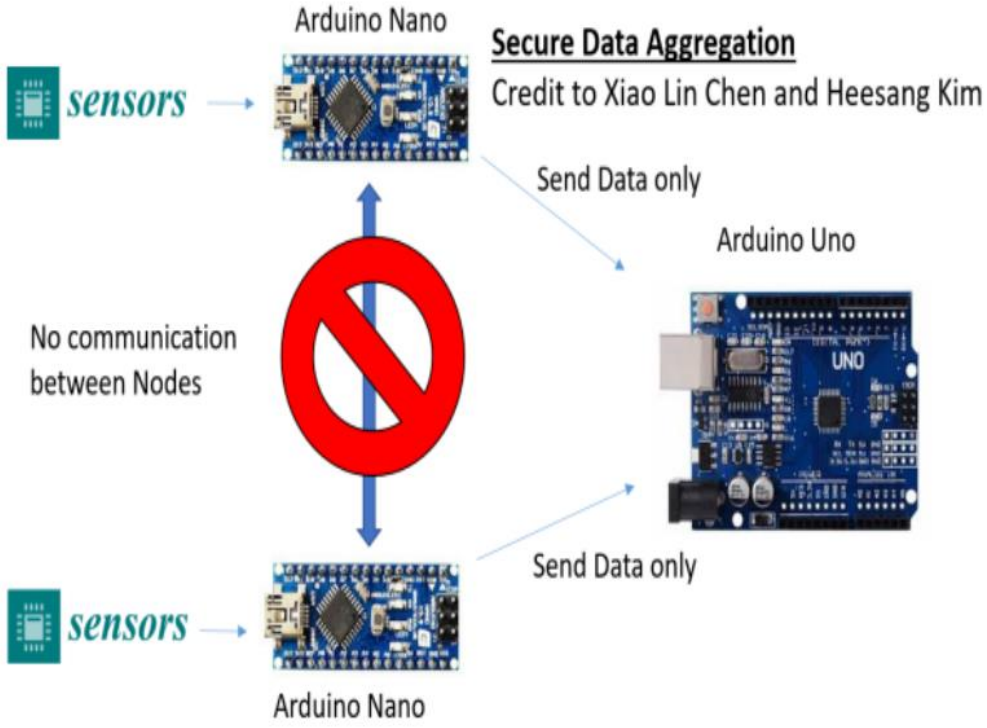

Рис. 2.6. Безпечна система агрегації даних

Протокол безпечної маршрутизації. Протокол маршрутизації – це мережеве з'єднання між пристроями в системі. Ідею безпечного протоколу маршрутизації необхідно розглядати, коли можна гарантувати безпеку передачі даних під час зв'язку. За допомогою протоколу безпечної маршрутизації мережеве з'єднання захищено від різних типів атак, таких як захоплення режиму, фізичне втручання, прослуховування, відмова в обслуговуванні тощо.

Існує кілька безпечних протоколів маршрутизації, зокрема:

ZigBee — безпечний і надійний протокол маршрутизації, який використовується в сенсорних мережах Raspberry Pi. Це стандарт бездротової сітчастої мережі з низьким енергоспоживанням, який використовується в

різноманітних програмах. ZigBee забезпечує безпечний зв’язок між вузлами та Raspberry Pi, забезпечуючи безпеку даних, що передаються між ними [9].

Z-Wave — ще один безпечний і надійний протокол маршрутизації, який використовується в сенсорних мережах Raspberry Pi. Це протокол бездротової сітчастої мережі, який використовується в різноманітних програмах. Z-Wave забезпечує безпечний зв’язок між вузлами та Raspberry Pi, забезпечуючи безпеку даних, що передаються між ними.

Thread — це безпечний і надійний протокол маршрутизації, який використовується в сенсорних мережах Raspberry Pi. Це малопотужний протокол бездротової сітчастої мережі на основі IPv6, який використовується в різноманітних програмах. Thread забезпечує безпечний зв’язок між вузлами та Raspberry Pi, забезпечуючи безпеку даних, що передаються між ними.

6LoWPAN — безпечний і надійний протокол маршрутизації, який використовується в сенсорних мережах Raspberry Pi. Це малопотужний протокол бездротової сітчастої мережі на основі IPv6, який використовується в різноманітних програмах. 6LoWPAN забезпечує безпечний зв’язок між вузлами та Raspberry Pi, забезпечуючи безпеку даних, що передаються між ними.

Виявлення вторгнення. Виявлення вторгнень у сенсорних мережах створює кілька проблем через унікальні характеристики цих мереж. По-перше, сенсорні мережі зазвичай розгортаються в суворих умовах, що робить сенсорні вузли вразливими до фізичних атак, таких як втручання та руйнування. По-друге, вузли датчиків часто мають обмежені ресурси, з обмеженою обчислювальною потужністю, пам’яттю та часом автономної роботи. Тому будь-яке рішення для виявлення вторгнень повинно бути легким і енергоефективним. По-третє, сенсорні вузли часто розгортаються у великій кількості, що ускладнює виявлення вторгнень у реальному часі. По-четверте, сенсорні вузли часто розгортаються в неконтрольованих і віддалених місцях, що ускладнює виконання технічного обслуговування та оновлення.

Існує декілька методів та інструментів виявлення вторгнень, які можна використовувати в сенсорних мережах.

Виявлення вторгнень на основі сигнатур — це техніка, яка порівнює вхідний мережевий трафік із попередньо визначеними сигнатурами або шаблонами відомих атак. Цей метод дуже ефективний у виявленні відомих атак, але він не в змозі виявити нові чи невідомі атаки.

Виявлення вторгнень на основі аномалій — це техніка, яка виявляє атаки шляхом моніторингу мережевого трафіку на наявність аномальної поведінки. Цей метод створює базову лінію нормальної поведінки мережі та виявляє відхилення від цієї базової лінії. Виявлення вторгнень на основі аномалій ефективне для виявлення нових або невідомих атак, але може призвести до хибних спрацьовувань.

Гібридне виявлення вторгнень поєднує методи виявлення вторгнень на основі сигнатур і аномалій. Цей метод використовує виявлення на основі сигнатур для виявлення відомих атак і виявлення на основі аномалій для виявлення нових або невідомих атак. Гібридне виявлення вторгнень є дуже ефективним у виявленні як відомих, так і невідомих атак [9].

Інструменти виявлення вторгнень:

SNORT — це система виявлення вторгнень із відкритим кодом, яка використовує виявлення вторгнень на основі сигнатур. SNORT легко налаштовується і може виявляти широкий спектр атак. SNORT є одним із найпопулярніших інструментів виявлення вторгнень для сенсорних мереж.

Bro — це інструмент аналізу мережі з відкритим кодом, який використовує комбінацію методів виявлення вторгнень на основі сигнатур і аномалій. Bro має широкі можливості налаштування та може виявляти широкий спектр атак.

Suricata — це система виявлення вторгнень із відкритим кодом, яка використовує комбінацію методів виявлення вторгнень на основі сигнатур і аномалій. Suricata має широкі можливості налаштування та може виявляти широкий спектр атак. Suricata відома своєю високою продуктивністю та масштабованістю.

OSSIM — це система виявлення вторгнень із відкритим кодом, яка використовує комбінацію методів виявлення вторгнень на основі сигнатур і

аномалій. OSSIM легко налаштовується і може виявляти широкий спектр атак. OSSIM відомий простотою використання та інтеграцією з іншими інструментами безпеки.

Висновки до другого розділу

Проведено аналіз історії розвитку Raspberry Pi, розглянуто протоколи безпеки сенсорних мереж та механізми безпеки.

Досліджено, що Raspberry Pi як і будь-який інший комп’ютерний пристрій, може бути вразливим до різних загроз безпеці, таких як несанкціонований доступ, зловмисне програмне забезпечення та кібератаки, проте за допомогою багатьох механізмів безпеки можна значно підвищити безпеку сенсорних мереж з використанням Raspberry Pi.

Розглянуто протоколи безпеки, де вони визначають набір правил і процедур для зв’язку між пристроями, що забезпечує безперебійний і надійний обмін даними.

3 ПОБУДОВА ЗАХИЩЕНОЇ СЕНСОРНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ ОБЛАДНАННЯ RASPBERRY PI

3.1 Апаратне забезпечення

Raspberry Pi є популярним вибором для проектів сенсорних мереж завдяки своїй низькій вартості та універсальності. Однак для забезпечення максимальної безпеки важливо вибрати правильну модель і аксесуари.

Raspberry Pi 4 — остання та найпотужніша модель, рекомендована для проектів сенсорних мереж. Також знадобиться блок живлення, SD-карта, футляр і мережевий інтерфейс, наприклад Ethernet або Wi-Fi. На рис. 3.1 представлний набір Raspberry Pi 4. На рис.3.1 показана інстальована Raspberry Pi 4 у футляр [10].

Рис. 3.1. Набір Raspberry Pi 4

Рис. 3.2. Інстальована Raspberry Pi 4

3.2 Встановлення операційної системи

Заванатаження образу Raspbian. На рис. 3.3 необхідно завантажити образ Raspberry Pi для Windows.

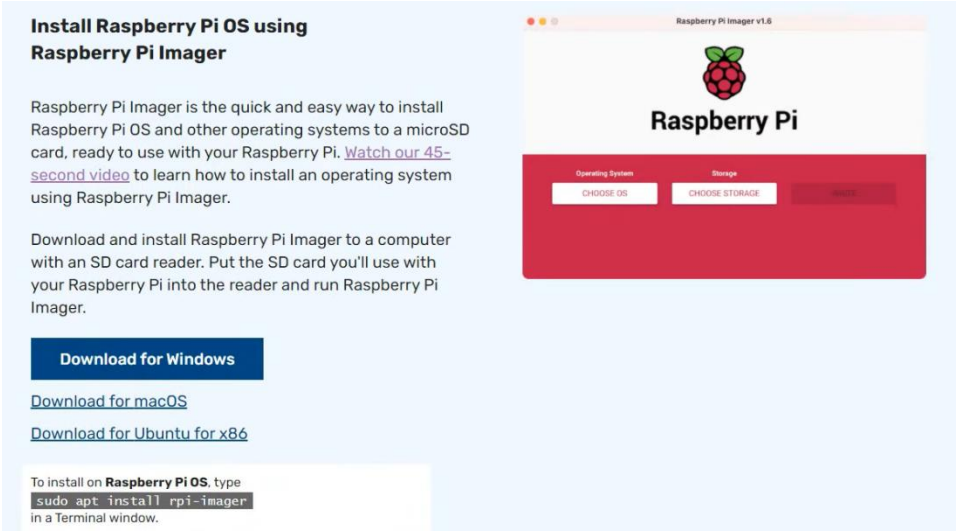

Рис. 3.3. Завантаження образу Raspberry Pi для Windows

Рис. 3.4. Raspberry Pi Imager

Після того, як встановили образ Raspberry Pi, відкрвається вікно з вибором операційної системи (рис. 3.5) та SD карти (рис. 3.8). На рис. 3.6 зображений випадаючий список з багатьма ОС на вибір. На рис. 3.7 зображена обрана ОС.

Рис. 3.5. Вікно з записом образу

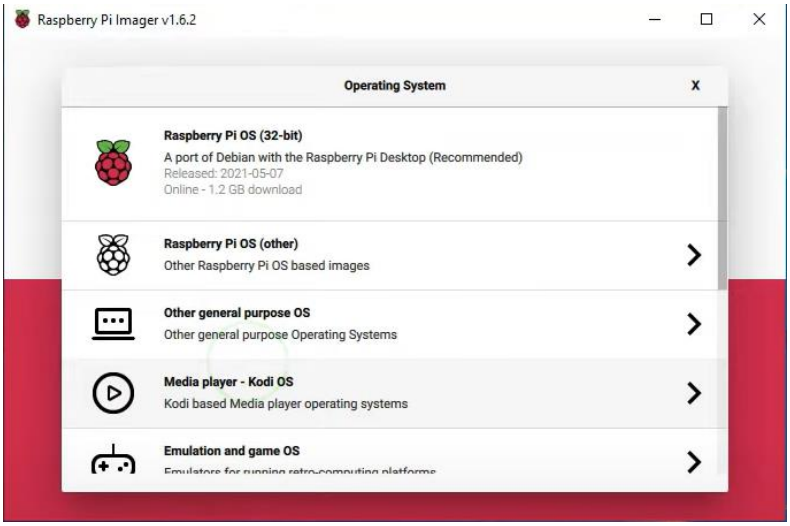

Рис. 3.6. Вибір ОС

Рис. 3.7. Обрана ОС

Обираємо потрібну SD карту для нашої Raspberry Pi (рис. 3.8). Якщо обрати не ту SD карту, то інсталювання видалить всі дані з вашої флешки.

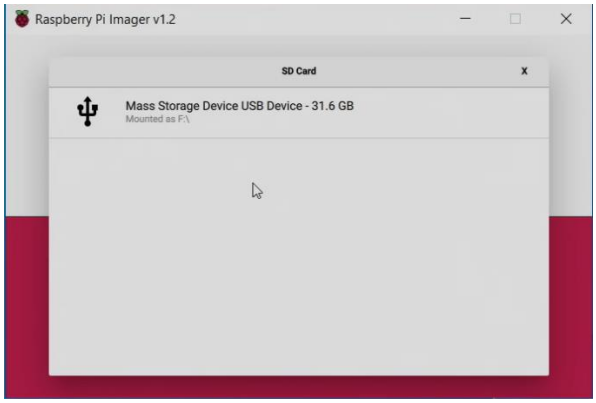

Рис. 3.8. Обираємо SD карту

Далі за допомогою кнопки «Записати» починається процес запису образу на SD карту. На рис. 3.9 показан процес запису образу.

Рис. 3.9. Процес запису образу

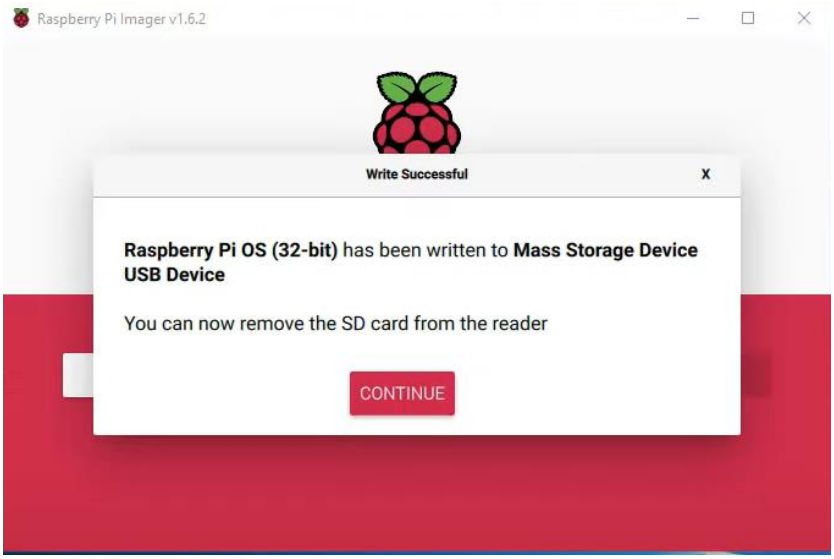

Рис. 3.10. Вікно з успішним записом образу на SD карту

Після того, як образ був записаний на SD карту, необхідно вставити флешку в Raspberry Pi та підключити всі периферійні пристрої, такі як: клавіатуру, мишу та монітор. На рис. 3.11 зображена підключена Raspberry Pi 4 [10].

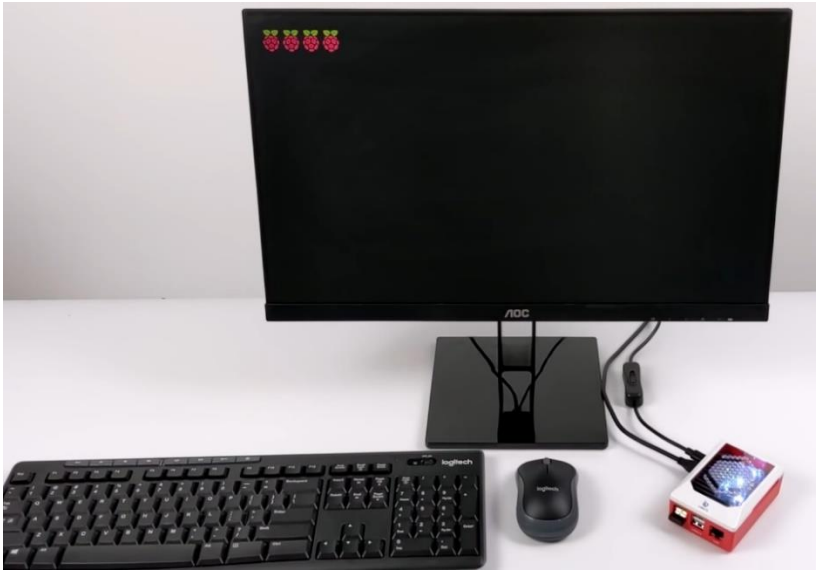

Рис. 3.11. Підключена Raspberry Pi 4

На рис. 3.12 показана встановлена операційна система Raspberry Pi.

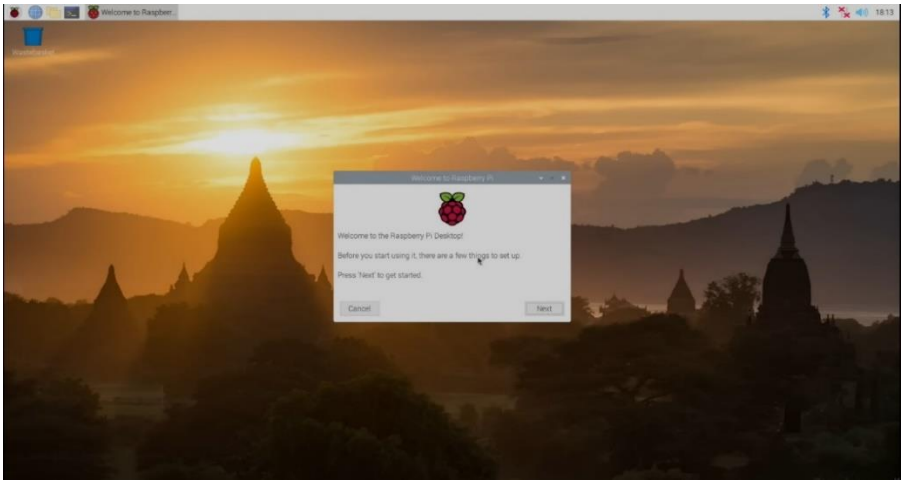

Рис. 3.12. Операційна система Raspberry Pi

Далі необхідно налаштувати операційну систему Raspberry Pi. На рис.3.13 показано про налаштування регіону та мови. На рис. 3.14 налаштовуємо пароль. Пароль за замовчуванням raspberry, але слід його змінити для безпеки Raspberry Pi.

Рис. 3.13. Налаштування регіону

Рис. 3.14. Встановлення паролю

На рис. 3.15 обираємо мережу до якої хочемо підключитися та вводимо пароль до неї.

Рис. 3.15. Обираємо мережу

Після налаштування ОС, повинні оновити Raspberry Pi, щоб мати останні патчі безпеки та виправлення помилок.

Рис. 3.16. Оновлення ОС

3.3 Встановлення програмного забезпечення безпеки

Антивірус — це досить корисне програмне забезпечення, яке підвищить безпеку пристрою Raspberry Pi. Наявність антивірусного програмного забезпечення зменшить шанси легкого злому Raspberry Pi, що дозволить користувачам вільно користуватися пристроєм.

```
pi@        :~ $ sudo apt-get install clamav && sudo apt-get install clamtk
Reading package lists... Done
Building dependency tree... 50%
```

Рис. 3.17. Встановлення антивірусу ClamAV

Fail2ban. Fail2ban – це програмне забезпечення для запобігання вторгненням, яке відстежує системні журнали на предмет невдалих спроб входу та блокує IP-адресу зловмисника.

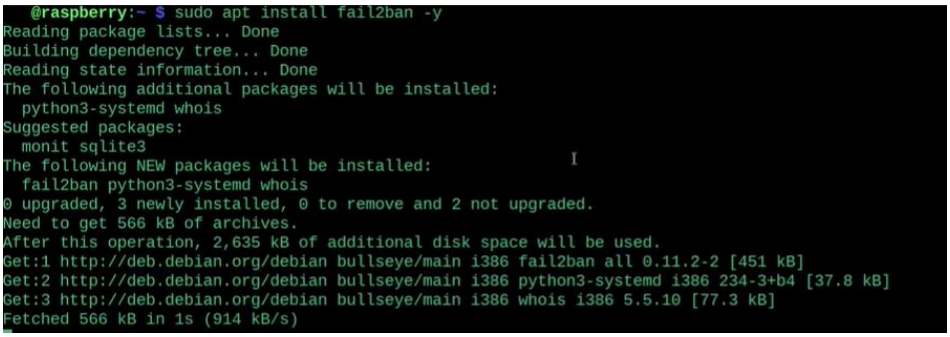

Рис. 3.18. Завантаження Fail2ban

Команда «sudo systemctl enable fail2ban --now» використовується для ввімкнення та запуску служби Fail2ban на ОС Raspbian.

Рис. 3.19. Запуск Fail2ban

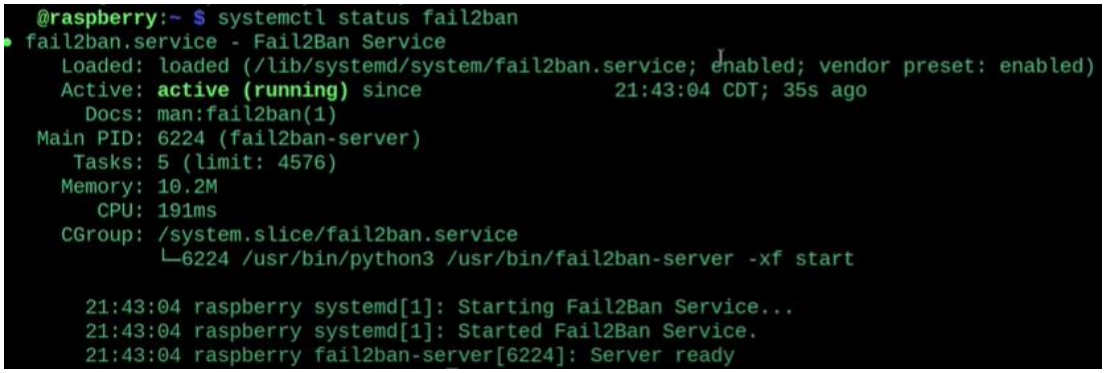

Рис. 3.20. Статус служби

Команда використовується для створення локальної копії файлу конфігурації Fail2ban на ОС Raspbian.

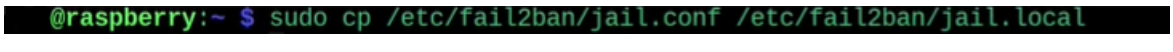

Рис. 3.21. Локальна копія файлу конфігурації

Рис. 3.22. Редагування файлу конфігурації

В цьому файлі необхідно редагувати bantime, findtime та maxretry. Якщо хтось зробить 3 помилки протягом 1 години, його буде заблоковано на 24 години [11].

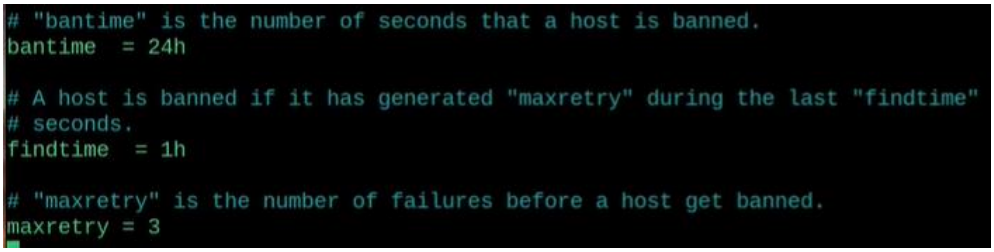

Рис. 3.23. Редагування файлу конфігурації

Далі необхідно налаштувати порти.

Рис. 3.24. Дозвіл до ssh

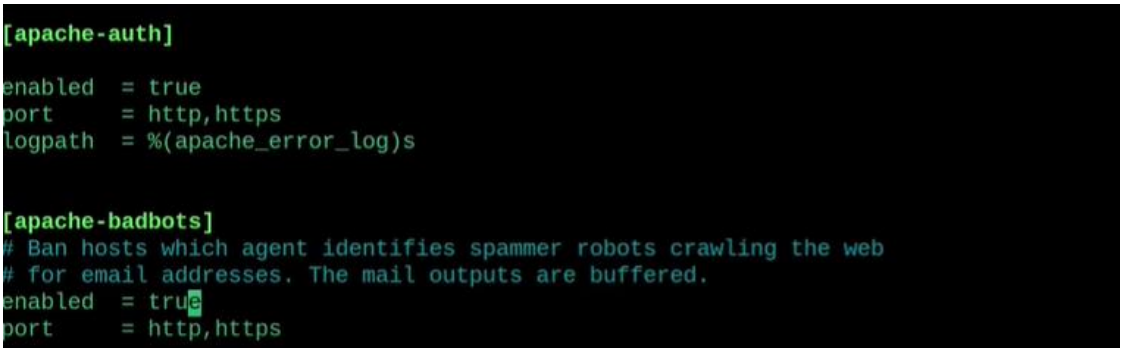

Рис. 3.25. Дозвіл до серверу

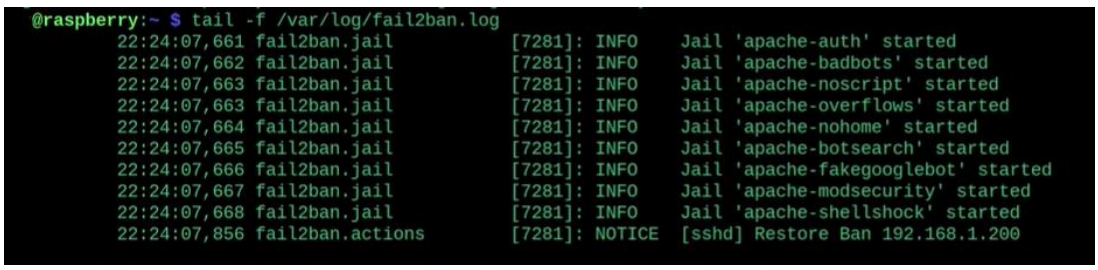

Рис. 3.26. Перегляд файлу журналу Fail2ban у реальному часі

3.4 Налаштування мережевої безпеки

Брандмауер є важливим інструментом безпеки для будь-якої системи, підключеної до мережі, включаючи Raspbian OS. Це може допомогти захистити Raspberry Pi від різних типів атак і забезпечити конфіденційність, цілісність і доступність ваших даних [11].

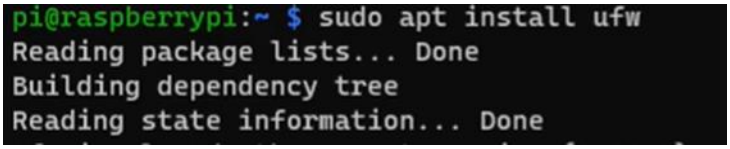

Рис. 3.27. Встановлення брандмауеру

Рис. 3.28. Запуск фаєрволу

Щоб підключитися до серверів, потрібно надати брандмауеру доступ до портів. Порт 80 потрібен для HTTP і 443 для HHTPS. Якщо Raspberry Pi не підключається до жодного сервера, потрібно перевірити документацію та дізнатися, які порти використовує сервер.

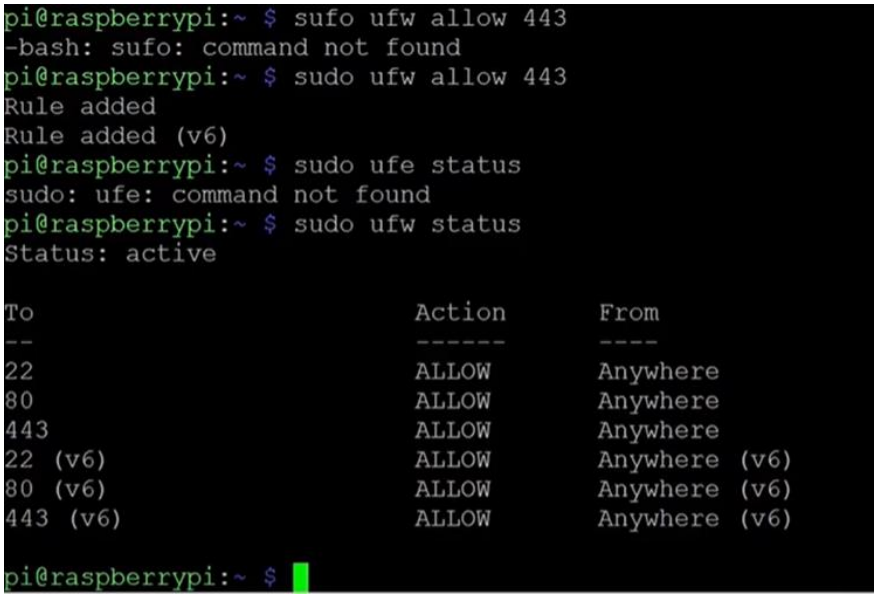

Рис. 3.29. Дозвіл веб-порту 80 для HTTP і 443 для HTTPS

Обмеження швидкості брандмауеру. Обмеження швидкості – це техніка, яка використовується для контролю швидкості вхідного мережевого трафіку, щоб запобігти перевантаженню мережі та захистити від атак DoS.

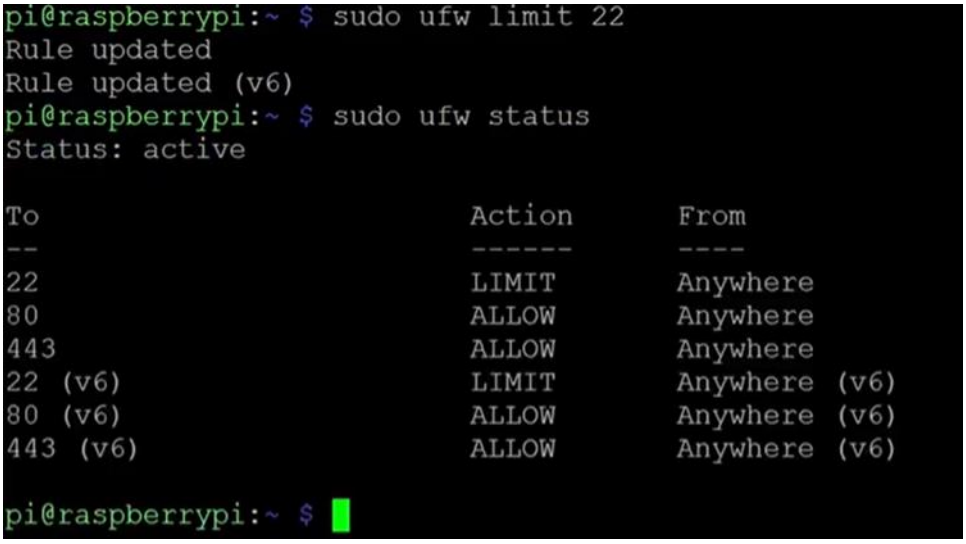

Рис. 3.30. Обмеження швидкості для порту 22

Як видно, порт 22 (ssh) змінив свій статус на «allow», що означає, що він не дозволить більше 6 з'єднань з одного ip-з'єднання протягом 30 секунд.

TCP/UDP. DNS працює як на UDP, так і на TCP на порту 53. Можна дозволити лише TCP-трафік для DNS і заблокувати UDP-трафік, та можна налаштувати брандмауер так, щоб блокувати вхідний UDP-трафік на порту 53, дозволяючи вхідний TCP-трафік на порту 53 [11].

Рис. 3.31. Дозвіл порту 53 TCP

Налаштування дозволу підключення по IP. Можна дозволити ssh приймати лише одну IP-адресу і блокувати трафік з інших IP-адрес.

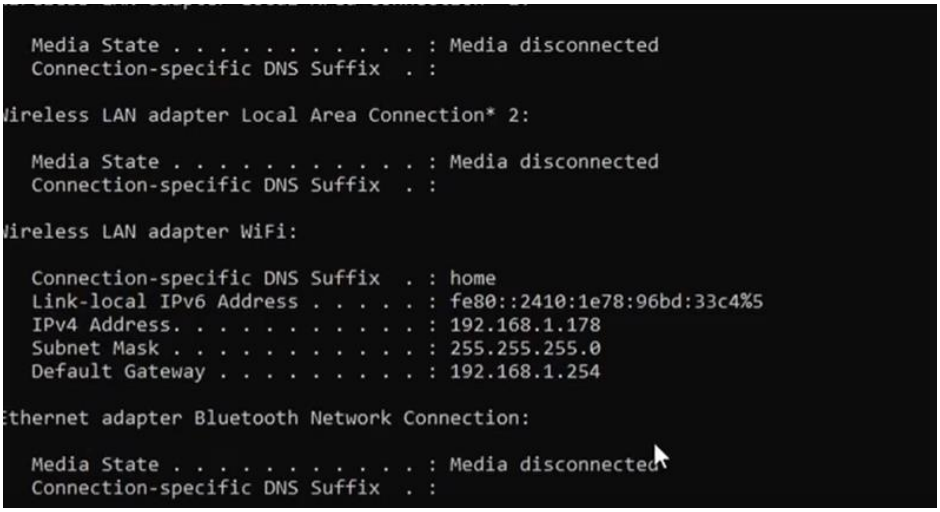

Рис. 3.32. IP-адреса нашої машини

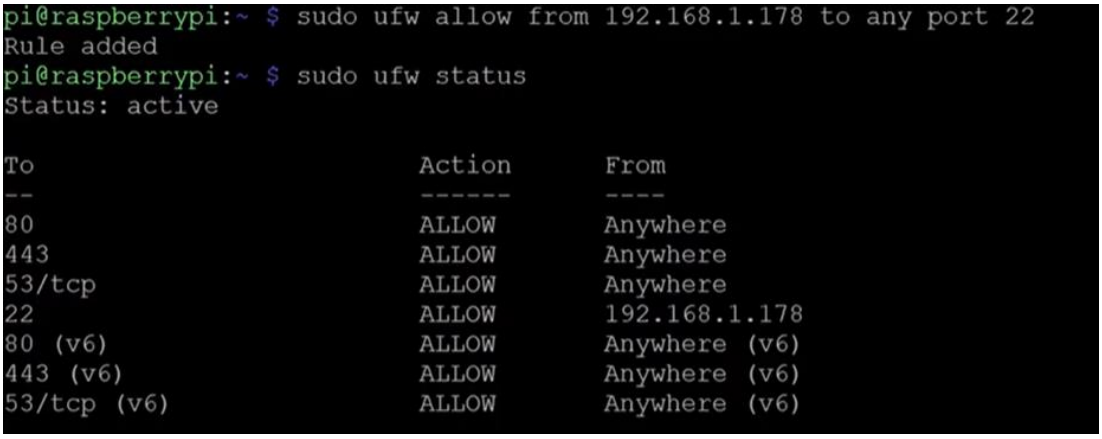

Рис. 3.33. Дозвіл до конкретної IP-адреси

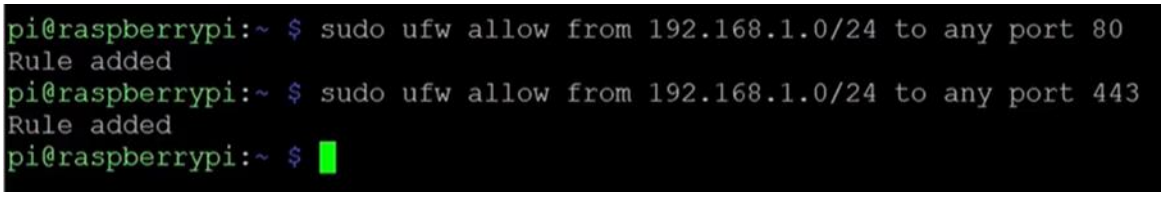

Рис. 3.34 Дозвіл конкретного IP діапазону та портів

3.5 Шифрування передачі даних

Для шифрування передачі даних в ОС Raspbian можна використовувати протокол Secure Shell (SSH), який забезпечує безпечне зашифроване з’єднання між двома комп’ютерами через незахищену мережу [11].

По-перше, потрібно генерувати ключі SSH за допомогою інструменту SSH-keygen, який уже встановлено на Raspberry Pi.

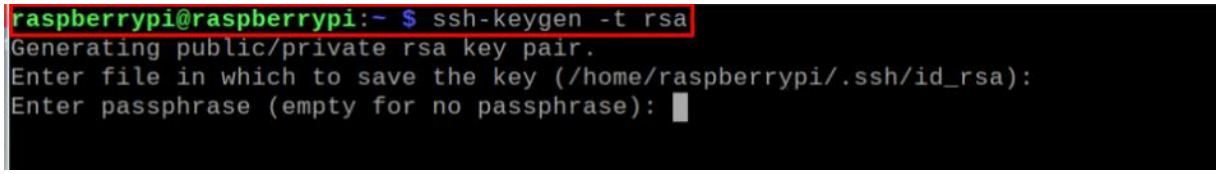

Рис. 3.35. Генерація ключів

Далі необхідно зберегти ключі у файлі за замовчуванням.

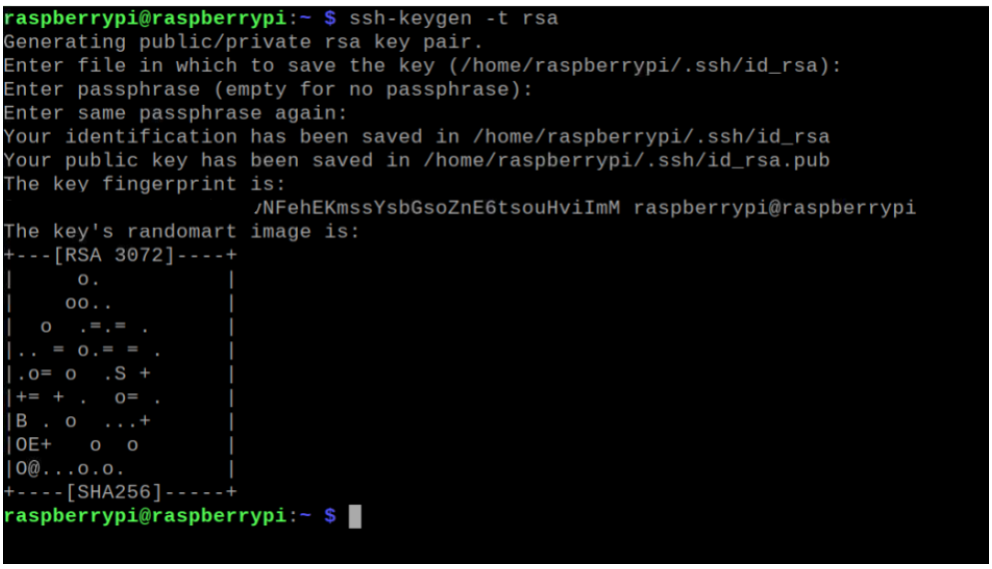

Рис. 3.36. Згенеровані ключі

Далі необхідно скопіювати файл id_dsa.pub у Raspberry Pi.

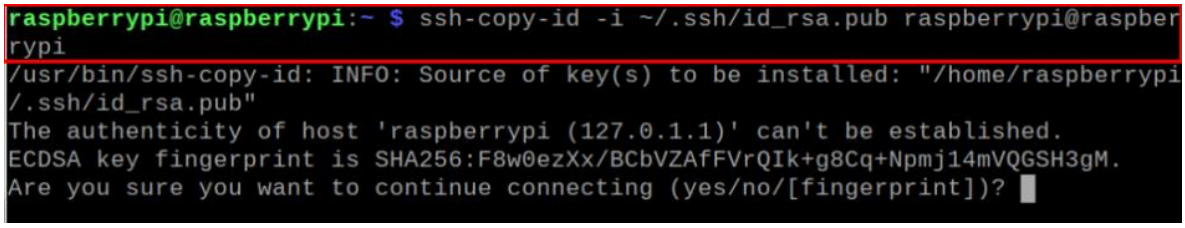

Рис. 3.37. Копія файлу

Після налаштування необхідно скористатися наступною командою, щоб увійти в машину без пароля.

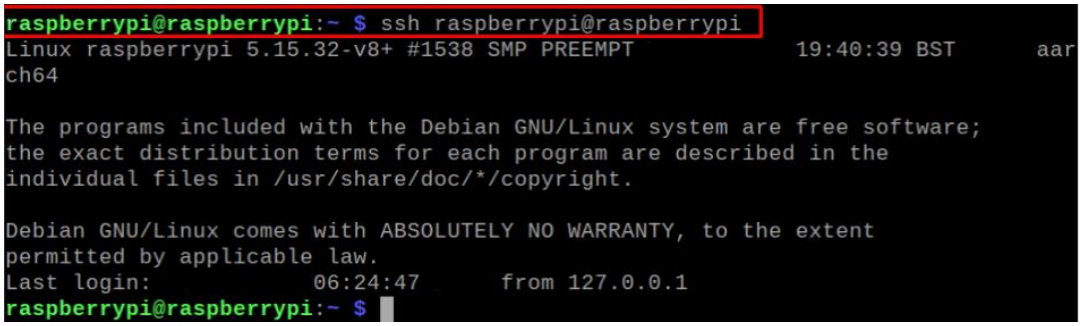

Рис. 3.38. Вхід в машину

Тепер, коли ключі SSH налаштовано на Raspberry Pi, настав час дозволити довіреному користувачеві отримати доступ до пристрою без використання пароля.

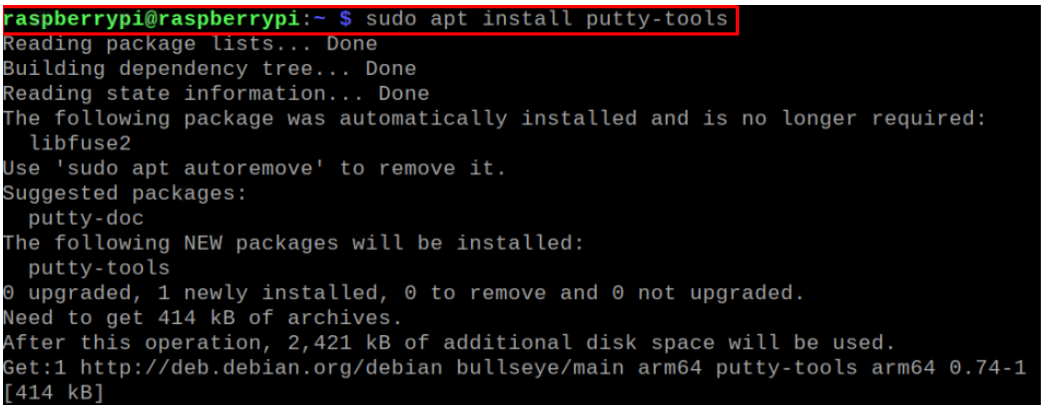

Рис. 3.39. Заванатаження Putty

Далі необхідно створити файл .ppk, який містить інформацію про авторизацію Raspberry Pi.

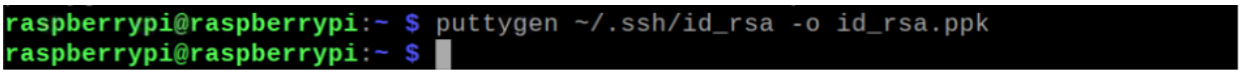

Рис. 3.40. Створення файлу

Необхідно відкрити PuTTY у системі та перейти до параметра «Auth» у розділі SSH.

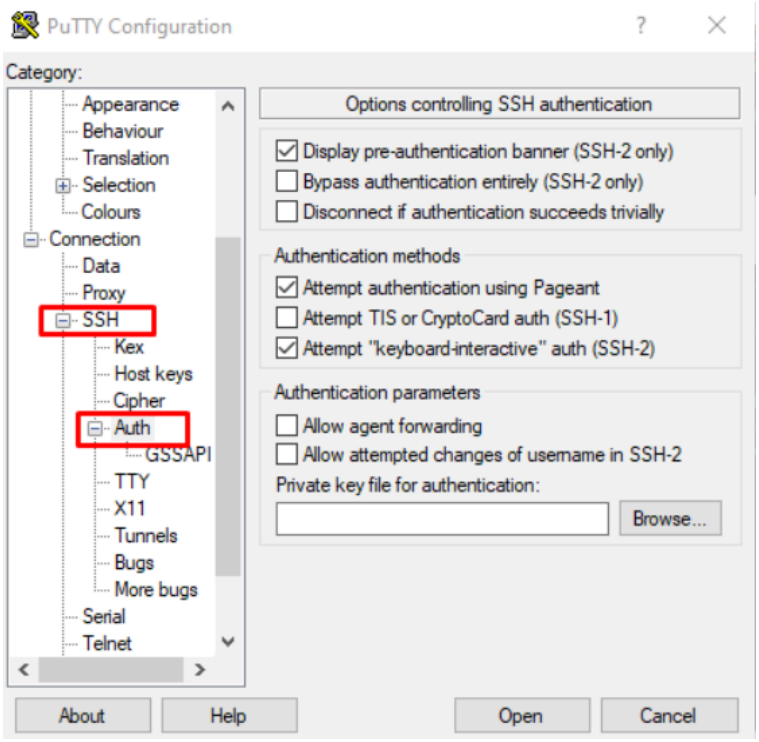

Рис. 3.41. Параметр «Auth»

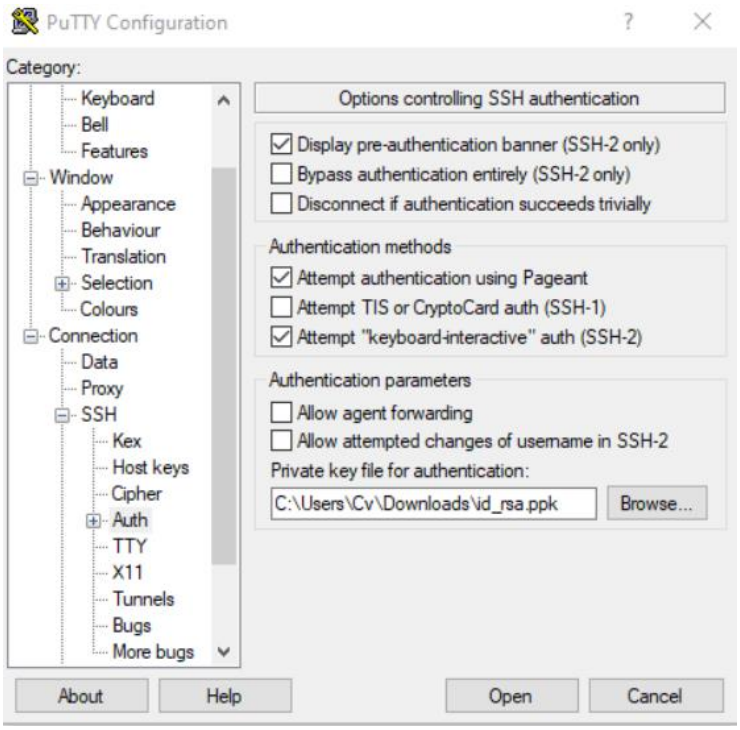

Рис. 3.42. Заванатаження файлу “id_rsa.ppk”

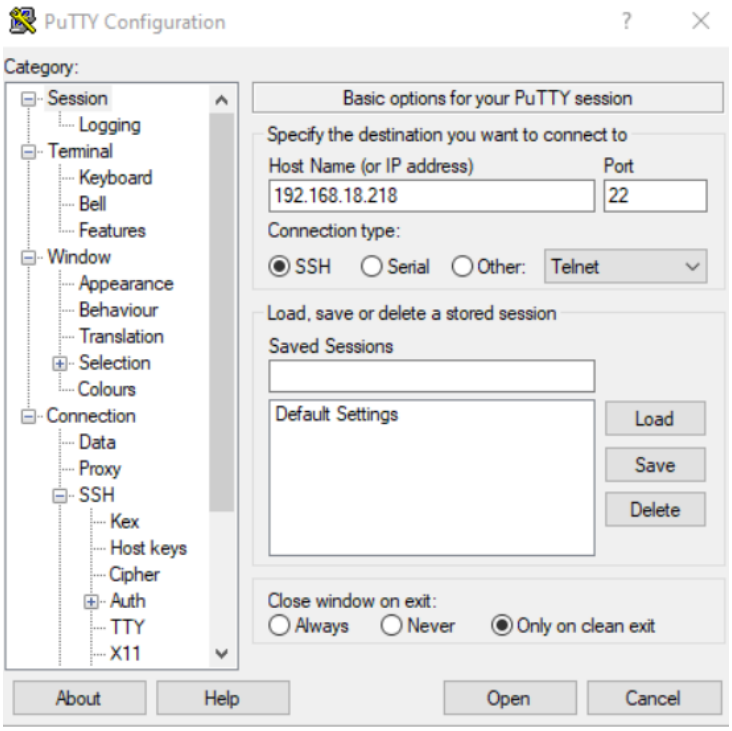

Рис. 3.43. Raspberry Pi IP адрес

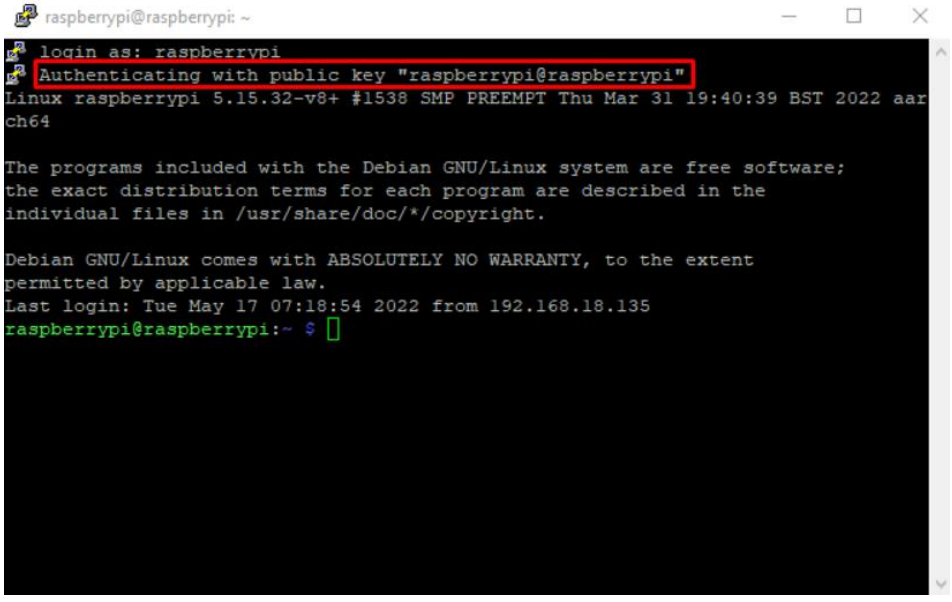

Рис. 3.44. Підключення до машини

Ключі SSH є найбезпечнішими параметрами порівняно з входом на основі пароля, що дозволяє лише певному користувачеві отримати доступ до пристрою. Наведені вище вказівки допоможуть убезпечити пристрій Raspberry Pi, налаштувавши ключі SSH. Після налаштування можна використовувати ці ключі для доступу до пристрою з будь-якої системи через PuTTY віддалено без введення пароля [11].

3.6 Рекомендації щодо побудови захищеної сенсорної мережі

Raspberry Pi — це популярний одноплатний комп’ютер, який набув великої популярності в останні роки завдяки своїй доступності, універсальності та простоті використання. При правильному налаштуванні та конфігурації Raspberry Pi можна використовувати для створення різноманітних IoT-проектів, включаючи сенсорні мережі.

Однак безпека є критичною проблемою, коли мова йде про створення будь-якої мережі, особливо сенсорної мережі.

Остання версія ОС Raspberry Pi. Один із найпростіших способів захистити мережу датчиків Raspberry Pi — це використовувати останню версію ОС Raspberry Pi. Кожен новий випуск операційної системи містить оновлення безпеки, які допомагають захистити від вразливостей і експлойтів. Обов’язково необхідно оновлювати ОС Raspberry Pi, регулярно перевіряючи наявність оновлень і встановлюючи їх.

Використання надійного паролю. Це один із найпростіших заходів безпеки, але про нього варто згадати. Обов’язково необхідно використовувати надійний пароль для Raspberry Pi і не використовуйте пароль за умовчанням. Надійний пароль має містити принаймні 12 символів і містити поєднання великих і малих літер, цифр і символів.

Двофакторна автентифікація. Двофакторна автентифікація додає додатковий рівень безпеки сенсорній мережі Raspberry Pi. Якщо ввімкнено двофакторну автентифікацію, потрібно буде ввести код, згенерований програмою автентифікації на телефоні, крім пароля. Це значно ускладнює зловмисникам отримати доступ до вашого Raspberry Pi, навіть якщо їм вдається вгадати пароль.

Ключі SSH замість паролів. Ключі SSH забезпечують більш безпечний спосіб входу в Raspberry Pi, ніж паролі. За допомогою ключів SSH користувач створює пару відкритий/приватний ключ і зберігаєте закритий ключ на своєму комп’ютері. Коли користувач хоче увійти до свого Raspberry Pi, він використовує

закритий ключ для автентифікації замість пароля. Це значно ускладнює зловмисникам вгадати або зламати пароль.

Брандмауер. Брандмауер — це програма, яка відстежує та контролює вхідний і вихідний мережевий трафік. Використовуючи брандмауер, можна заблокувати небажаний трафік у вашій сенсорній мережі Raspberry Pi і дозволити лише трафік, необхідний для функціонування вашої сенсорної мережі. ОС Raspberry Pi постачається з вбудованим брандмауером під назвою ufw (Uncomplicated Firewall), який можна використовувати для налаштування правил брандмауера.

Шифрування даних. Якщо сенсорна мережа Raspberry Pi передає конфіденційні дані, наприклад особисту інформацію або фінансові дані, важливо зашифрувати ці дані, щоб запобігти їх перехопленню зловмисниками.

VPN. Якщо потрібно отримати доступ до мережі датчиків Raspberry Pi з-за меж локальної мережі, важливо використовувати VPN (віртуальну приватну мережу), щоб захистити з’єднання. VPN створює безпечний зашифрований тунель між вашим пристроєм і Raspberry Pi, що значно ускладнює зловмисникам перехоплення вашого трафіку [11].

Підсумовуючи, побудова безпечної сенсорної мережі Raspberry Pi є важливою для захисту даних, що передаються. Захищені протоколи, автентифікація, авторизація, VPN, брандмауер, фізична безпека, регулярні перевірки безпеки та надійні паролі – все це є важливими для побудови безпечної мережі датчиків Raspberry Pi. Дотримуючись цих рекомендацій, можна переконатися, що мережа датчиків Raspberry Pi безпечна та захищена від несанкціонованого доступу.

Висновки до третього розділу

Реалізована захищена сенсорна мережа з використанням Raspberry Pi.

Проведено аналіз існуючих інструментів щодо побудови захищеної сенсорної мережі Raspberry Pi на бізі Raspbian ОС.

Розроблено рекомендації щодо побудови захищеної сенсорної мережі Raspberry Pi.

ВИСНОВКИ

В бакалаврській роботі отримано наступні наукові та науково-практичні результати:

— досліджено поняття сенсорних мереж та розкрито поняття актуальності і важливості захисту сенсорних мереж в межах охорони здоров’я, моніторингу навколишнього середовища, розумних будинків та кібербезпеки.

— розглянуто компоненти та архітектуру бездротових мереж. Досліджено історію розвитку Raspberry Pi;

— проаналізовано питання безпеки сенсорних мереж та розглянуто поширені атаки, такі як: відмова в обслуговуванні, атаки глушіння, атаки компрометації вузлів, атаки Сибілу тощо;

— проведено аналіз особливостей побудови сенсорних мереж Raspberry Pi. Розглянуто налаштування системи моніторингу мережі, встановлення необхідного програмного забезпечення, налаштування мережі датчиків, налаштування системи виявлення вторгнень;

— проведено аналіз протоколів безпеки сенсорних мереж Raspberry Pi. Розглянуто механізми безпеки, такі як: шифрування даних, брандмауер, захищене віддалене підключення, безпечне агрегування даних, протоколи безпечної маршрутизації та виявлення вторгнення;

— реалізовано захищена сенсорна мережа з використанням Raspberry Pi. Досліджено функціонал існуючих інструментів щодо побудови захищеної мережі Raspberry Pi на базі Raspbian ОС;

— розроблено рекомендації щодо побудови захищеної сенсорної мережі з використанням обладнання Raspberry Pi.