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 ПІДВИЩЕННЯ РІВНЯ БЕЗПЕКИ ПРИ ПЕРЕДАЧІ ІНФОРМАЦІЇ В МЕРЕЖІ ІОТ»

Виконала студентка 4 курсу, групи БСД-43
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Хоменко А.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. Internet of Things (IoT), на даний момент є надзвичайно популярним та актуальним. Інтернет речей, представляє з'єднання практично всіх пристроїв, якими можна контролювати та керувати ними онлайн. IoT — це мережа транспортних засобів, фізичних об'єктів, будівель, пристроїв тощо деякі інші елементи, вбудовані в програмне забезпечення, підключення до мережі, електроніки та датчиків, що дозволяє цим об'єктам обмінюватися та збирати дані.

Дана технологія має ряд переваг, що нами було досліджено в роботі. Новітнє рішення, яке дозволяє дистанційно контролювати та керувати пристроями. Саме, це дозволяє підвищити точність, ефективність та економічний зріст.

Різноманітність пристроїв, які мають доступ до Інтернету, з кожним днем збільшується, а поряд із ними і вразливості для даних об'єктів. Тому, мають потребу в кращому зберіганні, обробці та захисту інформації, які містять пристрої. Для того, щоб зменшити вразливості, ми навели ряд рекомендації, що допоможуть підвищити рівень захисту в мережі.

Завжди, буде залишатися в пріоритеті безпека інформації та даних, які обробляються в мережі, особливо коли використовується велика кількість пристроїв.

Для того, щоб виконати дану проблему, потрібно підходити комплексно, тобто використовувати всі рекомендації разом. IoT є великою мережею, тому має вразливість до складних атак.

Мережа активно розвивається, тому виникають ситуації, які потребують більше часу, задля аналізу та в подальшому вирішенні проблеми.

Також, є випадки коли пристрої, які виконують функції IoT, розташовані за межами контрольованої зони. Для них, потребується більше часу, для того щоб

контролювати їхній життєвий шлях. Виконується задля уникнення вразливостей, які можуть використати зловмисники.

В роботі, детально надано рекомендації, для підвищення захисту в мережі та уникнення несанкціонованого доступу до інформації.

Об'єкт дослідження — безпечна передача інформації в мережі IoT.

Предмет дослідження — методи і засоби ідентифікації стану інформаційної безпеки пристроїв IoT.

Мета роботи — розробити рекомендації щодо безпеки використання пристроїв та передачі інформації в мережі IoT.

Завдання бакалаврської роботи:

- дослідити сучасну архітектуру IoT;
- розглянути область використання IoT;
- дослідити існуючі загрози мережі IoT;
- проаналізувати вразливості у мережі IoT;
- виконати рекомендації задля уникнення або зменшення загроз у мережі IoT.

Методи дослідження — опрацювання літератури за даною темою, теорія інформації, стандарти в сфері кібербезпеки.

1 АНАЛІЗ АРХІТЕКТУРИ МЕРЕЖІ ІОТ ТА ЇЇ ПЕРЕВАГИ

1.1 Концепція IoT

Найбільш популярною та доступною мережею являється Internet of Things (IoT). Що собою представляє IoT? IoT - це система взаємопов'язаних обчислювальних пристроїв, які в свою чергу забезпечені унікальними ідентифікаторами та можливістю передачі даних через мережу, яка не вимагає зв'язку «людина-людина» або «людина-комп'ютер». Дана система має вплив на багато сфер та застосовується кожним з нас. Технологія відповідає за збір інформації в будь-яких умовах, та може знайти використання у багатьох сферах. IoT представимо далі, як систему, яка:

- IoT являється сучасною інновацією в сфері технологій;
- IoT є однією з важливих технологією на сучасному ринку;

Вплив IoT з кожним роком підвищується та стає більш затребуваний. Також, системи IoT можуть відповідати за виконання дій, наприклад: інтелектуальні торгові системи можуть контролювати ваші покупки, через відстеження інформації у мобільному пристрої. Користувачам у процесі надається інформація про спеціальні пропозиції, саме для них, а також можуть бути запропоновані пропозиції для місць, які вони бажатимуть відвідати. Інші функції, які можна запропонувати відносяться до розширення автоматизації та функцій безпеки будинку. Продукти IoT можна класифікувати, за такими категоріями, як:

- «розумний» будинок;
- «розумне» середовище;
- «розумне» підприємство.

Розглянемо, що являє собою інформаційно-комунікаційні технології (IT), це засіб надійності та безпеки, та забезпечення систем для критичних та комерційних доменів [1].

За допомогою технології IoT можна створювати динамічні мережі, які складаються з кількох міліардів елементів, які в свою чергу взаємодіють між собою.

Рис. 1.1. Взаємодія IoT

Існує багато факторів, за допомогою яких виник IoT, основні з них:

- збільшення пропускної здібності інтернету;
- здійснення доступу для користувачів і пристроїв до мережі із великої кількості місць;
- збільшення кількості пристроїв, які мають доступ до інтернету;
- збільшення потреб, які пов’язані з взаємодіями в Інтернеті;
- розвиток інфраструктури інтернету речей.

До перших представників Інтернету речей можна віднести Machine-to-Machine, M2M). Дана технологія дозволяє машинам обмінюватися інформацією один з одним. Наприклад, банкомати можуть автоматично передавати інформацію по GSM-мережах, про те що в них закінчилися кошти або навпаки, що коштів багато і потрібно, щоб прийшли інкасатори. Застосування даної технології широко поширене та застосовується у багатьох сферах, таких як: медицина, логістика, енергетика та багато інших. Один з найбільш популярних методів M2M являється дистанційний моніторинг і управління процесами за допомогою різних датчиків, міток. Цей метод називається Radio frequency identification (RFID).

Мітки допомагають детального відслідковувати процеси виготовлення продукції. А також, допомагають оптимізувати логістичні ряди, мінімізувати витрати на транспорт, та найголовніше знизити людський фактор на всіх етапах виготовлення продукції та продажу товару. Саме, за допомогою даних міток, можна в будь-який момент відслідковувати стан товару, а також вони можуть повідомити про неполадки в роботі.

M2M являється основою для концепції Інтернету речей. Але, з розвитком IoT, яка стала більш розвинутою, ніж M2M, тому що міжмашинне взаємодія представляє взаємодію між машинами, а інтернет речей більш широке поняття, яке в першу чергу взаємодіє між машиною і людиною. Різного роду інновації, виникають на основі інтернету речей та проявляються на всіх етапах бізнес-процесу [1].

Основні характеристики IoT:

- будь-яку річ можна приєднати до глобальної інформаційно-комунікаційної інфраструктури.
- IoT пристрої базуються на різних апаратних платформах і мережах. Вони можуть взаємодіяти з іншими пристроями або платформами через різні мережі.
- динамічні зміни, які характерні для стану пристроїв, наприклад підключений або непідключений стан, а також місцезнаходження та швидкість. Крім того, можуть змінювати динамічно кількість пристроїв.
- широкомасштабність.

Вимоги, які мають значення для IoT:

- з’єднуються на основі ідентифікації.
- функціональна сумісність: це потрібно для забезпечення функціональної сумісності неоднорідних та розподілених систем з метою зменшення різних типів інформації.
- організація автономних мереж, це допоможе адаптуватися до різних областей застосування, різних середовищ передавання даних та великої кількості пристроїв різних типів.

- надання автономних послуг. Послуги, надаються за допомогою автоматичного збору, передачі та обробки даних на основі правил.
- можливості, які засновуються на визначенні місця розташування. Потрібно, щоб інформація про місцезнаходження визначалася і відслідковувалася автоматично.
- безпека. Кожин пристрій в IoT, має зв'язок із Інтернетом, тому повинна бути забезпечена конфіденційність, цілісність та доступність. Необхідно об'єднувати різні принципи і методи забезпечення безпеки.
- потрібно, щоб в IoT забезпечувався захист особистого життя користувачів. Пристрої, можуть містити особисту інформацію про їхніх користувачів та власників. Тому, необхідно, щоб IoT забезпечував захист даної інформації при передачі, зберіганні, аналізу і обробки даних.
- потрібно, щоб в IoT підтримувалися високоякісні та захисні послуги, які пов'язані з організмом людини. Законодавчі та нормативні акти, містять дану інформацію.
- автоматична конфігурація. Дана вимога потрібна для того, щоб оперативно створювати, формувати і встановлювати конфігурацію на основі семантики з метою безперешкодної інтеграції та взаємодії приєднаних речей до додатків.
- управління. Для того, щоб в IoT підтримувалася управління для забезпечення нормальної функціонування мережі.

1.2 Архітектура IoT

У рекомендаціях Y.2060 «Глобальна інформація. Інфраструктура, аспекти протоколу. Інтернет та наступні покоління. Мережа наступних поколінь - структура та функціональні архітектурні моделі» вказано еталонну модель IoT, яка складається з чотирьох базових горизонтальних рівнів:

- рівень додатків IoT;
- рівень підтримки додатків та послуг;

- мережевий рівень;
- рівень пристроїв.

Дана модель зображена на рисунку 1.2:

Рис. 1.2. Еталонна модель IoT

Рівень додатків IoT в даних рекомендаціях детально не розглядається. Рівень підтримку додатків і послуг містить загальні рекомендації для різних об’єктів IoT по обробці і зберіганню даних, а також можливості, які необхідні для деяких додатків IoT або груп даних додатків. Мережевий рівень включає у себе мережеві можливості, а саме функції управління ресурсами мережі доступу і транспортної мережі, управління мобільністю, функції авторизації, аутентифікації і розрахунків, AAA, а також транспортні можливості, тобто забезпечення зв’язку мережі для передачі інформації додатку і послуг IoT. Рівень пристроїв включає можливості пристроїв і можливості шлюза. Можливості пристроїв забезпечують прямий обмін з мережею зв’язку, обмін через шлюз. Можливості шлюза забезпечують підтримку багатьох інтерфейсів для пристроїв, і для мереж доступу/транспортних мереж [1].

Існують, також два вертикальних рівні, це – рівень управління і рівень безпеки, які охоплюють всі чотири горизонтальні рівні. Можливості вертикального рівня експлуатаційного управління забезпечують управління наслідками збоїв, можливостей мережі, конфігурації, безпеки. Основними об'єктами управління є пристрої, локальні мережі і їх топологія, трафік. Можливості вертикального рівня безпеки будуть залежати від горизонтального рівня. Для рівня підтримки додатків і послуг визначені функції AAA та антивірусний захист, тести і цілісність даних. Для мережевого рівня представлені можливості авторизації, аутентифікації. На рівні пристроїв є можливість авторизації, аутентифікації, контролю доступу, конфіденційності даних.

Зазначимо, що модель передачі даних в Інтернеті речей буде відрізнятися від існуючої моделі передачі даних через Інтернет. В моделі IoT фігурують два важливих поняття. Мережа, яка має обмеження буде мати низьку швидкість, тобто менше 1Мбіт і також мати високі затримки. Мережа, яка не матиме обмеження характеризується високими швидкостями передачі даних і схожа на існуючу мережу Інтернет.

На рис. 1.3 зображено дві моделі, та їх різниця між ними.

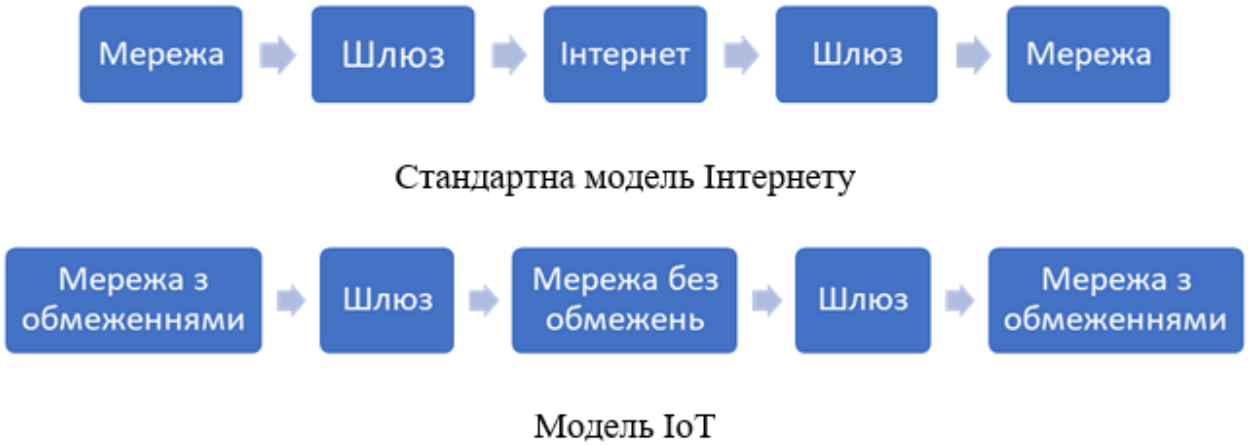

Рис. 1.3. Порівняння моделей передачі даних в інтернеті і в IoT

Розглянемо більш детально кожен рівень еталонної моделі IoT та функції, які реалізуються на них [1].

Рівень пристроїв. Найнижчий рівень архітектури IoT, який складається із «smart» об’єктів, які інтегровані із сенсорами(датчиками). За допомогою сенсорів, реалізується підключення фізично і віртуально, та забезпечується збір і обробка інформації в реальному часі. Існують різні типи сенсорів для різноманітних цілей, наприклад для визначення температури, швидкості, місцезнаходження та інше. Сенсори мають невелику пам’ять, що дає можливість записувати деяку кількість результатів. Також, сенсори можуть вимірювати фізичні параметри контрольованого об’єкта. Вони класифікуються по різних задачах, наприклад сенсори для тіла, сенсори для побутової техніки, сенсори для транспорту.

Більшість сенсорів потребують підключення з шлюзом, які реалізуються з використанням мережі, Ethernet і Wi-Fi або особистої мережі. Сенсори, які не потребують підключення до шлюзу можуть підключатися з використанням глобальної безпровідної мережі WAN. Сенсори, які характеризуються низьким споживанням енергії та низькою швидкістю передачі даних, створюють відомі безпровідні сенсорні мережі Wireless Sensor Network. WSN з кожним днем стають популярнішими, оскільки підтримують більше сенсорів з підтримкою роботи від батареї і доступні на великій площі.

Можливості пристроїв:

- пряма взаємодія: пристрої можуть збирати інформацію самостійно в мережі зв’язку і можуть отримувати інформацію (наприклад, команди) із мережі зв’язку.
- непряма взаємодія: можуть збирати інформацію за допомогою можливостей шлюзу. На іншій стороні, можуть непрямим образом отримувати інформацію із мережі зв’язку.
- організовувати спеціальні мережі: коли потрібно буде підвищити масштабованість і швидко розвернути мережу, тобто пристрої мають можливість створювати мережі довільно.
- режим сну та пробудження: можливості пристроїв можуть підтримувати механізми «Сон» та «пробудження», щоб заощадити енергію.

Можливості шлюза:

- підтримка кількох інтерфейсів: на рівні пристрої можуть використовувати можливості шлюза з використанням різних провідних і безпровідних технологій, такі як: шина локальної мережі, Bluetooth або Wi-Fi. Також, шлюз має можливість обмінюватися даними з використанням різних технології, таких як , Ethernet, цифрові абонентські лінії (DSL) та інші.

- існують дві ситуації, в яких потрібно можливості шлюза. Перша, коли для зв'язку на рівні пристроїв потрібно використовувати різні протоколи рівня пристрої. Інша ситуація, коли для зв'язку, на рівні пристрої і рівня мережі використовуються різні протоколи, протокол технології ZigBee на рівні пристроїв і протокол технології 3G на рівні мережі.

Рівень шлюзів і мереж. На першому рівні створюється велика кількість даних, яка потребує надійної і провідної або безпровідної мережі в якості транспортного середовища. Існують мережі зв'язку, які використовують різні протоколи, які можуть використовуватися для підтримки M2M і їх додатків. Дані мережі потрібно забезпечувати необхідними значеннями якості передачі інформації, і також пропускну здібність і безпеку. Даний рівень складається із конвергентної мережевої інфраструктури, яка створюється за допомогою інтеграції різних мереж в єдину мережеву платформу. Саме, завдяки конвергентному абстрактному мережевому рівні в IoT дозволяє через шлюзи кільком користувачам використовувати ресурси в одній мережі без пошкодження конфіденційності, безпеки [1].

Даний рівень складається із наступних можливостей:

- можливість організації мережі: представляє функції управління мережею, такі як управління доступом і ресурсами транспортування, управління мобільністю або аутентифікацією, авторизацією і облік (AAA).

- можливість транспортування: призначена для представлення з'єднання для транспортування інформації у вигляді даних, які відносяться до послуг і додатків IoT, а також транспортування інформації контролю і управління, яка відноситься до IoT.

Сервісний рівень. Сервісний рівень складається з різних інформаційних послуг, які допомагають автоматизувати бізнес-процеси: підтримка операційної і бізнес діяльності, різної аналітичної обробки інформації, зберігання даних, забезпечення інформаційної безпеки, управління бізнес-правилами, управління бізнес-процесами.

Рівень підтримки послуг і підтримки додатків складається із наступного:

- загальні можливості підтримки: це типові послуги, які можуть використовуватися різними додатками IoT, такими як обробка і зберігання даних. Дані можливості можуть бути активовані спеціальними можливостями підтримки, наприклад для створення інших можливостей підтримки.
- спеціальні можливості підтримки – це конкретні можливості, які назначені для спеціального додатку. В реальному застосуванні можуть бути визначені, для того щоб надати різні функції підтримки різним додаткам IoT.

Рівень додатків. На четвертому рівні архітектури IoT існують різні типи додатків для сфер діяльності (енергетика, медицина, освіта і т.д.). Додатки можуть бути призначені, як специфічно для деякої області, так і використовуватися в різних сферах.

Можливості управління. Можливості управління IoT охоплюють традиційні класи помилок, обліку, показників роботи і безпеки (FCAPS).

Можливості управління IoT:

- управління пристроями, наприклад дистанційна активація і деактивація пристроїв, діагностика, оновлення прошивки або програмного забезпечення, управління робочим станом пристрою;
- управління топологією локальної мережі;
- управління трафіком і перезавантаженням, наприклад знаходження умов перезавантаження мережі і реалізація резервних ресурсів для термінових або важливих потоків трафіка.

Спеціальні можливості управління пов’язані з потребами додатків.

Можливості забезпечення безпеки. Існує два види забезпечення безпеки: загальні можливості забезпечення безпеки і спеціальні можливості забезпечення безпеки. Загальні можливості не залежать від додатку і включають:

- на рівні додатку: авторизація, аутентифікація, захист конфіденційності і цілісності даних додатку, захист особистого життя, облік безпеки і антивірусна програма.
- на рівні мережі: авторизація, аутентифікація, конфіденційних даних, а також захист цілісності даних.
- на рівні пристрою: аутентифікація, авторизація, перевірка цілісності пристрою, управління доступом, захист конфіденційності і цілісності даних.

1.3 Переваги IoT

Максимально більше людей та компаній впроваджують технологію IoT. Як зазначалося раніше, це допомагає ідентифікувати можливі проблеми та забезпечує точність у всіх процесах, що полегшує роботу для людей. Деякі випадки дозволяють повністю виключити людське втручання. Технологія Інтернету речей використовується, майже всюди, це і доставка, функціональність обладнання, платежі та отримання рахунків [3].

- **Доставка**. У процесі доставлення можуть виникати проблеми, але IoT допомагає їх вирішувати. Дана технологія може змінювати маршрут, вносити автоматично зміни в систему. Застосувавши в процесі доставки IoT проблеми зменшується, а ефективність системи збільшиться. В результаті, компанії будуть розвиватися швидше та буде збільшуватися їх клієнтська база.
- **Застосування машин у виробничих процесах.** У даному процесі використання IoT служить способом збору інформації, а також технологія допоможуть завчасно виявити проблему та вирішити її. IoT містить детальну інструкцію по вирішенню проблеми та як правильно її виконати.

- **Аналіз тенденцій та рекомендації.** Головна перевага IoT збирання та аналізування даних. Функція допомагає покращити результати для компаній аналізуючи їх інформацію.
- **Автоматизована передача даних.** Дане інноваційне рішення дозволяє торговим автоматам розпізнавати падіння запасів, розміщувати замовлення на додаткові продукти та створювати платіж відповідному постачальнику. Застосувавши в лікарнях, допоможе розміщувати нові замовлення на постачання до того, як поточні запаси вичерпуються, що в подальшому покращить результати.

Отже, IoT покращує компанії завдяки своїм перевагам, тому поточні процеси стають зрозумілішими та якіснішими.

Висновки до першого розділу

Досліджено мережу Internet of Things (IoT), яка в свою чергу забезпечена унікальним ідентифікатором та можливістю передачі даних через мережу, яка в свою чергу не вимагає зв’язку «людина-людина» або «людина-комп’ютер».

Проаналізовано архітектуру IoT, яка складається з чотирьох базових горизонтальних рівнів. Розглянуто та детально досліджено кожен рівень. Виокремлено, що модель передачі даних відрізняється від існуючої моделі передачі даних через Інтернет.

Зазначено, що мережа IoT має ряд переваг, що допомагає ідентифікувати можливі проблеми та забезпечити точність у всіх процесах.

2 ДОСЛІДЖЕННЯ СТАНДАРТІВ ПЕРЕДАЧІ ДАНИХ В ІОТ

2.1 Класифікація технологій передачі даних в IoT

Технологія IoT використовує різні варіанти мережі зв'язку для передачі даних. Комунікація невеликого радіусу дії, основані на таких технологіях, як RFID, NFC, Bluetooth, Wi-Fi та багато інших. Для більшого радіусу дії використовуються на основі різних стільникових мереж, мереж бездротового широкосмугового доступу та інші [2].

В IoT використовують чотири основні типи мережевих технологій, розглянемо більш детально кожну з них.

Перша мережа, це PAN (Personal Area Network). Дана мережа, поєднує всі персональні пристрої користувача, наприклад телефон, ноутбук та інше. В IoT дана мережа налаштовується «навколо» пристрою.

Друга мережа, LAN (Local Area Network) – мережа, призначена для невеликої території. До даної мережі, також відноситься і CAN (Controller Area Network) – мережа, яка орієнтована на об'єднання в єдину мережу різні виконуючі пристрої і датчики в межах окремого підприємства.

Третя мережа, MAN (Metropolitan Area Network), об'єднує окремих користувачів і локальні мережі в рамках міста.

Четверта мережа, WAN (Wide Area Network), глобальна мережа, яка пов'язує користувачів і мережі.

В IoT використовують дротові та бездротові мережі. Бездротові мережі, можна розділити:

- WPAN (Wireless Personal Area Network): радіус дії від кількох сантиметрів до кількох метрів. Фізичний та канальний рівень регламентується стандартом IEEE 802.15.4. Дану мережу застосовують, як для об'єднання окремих пристроїв, так і для глобальної мережі Інтернет.

- WSN (Wireless Sensor Network): мережа, яка об’єднує багато датчиків(сенсорів) виконуючих пристроїв, та між собою, поєднана радіоканалом. Область покриття мережі сягає від кількох метрів до кількох кілометрів.
- TAN (Tiny Area Network) – мережа, яка використовується у невеликих офісах, домах. В основному, це домашні мережі, які об’єднують комп’ютера, телефони, побутові пристрої. Найчастіше дані мережі будуються на основі технології Wi-Fi.

2.2 Реалізація та застосування стандартів

Для якісної взаємодії великої кількості пристроїв в IoT використовують різні стандарти і протоколи. Розглянемо більш детально деякі з них.

Стандарт IEEE Std 802.15.4, призначений для бездротових персональних мереж WPAN. Даний стандарт реалізує два рівня стека протоколів: фізичний рівень (PHY) і рівень доступу до середовища (MAC).

Фізичний рівень, визначає спосіб передачі даних, інтерфейс організації зв’язку, апаратні особливості і параметри, які будуть необхідні для налаштування мережі. Також, забезпечує двосторонню напівдуплексну передачу даних, підтримуючи шифрування AES 128. Важливою особливістю стандарту, є обов’язкове підтвердження доставки повідомлень [4].

Стандарт визначає два типи вузлів мережі:

1. Повнофункціональний пристрій FFD (Fully Function Device), який зможить реалізувати функцію координації роботи і встановлення параметрів мережі, так і працювати в режимі типового вузла.
2. Пристрій з обмеженим набором функцій FFD (Fully Function Device), зможить підтримувати зв’язок тільки із повнофункціональним пристроєм.

В будь-якій мережі повинен бути, хоча б один FFD, який буде реалізувати функцію координатора.

На канальному рівні стандарту використовуються мережі, які можуть бути P2P (peer-to-peer, point-to-point) або мати топологія «зірка».

Стандарт IEEE Std 802.15.4 описує, тільки два рівня мережевої моделі OSI, інші рівні описують спеціальні комунікаційні протоколи. Одним із них являється **ZigBee**.

Специфікація даного стандарту орієнтована на додаток, який гарантує безпеку передачі даних при невеликих швидкостях і довгої роботи мережевих пристроїв від батареї. Стандарт ZigBee за основу має стандарт, який ми переглянули вище. Основною особливістю стандарту, є те що він підтримує, не тільки прості мережі, такі як зірка, а і самоорганізуючу та самовідновлювальну mesh, топологію з ретрансляцією та маршрутизацією повідомлень. Ще однією перевагою стандарту, це можливість вибору алгоритму маршрутизації, в залежності від вимог мережі, а також забезпечує легке обслуговування та модернізацію. Протокол дозволяє мережі знаходитися в «сонному» режимі більшу частину часу, що дозволяє вузлам працювати від батареї довше [5].

Мережа ZigBee є самоорганізована, тобто всі вузли мають можливість самостійно визначати і корегувати маршрути доставлення даних. Більш сучасним являється стандарт ZigBee RF4CE, який розроблений для дистанційного управління у аудіо/відео пристроях, наприклад телевізори. Вони мають ряд переваг, включаючи управління в зоні непрямої видимості, або управління із розпізнанням жестів і сенсорним введенням.

Інший стандарт, який забезпечує взаємодію невеликих бездротових мереж з мережею IP по протоколу Ipv6 з невеликою енергозатратою **- 6LoWPAN (IPv6 Low-Power Wireless Personal Area Network).** Даний стандарт застосовується для організації датчиків і автоматизації житлового і офісного приміщення з можливостями управляти через інтернет, але також використовується і для реалізації простих безпровідних мереж датчиків.

Архітектура мережі 6LoWPAN відрізняється від інших, так як використовують спеціальне комутаційне обладнання, маршрутизатори і інше. Мережі 6LoWPAN складаються із вузлів, які можуть виконувати роль маршрутизатора. Вузол, який може виконувати маршрутизацію у рамках мережі 6LoWPAN називається роутер. Граничний маршрутизатор відповідає за

взаємодію підмережі 6LoWPAN з мережею Ipv6, здійснює компресію/декомпресію заголовків IPv6 під час обміну із зовнішньою мережею, у разі підключення до мережі IPv4 може грати роль шлюзу IPv6↔IPv4.

Перевагою даного стандарту являється велика масштабованість мережі з підключенням IP-мережі, але не для всіх підходить даний тип управління. Даний тип протоколу потребує постійну активність маршрутизатора для коректної передачі даних, що є проблемою в сенсорних бездротових мережах.

Основні області застосування даного стандарту:

- інтелектуальні системи обліку.
- управління вуличним освітленням.
- промислова автоматика.
- логістичні системи.
- комерційні охоронні системи, системи контролю і управління доступом.

WirelessHART – протокол передачі даних по бездротовій ліній зв’язку. Безпровідна мережа складається із трьох основних елементів:

1. Безпровідні польові пристрої.
2. Шлюзи – забезпечують обмін даними між польовим пристроями і хост-додатками, під’єднаних до магістральної або іншої комунікаційної мережі.
3. Адміністратор мережі – відповідає за конфігурацію мережі, плануванням обміном даними між пристроями, маршрутизацією повідомлень і моніторинг стану мережі.

Перевагою являється, те що кожен пристрій може бути в якості маршрутизатора для повідомлення від інших пристроїв. Тобто пристрій не має необхідності звертатися напрям до шлюзу. Це розширює мережу і забезпечує більшу надійність. Пристрої завжди залишаються на зв’язку, навіть коли вони знаходяться в зоні дії інших пристроїв. WirelessHART підтримує кілька режимів передачі даних.

Технологія, яка використовується для невеликого радіусу дії називається **Bluetooth Low Energy (BLE).** Саме BLE використовує в 10 разів менше енергії і здатен передавати дані в 50 раз швидше, ніж звичайні Bluetooth.

Технологія розрахована на топологію «точка-точка» і «зірка». Основними областями застосування являється пристрої забезпечення безпеки, управління електрозасобами і домашні медичні пристрої, спортивні тренажери. Також, застосовуються в управлінні домашньою автоматикою, пристроями освітлення чи охорони, як мінімум в межах одного приміщення. Для того, щоб керувати в межах всього дому можливе використання BLE в якості шлюзу між пристроєм, який керує та мережею локальної автоматики.

За рахунок, низької енергозатратності та більш стійкої роботи в умовах великої кількості аналогічних пристроїв можна розглядати BLE як альтернативу пристроям NFC. Але, рекомендується застосовувати поєднання BLE з NFC. В даному випадку, Bluetooth Low Energy забезпечує великий радіус дії пристроїв роботи і велику кількість пристроїв, які працюють разом, а NFC для встановлення логічного з'єднання між парою пристроїв, забезпечуючи більш високий рівень безпеки за рахунок меншого радіусу дії.

Найбільш популярна технологія на сьогодні IEEE 802.11, більш відома, як **Wi-Fi.** Широке розповсюдження технологія отримала від використання в мобільних пристроях, ноутбуках.

Складається з фізичного рівня та канального з підрівнями управління доступу до середовища MAC (Media Access Control) і логічної передачі даних LLC (Logical Link Control). Фізичний рівень має різницю від інших технології, так як відрізняється у використанні частотного діапазону, методу кодування і тому має швидшу передачу даних. Пристрої, які використовують даний стандарт можуть працювати в трьох режимах:

- Legacy.
- Mixed.
- чистому, тобто в режимі в якому реалізується підвищена швидкість і збільшена передача даних.

Даний стандарт в складі містить і IEEE 802.11s, яка дозволяє організовувати ієрархічні бездротові ad-hoc мережі з мобільними та статичними вузлами, розширюючи функцію бездротового доступу в Інтернет.

Отже, проаналізувавши ряд протоколів, можна зробити висновок, що жоден протокол Інтернету речей не є найкращим та не вирішить всі поставлені завдання. Тому, спеціалісти повинні самостійно визначити, який найкраще протокол буде виконувати поставлені завдання у їх організації. Для того, щоб ефективніше визначити, який потрібно застосувати протокол, потрібно врахувати низку факторів, а саме живлення підключених пристроїв та де буде розміщено пристрої, до вимог безпеки.

Висновки до другого розділу

Досліджено чотири основні типи мережевих технологій. Зазначено, що в IoT використовують дротові та бездротові мережі.

Виокремлено, що для якісної взаємодії великої кількості пристроїв в IoT використовують різні стандарти та протоколи. Проаналізовано деякі з них. Виокремлено, що найбільш популярною технологією являється Wi-Fi. Досліджено, що протокол має швидку передачу даних, бо відрізняється фізичний рівень від інших технологій та має інший метод кодування.

3 АКТУАЛЬНІ ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МЕРЕЖІ IOT

3.1 Ризики для безпеки мережі IoT

На даний момент, безпека для пристроїв IoT стає все більш проблемною, тому що IoT набирає популярності. Багато пристроїв, не мають надійного захисту, не використовуючи навіть автентифікацію та шифрування, а отже стають вразливими та цікавими для зловмисника. До цього можна віднести пристрої, мережі, дані та користувачів. Злочинець здійснює атаку задля отримання інформації. Також, зловмисник може скомпрометувати вашу автоматичну консоль реєстрації, для того щоб отримати ваші дані; можуть зламати мережу компанії, або найпростіша дізнатися ваш ненадійний пароль та в результаті отримати доступ до вашої мережі, наприклад «Smart home» [5].

Атака на пристрій або на мережу називається атакою IoT.

Тому, для підвищення безпеки та захисту даних, розглянемо методи та способи захисту від атак, які спрямовані на мережу IoT.

Однією із серйозних загроз є доступ до конфіденційної інформації, яка зберігається на пристрої IoT. До даної інформації, відноситься, як особиста інформація (паролі, адреси), фінансова інформація (номери банківських карток) та інше.

Інша загроза, яка матиме серйозний вплив є встановлення шахрайських пристроїв у корпоративну мережу або у державних установах. Дана атака буде спрямована на виведення з ладу пристроїв, отримання інформації та в подальшому викрадення її.

Вразливості програмного забезпечення є актуальною проблемою. Багато пристроїв вразливі до даної атаки, із таких причин, як:

- ненадійний контроль доступу в системах IoT;
- обмежений бюджет для належного тестування та покращення безпеки;
- відсутність актуальних оновлень;

- застарілі пристрої, які не підтримують актуальні оновлення;
- не достатній захист від фізичних атак, за допомогою радіохвиль.

Також, пристрої IoT можуть бути використані для здійснення атаки на інші системи, з метою отримання інформації, даних та інше. Злочинці можуть отримати доступ, наприклад до телевізора, який буде вразливий та в результаті будуть вільно користуватися вашою мережею.

Розглянуто ризики, які часто спостерігаються в мережі IoT:

- порушення безпеки в транспортному засобі, дана атака спрямована на отримання доступу до транспорту, та виведення його з ладу. Дослідження показують, що дана атака виконується без відома водія.
- отримання доступу до пристрою IoT. Одна з найпоширеніших атак, яка спрямована на отримання інформації, крадіжки або пошкодження її.
- крадіжка даних, виконується для отримання, в основному фінансової інформації або особистої.
- незахищене підключення до Інтернету. Відсутність стандартів безпеки призведе до виконання даної атаки.
- вразливості у вбудованому програмному забезпечені. Пристрій, який має відкритий код, буде вразливий до атаки, що призведе до НСД (несанкціонованого доступу).

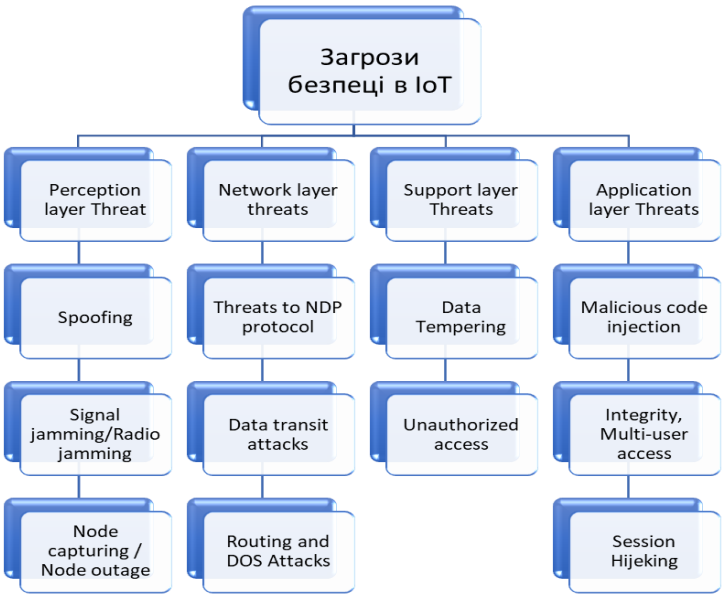

Рис. 3.1. Загрози безпеці в IoT

У таблиці 1 розглянуто атаки на різних рівнях IoT та їх вирішення.

Таблиця 3.1.

IoT атаки та їх вирішення

Layer	Attacks	Solutions
Perception layer		
Perception Nodes RFID	DoS, spoofing, time management, privacy protection, survivability	Access control, data encryption which includes non-linear key algorithms, IPSec protocol utilization
Sensor nodes	Node subversion, node failure, node authentication, node outage, passive information gathering	Node authentication, Sensor Privacy
Sensor Gateways	Misconfiguration, hacking, signal lost, DoS, war dialling, protocol tunnelling, man-in-the-middle attack	Message Security
Network layer		
Mobile Communication	Tracking, eavesdropping	Developing secure access control mechanisms to mitigate the threats by employing biometrics, public-key crypto primitives and time changing session keys.
Cloud Computing	Identity management, heterogeneity which is inaccessible to an authentic node, data access controls, system complexity, physical security, encryption, infrastructure security and misconfiguration of software	Identity privacy, Location privacy, Node compromise attack, Forward and backward security
Internet	Confidentiality, encryption, viruses, cyberbullying, hacking, identity theft, reliability, integrity and consent	Identity Management for confidentiality, Encryption schemes for confidentiality of communication channels
Application layer		
Application	Data privacy, Tampering Privacy, Access control, disclosure of information	Authentication, key agreement and protection of user privacy across heterogeneous networks

Пристрої IoT не завжди захищені, адже найбільше уваги приділяється захисту мобільних телефонів, ПК, ноутбуків, які мають вже базовий рівень безпеки [5]. Проте, такі пристрої, як smart TV або переносні пристрої, більш схильні до кібератак. Деякі пристрої, можуть бути вразливими до атак, якщо:

- не матимуть останніх оновлень;
- не зашифровано зберігають та обмінюються даними;
- мають застаріле обладнання;
- не захищені мережеві порти;
- відсутній захист конфіденційності.

Одна з найнебезпечніших атак, спричинена незахищеним зв'язком є man-in-the-middle (MitM). Зловмисники використовують дану атаку для того, щоб скомпрометувати процедуру оновлення та отримати контроль над вашим пристроєм, якщо він не буде використовувати безпечні механізми шифрування та автентифікації.

Значну увагу потрібно приділяти мобільним пристроям, адже вони слугують основним обладнанням для управління багатьох систем IoT. Саме, вони запускають та керують програмами IoT. Тому, являються одними з головних цілей для кібератак. За дослідженнями, на пристрої Android відбувається більше атак та є більш вразливі.

Пристрої, які підвищують продуктивність, можуть стати проблемою для вашої безпеки, та саме через них отримати доступ, наприклад до «smart home». Будь-який пристрій, який підключений до IoT є ціллю для атаки. Отримавши доступ до мережі, злочинці можуть компрометувати ОС та ПЗ. Але не тільки ваші пристрої, які є в мережі будуть вразливими, а і дані, які знаходяться в хмарі зазнають атак. Таким чином, витік даних буває, як із самих пристроїв, так і з хмарних середовищ, до яких вони підключені. Також, джерелом витоку є і сторонні програми, які містяться у вашій мережі.

У мережі IoT можна знайти різні атаки, але виділино деякі з них, а саме вразливості в :

- апаратних та програмних системах – являються центральними компонентами рамок IoT, які вразливі до атак.
- computer bugs можуть вивести з ладу операційну систему, програмне забезпечення.
- людські елементи та складність програмування – два фактори, що сприяють дефектам конфігурації ПЗ.

Людські загрози – загрози, створені людьми, наприклад внутрішні загрози, або зовнішні (особи, які знаходяться за межами організації) та мають на меті нанести пошкодження системі. Наведемо, деякі приклади даних загроз.

- неструктуровані загрози: використовуються новачками для злому системи.
- структуровані загрози: люди, які розуміють структуру системи, та створюють атаку на основі коду і сценарії, відомі як структуровані ризики.
- advanced Persistent Threats (APT): скоординований напад. Тобто, це атака яка спрямована на викрадення даних з таких галузей, як виробництво, банки.

3.2 Підвищення рівня безпеки для IoT

Єдиного рішення для захисту пристроїв IoT від усіх типів загроз не має, але дотримуватися загальних правил та рекомендацій можна захистити та зменшити ризики для пристроїв.

Для безпечної роботи потрібно дотримуватися тріади CIA – конфіденційність, цілісність і доступність даних. Порушення будь-якої складової буде призведено до неправильної роботи системи. Для того, щоб ефективно та безпечно передавати інформацію в системі потрібно дотримуватися наступних рекомендацій.

Конфіденційність: важлива функція безпеки в Інтернеті. Інформація не повинна розголошуватися не авторизованим користувачам. Потрібна, щоб будь-яка інформація, яка знаходить в мережі IoT була надана тільки авторизованим

користувачам. Дані, які зібрані комп’ютером не потрібно надсилати не зашифрованими каналами. Для того, щоб зловмисник не міг отримати передану інформацію потрібно виконувати шифрування даних. Коли відбувається шифрування даних, то система перетворює кожен біт даних в зашифрований текст, після чого виконує двоетапний процес перевірки, у якому два пристрої дозволяють доступ лише, тоді коли тест на автентифікацію виконаний двома пристроями, а також біометрична перевірка, у якій користувач має унікальну ідентифікаційну та біометричну автентифікацію.

Цілісність: повинна бути задля гарантування достовірності даних. Дана функція потрібна, для того щоб користувачі перевірили, чи отримані дані з інших пристроїв є автентичними. Цілісність є невід’ємною властивістю безпеки для користувачів IoT.

Автентифікація та авторизація: автентифікація пов’язана з надійністю, щоб кожна система в мережі мала можливість розпізнавати та автентифікувати інші пристрої. Оскільки IoT складається з великої кількості пристроїв, дана функція є важливою [6].

Доступність: основна мета Інтернету речей – зробити дані доступними для користувачів. Кінцевий користувач повинен негайно отримувати дані, як в звичайних ситуаціях, так і в критичних.

Облік: відповідає за резервування та підготовку до виконання політик безпеки мережі під час розробки стратегій безпеки в мережі. Дана функція не запобігає атакам, але допомагає переконатися, що інші заходи безпеки функціонують правильно.

Рекомендації, які потрібно дотримуватися у мережі Інтернету речей.

Спочатку, потрібно переконатися, що всі пристрої IoT налаштовані та захищені, як одна стратегія. Налаштування облікових записів користувачів та паролів, браундмауера, антивірусного програмного забезпечення та встановлення оновлень безпеки.

Також, потрібно бути підключеним та використовувати захищене бездротове підключення, задля уникнення несанкціонованого доступу від зловмисника.

Одне з головних правил, забезпечити всі пристрої сильним паролем. Можна використовувати безкоштовні генератори онлайн-паролів, щоб створити надійний пароль. Для маршрутизаторів та модемів, потрібно також відповідний захист, оскільки більша частина атак відбувається через них.

Використовуючи антивірусне забезпечення, потрібно надати перевагу платному ПЗ, ліцензійному, щоб уникнути зловмисних програм та вірусів. Потрібно, пам’ятати та мати надійні firewalls для захисту від вторгнень. Дані правила, потрібно підтримувати і в IoT infrastructures та хмарі.

Не потрібно, нехтувати засобами безпеки для кінцевих користувачів, адже зловмисник може використати їх облікові записи, як вразливість. Наприклад, використовуючи brute-force зловмисник отримає облікові дані користувачі, а потім і доступ до вашої IoT. Тому, дотримуйтеся захисту для всіх користувачів у мережі IoT. Найголовніше дотримуйтеся, strong password, а також для додаткової безпеки використовуйте двофакторну автентифікацію. Контролюйте, дозволи користувачів, а саме хто та до якої системи має доступ.

Потрібно регулярно оновлювати своє програмне забезпечення та операційні системи. Нехтуючи даним правилом, можна отримати вразливість через яку буде здійснено атаку. Тому, регулярно оновлюйте своє програмне забезпечення та додатки. Потрібно, завантажити останні версії для програм та оновлені патчі.

Регулярно, виконуйте аудит безпеки, задля виявлення вразливостей. Це ідеально для розкриття ризиків та вразливості IoT. Звіт з аудиту, дає вам рекомендації для забезпечення безпеки вашої мережі.

Необхідно, використовувати інструменти моніторингу для виявлення загроз. Firewall або спеціальний додаток, який визначить атаку IoT. Це буде, миттєве повідомлення, якщо хтось бажатиме отримати доступ до вашої мережі. В результаті, буде можливість попередити атаку [6].

Додаткові функції безпеки та їх особливості. Важливим забезпеченням безпеки пристроїв IoT являється безпечне середовище для підвищеної стійкості до атак, автентифікації, авторизації, конфіденційності, цілісності та створення безпечного середовища передавання даних. Розроблявши безпеку для пристроїв потрібно враховувати:

1. Різноманітність пристроїв та їх функціонал.
2. Дизайн системи та додатків, які використовуються в мережі, також врахувати хто є користувачами системи та які цілі в них.

Відкриті системи за основу взаємодіють використовуючи модель OSI, яка складається з 7 рівнів. Перший рівень, фізичний, відповідає за передачу та прийом даних на рівні проводів. Канальний рівень, відповідає за встановлення та завершення зв'язку, контролює трафік. Мережевий рівень реалізує маршрутизацію. Транспортний рівень відповідає за сегментацію повідомлень. Рівень сеансу несе відповідальність за встановлення, підтримку та завершення сеансу. Презентаційний рівень транслює код, перетворює дані. Останній рівень, рівень програми, включає спільне використання ресурсів та віддалений доступ до файлів, принтерів, керує мережею. Але, IoT має широкий різновид, тому дані 7 рівнів представлено в 3 рівні, розглянуті раніше. IoT має широкий потенціал та може використовуватися в різних сферах. Особливістю та перевагою являється те, що IoT може, як збирати дані, так і аналізувати дані для індивідуальних користувачів. Perception layer and network layer разом складають основу для IoT.

На даний момент, існує певне проміжне програмне забезпечення для пристроїв IoT. Вимоги, які необхідні для ПЗ розділяються на функціональні та нефункціональні. Функціональні вимоги складаються з послуг і функцій, такі як управління. Нефункціональні підтримують QoS та проблеми продуктивності. Internet of Everything (IoE) мають за мету об'єднати об'єкти, будівлі, дороги, міста. Дана функцію ускладнить забезпечення безпеки та розгортання Інтернету речей стає складнішим. Основною задачею проміжного програмного забезпечення є забезпечення безпечної передачі даних між верхнім і нижнім рівнем. Також, повинна бути гарантовано, що дані будуть дотримуватися і

цілісності. Ще однією гарантією буде те, що контрольні коментарі та запити від додатків або користувачів перевіряються, а система – невідмовна. Дані не повинні бути розголошені стороннім користувачам, тобто повинна дотримуватися функція конфіденційності.

Конфіденційність є невід'ємною частиною безпеки пристроїв у мережі IoT. Обробка даних повинна, бути прозора та законна. Розглянемо на прикладі, забезпечення конфіденційності даних у закладах охорони здоров'я. Пацієнти повинні знати, хто збирає та використовує їх дані. Також, контролювати хто має доступ до даних, та як вони передаються. Програми повинні надати функції, які забезпечують керування даними, а також зберігати анонімність даних. Дана технологія зберігання даних застосовується і в smart home, Smart transportation.

Автентифікація та авторизація. Автентифікація і контроль доступ займає велике значення в IoT. Якщо не буде відповідного контролю доступу, то архітектура IoT, буде скомпрометована, та зловмисник отримає до неї доступ. Отже, даний захист займає перше місце в захисті [6]. Контроль доступу складається із двох етапів: автентифікація та авторизацію.

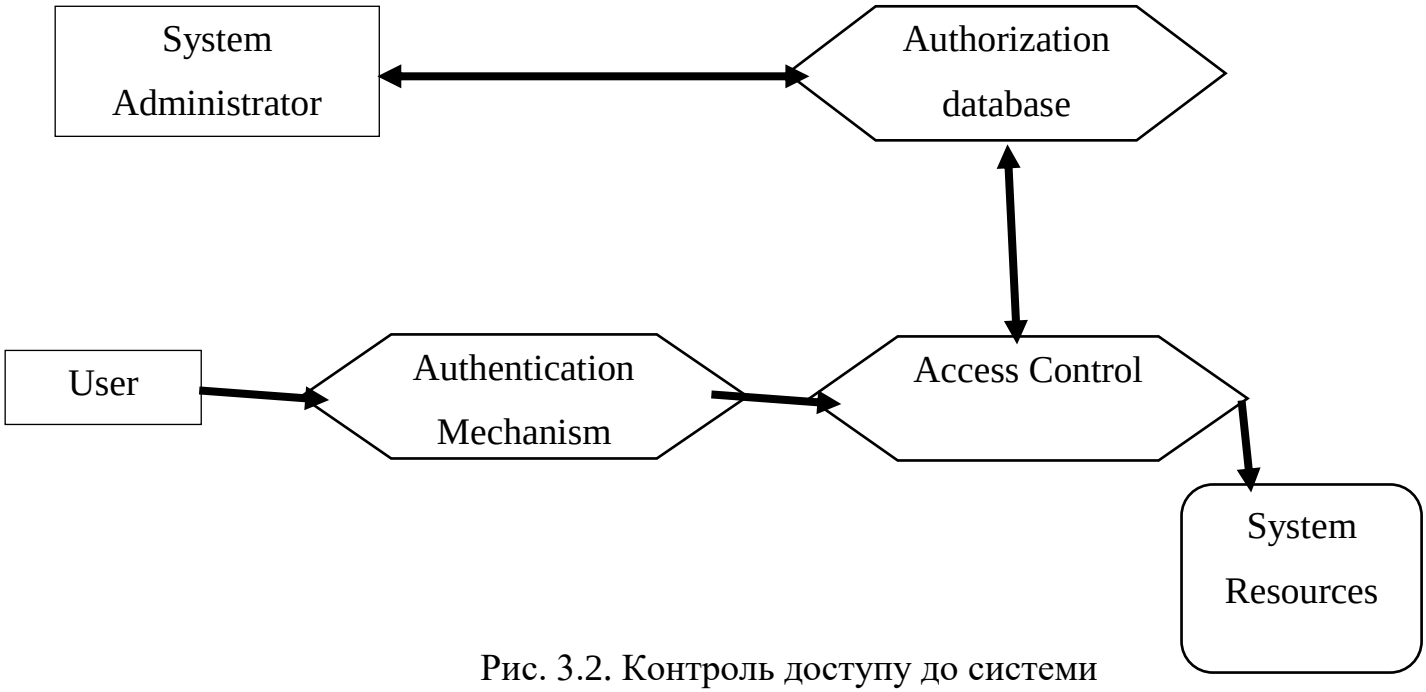

Рис. 3.2. Контроль доступу до системи

Автентифікація - процес перевірки ідентичності. Дана функція являється першим кроком, коли хтось хоче отримати доступ до системи. Автентифікація є найважливішою вимогою безпеки в IoT. Виконуючи автентифікація, здійснюється процес ідентифікації, ввівши свої особисті дані [6]. Щоб підтримати безпечний вхід потрібно встановлення сертифікатів. Саме вони є безпечним та обов'язковими для всіх протоколів автентифікації. Автентифікація залежить від деяких факторів, наприклад:

- паролі, ключі;
- Random Number Generators (RNG), ATM card, ID card;
- біометричні дані, такі як відбиток пальця.

Процес автентифікації містить у собі ряд криптографічних вимог для безпечної передачі інформації. Процес автентифікації відрізняється на кожному рівні, тому розглянуто більш детально кожен з них..

Perception Layer. Як зазначалося раніше, даний рівень містить всі апаратні пристрої для того, щоб отримувати дані із середовища IoT. На даному рівні автентифікація проходить, як звичайна автентифікація або peer authentication. Рівень криптографічних перетворень на рівня являється недостатнім.

На прикладі, розглянуто RFID-мітки. Якщо клонувати мітки, то процес автентифікації буде вразливим. Схему шифрування на основі ідентифікації (IBE) було виконано для безпечного каналу зв'язку між RFID -мітками. Також, протокол автентифікації можна реалізувати за допомогою генерації ключів Діффі-Хеллмана на основі еліптичних кривих. Коли, ключі будуть згенеровані, то їх можна передати, які в подальшому будуть використані як загальний симетричний ключ для безпечної передачі інформації через середовище.

1. Network Layer. Даний рівень інтегрований поверх протоколів TCP/IP. Саме, безпека мобільного зв'язку не оцінювалася критичною до моменту появи IoT. З появою даної технології схем, які були вбудовані більше не являються надійними. Існуючі алгоритми генерації ключів, які використовуються в TCP/IP протоколах не можливі для використання на мобільних пристроях. Attribute Based Encryption (ABE) схема, яка запропонована для мобільних пристроїв, але

масштабність схеми являється під питанням, так як містить багато пристроїв. Сучасні мобільні пристрої містять багато різноманітних функцій, одна з них це можливість отримувати біометричні дані, такі як відбиток пальця. Саме, ці дані можна використовувати, як унікальні дані для ідентифікації. Оскільки, більшість пристроїв використовує людина, то запропонований метод являється безпечним. Безпеку можна підвищити застосувавши багатофакторну автентифікацію Можна використовувати, не тільки для входу в систему, а і для підписання документів на перевірку ідентичності, а також для передачі безпечного ключа сеансу між сторонами, що спілкуються з відповідними схемами шифрування. Потрібно, перевіряти дані на цілісність, задля уникнення атак.

Важливе значення, займає зберігання даних, а саме Cloud Computing. Тому, автентифікація повинна використовувати надійні ключі, які генеруються за допомогою RSA. Ключі AES, TDES та інші використовуються для передачі даних між пристроями IoT та cloud storage. Проте, головною проблемою забезпечення безпеки являється конфіденційність даних користувачів. Рекомендовано для безпеки даних, використовувати blockchain і homomorphism. Використовуючи, дані рекомендації, автентифікація буде більш надійна та безпечна, оскільки у blockchain вузли ідентифікуються з хешів або відкритих ключів, а homomorphism – має додатковий рівень шифрування для захисту зв’язку.

Автентифікація, в основному здійснюється через Інтернет, та використовує протоколи SSL або IPSec, IoT використовує DTLS як протокол зв’язку. Китайською компанією було представлено локально централізовану та глобально розділену мережу під назвою Auth. Автентифікація розгортається на перефирійних пристроях, щоб надати авторизацію для локально зареєстрованих об’єктів, зберігаючи їхні облікові дані та політики доступу в базі даних. Оскільки дані зберігаються та розподіляються глобально в мережі і це допоможе підтримати довірчі відносини для надання авторизації для пристроїв IoT.

2. Application Layer. На даному рівні, визначається вимоги щодо різних підходів до механізму контролю доступу для різних програм. Наприклад, розглянуто використання рекомендацій безпеки для різних послуг.

- «Розумні» комунальні послуги. Зловмисники можуть отримати доступ до ваших пристроїв, якщо не будуть використані надійні методи безпеки. Отримавши доступ, потенційний зловмисник зможить порушить потік енергії мережевої підстанції, що призведе до перевантаження ядерного реактора. Автентифікація оператора мережі, може складатися з двофакторної автентифікації, імені користувача, пароля та RNG (Random Number Generator), якщо в пристроях є можливість використання біометричного входу доступу, то це підвищить вашу безпеку. Протоколи SSL можна використовувати для автентифікації. Доступ до лічильника може отримати споживач, він повинен базуватися, також на двофакторній автентифікації або біометрії. Повинні бути вбудовані механізми із протоколами автентифікації для виявлення фальсифікації.
- Пристрої IoT для охорони здоров'я. Доступ до даних у медицині надається, лише лікарям та пацієнтам. Тому, доступ повинен бути обмежений. Протокол автентифікації, повинен бути H2M (Англ. Human-to-Mashine, людина-машина). Доступ надається пацієнтам, тільки з використання двофакторної автентифікації на ПК. Якщо пацієнт використовує мобільний пристрій для отримання доступу, то можна застосувати трифакторну автентифікацію з використанням біометрії. Захист даних повинен бути ретельний, бо використовуються доступ до приватної та конфіденційної інформації. Доступ до хмарних сервісів лікарям надається з використання двофакторної автентифікації.
- Логістика. У транспортних засобах встановлення бездротових з'єднань може швидко змінюватися. Таким чином, між транспортними вузлами повинні бути прийняті механізми динамічної передачі для підтримки узгодженого з'єднання з транспортним вузлом, що зв'язується. Тому, підхід до автентифікації буде легший, оскільки вони дуже динамічні. Кожен транспортний засіб має вбудований приватний ключ для ідентифікації, пов'язаний із номером, виробником та моделлю транспортного засобу. Ключі генеруються із легшою процедурою, тому не потрібні дорогі ресурси. Використовують протоколи M2M, де машини є транспортними засобами. Перевірка ідентичності кожного засобу займає перше місце, для того щоб уникнути втручання зловмисника.

- Industrial Internet of Things, IioT. Більшість пристроїв підтримують протокол M2M через їх автоматизовані платформи. Процеси даних пристроїв працюють безперервно, оскільки їхні робочі цикли можуть тривати годинами. Якщо відбудеться одночасна автентифікація, то це знизить ефективність усієї «розумної» системи. Тому, повинна бути встановлена політика планової схеми автентифікації, яка не впливає на промислову продуктивність. Автентифікація відбувається тільки на керуючих машинах, оскільки тільки на одному пристрої вона може тривати годинами. Пристрої, на етапах автентифікації використовують складні криптографічні примітки, для забезпечення відповідного рівня безпеки.
- Smart Buildings, Environments and Cities. Загального протоколу автентифікації для «smart city» немає, тому що використовується багато пристріїв, і гарантувати безпеку всіх користувачів при єдиному протоколі не можливо. Але дану програму можна реалізувати врахувавши три рівні IoT. Перший рівень, гарантує для контролю сенсорної системи в розумному середовищі. Мережевий рівень інтегрує дані в Інтернеті, а також сервера до мобільних пристроїв. Мобільні пристрої використовують трифакторну систему автентифікації, а хмарні сервера та вузли маршрутизації автентифікованим за допомогою криптографічно згенерованих ключів.

Авторизація – надання прав автентифікованим пристроям. Спочатку особа виконує автентифікація, тобто перевірку. Кожному користувачеві надаються відповідні йому права (читання, редагування, виконання).

Висновки до третього розділу

Досліджено ризики для безпеки мережі IoT. Виокремлено, що одна із серйозних загроз це доступ до конфіденційної інформації, яка зберігається на пристрої IoT. Також, досліджено, що ще одною вагомою загрозою являється встановлення шахрайських пристроїв у корпоративну мережу або у державну установу.

Проаналізовано, що однією із найсерйозніших атак являється man-in-the-middle, якщо пристрій не буде використовувати безпечні механізми шифрування та автентифікацію.

Зазначено, що для безпечної роботи потрібно дотримуватися тріади CIA. Досліджено, що головним правилом являється встановлення надійного паролю на пристрої.

4 РЕКОМЕНДАЦІЇ ЩОДО ПІДВИЩЕННЯ БЕЗПЕКИ В МЕРЕЖІ IOT

4.1 Загальні рекомендації безпеки в мережі IoT

1. **Blockchain.** Blockchain – це розподілена база даних онлайн-записів. Дана технологія є прозорою, надійною, швидкою та надає автономні рішення. Blockchain створює захищені мережі, де пристрої IoT будуть з'єднуватися між собою, уникаючи загроз, а саме підробка пристрою. У мережі зареєстровано вузли, що дають змогу ідентифікувати і автентифікувати один одного без необхідності центрів сертифікації. Мережа має змогу масштабуватися, щоб підтримувати більшу кількість пристроїв та без потреби в додаткових ресурсів. Але, також дана технологія має і недоліки, наприклад із збільшення мережі, потрібно використовувати більше пам'яті, пропускної здатності та обчислювальної потужності. Остання властивість та час обробки є одним із елементів, які потрібні для збільшення швидкості, оскільки мережа IoT масштабна та різноманітна. Збільшення пам'яті для даної технології є великою проблемою. А також, на даний момент є невелика кількість людей, які розуміють технологію, тому є ще одною перешкодою для її впровадження.

2. **5G.** Дана технологія об'єднує в собі ряд можливостей та безліч функцій, що призвело до масштабності та популярності. Реалізація 5G впливає на застосування багатьох протоколів, особливо на перших двох рівнях. Запропонована мережа покращить послуги, як для користувачів, так і для операторів мережі. 5G стане доступною та приймається, як основна транспортна інфраструктура для Інтернету речей. На відмінну від інших мереж, дана мережа орієнтована на користувача. Передача між різними мережевими інтерфейсами має бути автентифікованою, а обмін інформацією під час передачі має бути захищеним і приватним. У IoT при використанні 5G буде інтегровано кілька підходів, а саме:

- кращий рівень безпеки для пристроїв отриманий шляхом використання нових механізмів безпеки, які будуть вбудовані у ідентифікатор абонента.

- рекомендовано впровадити для використання фізичний рівень захист, такі як радіочастотні відбитки пальців.

3. **Fog and Edge Computing.** Fog computing - децентралізована обчислювальна інфраструктура, у якій дані, обчислення, сховище та програми ефективно розподіляються між джерелом даних і хмарою. Дана технологія, є більш обширною, ніж cloud storage. Основна мета: збільшити ефективність, та зменшити кількість даних, які переносяться в хмару, для обробки, аналізу та зберігання. Запропоновано технологію, яка виконує обробку даних в маршрутизаторі, шлюзі на пристрої, який надсилає їх далі до джерел, щоб обробити, тобто зменшує корисну пропускну здатність cloud. Властивість, яку має Fog computing, а саме розподілення даних, допомагає вирішити проблему великої кількості даних, яка надходить від пристроїв, які знаходяться в мережі IoT. Мережа Fog computing доповнює хмару та допомагає час від часу проводити аналітичні обчислення. Технологія має ряд переваг, а саме мобільні обчислення, низька вартість комп'ютерних компонентів і абсолютна кількість пристроїв IoT.

Одна з найбільших переваг Edge Computing скорочення часу дії та часу відгуку до мілісекунд, та зберігають мережеві ресурси. Основні переваги Edge:

- журналювання: запропоноване надійне журнулювання, яке включено в журнал подій безпеки.

- перевірка оновлень: оновлення мають доставлятися через захищений канал і мати підтвердження після завантаження. Перевірка, підпис повинні гарантувати, що оновлення перевірені та не мають шкідливо програмного забезпечення.

- шифрування: дані можуть бути розкритті та викриті, якщо не мають відповідного рівня безпеки.

- шифрування комунікацій: зашифровані комунікації повинні відбуватися завжди, наскільки це можливо.

Проте, також мають і недоліки, наприклад: викликають велику кількість проблем із безпекою, ліцензуванням і конфігурацією. Мають більшу можливість вразливості до атак, таких як зараження ШПЗ. Також, мають більші витрати на ліцензування. Недопрацьоване керування пристроями викликає проблеми в конфігурації. Адміністратори можуть ненавмисно створити вразливі місця в безпеці, нехтуючи оновленнями та не змінюючи пароль за замовчуванням на кожному пристрої.

4. **Cloud.** Cloud – відноситься до частини управління Інтернету речей. Зазвичай, складається із зберігання даних, звітності та аналітики. Основні функції Cloud:

- автентифікація – хмарні компоненти надають комплексну автентифікацію, яка включає багатофакторну автентифікацію.
- Secure web interface – має будову за допомогою технологій, які створюють рішення для звичайних вразливостей, які можуть бути у веб-додатках.
- Encrypted storage – сховище повинно бути зашифроване, відповідно до політики безпеки.
- регулярний аудит - потрібно відстежувати інформацію задля контролю термінів.

5. **Gateway.** Gateway – дозволяє підтримувати додаткові пристрої або дозволяє їм з’єднуватися з хмарними компонентами. Контролюють та створюють просте з’єднання між незахищеною, але надійною локальною мережею, та захищене з’єднання з ненадійними підключеннями в Інтернету. Функції:

- Storage – зберігає мінімальну кількість інформації в зашифрованому вигляді.
- Alerting and logging – маючи доступ до великої кількості інформації, повинен сповіщати та виконувати реєстрацію в журналі подій.
- Service denial and replay attack mitigation – має здатність до виявлення attack mitigation.

6. **Mobile.** Мобільні пристрої в мережі Інтернету речей відрізняються можливостями. Деякі пристрої будуть надавати дані з додаткових пристроїв, інші

дозволять керувати цими пристроями, а також є можливість керувати хмарою та переглядати аналітику. Потрібно врахувати:

- Local storage security considerations – потрібно пам’ятати про обмежену кількість сховища.
- Strong audit trail of mobile interactions – потрібно виконувати аудит безпеки в журналі безпеки про взаємодію мобільних пристроїв.
- Encrypted communications channels – надійні зашифровані канали зв’язку.
- Multi-factor authentication – на мобільних пристроях повинна бути виконана багатофакторна автентифікація.

4.2 Практична реалізація рекомендацій безпеки

AWS Greengrass - програмне забезпечення, яке призначене для обміну повідомленнями, синхронізацією та виконання висновку для підключених пристроїв. Використовуючи дану програму є можливість запускати функцію AWS Lambda, яка допомагає підтримувати синхронізацію даних пристрою та безпечно спілкуватися із іншими, навіть якщо вони не підключені до Інтернету [8].

AWS Lambda гарантує, що IoT-пристрої можуть швидко реагувати на локальні події, мінімізують витрати на передачу даних до хмари.

ML Inference — це функція AWS Greengrass, яка дозволяє легко виконувати логічні висновки машинного навчання локально на пристроях Greengrass Core за допомогою моделей, створених і навчених у хмарі [8].

Дана програма має ряд переваг, наведемо деякі з них. Працюючи з програмою можете використовувати мови та моделі програмування, щоб створювати та тестувати програмне забезпечення пристрою у хмарі, а потім розгортати його на своїх пристроях. Включає можливість, налаштувати програму для пристрою передачі даних лише необхідної інформації назад у хмару. AWS Greengrass автентифікує та шифрує дані пристрою в усіх точках з’єднання за допомогою можливостей безпеки та керування доступом AWS IoT Core. Таким

чином, дані ніколи не обмінюються між пристроями, коли вони спілкуються один з одним і хмарою, без підтвердженої ідентифікації [8].

Розмір пристрою IoT не впливає, підключити можна, як невеликий пристрій, так і великі побутові прилади [9].

Одна з переваг, використання програми, якщо пристрій втрачає зв'язок із хмарою, підключені пристрої продовжують взаємодіяти один з одним по локальній мережі.

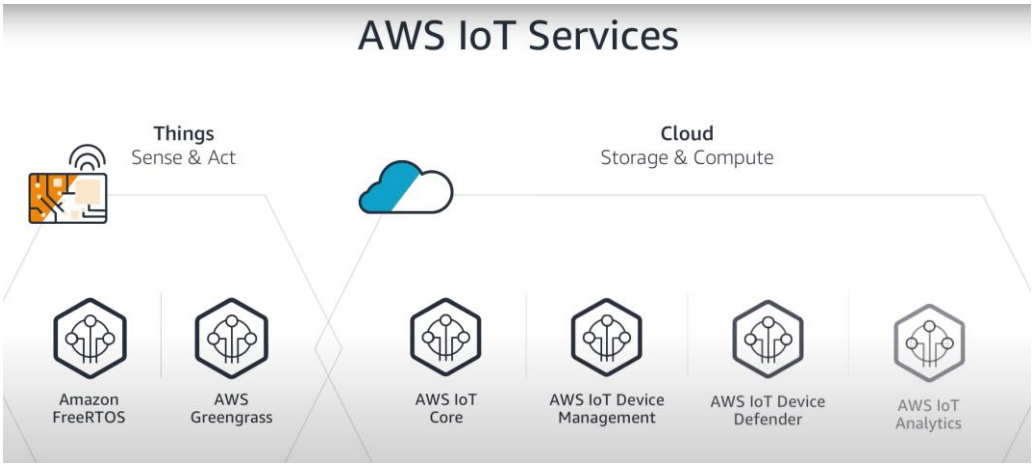

Рис. 4.1. AWS IoT Services

AWS IoT Greengrass дає змогу використовувати, готові програмні модулі, які називаються компонентами. Після того, як виконано підключення додатків IoT, AWS IoT Greengrass дозволить віддалено розгортати, налаштовувати та керувати цими додатками [9].

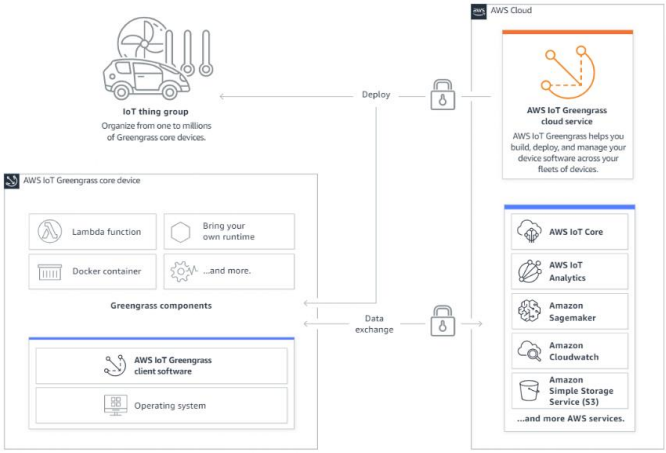

Рис. 4.2. Взаємодія з AWS IoT Greengrass та іншими службами AWS

AWS IoT Greengrass надає компоненти, які можна розгорнути на основних пристроях. Саме, ці компоненти дозволяють пристроям підключатися та спілкуватися з основними пристроями. За допомогою AWS IoT Device Management, є можливість підключати нові типи пристроїв і застосовувати їх масово. Також, підтримує каталог інформації про пристрої і конфігурацію. Підтримує функцію, відслідкування та проведення діагностики усунення проблеми, а потім дозволяє виконувати оновлення по бездротовій мережі для всіх пристроїв [10].

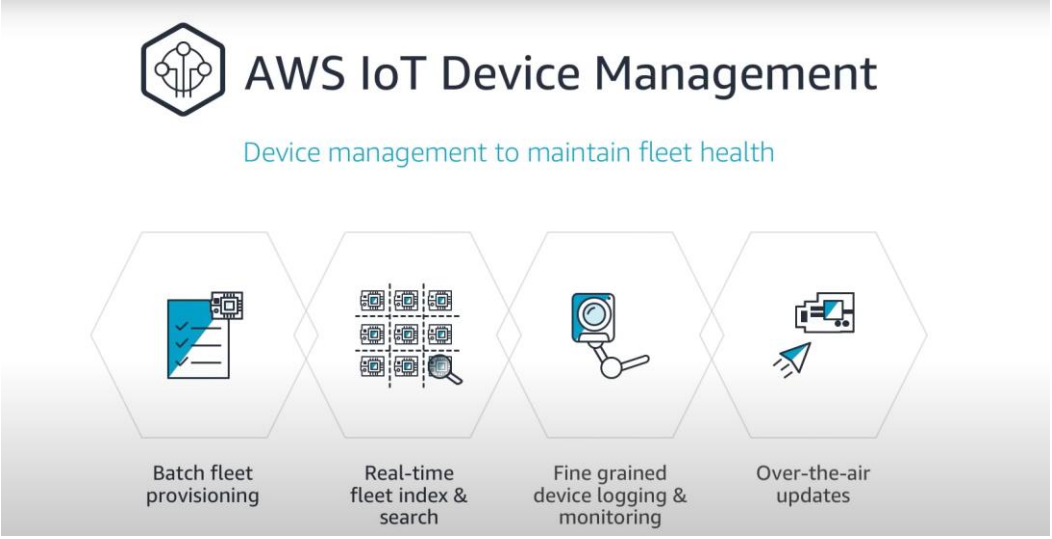

Рис. 4.3. AWS IoT Device Management

З допомогою, AWS IoT Device Defender, допомагає постійно перевіряти ваші пристрої, відслідковує та повідомляє про нетипову поведінку, яка може вказувати на потенційну проблему безпеки, та попереджує Вас, якщо виконуються нетипові дії, наприклад, трафік із пристрою виконується із неавторизованої IP-адреси. В решті, дана функція дозволяє корегувати дії для забезпечення безпеки пристроїв.

AWS IoT Analytics дозволяє виконувати аналітику пристроїв Інтернету речей. Тобто, виконується повне управління аналітичними службами, яка дозволяє легко аналізувати дані Інтернету речей. Із її допомогою, можна виконувати аналітику великих об’ємів даних, не переймаючись про всі витрати та складності, які зазвичай потрібні для створення власної платформи аналітики IoT.

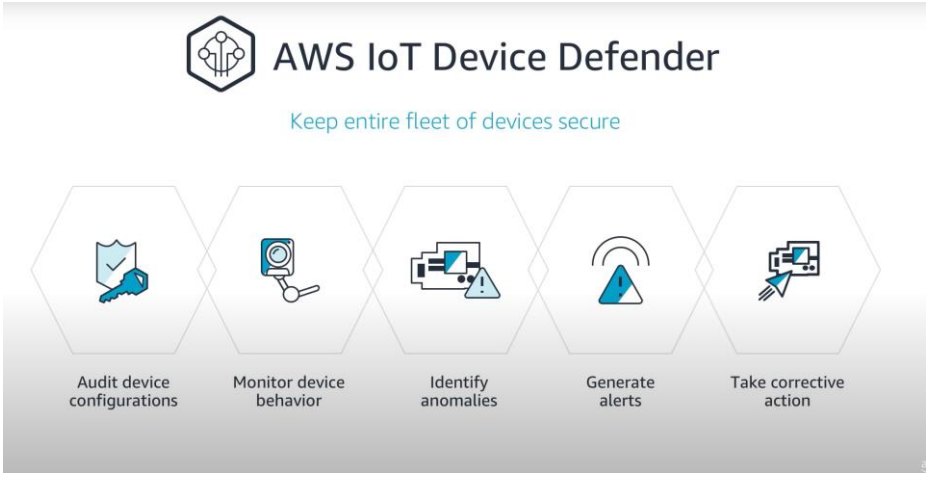

Рис. 4.4. AWS IoT Device Defender

Далі, відбувається фільтрація, перетворення даних IoT. Перед, тим як виконати збереження даних IoT, можна легко запросити свої дані з допомогою влаштованого механізму запитів. Подвійна аналітика підтримує більш складну аналітику, готуючи дані для машинного навчання використовуючи готові шаблони.

Рис. 4.5. AWS IoT Analytics

На практиці, створено пристрій, який дозволить передавати пристрій із пристрою в хмару AWS IoT.

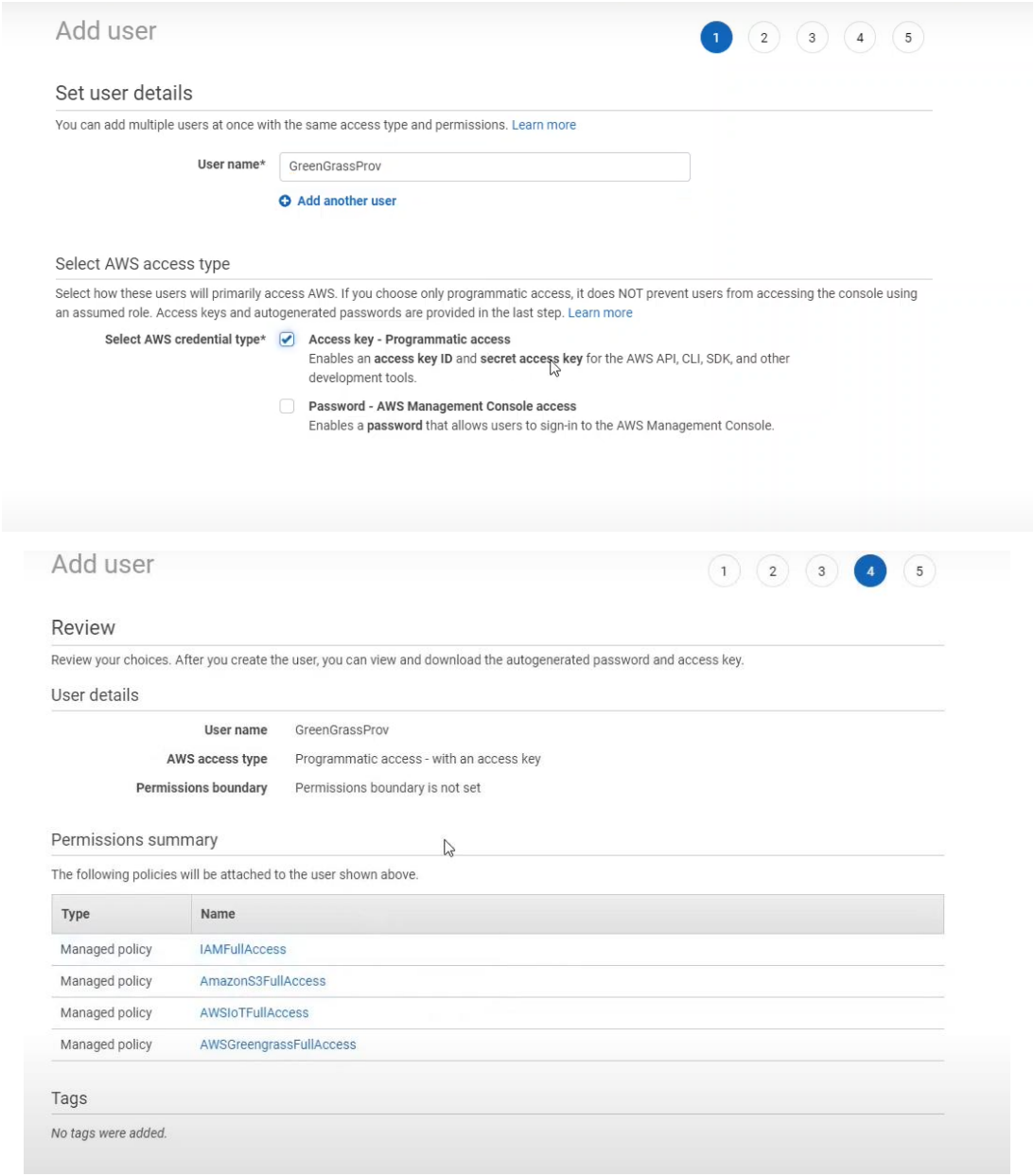

Рис. 4.6. Створено користувача

Далі, налаштовано облікові дані на пристрої. Для цього, потрібно розмістити ідентифікатор ключа доступу та секретний ключ доступу, а також завантажено останню версію програмного забезпечення AWS IoT Greengrass Core.

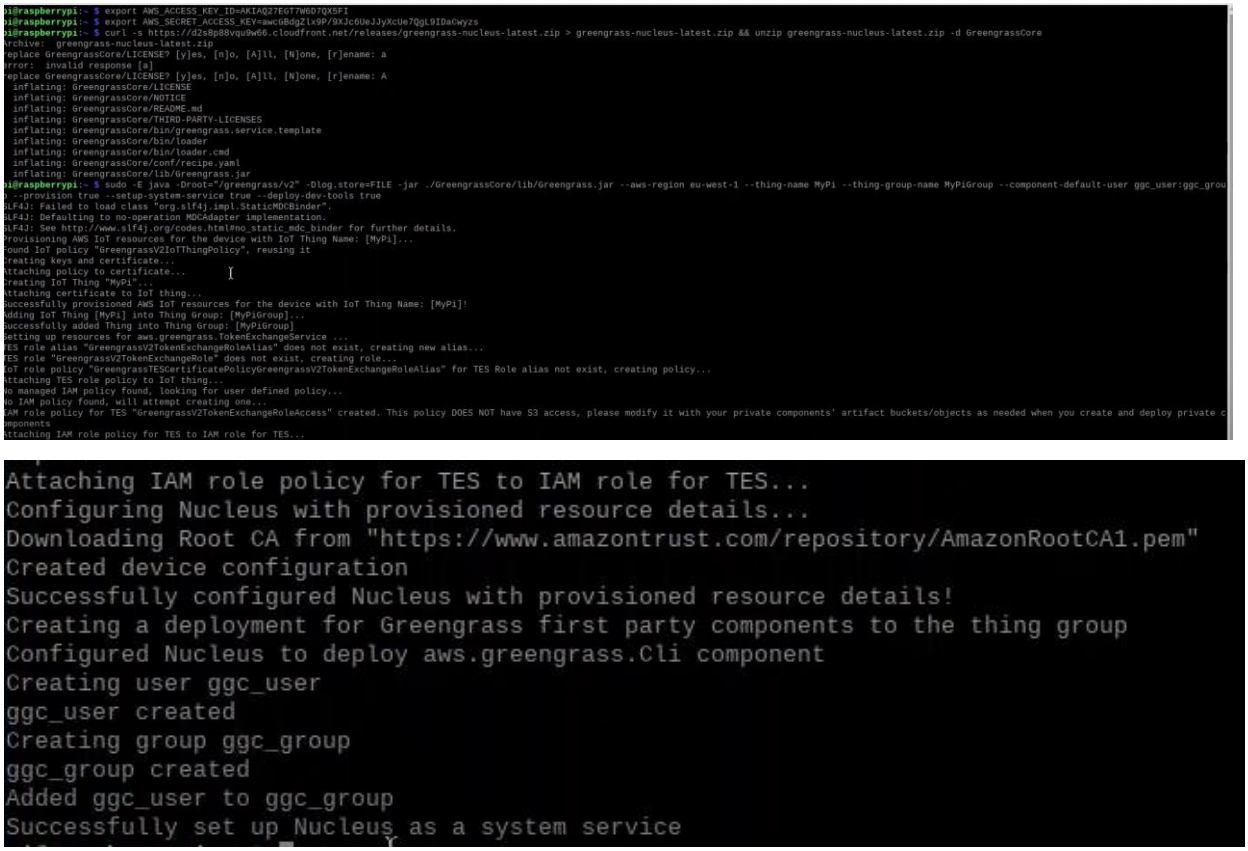

Рис. 4.7. Створено облікові дані на пристрої

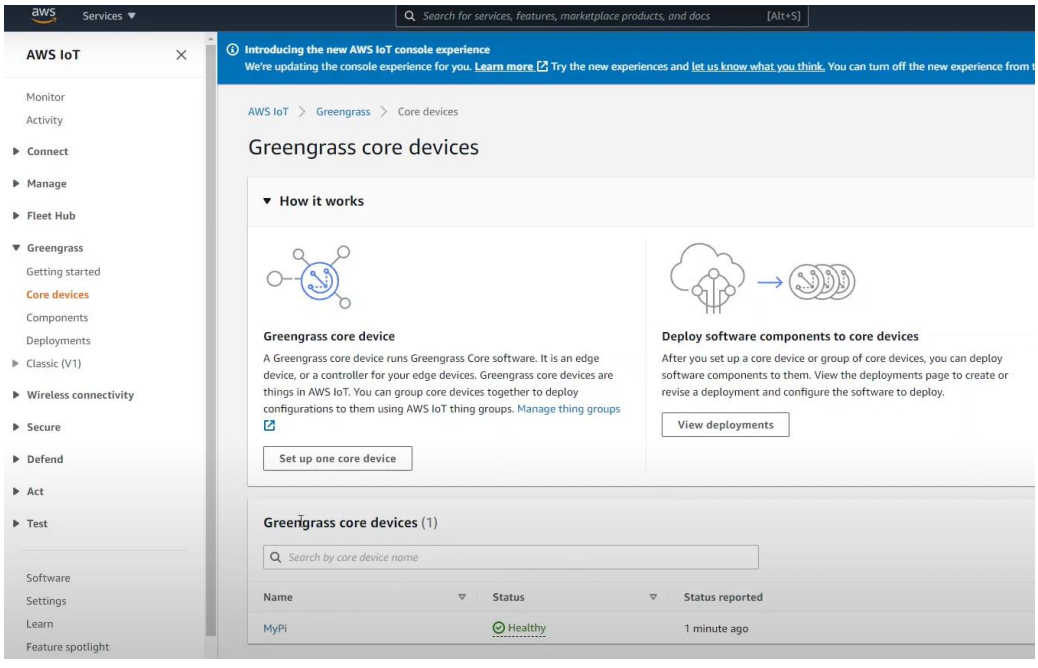

Рис. 4.8. Створено користувач

У консолі, відображено підключення пристрою, який є справним, по статусу Healthy. Виконано, віддалене розгортання на пристрої, додавши додатковий компонент [10].

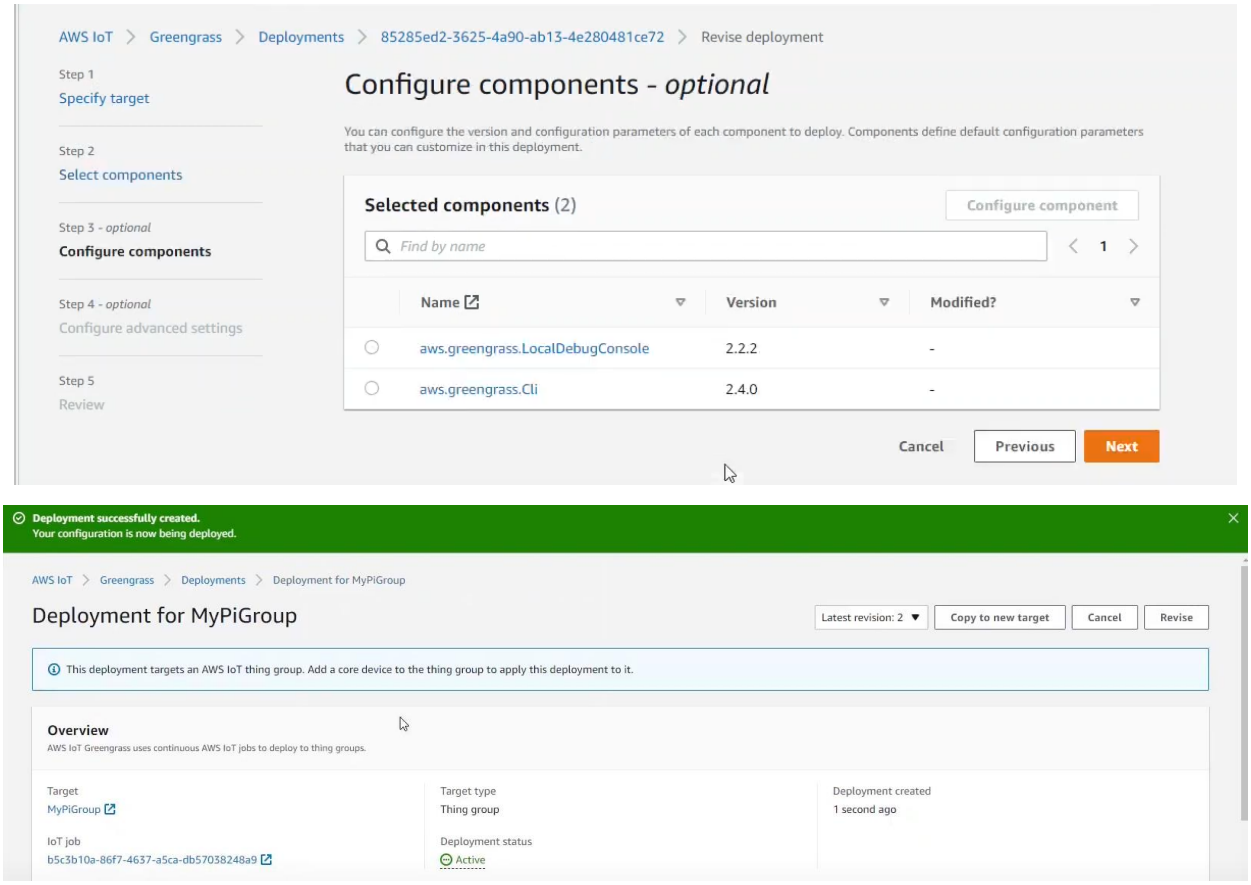

Рис. 4.9. Додавано компонент

На пристрої використано команду для отримання списку компонентів, які працюють на даному пристрою.

Рис. 4.10. Виконано перевірку

За допомогою AWS IoT Greengrass, яка складається із хмарного сервісу та програмного забезпечення AWS IoT Greengrass Core, можна запускати журнали в Amazon CloudWatch Logs і в локальну файлову систему основного пристрою. Журнал, використовують для моніторингу подій та вирішення проблем. Записи включають позначку часу, рівень журналу та інформацію про подію.

Програмне забезпечення записує журнали лише в локальну файлову систему. Журнали файлової системи переглядаються в реальному часі, щоб можна переглянути компоненти, які розроблено.

Розглянуто хмарну безпеку, яка є найвищим пріоритетом. Модель безпеки заснована на спільній відповідальності між AWS та користувачем, тобто відбувається безпека хмари та безпека в хмарі.

Безпека хмари - AWS відповідає за захист інфраструктури, яка запускає служби AWS у хмарі AWS. AWS також надає послуги, якими можете безпечно користуватися.

Безпека в хмарі – Ваша відповідальність визначається сервісом AWS, який використано. Користувач несе відповідальність за інші фактори, зокрема конфіденційність даних, вимоги вашої компанії та відповідні закони та нормативні акти.

Отже, AWS IoT Greengrass — це хмарна служба Інтернету речей (IoT) із відкритим вихідним кодом, яка допомагає створювати, розгортати й керувати додатками IoT на ваших пристроях. Використовуючи дану програму, Ви зможете створити програмне забезпечення, яке дозволить вашим пристроям працювати локально на основі даних, які вони генерують, запускати прогнози на основі моделей машинного навчання, а також фільтрувати дані пристроїв. Пристрої Greengrass також можуть безпечно обмінюватися даними з AWS IoT Core і експортувати дані IoT у AWS Cloud. Ви також можете використовувати AWS IoT Greengrass, щоб пакувати та запускати програмне забезпечення за допомогою функцій Lambda, контейнерів Docker, власних процесів операційної системи або користувацького середовища виконання.

Виконуючи дослідження та вивчення програми, є висновок, що безпека IoT має багато вразливостей, деякі з них розглянуто, та застосовано рекомендації задля їх уникнення [11].

Vulnerabilities. Вразливості виникають завжди, для Інтернету речей є вразливим місцем, оскільки бракує потужності безпеки. Ще одним фактором, поширенню вразливостей є обмежений бюджет на розробку та тестування безпечного програмного забезпечення.

Malware. Шкідливе програмне забезпечення заражає пристрої, щоб отримати доступ до них. Це є одна з найпопулярніших атак злочинців, IoT botnet найпоширеніший вид.

Connected devices. Пристрої, зберігають конфіденційну або особисту інформацію та маючи доступ в Інтернет можуть бути вразливі до атак.

Weak Authentication. Слабка автентифікація, яка може бути встановлена за замовченням є ціллю для атаки зловмисників, використовуючи дані, можна отримати доступ до мережі.

Lack of Updates. Якщо пристрої містить дефект, у їх кодові, то виробник повинен надати вирішення, тобто оновлення програмного забезпечення, задля уникнення вразливостей.

Lack of awareness. Користувачі системи, повинні знати правила мережі, задля уникнення атаки націленої на них.

Weak Interfaces. Використання незахищених інтерфейсів програм є однією із вразливостей IoT. Саме, ненадійне шифрування та перевірка пристрою є найпоширенішою проблемою інтерфейсу програм.

Untrustworthy connection. Пристрої IoT можуть спілкуватися без шифрування. На даний момент, є однією із найсерйозніших проблем безпеки.

Low Processing power. Якщо пристрої, мають низьку потужність, в результаті в них невеликий обсяг даних. Тому, не використовують всі рекомендації для захисту інформації не маючи firewalls та антивіруси. Отже, такі пристрої стають більш вразливими до атак. Рекомендовано, мати вбудовані заходи безпеки в мережу.

Connected Cars. Якщо, пристрій підключено до smart house, то вона також стає вразливою до атак, що призводить, навіть до крадіжки автомобіля. Зловмисники шукають слабкі місця системи, щоб використати її, та отримати доступ до мережі. Хакери можуть змінити налаштування контролю керування та змінити стан машини.

Для того, щоб використання Інтернету речей стало більш безпечним та захищеним, OWASP було розроблено кращі рішення, які допоможуть уникнути вразливості системи.

Для того, щоб мережа IoT була надійна повинні бути включені засоби контролю безпеки, які будуть встановлені, а також будуть відстежуватися та переглядатися через деякий час. Також, потрібно гарантувати захист всього периметру мережі IoT.

Практичні рекомендації для захисту IoT:

- IoT Endpoint Protection;
- IoT Gateway Security;
- Security Cloud API;
- розробка безпечної мережі;
- сучасне шифрування даних;
- захищене зберігання даних;
- впровадження виправлень та відновлення.

1. Використання унікальних облікових даних. Зазвичай, пристрої за замовченням мають імена користувачів та паролі, тому їх потрібно змінити [11]. Під час, зміни даних, використовуйте унікальні дані та пристрій повинен вимагати від користувача створити пароль, який буде відповідати кращому рівню захисту. В системі, не повинно бути спроб скидання паролю до попередніх налаштувань. Отже, дотримуйтеся використовувати кращі паролі для ваших облікових даних та інших механізмів автентифікації. Пов’язані онлайн-сервіси повинні використовувати багатофакторну автентифікацію, будь-яка інформація про користувача не повинна бути розкрита перед автентифікацією. Перед зміною паролю, повинно впевнитися, що саме відповідний користувач змінює його.

2. Завжди, зберігайте облікові дані та конфіденційні. Будь-яка інформація, повинна зберігатися в захищеному вигляді. Облікові дані, які є закодованими не дозволяється.

3. Перевіряйте вхідні дані. Перевірка потрібна для введення даних через інтерфейс користувача та передачі даних через API або між мережами в пристроях і службах.

4. Впровадження політики вразливостей. Політика розкриття вразливостей повинна бути надана організаціями, які надають послуги IoT, їх публічна інформація для розробників безпеки та інших осіб про проблеми. Вразливі місця потрібно усунути якнайшвидше за допомогою наданої процедури усунення вразливостей.

5. Оновлюйте програмне забезпечення. Програмне забезпечення на пристроях повинно бути динамічним і безпечно змінюватися. Оновлення виконуються негайно та не заважають роботі пристрою. Для кінцевих пристроїв, необхідно політика, щодо завершення терміну служби, яка буде вказувати протягом якого часу пристрій отримає оновлення програмного забезпечення. Користувачі повинні бути проінформовані про кожне оновлення. Пристрої, які неможливо фізично оновити, їх продукт повинен бути ізольованим та замінений.

6. Безпечна комунікація. Дані, які мають конфіденційну або приватно інформацію, повинні бути зашифровані при передачі. Усі ключі, потрібно зберігати в безпечному місці.

7. Зменшіть Exposed Attack Surface. Пристрої та служби повинні відповідати «принципу найменших привілеїв», що означає порти, які не використовуються, мають бути закриті, апаратне забезпечення не має відкривати доступ без потреби, служби не повинні бути доступними, якщо ними не користуються, а код має мати мінімальну функціональність, необхідну для функціонування служби.

8. Забезпечення цілісності програмного забезпечення. Для того, щоб перевіряти програмне забезпечення використовуйте процедуру безпечного завантаження. Якщо виявлено несанкціоновану модифікацію, пристрій повинен

повідомити користувача/адміністратора про проблему та не підключатися до будь-яких мереж, окрім тих, які необхідні для виконання функції оповіщення.

9. Захищений доступ до персональних даних. Служби та пристрої, які обробляють персональні дані повинні відповідати General Data Protection Regulation (GDPR) та Закону про захист персональних даних. Виробники пристроїв та послугу Інтернету речей повинні надавати інформацію користувачам, ким та як обробляються їхні дані. Це також, стосується і інших, які мають доступ до персональної інформації користувачів. Якщо дані обробляються за згодою споживачів, вони повинні збиратися законним і дозволеним способом, при цьому ці споживачі мають право відкликати свою згоду в будь-який час. Якщо система, наприклад Blockchain, де неможливо остаточно стерти дані, то користувачі повинні бути проінформовані про наслідки.

10. Системи, повинні бути стійкими до збоїв. Якщо цього вимагає їхнє використання або інші залежні системи, стійкість має бути інтегрована в пристрої та служби Інтернету речей, враховуючи потенційну можливість перебоїв у мережі передачі даних і електроенергії. Якщо, відбувається збій в мережі, то системи повинні залишатися в робочому стані та працювати локально наскільки це можливо та повинні відновлюватися. Якщо відбувається відключення електроенергії, повинні бути передбачені відновлення електроенергії. Також, повинні бути передбачені випадки, щоб не було широкомасштабного повторного підключення, а можливість приєднатися до мережі впорядкованим способом.

11. Монітор системи даних. Якщо дані збираються з пристроїв та служб IoT, то їх слід перевірити на наявність порушень у безпеці.

12. Видалення для клієнтів персональних даних повинно бути легким. Коли користувач, вирішив стерти власні дані або замінити пристрій, то особисті дані повинні негайно бути видаленими. Користувачам, повинна бути надана інформація про те, як виконати дану дію. Також, потрібно попередити, коли дані будуть видалені та вони повинні бути остаточно невідновлені.

13. Виконайте просте встановлення та обслуговування пристрою. Встановлення та обслуговування пристрою повинно бути легким та складатися із

кількох кроків. Споживачі також повинні отримати інструкції щодо безпечного налаштування своїх пристроїв.

Наведено, практичні рекомендації захищеної мережі IoT для виробника.

1. Сегментація мережі. Зловмисник, для того щоб отримати доступ до мережі можуть використовувати фішингові електронні листи для обману співробітників. Також, можуть використовувати і інші способи, задля отримання доступу. Тому, системи IIoT мають бути ізольовані належним чином. У результаті пристрої та датчики, які керують насосами, клапанами або будь-яким іншим компонентом системи SCADA, завжди повинні бути підключені до окремої мережі від решти IT-інфраструктури.

2. Ризики взаємодії між інформаційними технологіями (IT) та операційними технологіями (OT). Для того, щоб інтернет речей успішно функціонував потрібно взаємодія, як інформаційних технологій, так і операційних [11]. Проте, вони мають різні цілі та завдання. Операційні технології орієнтовані на якість, продуктивність та ефективність, а інформаційні технології на інфраструктуру, безпеку та управління. А також, вони мають окремі методи безпеки, оцінюючи різні загрози, зосереджуються на різних циклах виправлення, протоколах і так далі.

3. Деталізація контролю доступу. Сучасні системи керування, майже завжди мають систему розмежування доступу на основі ролей, а також можливість вибору груп, до яких мають отримання доступу для читання або читання-запису. Пропонується, застосовувати метод контролю доступу на основі атрибутів (Attribute-Based Access Control (ABAC)), який забезпечить кращий рівень безпеки.

4. Захищена сумісність. Основним стандартом взаємодії для розгортання сервіс-орієнтованої архітектури (SOA) є уніфікована архітектура OPC (OPC UA). Даний стандарт важливий для систем, які використовують цей протокол, щоб увімкнути та застосувати функції безпеки, які постачаються з ним. Це проблема, оскільки протокол може використовуватися для міжмашинного зв’язку між фабриками та заводами різних фірм і пристроями IoT у різних країнах.

5. Група екстреного реагування. Повинна, бути створена група, яка буде реагувати на надзвичайні ситуації та негайно впроваджувати рішення, задля вирішення проблеми. Отже, час від часу потрібно робити тренування з надзвичайних ситуації, щоб учасники відпрацьовували свої навички.

6. Створення процедури безпечного обслуговування. Підприємства, можуть використовувати профілактичні обслуговування, щоб зменшити втрати в бізнесі. Виконуючи, дане обслуговування, потрібно враховувати заходи пов’язані з безпекою.

Саме, хмарні технології є надзвичайно популярні для зберігання даних в мережі IoT. Для того, щоб отримати доступ до мережі, зловмисник може використовувати фішингові електронні листи, які націлені на користувачів. Як зазначалося раніше, пристрої повинні бути розділені, тобто відбувається сегментація мережі.

- Створення планових захисних заходів. Спочатку, створюється процедура управління інцидентами, які відповідають потребам організації. Ввиконайте, план реагування на інциденти, задля швидкого виявлення та негайного вирішення.

- Регулярно змінюйте паролі. Велика ймовірність, того що зловмисник отримає пароль від облікового запису, та матиме доступ до інформації. Тому, рекомендацією буде не тільки регулярно змінювати пароль, а і використовувати двофакторну автентифікацію, для додаткової безпеки. Отже, використовують секретний ключ, який передається через мобільний пристрій або телефонний дзвінок для підтвердження входу.

- Відстеження дій. Потрібно, щоб був створений план дій для моніторингу та аудиту виконаних дій користувачів.

- Слідкуйте, щоб ключі автентифікації знаходилися в безпеці. Потрібно, налаштувати автентифікацію для ідентифікації осіб, які отримують доступ до даних, що зберігаються в хмарі. А також, потрібно переконатися, що ключі автентифікації, зберігаються в надійному сховищі.

- Підтримуйте безпеку на всіх рівнях. Замість того, щоб захищати лише зовнішні рівні, необхідно розглянути всі рівні та запровадити методологію поглибленого захисту разом із засобами контролю безпеки.
- Механізм захисту даних та їх вирішення. Потрібно, щоб була створення процедура контролю доступу захисту даних. Всі рекомендації, дадуть змогу зменшити потребу в ручній і прямій обробці даних і мінімізує ймовірність людської помилки під час зміни конфіденційних даних.

Висновки до четвертого розділу

Досліджено функціонал програми AWS Greengrass. Виявлено, що переваг програма має багато, одна з них, якщо пристрій втрате зв'язок із хмарою, то підключені пристрої продовжують взаємодіяти один з одним по локальній мережі.

Виконано віддалене розгортання, одного із компонентів, який дає змогу локально підключатися по мережі.

Розроблено рекомендації для захисту мережі IoT, як для користувача, так і для виробника.

ВИСНОВКИ

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

- досліджено поняття Інтернету речей та доведено актуальність технології;
- розглянуто вимоги, які мають значення для IoT та архітектуру технології;
- виконано аналіз атак та вразливостей на IoT;
- проаналізовано ризики для безпеки мережі IoT;
- виконано аналіз загроз безпеці в IoT;
- проведено аналіз та виконано рекомендації для підвищення рівня безпеки для IoT;
- реалізовано використання програми AWS Greengrass, для обміну повідомленнями, синхронізацією та виконання висновку для підключених пристроїв;
- розроблено рекомендації для захищеної IoT мережі для користувача та виробника.