ЛАБОРАТОРНА РОБОТА №6

Інтеграція безпеки даних для систем інтернету речей

Мета роботи: ознайомитися з принципами забезпечення безпеки даних у системах Інтернету речей (IoT), навчитися реалізовувати базові методи захисту даних, такі як шифрування, автентифікація та контроль доступу.

1.1 Теоретичні відомості

Майже кожен пристрій Інтернету речей, який підключений до мережі, може отримати доступ до інфраструктури Інтернету речей, а також до ваших персональних даних. Коли з'являються нові лазівки в безпеці та потенційні вразливості, ризики, пов'язані з Інтернетом речей, виходять на новий рівень через сумісність, програми та автономне прийняття рішень. Тому безпека та конфіденційність даних є життєво важливими.

Інтернет речей – це мережа, яка об'єднує мобільну мережу, соціальні мережі, Інтернет і різні розумні об'єкти, щоб надати користувачам різноманітні послуги та додатки.

Покращуючи безпеку взаємодії об'єктів, надійність і сумісність, безпека на різних рівнях безпосередньо впливає на успіх систем Інтернету речей. Інтенет речей тепер може об'єднувати різні простори (наприклад, фізичне та цифрове), де різні датчики взаємодіють з фізичним простором. Ці датчики вже повністю використовуються практично у всьому, від іграшок до систем охорони здоров'я. Це показує, як різні небезпеки, які виникають у цифровому світі, починають діяти на реальний світ.

Система успішна, якщо вона може забезпечити безпеку від вразливостей. Багато в чому успіх додатків Інтернету речей та інфраструктури Інтернету речей залежить від забезпечення безпеки та уразливості. Вимогами

до безпеки Інтернету речей (IoT) є велика кількість нових інструментів, які вбудовані в організацію, а часом і в систему.

Всі пристрої, які є підключеними, мають потенціал отримати доступ до Інтернет-інфраструктури або особистих даних. Такі пристрої можна аналізувати та використовувати. У результаті аналізу цих даних можна створити невидимі посилання, які можуть бути спрямовані на конфіденційність людей або організацій. Незважаючи на те, що проблеми безпеки та конфіденційності є надзвичайно важливими, ймовірність небезпеки для об'єктів підвищиться, оскільки сумісність, гібридні програми та незалежне прийняття рішень створюють складність, прогалини в безпеці та потенційні вразливості.

У сфері інформаційних технологій існує ризик захисту даних, оскільки складність може створити високу вразливість у зв'язку з послугами. Більшість інформації, доступної в Інтернеті речей, пов'язана з нашими особистими даними, такими як дата народження, місце розташування, бюджет тощо. Однією з проблем великих даних є ризики, які застосовуються до кожного набору даних. Інтернет речей має бути реалізований законним, моральним, соціальним і політичним способом. При цьому слід враховувати юридичні, систематичні, технічні та бізнес-проблеми.

Хоча безпека була значною проблемою, найважливіші проблеми безпеки даних і конфіденційності все ще не визначені. Проблеми безпеки даних і конфіденційності не є новими для Інтернету речей, оскільки вони були вирішені ще з часів RFID.

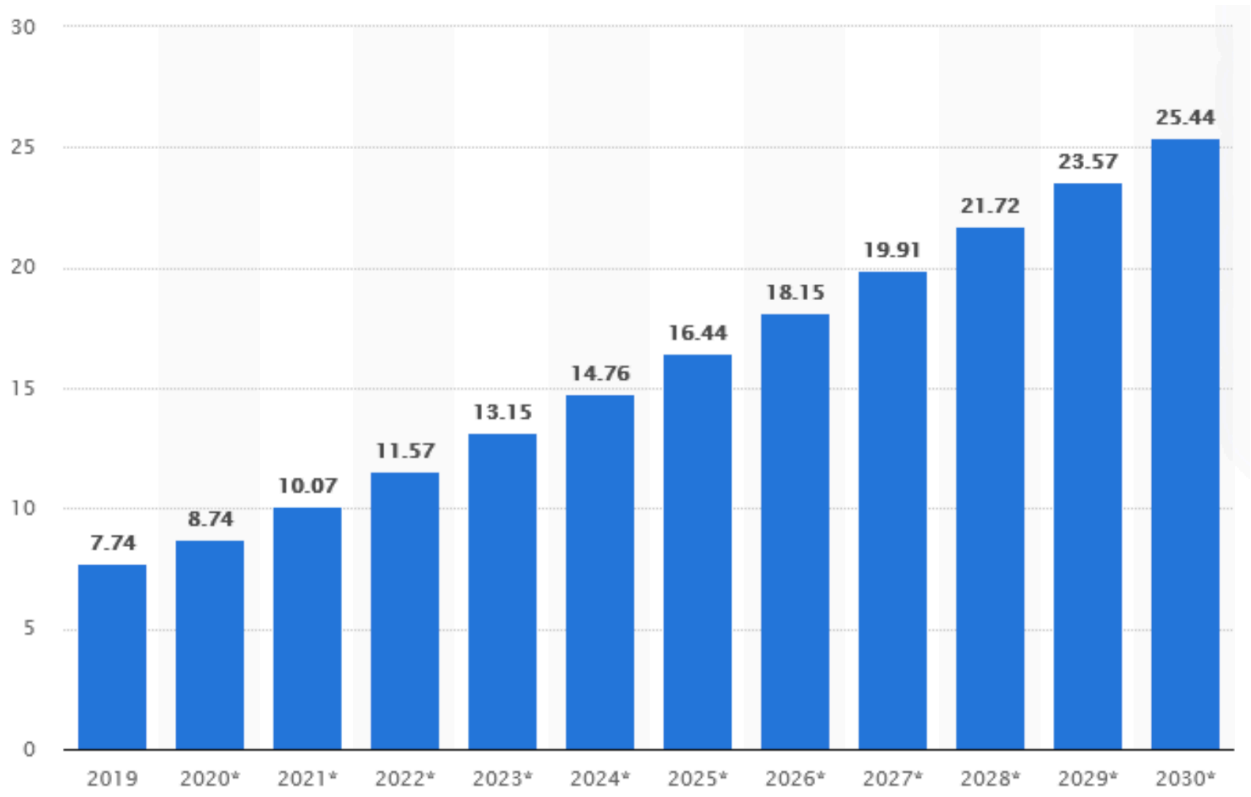

Рис. 1 Оцінка кількості підключених IoT пристроїв по всьому світу з 2019 до 2030 року за даними сайту statista

Відображені вимоги до безпеки системи, що складається з 6 основних критеріїв представлено на рис. 2 :

- критерій конфіденційності (1) - дані, захищені уповноваженими;
- критерій цілісності(2) - дані надійні;
- критерій доступності(3) - дані доступні, коли і де це потрібно;
- критерій безвідмовності(4) - послуга забезпечує надійний аудиторський шлях; критерій достовірності(5) - компоненти можуть підтвердити свою ідентичність;
- критерій секретності(6) - служба автоматично не бачить дані клієнтів.

Рис. 2 Вимоги безпеки IoT

Коли об’єкти в Інтернеті речей збирають та узагальнюють фрагменти даних, виникають ризики захисту даних. У зв’язку з тим, що місце, час і періодичність подій є контекстом для перегляду подій, зіставлення кількох точок дозволяє перетворити особисту інформацію. Це один із елементів виклику великих даних, і фахівці з безпеки повинні переконатися, що вони розглядають усі можливі загрози для конфіденційності. Довіра, секретність і конфіденційність даних є основними проблемами безпеки IoT.

Конфіденційність даних:

- недостатня аутентифікація / достовірність;
- небезпечні інтерфейси (Інтернет, мобільний телефон тощо);
- відсутність трансортного шифрування;
- збереження конфіденційності;
- управління доступом.

Секретність:

- секретність, захист даних та управління ризиками інформаційного забезпечення ;
- секретність за замовчуванням;
- політика конфіденційності;
- відстеження / профілювання / незаконна обробка.

Довіра:

- система управління особистості;
- небезпечне програмне забезпечення / прошивка;
- для забезпечення безперервності та доступності послуг;
- виконання шкідливих атак на пристрої та системи інтернету речей;
- втрата перевірки користувача / складність у прийнятті рішень.

Сучасні виробничі об’єкти та смарт-міста, які з’єднані в єдину платформу в першу чергу вимагають створення оптимальної архітектури безпеки пристроїв в інтернеті речей. Створювана безпека повинна відстежувати кожен підключений до мережі пристрій окремо, попереджати про можливий зловмисний доступ, або захищати чи відключити пристрої в міру необхідності та загрози. Тому, вкрай важливий процес для інтернету речей - це розробка і використання стандартів.

В області стандартизації, на всіх рівнях інтернету речей, ведеться найактивніша робота. В наш час розробкою стандартів займається деякі великі організації: IEEE (Institute of Electrical and Electronics Engineers) і ISO / IEC (International Electrotechnical Commission).

Збільшення кількості пристроїв Інтернету речей призводить до зростання ризиків для безпеки, оскільки зловмисникам стає легше маніпулювати величезною кількістю даних. Без достатньої безпеки пристрої IoT можуть втратити конфіденційні дані. Крім того, через низьку ціну, низьку потужність і низькі обчислювальні можливості, а також неоднорідність і масштаб мережі, пристрої IoT піддаються нападам і небезпекам безпеки.

Пристрої IoT вразливі до загроз не лише з технічних аспектів, але й через діяльність користувачів. Ось кілька причин, чому ці розумні пристрої все ще знаходяться в зоні ризику.

1. Обмежені апаратні та обчислювальні можливості: ці пристрої розроблені для конкретних програм, які вимагають лише обмежених можливостей обробки, залишаючи мінімальну область для безпеки та захисту даних для інтеграції.

2. Гетерогенна технологія передачі даних: ці пристрої спілкуються з різними типами пристроїв і часто використовують різні технології зв'язку, що ускладнює встановлення єдиних заходів захисту та протоколів.

3. Компоненти пристрою вразливі: мільйони розумних пристроїв можуть бути пошкоджені незахищеними або застарілими елементами.

4. Користувачі недостатньо обізнані про безпеку: через брак знань користувачів про безпеку розумні пристрої можуть бути піддані зонам ризику та ймовірним атакам. Багато пристроїв IoT дозволяють користувачам інтегрувати програми сторонніх розробників, що також може поставити пристрій у небезпечну зону.

5. Слабка фізична безпека: на відміну від центрів обробки даних Інтернет-сервісів, не лише користувачі, а й інші особи з поганими намірами мають фізичний доступ до основної частини компонентів IoT. Проблеми

безпеки поділяються на загрози програмного рівня та загрози апаратного рівня, як показано на рисунку

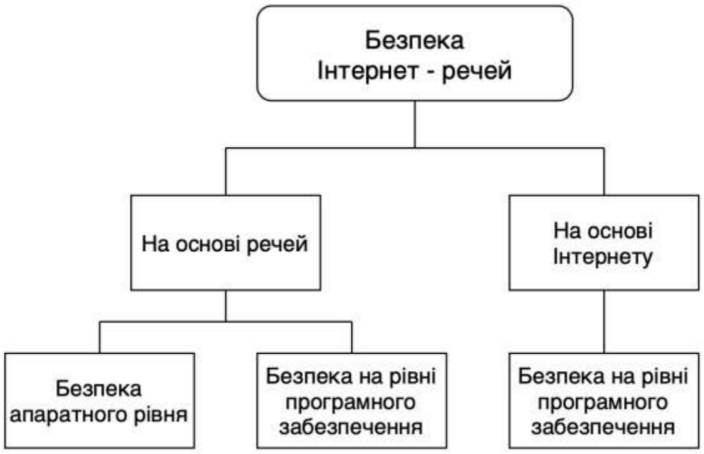

Рис. 3 – Атака на апаратне та програмне забезпечення

Атаки на програмне забезпечення, такі як втік інформації, незаконний доступ тощо, мають на меті змусити систему працювати неправильно та зібрати бажану інформацію, таку як дані кредитної картки, паролі тощо. Атаки на основі програмного забезпечення можуть бути обмежені за допомогою брандмауера, оновлених баз даних вірусів і використання найновішого програмного забезпечення. Зловмисники часто використовують атаки на рівні апаратного забезпечення та програмного забезпечення. Розробка захищених інтегральних схем (IC) або систем на кристалі (SoC) є першим кроком до створення повністю захищеного апаратного забезпечення. Під час виготовлення система може постраждати від однієї шкідливої схеми, яку розробники можуть не помітити.

Верхні елементи піраміди більш вразливі з мінімальним ймовірним впливом, а елементи нижчого рівня мають протилежні характеристики. Можна стверджувати, що кіберзагрози шукають більшого контролю та можливостей на нижчому рівні.

Дефекти в компонентах системи роблять систему чутливою та розширюють поверхню атаки. Зокрема, зловмисники намагаються отримати доступ для виконання своїх зловмисних дій за допомогою апаратного або програмного забезпечення системи Інтернету речей (IoT). Згідно зі звітом HP, половина комерційно доступного IoT має значний недолік безпеки. Раніше перераховані вразливості можуть розкрити конфіденційні дані в системах IoT, тому їм потрібно запобігати та реагувати. Аналіз безпеки мережі IoT складний, оскільки вона піддається різним типам атак. Тим не менш, велика кількість даних, створених Інтернетом речей, підвищує безпеку всієї системи.

Щоб убезпечити обладнання, необхідно розуміти цілі безпеки. Конфіденційність, цілісність і доступність відомі як тріада CIA. У таблиці 1 перераховані цілі безпеки запропоновані IAS, а також приведено їх визначення.

Таблиця 1 – Вимоги безпеки IoT

Вимоги безпеки	**Визначення**
Конфіденційність	Процес, під час якого суворо зберігається таємниця та конфіденційність інформації, що транслюється в ефірі та зберігається, і доступ до неї мають лише дозволені об’єкти або користувачі.
Цілісність	Процес, у якому не відбувається змінення даних I і забезпечується точність.
Невідмовність	Процедура, за допомогою якої система IoT перевіряє легітимність і походження події.

Доступність	Процес забезпечення доступності послуг для тих, хто їх потребує, навіть якщо сталося відключення електроенергії або поломка.
Приватність	Метод, за допомогою якого система IoT має доступ до приватних даних, дотримуючись правил і політик.
Аудит конфіденційності	Процес, за допомогою якого система IoT відстежує свої дії.
Відповідальність	Механізм, за допомогою якого користувачі системи IoT відповідатимуть за свої дії.
Надійність	Метод, за допомогою якого система IoT може підтвердити ідентифікацію особи та встановити довіру до третьої сторони.

Конфіденційність пов’язана з системою правил, які визначають, які особи мають право на доступ до інформації. Цілісність – ще одна функція, яка гарантує надійні послуги, щоб пристрої IoT отримували лише легітимні команди та інформацію. Доступність IoT гарантує, що функціональні можливості IoT доступні користувачам і законним об’єктам у будь-який час і місці.

Атаки на IoT поділяються на чотири категорії:

- фізичні атаки або атаки сприйняття;
- мережеві атаки;
- атаки на програмне забезпечення або програми;
- атаки на шифрування.

Рис. 4 Загрози безпеці Інтернету речей

Існує апаратні та програмні рішення, які можуть захистити пристрої IoT від потенційних атак. Це завдання програмного забезпечення захистити пристрої від програмних атак. Сучасні комп'ютерні системи складні для зламу математичних алгоритмів програмного забезпечення. Коли квантові комп'ютери досягнуть достатньої потужності, він, однак, зможе розгадувати математичні ключі за більш короткий час. Оскільки ключі зберігаються в енергонезалежній пам'яті (NVM) пристроїв у рішеннях безпеки на основі програмного забезпечення, пристрої схильні до атак. Програмні рішення безпеки можуть стати вразливими через появу квантових комп'ютерів. Таким чином, через фактор ризику існуючої програмної безпеки апаратне рішення може бути одним із варіантів.

2.2 Завдання до виконання лабораторної роботи

- Ознайомитися з теоретичними відомостями.
- Інтегрувати та описати принципи безпеки даних для IoT проекту згідно з варіантом.
    - Розумні парковки: Система моніторингу та резервування місць;
    - Інтелектуальна система керування шторами;

    - Інтелектуальна система керування електроспоживанням будинку;
    - Інтелектуальна система керування та оптимізації домашніх генераторів;
    - Застосунок для керування LED-стрічкою та освітленням;
    - Розумний інкубатор;
    - Система моніторингу периметру і виявлення загрози;
    - Інтелектуальна система догляду за садом;
    - Розумний термостат для опалення;
    - Розумні двері для домашніх тварин.
- Оформити звіт до лабораторної роботи.

2.3 Контрольні запитання

- У чому полягає роль автентифікації в системах Інтернету речей?
- Які є стандарти безпеки для IoT-пристроїв і мереж?
- Які протоколи безпеки застосовуються в IoT-системах?
- Які переваги та недоліки використання багатофакторної автентифікації для IoT-пристроїв?
- Які методи шифрування даних використовуються для захисту інформації в IoT-системах?

2.4 Зміст звіту

- Мета лабораторної роботи.
- Теоретичні відомості.
- Знімки екрану, які відображають виконане завдання.
- Висновки до роботи.