МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____ С.В. Казмірчук

«_____»_____ 2020 р.

На правах рукопису
УДК 004.056.5:510.22(043.3)

МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ «МАГІСТР»

Тема: Система забезпечення кібербезпеки на об'єктах критичної інформаційної інфраструктури

Автор: В. О. Карнаух

Науковий керівник: доцент кафедри КСЗІ А. Б. Петренко

Нормоконтролер: доцент кафедри КСЗІ А.В. Ільєнко

Київ 2020

ВСТУП

Інтернет речей (IoT) – це поєднання кібер-інфраструктури з фізичним світом. Кібер-інфраструктура включає в себе засоби інформаційних технологій (IT), такі як зберігання даних, хмарні послуги, операційні системи, програми, різні мережеві технології, служби резервного копіювання, моніторинг і механізми безпеки, а також процеси автентифікації, авторизації та аудиту. Фізична інфраструктура включає пристрої та датчики всіх форм, а також системи управління, які забезпечують належне функціонування цих елементів[1]. Безпека IT-інфраструктури IoT є необхідною, але недостатньою умовою, оскільки навіть якщо вона буде захищена передовими методами безпеки IT, будь-яке порушення фізичних пристроїв і датчиків може призвести до порушення всієї системи. Отже, якщо буде порушена робота пристроїв, то і дані, створені за допомогою цих пристроїв, скоріш за все будуть ненадійними. Безпека інфраструктури IoT вимагає комплексного підходу, починаючи від фізичних пристроїв і датчиків до послуг і даних у хмарі. Таке формулювання вимоги безпеки для технології IoT залишається проблемою, оскільки інфраструктура IoT зазвичай розробляється, розгортається і експлуатується не тільки IT-фахівцями, а й дизайнерами, розробниками та операторами фізичних пристроїв і машин. Кожен з них має свою мету і людина, що не розуміється на безпеці навряд чи буде перейматись такими питаннями. Наприклад, для розробників IT-інфраструктури, безпека та конфіденційність можуть бути однією з найбільш важливих функцій системи, разом з функціональністю, зручністю використання та вартістю. Проте, розробники фізичних машин можуть вважати більш важливими доступність і надійність машини, ніж безпека. Дослідження, як один з етапів нашої роботи, дало чітке розуміння того, що найслабшим місцем технології

IoT є передача даних. Тому ми розробили власну модель архітектури IoT та визначили, які засоби захисту пристроїв IoT мають використовуватись та надали рекомендації, щодо правильного впровадження таких систем.

РОЗДІЛ 1
ПРЕДМЕТНА ОБЛАСТЬ ТЕХНОЛОГІЇ IOT

Метою пристроїв, які підключені між собою і об’єднані в одну систему, є полегшення нашого з вами повсякденного життя. Саме це і є IoT - система взаємозв’язаних обчислювальних пристроїв, механічних і цифрових машин, об’єктів, тварин і людей, яким надаються унікальні ідентифікатори і мають змогу обмінюватися даними в мережі[2].

1.1 Загальний огляд технології IoT

Термін “Інтернет речей” як поняття вперше згадувався в 1990-х роках. Поточний формат вислову був запропонований Кевіном Аштоном у 1999 році[3]. За даними Gartner, індустріальний Інтернет складається з фізичних пристроїв, здатних контролювати навколишнє середовище і передавати дані моніторингу іншим пристроям і здійснювати дії, що ґрунтуються на отриманих даних інтелектуально. Інакше кажучи, поняття “Інтернет речей” (Internet of Things, IoT) стосується пристроїв, з’єднаних між собою різними способами та каналами зв’язку. Ці пристрої здатні передавати дані і обмінюватися ними один з одним. Спосіб зв’язку і шляхи передачі можуть бути або бездротовими, або дротовими, в залежності від пристрою IoT і його призначення. За даними різних науково-дослідних інститутів, таких як Gartner (2017), до 2020 року в світі буде встановлено до 25 мільярдів IoT-пристроїв[4]. Однак, цей показник може бути набагато вищим.

Міжнародний союз електрозв’язку (ITU) визначає IoT як глобальну інфраструктуру інформаційного суспільства, яка призначена для взаємодії фізичних та віртуальних активів, речей, що базуються на взаємодіючих каналах зв’язку та технологіях.

Лоуренс Міллер в праці “Безпека IoT для чайників” (2016) [5] визначає IoT наступним чином: IoT охоплює пристрої та об’єкти, сполучені між собою різними протоколами зв’язку. У ролі таких пристроїв можуть виступати обчислювальні машини, ноутбуки або звичайні персональні комп’ютери, чи навіть планшети та смартфони. Каналами зв’язку в IoT, як правило, виступає Bluetooth і Long Range Wide Area, або бездротові шляхи передачі на основі мобільного зв’язку, такі як 3G і 4G. Ці шляхи передачі, як правило, визначаються як протоколи малої потужності, тому що зазвичай пристрої IoT посилають невелику кількість даних з низькою швидкістю передачі. У майбутньому пристрої IoT зможуть спілкуватися з інфраструктурою на великих відстанях сучасними технологіями, такими як мобільні мережі 5-го покоління, скорочено 5G.

Як вище було зазначено, до 2020 року в світі може функціонувати до 25 мільярдів IoT-пристроїв. Однак, кількість підключених пристроїв може бути ще вищою через реалізацію новітніх розробок. Раніше тенденція до зростання досягала 31% з року в рік. Наразі споживчий сегмент становить 63% від загальної кількості пристроїв IoT.

Коли йдеться про майбутнє IoT, слід враховувати також і тенденцію до здешевлення ринкової вартость приладів IoT.

Слід зазначити, що незважаючи на те, що велику кількість приладів IoT купують приватні споживачі, більше в пристрої IoT інвестує бізнес-сторона. Так, у 2017 році 57% витрат на ринок IoT прийшли з бізнес-сторони[6]. Таблиця 1.1 показує вартість ринку IoT від 2016 року до 2019 року.

Таблиця 1.1 – Ринкова вартість приладів IoT (в дол. США)

Категорія	2016 рік	2017 рік	2018 рік	2019 рік
Приватні споживачі	532 515	725 696	985 348	1 494 466
Міжгалузеві підприємства	212 069	280 059	372 989	567 659
Спеціалізовані підприємства	634 921	683 817	736 543	863 662
Загальна сума	1 379 505	1 689 572	2 094 881	2 925 787

Економічний вплив IoT вимірюється трильйонами, а кількість пристроїв IoT вимірюється мільярдами.

Щоб триматись на плаву такого швидкого розширення, промислові постачальники інтенсивно діють, щоб розширити свої пропозиції приватної хмари, в той же час як відомі інтернет-монополісти, включаючи Alibaba, Amazon Web Services, Google, IBM і Microsoft, створюють власні хмарні послуги.

Неприємна реальність полягає в тому, що підключені пристрої є потенційними цілями для тих, хто шукає несанкціонований доступ до мережі, зловмисний контроль над пристроєм або викрадення даних. Зростаюча складність екосистем IoT посилює ці небезпеки, оскільки пристрої, що постачаються багатьма виробниками і пропонують різні рівні безпеки, можуть привести до несподіваних вразливостей, непередбачених результатів і небезпечної роботи.

Наприклад, будь-яке обладнання, підключене до IoT, будь то повітряний компресор, пральна машина або пасажирський транспортний засіб, може управлятися дистанційно. Більш того, інтелектуальні енергосистеми, які керують розподілом енергії і води, можуть, в разі втручання або незаконного доступу, представляти серйозну загрозу для здоров’я людини і нашої безпеки як спільноти.

Люди, які прагнуть нашкодити або вкрасти інформацію, постійно розробляють нові способи отримання доступу, злому систем і збору даних. Результати можуть бути руйнівними. Потенційні витрати на відновлення величезні. Тільки за останні два роки економічний збиток від кіберзлочинності перевищив трильйон доларів. Навіть обмежена атака шкідливого ПЗ, яка перешкоджає роботі, але не може отримати конфіденційні дані, може коштувати організації сотні мільйонів доларів у вигляді втраченого бізнесу, зіпсованої репутації, тимчасових обхідних шляхів, відкликання продуктів, зв'язків з громадськістю та довгострокових виправлень.

1.2 Функціональні складові IoT

Пристрої IoT можна поділити на споживчі пристрої (напр. побутова техніка, домашні девайси і т.і.), а також прилади для промислового використання (напр. датчики вимірювання температури, вологості та руху і т.і.).

Так, типовими побутовими приладами є, наприклад, камери відеоспостереження, мережеві комутатори, маршрутизатори та мережеві сховища (NAS), холодильники, смарт-телевізори та автомобілі. Для домашньої автоматизації, тобто розумних будинків, використовуються такі типові пристрої, як системи опалення та вентиляції, системи керування освітленням, датчики контролю рівня вологості повітря та ін.

Коли мова йде про промисловий IoT, потрібно згадати термін "Промисловість 4.0" [7]. "Промисловість 4.0" охоплює різні види автоматизації та технології обміну даними. Її також називають "розумною (смарт) фабрикою". Смарт-фабрика охоплює кібер-фізичні системи, Інтернет речей, хмарні обчислення та когнітивне навчання. Тобто, термін "Промисловість 4.0" означає, що промислові машини і датчики спілкуються один з одним практично без втручання людини. Тому автоматизація

“Промисловість 4.0” разом з інтелектуальним моніторингом забезпечує більш високий рівень автоматизованого виробництва, що підвищує якість продукції для кінцевого споживача. Беручи за основу моніторинг результатів датчиків, машини можуть коригувати свою роботу більш ефективно. Як правило, домашні комп’ютери та ноутбуки або мобільні телефони не вважаються пристроями IoT.

1.3 Ядро та класифікація атак IoT

Існує три окремі складові (величини) що використовуються для того, щоб розрізнити пристрої IoT від традиційних настільних комп’ютерів і становлять основу для поставлених завдань, а саме це є сила, пропускна здатність та вимоги до обробки (час). Ці обмеження завжди будуть присутні в IoT, тому, від того як вони працюватимуть, і в якій мірі пристрій обмежений різними умовами, визначатиме, як пристрій і його механізми безпеки розроблятимуться і реалізовуватимуться. Обсяг доступної потужності значною мірою буде впливати на проблеми та можливі доступні рішення. Використовуючи обмеження потужності як основного диференціатора систем IoT, простір IoT поділяється на окремі категорії: суворо обмежені, необмежені та змішані системи. Якщо пристрій сильно обмежений потужністю, можливість обробки та доступність, ймовірно, будуть низькими, оскільки він не буде працювати безперервно для економії енергії. Про LCD дисплеї можна забути оскільки звичайними користувацькими інтерфейсами в цих пристроях є кнопки, світлодіоди, мікрофони або інші датчики. Необмежені пристрої менше будуть обмежені пропускною здатністю, але, разом з тим, будуть і менш мобільними, ніж будь-яка з інших категорій. Змішані системи зазвичай включають в себе безліч типів бездротового зв’язку і потребують більше можливостей обробки на необмежених вузлах для обробки запитів від обмежених

пристроїв. В залежності від того який підхід буде використовуватись для захисту пристрою, вирішуватиме до якої категорії буде відноситись продукт.

Деякі проблеми можуть дуже швидко перетворитися на дуже серйозні і стати настільки фундаментальними, що можуть впливати на всі інші проблеми в середовищі. Одне з найскладніших питань в IoT впливає одразу на всі три обмеження: це процес підключення. Розподіл ключів на пристрої з невеликою потужністю обробки сам по собі є проблемою, а разом з низькою доступністю і відсутністю інтерфейсу користувача робить його ще складнішим. У найдоступніших пристроях можна запровадити концепцію інфраструктури публічних ключів (PKI) [8] для керування авторизацією, але протоколи, такі як Secure Sockets Layer (SSL) [9], протокол захисту транспортного рівня (TLS) [10] або Datagram Transport Layer (DTLS)[11] протокол датаграм транспортного рівня, часто вимагають занадто багато від девайсів IoT, що призводить до широкого використання Pre-Shared Key (PSK) [12] у найменш здатних пристроях IoT сьогодні. Багато протоколів, призначених для менш здатних пристроїв, використовуватимуть процес прямого сполучення, що зазвичай вимагає взаємодії з користувачем для ініціювання створення пари. Деякі рішення потребують натискання кнопки і фізичного втручання, що часто є поганим рішенням, якщо вузли монтуються в недосяжних місцях, у той час як інші вимагають введення або просто прийняття ключа з'єднання. Існують також інші рішення, такі як використання зовнішніх портів для підключення до комп'ютера або мультимедійного пристрою, з використанням іншого бездротового зв'язку, наприклад радіочастотної ідентифікації (RFID)[13], з використанням фоторезистора (світловий датчик) або просто аудіозв'язок через мікрофон. Поствиробниче управління є важкою і потенційно серйозною проблемою для IoT. Коли продукт поставляється, і в ньому виявляють вразливість системи безпеки, то виникає необхідність терміново випустити оновлення пристроїв. Якщо ж цього не зробити, то доведеться відкликати кілька партій

пристроїв, що призведе до величезних економічних втрат. Особливу увагу варто приділити тому, наскільки руйнівним і шкідливим може бути оновлення, і чому виробникам так важливо використовувати автентифікацію та авторизацію, щоб гарантувати, що оновлення було отримано від виробника та не було підроблене третьою стороною.

Необхідно вибрати правильний вид захисту.

Одна справа – знати, що кожному пристрою IoT потрібен базовий рівень захисту, але який спосіб є найкращим для реалізації цієї безпеки? Зрештою, не кожен пристрій стикається з таким самим профілем ризику – інтелектуальний пристрій, підключений до домашньої мережі WiFi, відрізняється від механізму управління на атомній електростанції – і існує потреба в балансі типу захисту з вартістю впровадження та підтримання цього захисту.

Перш за все, при визначенні безпеки пристроїв IoT, потрібно розглянути операційне середовище. Як пристрої взаємодіятимуть із системами навколо них, і які конкретні ризики пов’язані з цими взаємодіями?

Наприклад, які пристрої IoT будуть завантажувати дані в хмару, а які хмарні служби отримуватимуть дані? Хто керуватиме кожним пристроєм? Яке обладнання буде використовуватися для керування пристроями, і яке програмне забезпечення буде дозволено запускати і коли? Чи є платіж, пов’язаний з використанням пристрою IoT? Чи буде пристрій IoT співіснувати з потенційно уразливим обладнанням та додатками?

Охарактеризувавши кожний пристрій як частину великої екосистеми, і спрогнозувавши загрози в цій конкретній екосистемі, можна дізнатися, який захист буде найкращим чином працювати, і як його розгортати.

Захист IoT – це більше, ніж захист пристрою під час підключення до мережі. Майже в кожній точці екосистеми IoT, і протягом усього життя будь-якого пристрою IoT, є можливості для несанкціонованого доступу –

від проектування та виробництва – до того, як елементи інтегруються, впроваджуються і навіть утилізуються.

Незважаючи на те, що зараз актуально висвітлювати проблему експлуатації слабкої захищеності пристроїв (наприклад, незашифровані підключення або ненадійний контроль доступу), а також пошкодження, завдані атаками “Відмова в обслуговуванні” (DDoS), існує багато різних видів саботажу і список тільки стає довшим. Наприклад, віддалені, масштабовані атаки тепер можуть витягувати інформацію на фізичному рівні або фізично змінюють вміст пам’яті, що донедавна було можливим лише за допомогою локальної атаки.

Таблиця 1.2 – Атаки у кіберпросторі

Тип атаки	Принцип роботи
Соціальна інженерія	Різні методи, включаючи брехню, хабарі, шантаж і погрози, які використовуються окремими особами, щоб задіяти інших для атаки на інформаційні системи.
Слабка безпека	Експлуатація систем, які недостатньо захищені. Цей вид включає в себе довгий список поганих звичок безпеки, включаючи використання з’єднань, які не використовують шифрування, цілісність даних або автентифікацію, використання ненадійного контролю доступу, включаючи паролі за замовчуванням або незахищені облікові дані, які легко дістати або навіть загальнодоступні, використання систем, які можуть

	бути легко зламані, а також використання погано налаштованих стеків зв’язку з відкритими портами і т. д.
Експлуатація вразливостей	Вразливість системи, така як програмна або апаратна помилка, використовується для непередбачуваної поведінки системи, в тому числі виконання довільного коду, доступ до даних і відмова в обслуговуванні.
Атака по стороннім каналам	Шляхом локального або віддаленого спостереження та вимірювання фізичних параметрів роботи системи, таких як енергоспоживання, електромагнітні випромінювання або навіть звук, можна отримати певні дані, включаючи ключі, і використати їх для зламу системи.
Fault injection (занесення вразливостей)	Модифікації, що виконуються локально або віддалено, що змінюють поведінку системи, вводяться в апаратне або програмне забезпечення системи. Можуть бути змінені місця пам’яті, значення шини тощо.
Виробнича атака	Збиток, нанесений під час виробництва, наприклад, викрадення інтелектуальної власності або облікових даних, зниження рівня безпеки, додавання прихованих функцій або зміна функціональності, включаючи

	незаконну зміну програмного забезпечення або запровадження контрафактних компонентів.
Реверс-інженерія програмного та апаратного забезпечення	Завдяки програмному забезпеченню зловмисник зазвичай намагається розшифрувати спробу програміста замаскувати, як працює код, а за допомогою апаратних засобів, атака зазвичай включає в себе прорив фізичних бар'єрів, створених під час виробництва, які приховують архітектуру схеми.

Цілодобова робота є невід'ємною частиною багатьох програм IoT, і особливо в розумних містах і промисловості 4.0. Будь то розумна комунальна мережа, точна техніка на заводі, автоматизація у ланцюжку поставок або розумний міський транспорт, добре продумана архітектура системи – підтримуються стандартними методами для надійної автентифікації, ефективного захисту даних і точного керування командою – забезпечує захист, необхідний для мінімізації потенційного простою, пов'язаного з безпекою пристрою.

При належному забезпеченні, IoT захищається протягом усього життєвого циклу, а також ефективно захищає дані, збільшує продуктивність, гарантує роботу та захищає людей.

IT-безпека – це велике і різноманітне середовище, і не завжди очевидно, що насправді означає цей термін. Цей термін також тісно пов'язаний з більш широкою концепцією інформаційної безпеки. В контексті IoT інформаційна безпека тісно пов'язана із захистом конфіденційності користувача. Багато дослідників сходяться на думці, що забезпечення безпеки Інтернету речей є однією з найсерйозніших проблем безпеки, з якими ми стикаємося сьогодні. У нас вже є багато речей,

пов’язаних з Інтернетом, мобільними платформами, підключеними кухонними пристроями, автомобілями і промисловими системами управління. Тому вже є багато систем, як малих, так і великих, які збирають і обробляють дані в нашому повсякденному житті. Проте, велич IoT полягає в тому, що всі ці системи з’єднуються разом і дозволяють пристроям взаємодіяти один з одним через системи. Це вимагає нових архітектур для IoT, і тут IoT знаходиться тільки на початковій стадії розробки. Область ще не сформувалася, немає загальноприйнятих стандартів і архітектур, але в різних організаціях ведеться велика робота з цього приводу. Тільки в Європі існує кілька дослідницьких проектів, в яких розробляються архітектури для IoT, такі як IoT Open Platforms, IoT European Research Cluster, IoT European Platforms Initiative і IoT Architecture.

Проблеми безпеки та конфіденційності IoT існують через специфічність характеристик мереж IoT, які роблять їх унікальними.

Такими характеристиками є:

- неконтрольоване середовище;
- неоднорідність;
- потреба у масштабованості;
- обмеженість ресурсів.

Таблиця 1.3 – Можливості та ризики IoT[14]

Можливості IoT	**IoT Ризики**
● Покращення використання активів ● Оптимізація в режимі реального часу ● Більш глибоке розуміння кінцевого користувача ● Розширення прийняття рішень	● Кіберзлочинність, кібервійна і кібертероризм ● Порушення даних і конфіденційності ● Ботнети, програми-вимагачі та інші шкідливі програми ● DDoS-атаки та інші види саботажу

● Більш автономне функціонування фізичних активів ● Більш легкий доступ до інформації та послуг	● Несправність пристрою через пульт дистанційного керування ● Викрадення інтелектуальної власності (ІВ)

Можна, однак, стверджувати, що останній пункт про ресурси є менш дійсним. Існує широко поширена модель IT-безпеки, яка базується на трьох бажаних характеристиках безпеки систем, часто скорочених як ЦКД(тріада CIA) [15] : цілісність (тобто забезпечення даних не змінюється), конфіденційність (тобто запобігання несанкціонованому доступу до даних), а також доступність (тобто забезпечення доступності даних у разі потреби).

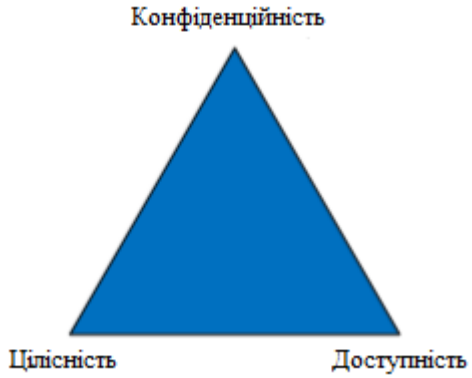


Рисунок 1.1 – Тріа да CIA

Ці властивості часто описуються у вигляді трикутника, в якому властивості розміщуються у вершинах. Протягом багатьох років модель була модифікована рядом альтернативних ключових властивостей, але основні властивості ЦКД завжди залишалися. А от що не було підкреслено, так це те, що ці три властивості ніколи не можуть бути повністю досягнуті одночасно, оскільки вони взаємовиключні. Наприклад, з огляду на однакові ресурси, неможливо збільшити доступність, не порушуючи конфіденційності, цілісність або одночасно обидві властивості. Для загальних комп'ютерних систем обробки інформації традиційно безпека

майже повністю зосереджується на властивості конфіденційності, але для більшості вбудованих систем і IoT можна стверджувати, що два інших аспекти є найбільш важливими, або принаймні набагато більше важливим, ніж у інформаційних системах. Ефект цього полягає в тому, що механізм безпеки часто зосереджується виключно на захисті конфіденційності даних. Іншим спостереженням є те, що відмінності в підходах у багатьох випадках серйозно гальмують співпрацю між адміністраторами системи управління і стандартними IT-систем. Питання по більшу важливість між конфіденційністю та доступністю створює проблеми, які є джерелом багатьох витікаючих з цього проблем безпеки IoT. Через нещодавній всплеск комп'ютеризації всього, від мікрохвильових печей до систем озброєння, ми більше не можемо обходити стороною це питання. Багато систем IoT будуть пов'язані між собою у великих мережах, і вони не будуть працювати взагалі, якщо застосовувати стратегію безпеки, яка в першу чергу направлена на конфіденційність, тому ми не можемо ігнорувати інший аспект безпеки. Ці системи будуть підлягати антагоністичним загрозам, з якими ми так чи інакше маємо справу. Навіть якщо домен IoT ще не зрілий, у нас вже є безліч пристроїв, підключених до Інтернету, які є частиною систем різних розмірів. Щоб зрозуміти загрози та вразливості IoT, можна почати з дослідження деяких з цих пристроїв.

1.4 Напрям досліджень формування системи захисту IoT

Фахівці виділили кілька критеріїв, які можуть привести до справжнього хаосу в інфраструктурі Internet of Things. .Далі наведені деякі з них.

Швидко зростаючий парк IoT-пристроїв. Сьогодні до мережі підключається близько 6 000 000 нових «речей» щодня! Якщо врахувати, що

кожен девайс має не одну «дірку» в системі безпеки, а кілька, то ситуація складається дійсно критична.

Слабка захищеність величезних масивів призначених для користувача даних. Додамо, що для коректної роботи багато IoT-пристрої збирають не тільки паролі, але і інформацію іншого типу, починаючи від імені користувача і закінчуючи фактами з біографії. Очевидно, що там, де зберігаються безлічі взаємопов'язаних даних, потрібно і надійний захист. Інтернет речей поки цим похвалитися не може.

Можливість швидко створити потужний ботнет з мільйонів пристроїв, підключених один до одного. До появи IoT ця проблема стояла не так гостро, що пов'язано, перш за все, з втратою «автономії» предметів фізичного світу - з настанням ери Internet of Things «інтернет-речі» вже не працюють самі по собі, а інтегровані в єдину комунікаційну структуру.

Очевидно, що проблеми безпеки Інтернету речей вимагають негайного пошуку рішень, що і підтверджує наш огляд. І побоювання експертів, на жаль, виправдані - IoT в його сучасному вигляді дає великі можливості для діяльності кіберзлочинців. Наведемо декілька реальних прикладів.

Однією з областей, де за останні роки, повністю впроваджено вбудовані системи, є медичні центри та лікарні. Приклад, який показує, як щось може піти не так, – з Панами. В “Національному інституті онкології” на рубежі століття виникла проблема з радіаційною апаратурою для лікування хворих на рак [16]. Програмне забезпечення, яке використовувалося для розрахунку дози опромінення, періодично допускало похибки в обчисленнях, в результаті чого велика кількість пацієнтів отримувала збільшену дозу, і деякі з них навіть не вижили. Це не є прикладом порушення безпеки в IoT як такої, а більше вказівка на те, що медичні інструменти є складними і схильними до помилок, навіть коли вони використовуються кваліфікованими користувачами.

Stuxnet [17]. Коли перші повідомлення про черв'яка Stuxnet почали з'являтися влітку 2010 року, це викликало певний інтерес до IT-спільноти безпеки. Це був перший раз, коли хтось бачив шкідливе програмне забезпечення, яке було спеціально створене для маніпулювання системами управління.

По-перше, це була спроба зібрати інформацію з бази даних проекту в системі Siemens WinCC, використовуючи стандартний пароль, який був загальним для всіх встановлених систем цього типу. Наприклад, перше враження авторів полягало в тому, що черв'як, ймовірно, був результатом чийогось експерименту, який знайшов новий пароль за замовчуванням і перевірив, наскільки поширеним він був. Незабаром стало очевидним, що все було набагато серйозніше. Цей опис Stuxnet базується, перш за все, на трьох джерелах: в першу чергу, білій книзі, опублікованій антивірусною компанією Symantec, яка провела дослідження черв'яка, проектах FOI, які вивчали зразок коду Stuxnet, і Confront and Conceal, книга репортера New York Times Девіда Е. Сенджера [18] . Хоча немає твердих доказів, і жодна держава офіційно не визнала відповідальність за розробку Stuxnet, багато доказів вказує на Ізраїль і США як на походження цього шкідливого ПЗ. Атака була розроблена для маніпулювання програмованим логічним контролером (PLC) [19], який контролював швидкість роботи центрифуг в ядерній установці в Натанзі і, знищуючи їх, порушувався процес збагачення. Ці центрифуги були центральною частиною процесу збагачення ядер і чутливі до змін швидкості обертання. Атака вимагала точної інформації про структуру системи у всіх її деталях, і ізраїльтяни, які нібито проникли до іранської ядерної програми, отримали цю інформацію. Системи управління були стандартними системами від Siemens і були легкими для отримання. Центрифугу було важче придбати. Проте Сполученим Штатам вдалося зайняти декілька, що залишилося, коли Лівія призупинила свою ядерну програму, і вони могли бути використані для "деструктивного тестування". Центрифуги Лівії були подібні до Ірану. Незважаючи на те, що атака Stuxnet

не є типовою проблемою безпеки IoT (мережа об’єкта була мережею з повітряним рознесенням), однак, вона демонструє потенціал і вплив проблем безпеки в IoT, де пристрої з’єднані з Інтернетом і атаки можуть бути розроблені безпосередньо для маніпулювання фізичними системами.

Висновки за розділом 1

Інтернет речей, як і будь-яка технологія, що стрімко розвивається, несе за собою ряд “хвороб”, серед яких найбільш серйозною є проблема безпеки. Чим більше “розумних” пристроїв підключається до мережі, тим вище ризики, пов'язані з несанкціонованим доступом в IoT-систему і використанням її можливостей зловмисниками. Сьогодні зусилля багатьох компаній і організацій в сфері IT спрямовані на пошук рішень, які дадуть змогу мінімізувати загрози, які гальмують повноцінне впровадження IoT.

РОЗДІЛ 2
МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ IOT

При розробці системи важливо знати вразливості, яким вона може піддаватися та спланувати стратегію безпеки на самому початку розробки продукту, адже знаючи, як зловмисники можуть скомпрометувати систему, можна спочатку зменшити відповідні ризики. Таким чином, наступний розділ охоплює тенденції безпеки в області IoT, він має на меті надати уявлення про те, які питання безпеки були виявленні, від яких в більшій мірі потерпають інформаційні ресурси.

2.1 Основні положення загроз безпеки в області IoT

Перш за все, варто дати визначення терміну “кібербезпека”. Оксфордський словник англійської мови визначає кібербезпеку таким чином: “Стан захищеності від злочинного або несанкціонованого використання електронних даних, або заходи, вжиті для досягнення цієї мети”. На практиці вищезазначене речення означає, що будь-яке несанкціоноване або кримінальне зловживання електронними даними чи пристроєм розуміється як кібер-загроза. Маніпулювання фізичними активами також можна прийняти як загрозу кібербезпеки. Проте зв’язок між кібербезпекою та інформаційною безпекою досить невеликий, оскільки у багатьох випадках питання кібербезпеки можна перетворити на питання інформаційної безпеки і навпаки. Багато громадських джерел перераховують ці терміни як синоніми.

Відповідно до стандарту ISO/IEC 27032:2012 [20], кібербезпека – це безпека в кіберпросторі. Стандарт визначає зв’язок терміну з мережевою,

прикладною, Інтернет безпекою та безпекою критичних інформаційних інфраструктур. У стандарті наводиться візуалізація зв'язку цих різних термінів (рис. 2.1). З точки зору міжнародних експертів всі ці терміни об'єднує поняття інформаційної безпеки.

Рисунок 2.1 – Зв'язок терміну "кібербезпека" з термінологічним базисом стандарту ISO/IEC 27032

Таким чином кібербезпека – набір засобів, стратегій, принципів забезпечення безпеки, заходів щодо забезпечення безпеки, керівних принципів, підходів до управління ризиками, дій, професійної підготовки, практичного досвіду, страхування і технологій, які можуть бути використані для захисту кіберпростору, ресурсів організації і користувача

Загрози – це різні дії, які можуть призвести до порушень інформаційної безпеки [20]. Іншими словами, це потенційно можливі події/процеси або дії, які можуть завдати шкоди інформаційним та комп'ютерним системам. Загрози ІБ можна розділити на два типи: природні і штучні. До природних відносяться природні явища, що не залежать від людини, наприклад, урагани, повені, пожежі і т.п. Штучні загрози залежать безпосередньо від людини і можуть бути навмисні і ненавмисні. Ненавмисні загрози виникають через необережність, неуважність і незнання. Прикладом

таких загроз може бути установка програм, які не входять до числа необхідних для роботи, в подальшому порушують роботу системи, що і призводить до втрати інформації. Навмисні загрози, на відміну від попередніх, створюються спеціально. До них можна віднести атаки зловмисників як ззовні, так і з середини компанії (наприклад, яка обслуговує будинок та має певний рівень доступу до його технічних систем). Результат цього виду загроз – значні втрати власником фінансових, інтелектуальних та інформаційних активів.

Класифікація [21]. Залежно від різних способів класифікації всі можливі загрози інформаційної безпеки можна розділити на наступні основні підгрупи:

- небажаний контент;
- несанкціонований доступ;
- витік інформації;
- втрата даних;
- шахрайство;
- кібервійни;
- кібертероризм.

Небажаний контент включає в себе не тільки шкідливі програми, потенційно небезпечні програми і спам, які безпосередньо створені для того, щоб знищити або вкрасти інформацію, але і сайти, які заборонені законодавством, або небажані сайти, що містять інформацію, яка не відповідає віку споживача.

Несанкціонований доступ – перегляд інформації співробітником, який не має дозволу користуватися даною інформацією, шляхом порушення посадових повноважень. Несанкціонований доступ призводить до витоку інформації [22]. Залежно від того, яка інформація і де вона зберігається, витоку можуть організовуватися різними способами, а саме через атаки на сайти, злом програм, перехоплення даних по мережі, використання несанкціонованих програм.

Витік інформації в залежності від того, чим вона була викликана, може поділятися на навмисну і випадкову. Випадкові витоки відбуваються через помилки обладнання, програмного забезпечення і людини. А умисні, на відміну від випадкових, організовуються навмисно, з метою отримати доступ до даних, завдати шкоди.

Втрату даних можна вважати однією з основних загроз інформаційній безпеці. Порушення цілісності інформації може бути викликано несправністю обладнання або навмисними дії користувачів, будь то вони співробітниками або зловмисниками. Не менш небезпечною загрозою є фрод (шахрайство з використанням інформаційних технологій).

До шахрайства можна віднести не тільки маніпуляції з кредитними картами і злом онлайн-банку, але і внутрішній фрод. Метою цих економічних злочинів є обхід законодавства, політики, нормативних актів компанії, привласнення майна.

Щорічно по всьому світу зростає терористична загроза, поступово переходячи у віртуальний простір.

2.2 Статистичні відомості з області кіберзахисту

Кіберзлочинний світ постійно змінюється, створюючи нові вектори кібератак. Згідно з дослідженнями компанії Positive Technologies та інших авторитарних компаній нижче наведені результати численних розслідувань.

У I кварталі 2018 року, було відзначено певні тенденції, що наведені нижче. Кількість унікальних кіберінцидентів продовжила рости і на 32% перевищила показники аналогічного періоду в 2017 році [23] .

Істотно зросла частка атак, націлених на отримання даних. Причому зловмисників переважно цікавили персональні дані, а також облікові записи і паролі для доступу до різних сервісів і систем.

Зловмисники в подальшому або намагаються продати цю інформацію на чорному ринку, або продовжують з її допомогою свої атаки.

Найпоширенішим методом атак стало використання шкідливого ПЗ. Цей метод зловмисники часто комбінували з іншими, наприклад з соціальною інженерією або експлуатацією веб-вразливостей.

Самим використовуваним типом шкідливого ПЗ стало шпигунське. З його допомогою зловмисники отримували не тільки персональні дані користувачів і комерційну таємницю компаній, але і облікові дані від різних сервісів і систем, що дозволяло розвивати атаку на внутрішню інфраструктуру.

Більше за інших від кібератак постраждали приватні особи, причому п’ять з кожних шести атак були скоєні з використанням шкідливого ПЗ. Причиною великої кількості успішних атак може бути відсутність антивірусів на пристроях жертв, а також неуважне ставлення до завантажуваних з інтернету файлів і відкривання посиланнях.

У 2017 році було помічене зростання ботнетів, в тому числі за рахунок нових IoT-пристроїв; істотно збільшилася потужність DDoS-атак [24]. І ось, в останній день зими було зафіксовано найпотужніша DDoS-атака в історії – 1,35 терабіта в секунду.

У I кварталі 2018 роки були відзначені значні зміни в мотивації зловмисників. Так, зросла частка атак, спрямованих на отримання даних (36% – замість 23%, середньорічного значення в 2017-му). Це не означає, що злочинців стали менше цікавити гроші, фінансову вигоду вони переслідували більш, ніж в половині кібератак (53%). Основна причина криється в тому, що слідом за атакою, в ході якої були отримані дані, зловмисники або продовжать злочинні дії на адресу жертви або її клієнтів і контрагентів (наприклад, якщо була вкрадена клієнтська база), або спробують продати інформацію на чорному ринку.

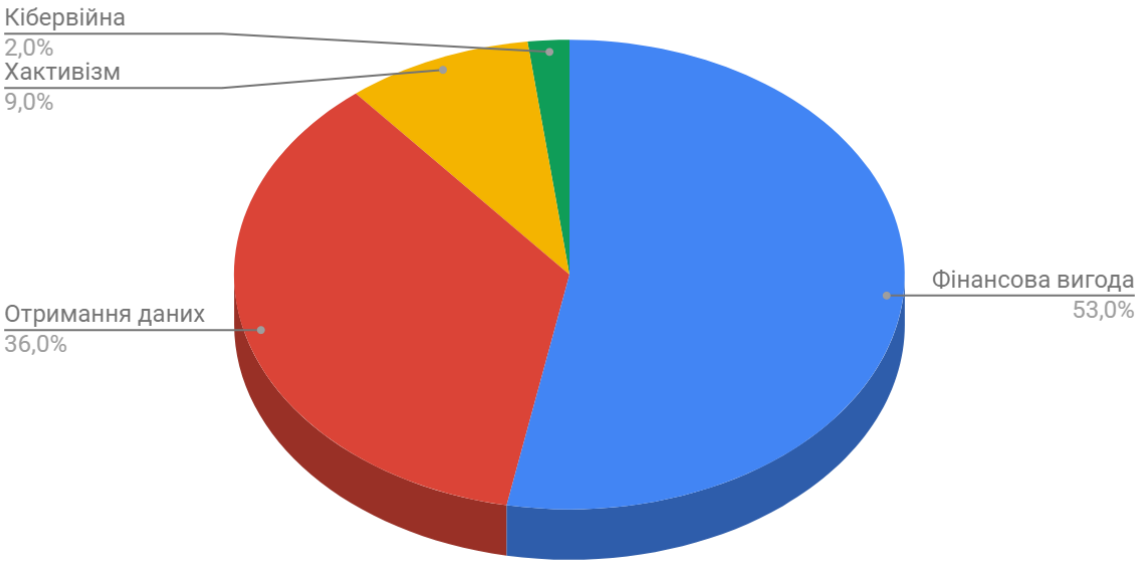


Рисунок 2.2 – Мотиви зловмисників

У 36% атак зловмисникам ставала відома конфіденційна інформація жертви. Ми розглянули, яка інформація найбільше привертала увагу злочинців. У третині випадків (33%) це були персональні дані, а в 28% – облікові записи і паролі для доступу до різних сервісів і систем. Варто відзначити, що, отримавши облікові дані, зловмисники часто продовжували атаку і отримували доступ до критично важливих інфраструктурних об’єктів, таким як бази даних, робочі станції директорів і бухгалтерів, сервери управління (наприклад, веб-ресурсами).

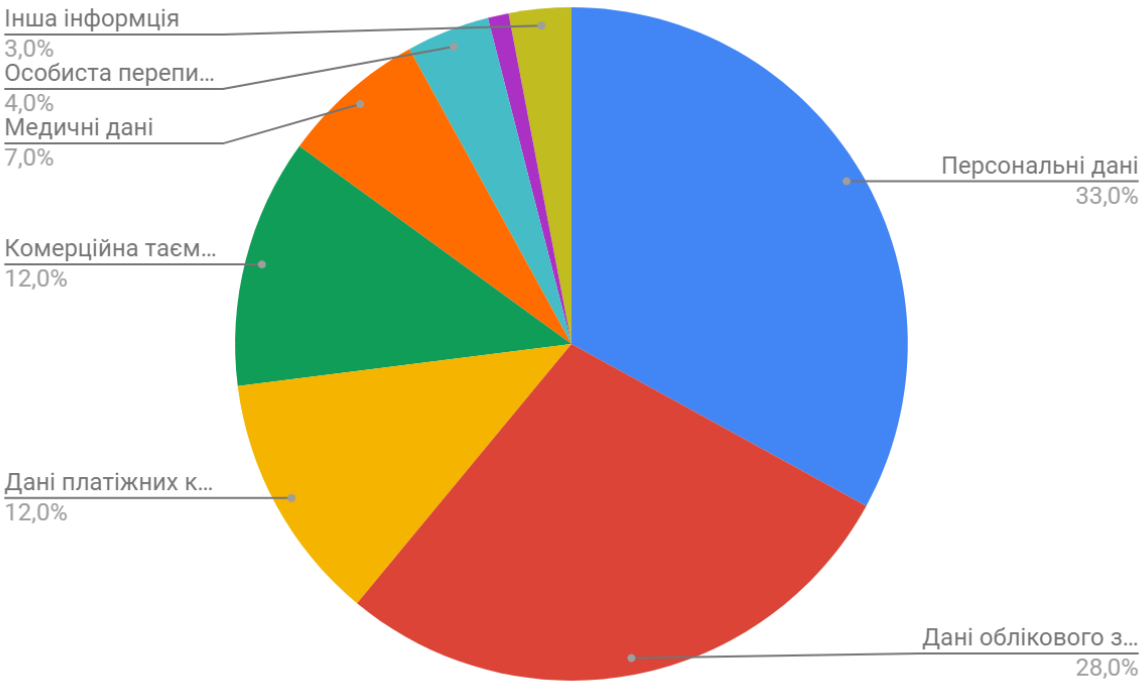


Рисунок 2.3 – Типи даних, які є ціллю викрадення

Найзначніша частина атак (28%) була спрямована на приватних осіб. Продовжує рости і частка кіберінцидентів, націлених на державні установи.

В рамках однієї кібератаки стали все частіше застосовуватися одночасно кілька методів. Наприклад, в 18% атак зловмисники одночасно використовували і шкідливе ПЗ, і методи соціальної інженерії, а в 5% – експлуатували веб-вразливості і застосовували шкідливе ПЗ.

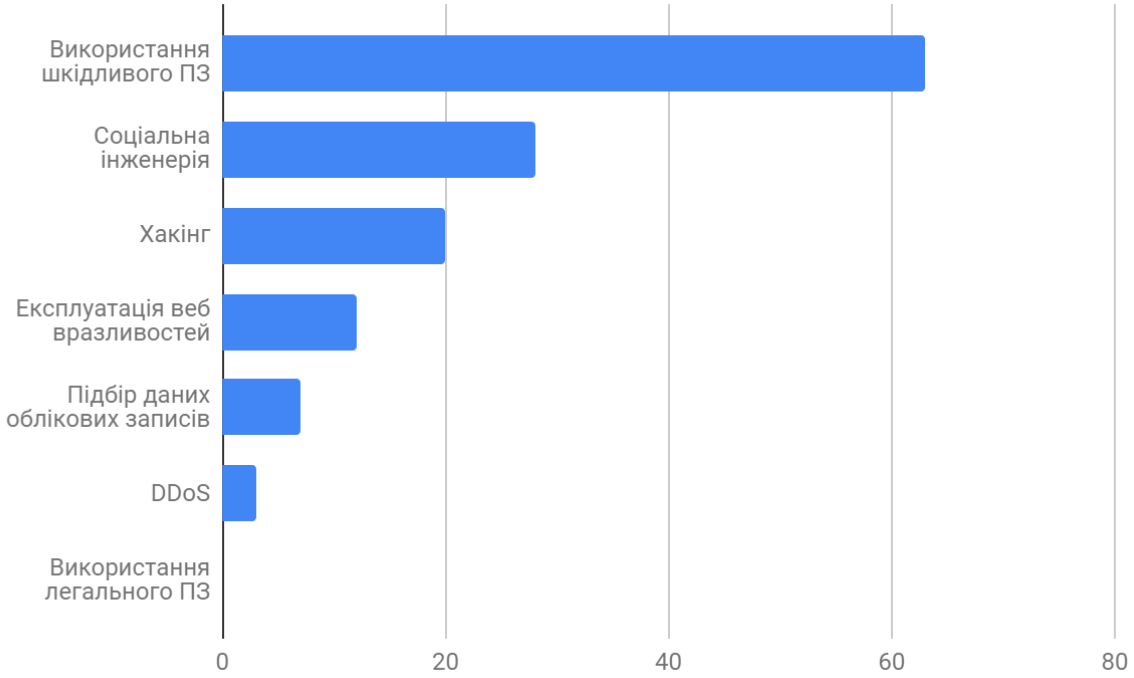


Рисунок 2.4 – Методи атак

Порушення інформаційної безпеки може бути викликано як спланованими діями зловмисника, так і недосвідченістю співробітника. Користувач повинен мати хоч якесь поняття про ІБ, шкідливий програмному забезпеченні, щоб своїми діями не завдати шкоди компанії і самому собі. Щоб пробитися через захист і отримати доступ до потрібної інформації зловмисники використовують слабкі місця і помилки в роботі програмного забезпечення, веб-додатків, помилки в конфігураціях фаєрволів, прав доступу, вдаються до прослуховування каналів зв'язку і використання клавіатурних шпигунів.

Втрата інформації може бути обумовлена не тільки зовнішніми атаками зловмисників і недбалістю співробітників, але і працівниками компанії, які зацікавлені в отриманні прибутку в обмін на цінні дані організації, в якій працюють або працювали. Те, що буде проводитися атака, залежить від типу інформації, її розташування, способів доступу до неї і рівня захисту. Якщо атака буде розрахована на недосвідченість жертви, то можливе використання спам розсилок. Оцінювати загрози інформаційної

безпеки необхідно комплексно, при цьому методи оцінки будуть відрізнятися в кожному конкретному випадку. Наприклад, щоб виключити втрату даних через несправність обладнання, потрібно використовувати якісні комплектуючі, проводити регулярне технічне обслуговування, встановлювати стабілізатори напруги. Далі слід встановлювати і регулярно оновлювати програмне забезпечення.

Окрему увагу потрібно приділити захисному ПЗ, бази якого повинні оновлюватися щодня:

- захист від небажаного контенту (антивірус, антиспам, веб-фільтри, антишпигуни)[25];
- фаєрволи і системи виявлення вторгнень;
- IPS (Intrusion Prevention System) [26];
- IDM (identity management)[27];
- PUM (Potentially Unwanted Modification) захист веб-додатків 28
- анти-DDoS[29];
- WAF (web application firewall) [30];
- аналіз вихідного коду;
- антифрод;
- захист від націлених атак;
- SIEM (Security information and event management) [31];
- системи виявлення аномальної поведінки користувачів (UEBA);
- захист АСУ ТП;
- захист від витоків даних;
- DLP (Data Loss Prevention);
- шифрування;
- захист мобільних пристроїв;
- резервне копіювання.

Організувати інформаційну безпеку допоможуть спеціалізовані програми, розроблені на основі сучасних технологій. Прикладом таких технологій запобігання витоку конфіденційних даних є DLP-системи[32]. А в боротьбі з шахрайством слід використовувати анти-фрод системи, які надають можливість моніторити, виявляти і управляти рівнем фрода.

IoT – це нова парадигма, яка в майбутньому змінить нашу взаємодію з об'єктами і комп'ютерами. Вона являє собою глобальну мережу пристроїв, що взаємодіють один з одним через Інтернет для виконання корисних дій.

Незважаючи на зручну технологію, використання технології IoT додасть в наше життя додаткові ризики, яких не було в традиційному Інтернеті. Це пов'язано перш за все з тим, що технологія IoT дозволяє віртуальному світу безпосередньо впливати на фізичний світ.

Тому безпека має першорядне значення для технології IoT. Таким чином, ця робота має перед собою дві мети. По-перше, ми визначимо проблеми безпеки для технології IoT, а також виділимо підходи вже розроблені спеціалістами для їх вирішення. Це дозволить нам побачити стан цієї технології разом з тим, що ще потрібно зробити в майбутньому. По-друге, ми проаналізуємо деякі протоколи безпеки, запропоновані академічними колами, і оцінимо, чи забезпечують вони конфіденційність і автентичність відбитку.

Результати аналізу протоколів безпеки показують, що менше половини запропонованих протоколів забезпечують цілісність і конфіденційність; незважаючи на те, що їх відповідні документи стверджують, що вони інакше. Тому ми наголошуємо на тому, що повинні проводитися хороші експертні перевірки і що протоколи повинні бути перевірені, для того щоб гарантувати, що те, що пропонується, працює так, як описано.

Інтернет речей – це нова технологія, яка передбачає віртуальний зв'язок фізичних об'єктів. Основна ідея Інтернету речей – підключення вбудованих пристроїв до повсякденних об'єктів, щоб зробити їх

інтелектуальними об’єктами/пристроями. Ці інтелектуальні пристрої, які підключені до Інтернету, будуть унікально ідентифікованими і зможуть спілкуватися один з одним; з метою виконання складних завдань на благо людства. Таким чином, ці пристрої вимагають здатності збирати, обробляти і передавати інформацію.

Втілення в реальність IoT можливо тільки завдяки використанню та інтеграції існуючих технологій, таких як інтелектуальні сенсорні мережі, радіочастотна ідентифікація, технології бездротового високочастотного зв’язку малого радіусу дії (NFC) [33], мобільної технологія і самого Інтернету. Завдяки інтеграції цих технологій в єдину систему Internet of Things буде складатися з величезної кількості пристроїв; від складних і потужних серверів до простих обмежених RFID-чипів[34]. Таким чином, з огляду на неоднорідну природу середовища IoT, очікується, що деякі пристрої будуть обмеженими пристроями.

Обмежені пристрої – це пристрої, які можуть утворювати мережі з низькою пропускною здатністю і високою ймовірністю втрати пакетів. Це пов’язано з тим, що ці пристрої мають обмежені можливості обробки, потужність, пам’ять і пропускну здатність. З огляду на ці обмеження, традиційні рішення проблем безпеки, які спочатку були розроблені для Інтернету, не працюватимуть, перш за все тому, що ці рішення вимагають великої кількості ресурсів і енергії, якими обмежені пристрої, швидше за все, не володіють. Проте, ця проблема не залишилася непоміченою академічною спільнотою, і з тих пір велика кількість досліджень було направлено на поліпшення і розробку рішень, які можуть функціонувати на пристроях з обмеженими можливостями.

Нас цікавить Інтернет речей тому, що це нова технологія з можливістю змінити світ і те, як ми живемо в ньому. На сьогодні уже налічується дуже велика кількість таких пристроїв, і корпорації можуть побачити ті можливості, які має продемонструвати цей ринок, що розвивається. Це особливо актуально в таких областях, як охорона здоров’я,

транспорт і логістика, розумні будинки, виробництво енергії і допомога в разі стихійних лих.

Однак, як і всі нові технології, IoT стикається з проблемами, які необхідно подолати, щоб забезпечити успішне розгортання технології в великих масштабах.

Деякі з ключових проблем, знаходяться в наступних областях:

- безпека і конфіденційність;
- правові обмеження;
- підзвітність;
- бізнес-моделі;
- довіра;
- стандартизація.

Проблема безпеки особливо важлива, так як технологія IoT призначена для збору інформації про навколишнє середовище, в якому вона знаходиться в даний момент. Тому більшість пристроїв, що працюватимуть з цією технологією матимуть справу з дуже делікатною інформацією для людей і корпорацій. Наприклад, кардіостимулятори, інтегровані з технологією IoT, дозволяють лікарям-практикам отримувати в реальному часі дані про серцево-судинні показники пацієнтів. Таким чином, це дозволяє лікарям бути негайно поінформованим, якщо пристрої IoT зафіксують незвичайний серцевий ритм. Ця функція є дуже корисною, проте зібрана інформація є делікатною по відношенню до пацієнта, і він/вона не хотів би, щоб всі мали до неї доступ. Таким чином, безпека має першорядне значення для реалізації та успішного розвитку IoT.

Отже, що саме ми маємо на увазі під безпекою? Зазвичай, коли безпека згадується у контексті інформаційних технологій (IT), то основна увага приділяється моделі безпеки ЦКД [35]. ЦКД виступає за конфіденційність, цілісність і доступність даних і інформації. Крім того, існує модель AAA (Authentication, Authorization, Accounting)[36], яка також

визначає важливі компоненти безпеки – автентифікацію, авторизацію та облік. Безпека IoT буде охоплювати ці дві моделі.

Ці дві моделі безпеки були розроблені для Інтернету, яким ми його знаємо на сьогодні, і рішення проблем безпеки були розроблені для традиційного Інтернету, проте вони не були розроблені з урахуванням особливостей IoT, середовище якого складається з обмежених пристроїв. Наприклад, типові механізми криптографії та безпеки займають багато ресурсів з точки зору пропускної здатності, обчислювальної потужності, пам'яті та фактичної потужності; відтак в IoT вони не можуть бути використані, так як були розроблені для пристроїв, де обмеження цих ресурсів не було проблемою.

З огляду на всю цю інформацію, видно, що IoT – цікавий напрямок, але все ще знаходиться в зародковому стані. Крім того, було проведено чимало досліджень в області IoT, його можливого використання, а також аспектів безпеки і конфіденційності IoT. Ця дипломна робота буде зосереджена на аспекті безпеки Інтернету речей. Однією з основних цілей цієї роботи є проведення огляду стану безпеки щодо IoT на даний момент, аби скласти повну картину того, що було зроблено, яким питанням приділялося більше уваги і, що найбільш важливо, що ще необхідно зробити.

Друга мета – дослідити деякі із запропонованих протоколів для пристроїв IoT, вони будуть проаналізовані і змодельовані, щоб визначити, чи є вони безпечними і чи відповідають заявленим можливостям. На додаток до пропонованих протоколів буде також проаналізовано стандартизований протокол безпеки DTLS, щоб переконатися, що він також забезпечує функції безпеки.

2.3 Класифікація впливів на систему безпеки IoT

В цьому пункті висвітлюються проблеми, виявлені після ознайомлення та аналізу існуючих досліджень в області безпеки для IoT. Таким чином, спочатку будуть визначені проблеми. Після цього – пояснення кожної проблеми: що це таке і чому це важливо для Інтернету речей.

Ключовими проблемами, визначеними в такий спосіб, є:

- автентифікація;
- безвідмовність;
- авторизація;
- конфіденційність;
- цілісність;
- приватність;
- анонімність;
- право на забуття;
- самостійне налаштування;
- справжність програмного забезпечення;
- апаратне забезпечення захисту від несанкціонованого доступу;
- доступність;
- управління ключами;
- довірче управління.

Автентифікація. Автентифікація – це процес визначення того, чи дійсно хтось або щось дійсно є тим, за кого себе видає; а не зловмисник, який претендує на те, що йому не належить [37]. У реальному світі люди виконують процес автентифікації увесь час, коли ми розмовляємо один з одним; оскільки ми можемо розпізнавати один одного за допомогою різних факторів, таких як риси обличчя, колір волосся, голос і так далі.

Цей процес ідентифікації не обмежується людиною, електронні пристрої також повинні розуміти, з ким вони спілкуються. Для IoT автентифікація є важливою, оскільки більшість комунікацій відбуватиметься без взаємодії з користувачем. Крім того, властивість гарантувати, що доступ до мережі з ресурсами та інформацією отриманий необхідними пристроями, датчиками і користувачами також є важливим питанням безпеки. Також необхідно забезпечити отримання інформації, команд і запитів від правильних пристроїв.

Для прикладу можна взяти платежі по кредитній картці через технологію близьких комунікацій (NFC). Якщо сервер банків не гарантуватиме, що платіжний запит надходить з картки конкретних клієнтів, то зловмисник може легко використовувати цей обліковий запис клієнтів для здійснення покупок.

Таким чином, деякі загальні засоби забезпечення автентифікації полягають у використанні паролів, цифрових підписів і протоколів запиту та відповіді. Біометрія також може бути використана, але цей тип автентифікації надто складний у обчислювальному відношенні для використання обмеженими пристроями IoT, які ми маємо сьогодні.

Безвідмовність. Безвідмовність – це спосіб забезпечення ідентичності об’єкта, який генерує конкретне повідомлення. Зазвичай це досягається за рахунок використання цифрових підписів, оскільки дозволяє точно визначити, яка сторона створила повідомлення [38]. Зазвичай це має особливе значення з точки зору відстеження незаконних дій в Інтернеті, оскільки надає можливість забезпечити отримання підзвітності.

Однак, для Інтернету речей її важливість може варіюватися в залежності від сфери в якій використовується система. Наприклад, в секторі охорони здоров’я важливо, щоб коригування ліків, що відправляються в певну систему IoT, що підтримує автоматизовану систему дозування ліків для пацієнта, приймалися тільки від лікаря пацієнта. Це означає, що за таких обставин необхідно забезпечити відхилення відмови.

Крім того, безвідмовність можна, можливо розглядати як підкомпонентну автентифікацію, що також використовує підписи, але не має більше жорсткої вимоги в тому значенні, що відправник повідомлення повинен бути однозначно ідентифікований .Наприклад, автентифікація може бути встановлена через симетричний ключ, за допомогою чого об'єкти з цим ключем можуть законно отримувати доступ до системи або мережі. Однак це не забезпечить відмову від авторства, оскільки немає ніяких відмінностей від повідомлень, що генеруються об'єктами, які зв'язуються з симетричним ключем. Отже, цифрові підписи це єдиний засіб забезпечення цієї функції безпеки.

Авторизація. Механізми авторизації та контролю доступу використовуються для обмеження привілеїв, які має пристрій, і визначає, які дії може виконувати пристрій [39]. Ця можливість може бути пов'язана з доступом до ресурсів і даних. Як результат, механізми авторизації визначають операції, які кожен пристрій здатний виконувати, і інформацію, до якої він має доступ. Крім того, через широке застосування та великі масштаби середовища IoT, не важко уявити, що деякі пристрої схильні до ризику. Таким чином, механізми авторизації забезпечують обмеження на операції, які зловмисник може виконати у випадку якщо система буде зламана. Простим прикладом механізму контролю доступу є облікові записи користувачів, за допомогою яких особи входять на свої комп'ютери. Після початкового входу, що є автентифікацією, дії, які користувач може виконати, будуть визначені елементами управління авторизацією. Наприклад, деякі користувачі матимуть привілеї адміністратора, які дозволять їм робити все, а інші користувачі обмежені в своїх діях. Зазвичай це забезпечується шляхом використання механізмів контролю доступу на основі використання ролей (Role based access control, RBAC), на основі використання атрибутів (Attribute based access control, ABAC) та списків можливостей.

Конфіденційність. Конфіденційність є засобом забезпечення того, щоб доступ до інформації мали лише ті люди та пристрої, які повинні його мати [40]. Забезпечення конфіденційності інформації є дуже важливим для пристроїв IoT, оскільки інформація збирається звідусіль, то може набувати самого особистого характеру і власники інформації не хотіли б, що б та була якимось шляхом оприлюднена чи стала доступною для кого-небудь. Наприклад: пристрій IoT просто передає всю інформацію, яку він збирає, про ваш щоденний графік в чистому вигляді через Інтернет, тоді зловмисник може легко визначити, коли буде найкращий час, щоб пограбувати ваш будинок. Конфіденційність зазвичай досягається за допомогою шифрування та криптографічних механізмів і особливо важливо зберегти її, коли вузли IoT передають інформацію один одному. Забезпечення конфіденційності також має передбачати запобігання прослуховуванню за допомогою криптографічних механізмів.

IoT є “природним” наступним кроком у розвитку Інтернету. Отже, можна проаналізувати вплив останніх тенденцій інформаційних технологій (наприклад, засоби масової інформації соціальних мереж, смартфонів та великих даних) на приватне життя окремих осіб, щоб передбачити потенційний вплив IoT на конфіденційність користувачів. Одним з наслідків нинішнього швидкого технологічного розвитку та глобалізації є те, що масштаби збору та обміну персональними даними значно збільшилися в усіх секторах за кількістю учасників, областей застосування, часу зберігання даних, розподілу та обміну інформацією між учасниками. Особи все частіше передають особисту інформацію на публіку та глобально. Збір даних, і багаторазове подальше використання даних суб’єктами є реальністю, величезні обсяги даних обробляються в режимі реального часу. Деякі великі корпорації, в результаті розробки в цілому та власних бізнес-стратегій, мають доступ до все більшого обсягу персональних даних і таким чином здатні зобразити більш повну картину особи. Такий розвиток пов’язаний з оцифруванням та поступовою зміною відношення до обробки інформації, як

у державному управлінні, так і в бізнесі, відтак ситуація з оперуванням даними значно змінилась.

Раніше організації мали конкретну мету у створенні персональної бази даних. Тепер вони мають різні цілі:

у минулому вони збирали інформацію, оскільки існувала чітка потреба. Тепер вони збирають дані для того, щоб ті “могли бути корисними на майбутнє”;

- у минулому було важливо, з точки зору витрат, скорочувати термін зберігання даних. Тепер вважається великою перевагою тривале збереження даних;
- раніше пошук та аналіз мали конкретну мету. Тепер великі дані та інтелектуальний аналіз даних є реальністю;
- у минулому персональні дані збиралися за допомогою спеціальної реєстрації. Тепер вона виникає більш-менш автоматично, коли людина виконує якісь дії і використовує онлайн-службу;
- особисті дані стали товаром, який збирають, обробляють і продають.

Цілісність. Цілісність є властивістю забезпечення того, щоб інформація/дані були правильними і не були пошкоджені або модифіковані будь-якими способами, або несанкціонованими особами. Це, як правило, має ключове значення при передачі інформації від одного пристрою до іншого, оскільки саме тут часто відбуваються атаки. Цілісність даних дуже важлива для систем IoT, так як для правильного функціонування системи IoT потрібен точний збір інформації датчиками. Таким чином, системи повинні гарантувати, що шкідливе спотворення даних неможливе, але якщо це вже сталося, то система повинна мати можливість виявляти цей інцидент. Прикладом, де може виникнути складна ситуація пов’язана зі зміною даних, є в секторі охорони здоров’я. Уявіть собі, якщо пацієнт переживає серцевий напад, а зловмисник змінює повідомлення, надіслані датчиками, щоб

сказати, що пацієнт перебуває в ідеальному стані здоров'я. Очевидно, що це страшна ситуація, коли цілісність отриманої інформації має вирішальне значення. Додатково, цілісність зазвичай досягається за рахунок використання стійких до зіткнення хеш-функцій і цифрових підписів.

Приватність. Враховуючи величезну кількість інформації, яку пристрої IoT збиратимуть про людей, не дивно, що приватність викликає занепокоєння в Інтернеті речей. Приватність може бути охарактеризована як "право індивідів визначати для себе, коли, як і в якій мірі інформація про них передається іншим" [41]. Приватність по своєму задуму є одним з можливих способів забезпечення цієї можливості. Це також пов'язано з концепцією забезпечення доступу до інформації на основі найменших привілеїв, необхідних для виконання дії. Наприклад, навіть якщо пристрій має повний доступ до всього, що знаходиться в мережі IoT, коли потрібно виконати дію, яка вимагає лише одного ресурсу, тоді пристрій повинен обмежуватися лише використанням цього ресурсу під час виконання конкретної дії. Крім того, зазвичай вважається, що шифрування гарантує конфіденційність і так воно і є, але лише в певній мірі, що запобігає зчитуванню інформації під час передачі і, можливо, під час зберігання. Проте центральний сервер, який зберігає та обробляє цю інформацію, все ще матиме доступ до всієї цієї інформації. Таким чином, анонімність також відіграє важливу роль у забезпеченні приватності. Право на забуття також є субкомпонентністю приватності, що буде описана нижче.

Анонімність. Анонімність – це концепція роз'єднання або видалення з'єднання з певним користувачем із зібраних даних [42]. Таким чином, жоден окремий користувач не повинен бути ідентифікований з урахуванням даних, що були зібрані. Це є загальною проблемою для великих даних і враховуючи величезну кількість інформації, яку очікується в обізі між пристроями IoT, вона потрапить у цю сферу.

Право на цифрове забуття. Право на цифрове забуття – це ідея повного видалення елемента або частини даних з цифрового світу. Враховуючи

величезну кількість даних, які передбачається збирати пристроями IoT, велика її кількість, ймовірно, буде особистого характеру. Тому, дуже важливо мати змогу бути впевненим в тому, що інформація буде видалена одразу ж, як вона вже не буде потрібною.

Самоналаштування. Оскільки технологія IoT передбачає підключення до Інтернету мільярдів пристроїв. Буде нереально припустити, що користувачі будуть готові вручну взаємодіяти і налаштувати ці пристрої індивідуально, щоб вони могли функціонувати. Таким чином, важливо, щоб ці пристрої могли самостійно налаштовуватися і керувати механізмами контролю доступу динамічно, без втручання користувача або принаймні з мінімальним втручанням користувача.

Придбавши велику кількість нових IoT пристроїв, які користувач планує впровадити в свою домашню мережу, йому не буде дуже зручно налаштовувати окремо кожен з них. А з розвитком IoT кількість пристроїв, що можна буде підключити лише зростатиме, та звичайна людина не захоче налаштовувати вручну. Слід зазначити, що це питання не обмежується безпечним завантаженням, а також роботою і налаштуваннями під час виконання звичайних операцій.

Справжність програмного забезпечення. Забезпечення справжності та цілісності програмного забезпечення, встановленого на пристроях, важливо для будь-якої IT системи. Особливо це стосується середовищ IoT, оскільки пошкоджене програмне забезпечення може дозволити обійти механізми безпеки на місці.

Прикладом того, де це може мати катастрофічні наслідки, є випадок, коли шкідлива програма на пристрої IoT копіює і пересилає всю інформацію, яку вона збирає, на комп’ютер зловмисника і, отже, обходить всі заходи безпеки.Звичайний засіб захисту від цього на сьогодні - це змусити постачальників програмного забезпечення підписувати своє програмне забезпечення.

Апаратний захист від злому і фізична безпека. Очікується, що пристрою IoT будуть працювати без нагляду і будуть впроваджені в незахищених середовищах,таких як міські вулиці, ліси і автостоянки. Отже, це дозволяє їм бути легко доступними для зловмисників, що збільшує ризик фізичних атак, а також можливість підробки. Це підкреслює необхідність наявності вбудованих механізмів захисту від несанкціонованого доступу під вбудовані мікросхеми пристроїв IoT для запобігання атак, таких як зворотне проектування і злам пристроїв. Можливі механізми захисту від зламу включають в себе інтеграцію апаратних елементів і використання апаратних значень як частину процесу генерації ключа. Прикладом цього є фізичні функції, що не можна клонувати фізично (Physical Unclonable Function, PUF) [43], які використовуються для того, щоб гарантувати, що якщо зловмисник підробить пристрій, то характеристики пристрою будуть змінені, що, в свою чергу, призведе до зміни клавіш.

Доступність. Доступність для IT-систем означає, що система повинна бути запущена і працювати для діючих користувачів при будь-яких умовах експлуатації. Таким чином, час роботи системи має бути максимально великим, щоб забезпечити правильну роботу системи. Проте, забезпечення доступності для середовищ IoT є ще більш складним завданням, ніж для традиційного Інтернету, через обмежений характер пристроїв IoT, що робить його вразливим для атак з використанням енергії, до яких звичайні пристрої не схильні.

Поширеною атакою на доступність є відмова в обслуговуванні (Denial of service, DoS) і розподілена відмова в обслуговування (Distributed DoS, DDoS), коли зловмисник блокує мережу шляхом передачі непотрібного трафіку, щоб заблокувати доступ цільовим користувачам. Ця атака поширена в Інтернеті, і IoT успадкував цю вразливість.

Доступність є важливим аспектом IoT, оскільки деякі пристрої є життєво важливими. Хорошим прикладом цього є медичне обслуговування

для кінцевого моніторингу пацієнтів, де збір даних в реальному часі надзвичайно важливий.

Для IoT, забезпечення доступності системи включає в себе кілька факторів, таких як реалізація ефективних протоколів та механізмів шифруваня, інтеграція механізмів збору та економії енергії та навіть провадження контрзаходів щодо DoS. Всі вони об'єднуються для забезпечення доступності в контексті IoT.

Управління ключами. Управління ключами в першу чергу стосується управління ключами безпеки, і, з огляду на масштаб IoT, це, очевидно, важливо. Зокрема, через те, що якщо ключі безпеки стають доступними для зловмисника або якщо зловмисник якимось чином придбав їх, він/вона матиме змогу отримати всю інформацію, що відправляється з пристроїв IoT.

Крім того, управління ключами – це не просто безпечне зберігання ключів безпеки, це генерація або створення ключа, поширення ключа, зміна або оновлення ключа, а також знищення.

Зазвичай це досягається за рахунок використання безпечних протоколів обміну ключами для генерації ключів і механізмів шифрування для зберігання ключів.

Довірче управління. З огляду на те, що мережі IoT будуються на основі сенсорних пристроїв для збору інформації, дуже важливо забезпечити вірогідність того, що конкретний пристрій працює чесно (коректно), і відправляє назад правильну і достовірну інформацію. Отже, без застосування механізмів довіри неможливо буде визначити, чи правильно працює система.

Так чи інакше, загальні механізми криптографічного контролю забезпечують лише захист достовірності даних і справжність пристроїв. Отже, несправні або зламані пристрої, що надають неправильні дані, залишаться непоміченими. З огляду на цей контекст, з точки зору мереж, автентифікація, конфіденційність та цілісність інформації, що передається цілком прийнятні, оскільки інформація надходить з пристрою, якому

довіряють. Проте, достовірність або якість інформації буде під питанням. Ось чому довірче управління є важливим, так як воно дозволяє контролювати, коли пристрій буде вести себе інакше чи незвичайно. Системи виявлення загроз (Intruder detection systems, IDS), є одними з можливих варіантів вирішення для забезпечення довіри у середовищі IoT.

Висновки за розділом 2

Для IoT-пристроїв безпека полягає, перш за все, в цілісності коду, перевірці автентичності користувачів (пристроїв), встановлення прав користування, а також можливістю відображення віртуальних і фізичних атак. Але по факту, більшість з працюючих сьогодні IoT-пристроїв елементами захисту не забезпечені, мають доступні ззовні інтерфейси управління, дефолтні паролі, не використовують необхідні стандарти, не шифруються канали тощо. Отже виникає необхідність у визначенні архітектури IoT, що може належним чином описати необхідні стандарти, протоколи та засоби захисту на кожному з її рівнів.

РОЗДІЛ 3

ПОБУДОВА МОДЕЛІ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ІОТ

У нашому дослідженні, на основі якого була побудована модель, ми сфокусувалися виключно на вимогах для забезпечення безпеки в самих пристроях IoT, захищеної взаємодії між ними і залишили за рамками цієї статті аспект розробки безпечного програмного коду. Звичайно, багато які з цих пристроїв часто взаємодіють з традиційними бекенд-системами, які працюють в приватному центрі обробки даних або в хмарі. Ми припускаємо, що захищеність цих систем на належному рівні. Однак потрібно пам'ятати, що якщо традиційні IT-системи пускають у хід IoT-пристрої або обробляють дані від них, то небезпечна взаємодія IoT з традиційними IT-системами може повністю підірвати всю безпеку, яку ви вбудували в свою систему IoT.
[44]

3.1 Модель найбільш поширеної архітектури IoT

У цьому розділі буде розглянута найбільш поширена архітектура IoT, яка включає в себе дві, на перший погляд несумісні речі: з одного боку – це велика кількість периферійних пристроїв з малими обчислювальними потужностями, низьким енергоспоживанням, високою швидкістю реакції на події, а з іншого боку – хмарні сервера з високою обчислювальною потужністю для обробки великого масиву даних, їх зберігання та класифікації, часто з елементами машинного інтелекту і аналітики. Ці два світи використовують абсолютно різні принципи побудови і внутрішньої архітектури.

Основні пристрої або прилади IoT зазвичай складаються з наступних частин з точки зору архітектури:

1) датчик або будь-який інший смарт-об’єкт;

2) транспортний шар (повітряний або провідний);

3) комутатори або маршрутизатори;

4) сервер збору даних.

Основними модулями в середовищі IoT є, як правило, датчики для збору вимірюваних даних, транспортний рівень для доставки даних отриманих з датчиків, обчислювальні пристрої та додатки для аналізу даних та обробки для зберігання даних [45]. На рисунку 3.1 зображена найпоширеніша архітектура середовища IoT.

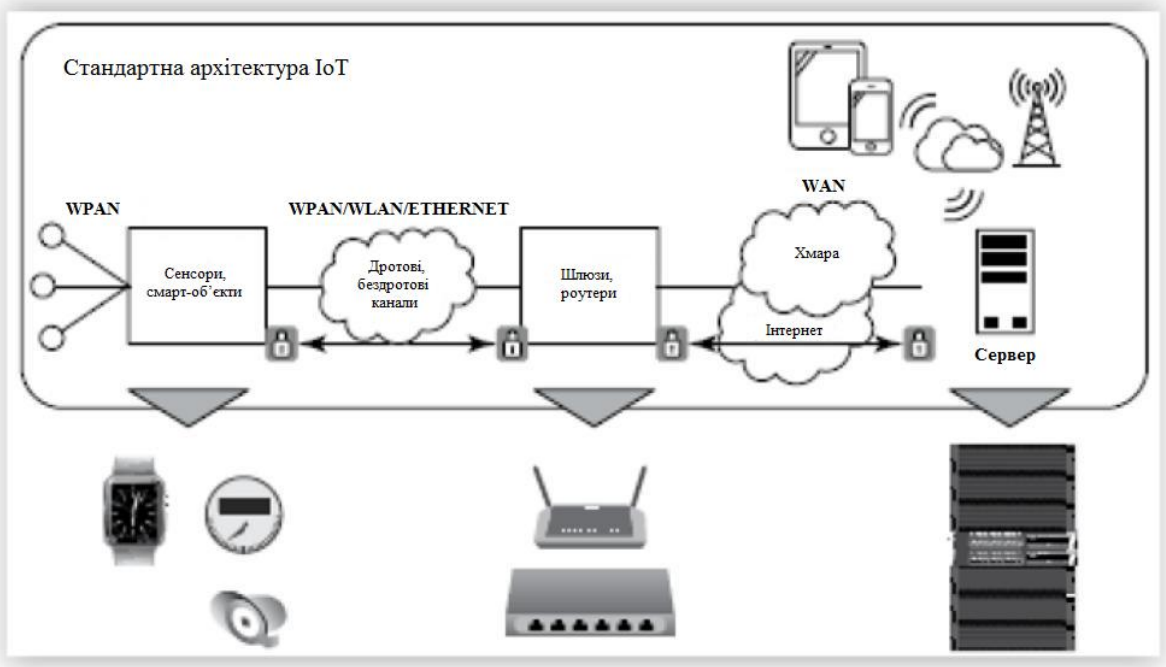


Рисунок 3.1 – Архітектура та функціональний огляд системи IoT

Як ми бачимо вище, ключові компоненти – це не просто датчики або розумні об’єкти і сервери для збору даних, а й передача даних, мережа, що має дуже важливу роль у цій архітектурній концепції. Мережа разом із використовуваним протоколом відіграє значну роль в обладнанні IoT. Основні компоненти архітектури IoT більш детально описані далі. Якщо

розглядати сам пристрій IoT і виключити всі зовнішні пристрої, такі як шляхи передачі, мережні компоненти, наприклад маршрутизатори і сервери аналізу даних, то внутрішня архітектура спрощеного пристрою IoT може бути такою як вона є представлена на рис. 3.2.

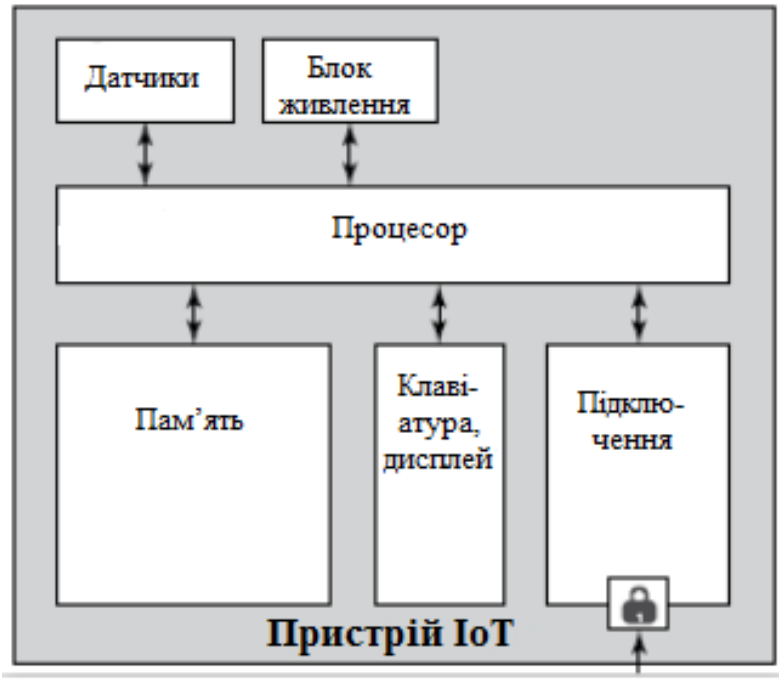


Рисунок 3.2 – Спрощена внутрішня архітектура пристрою IoT

Присутня подібність в архітектурі пристроїв IoT, коли вона порівнюється з звичайними комп'ютерами. Як можна побачити, пристрій IoT включає в себе головний процесор, який відповідає за контроль і управління цим пристроєм. Пам'ять використовується для зберігання даних з датчиків, а також для зберігання коду програми для запуску дій. Пристрої вводу/виводу, такі як клавіатура та монітор, призначені для користувацьких інтерфейсів. З'єднання реалізується через мережу, дротову або бездротову. Якщо мережа бездротова, існують різні способи її реалізації: WIFI Ethernet, Bluetooth або мобільний зв'язок через GSM 4G. Джерело живлення забезпечує необхідну потужність системи. Датчики збирають наприклад дані температури навколишнього середовища. Це ті ж модулі та компоненти, які є основною частиною звичайної архітектури комп'ютера.

Різниця між пристроями IoT і звичайними комп'ютерами полягає в датчиках, призначених для збору інформації з навколишнього середовища.

Крім того, однією з ключових відмінностей між IoT і звичайним комп'ютером є розмір. Як правило, пристрої IoT набагато менші, а споживча потужність значно нижча, ніж у звичайних комп'ютерів. Зазвичай пристрої IoT можуть працювати з невеликими акумуляторами або змінними батареями.

Датчики. Метою датчиків є збір вимірюваних даних з машини, пристрою або навколишнього середовища. Датчик являє собою електронний компонент, який перетворює зміну температури, вологість або рух в електронний формат і передає дані на комп'ютер. Датчики широко використовуються в промисловості для вимірювання різних параметрів і в побутових приладах IoT. Датчики використовуються в побутових приладах різного призначення. Наприклад, датчики використовуються в автомобілях для вимірювання рівня вихлопу газу і на основі цієї інформації вони регулюють налаштування бензину і кисню двигуна автомобіля. Однією з областей для датчиків є інфрачервоні датчики, що використовуються для дистанційного керування ящиками для домашніх розваг, для виявлення руху та детекторів вторгнення [46].

Таблиця 3.1 – Типи датчиків [47]

Тип датчиків	Опис датчика	Приклад датчиків
Позиції	Датчик положення вимірює положення об'єкта; вимірювання положення може бути або в абсолютному вираженні (абсолютний датчик положення), або у відносних термінах (датчик переміщення). Датчики положення можуть бути лінійними, кутовими або багатоосьовими.	Потенціометр, інклінометр, датчик наближення
Присутності та руху	Датчики присутності виявляють наявність людей і тварин у зоні спостереження, а датчики руху визначають рух людей і предметів. Різниця між ними полягає в тому, що датчики присутності будуть генерувати сигнал навіть тоді, коли людина нерухома, а датчик руху не буде.	Електричне око, РАДАР

Швидкості та прискорення	Датчики швидкості (швидкості руху) можуть бути лінійними або кутовими, та вказують, як швидко об’єкт рухається або як швидко він обертається. Датчики прискорення вимірюють зміни швидкості.	Акселерометр, гіроскоп
Сили	Датчики сили визначають, чи застосовується фізична сила і чи величина сили виходить за межі порогу.	Датчик сили, віскозиметр, тактильний датчик
Тиску	Датчики тиску пов’язані з датчиками прикладеного зусилля і вимірюють силу, яку застосовують рідини або гази. Тиск вимірюється з точки зору дії сили на одиницю площі.	Барометр, датчик бурдону, п’єзометр
Потоку	Датчики потоку визначають швидкість потоку рідини. Вони вимірюють об’єм (масовий потік) або швидкість (швидкість потоку) рідини, що пройшла через систему за заданий період часу.	Анемометр, датчик масової витрати, лічильник води
Акустичні	Акустичні датчики вимірюють рівні звуку і перетворюють цю інформацію в цифрові або аналогові сигнали.	Мікрофон, геофон, гідрофон
Вологості	Датчики вологості визначають вологість (кількість водяної пари) у повітрі або масі. Рівні вологості можна виміряти різними способами: абсолютна вологість, відносна вологість, масове співвідношення тощо.	Гігрометр, датчик вологості ґрунту
Світла	Світлові датчики виявляють наявність світла (видимого або невидимого).	Інфрачервоний датчик, фотоприймач, детектор полум’я
Радіації	Радіаційні датчики виявляють випромінювання в навколишньому середовищі. Випромінювання можна відчути за допомогою сцинтиляційного або іонізаційного виявлення.	Лічильник Гейгера – Мюллера, сцинтилятор, детектор нейтронів
Температури	Датчики температури вимірюють кількість тепла або холоду, який присутній в системі. Вони можуть бути в цілому двох типів: контактні та безконтактні. Контактні датчики температури повинні перебувати у фізичному контакті з об’єктом, що відчувається. Безконтактні датчики не потребують фізичного контакту, оскільки вимірюють температуру через конвекцію і випромінювання.	Термометр, калориметр, датчик температури

Датчик не функціонує сам по собі – він є частиною великої системи, що включає мікропроцесори, модемні мікросхеми, джерела живлення та інші пов’язані з ними пристрої. За останні два десятиліття обчислювальна потужність мікропроцесорів значно покращилася, подвоюючи свою силу кожні три роки як це зображено на рисунку.

Спостерігається швидке зростання використання міні-сенсорів, які можна вбудовувати в смартфони та одяг. Датчики мікро-електромеханічних систем (МЕМС) – невеликі пристрої, що поєднують цифрову електроніку та механічні компоненти. Аналогічним чином працюють і біосенсори, які можна носити і навіть вшивати в організм, створюють нові можливості для галузі охорони здоров’я.

Ціна датчиків постійно знижувалася протягом останніх років, як показано на наступному рисунку, і очікується, що це падіння цін продовжиться і в майбутньому. Що робить їх ще більш доступними для використання навіть у величезній кількості [48].

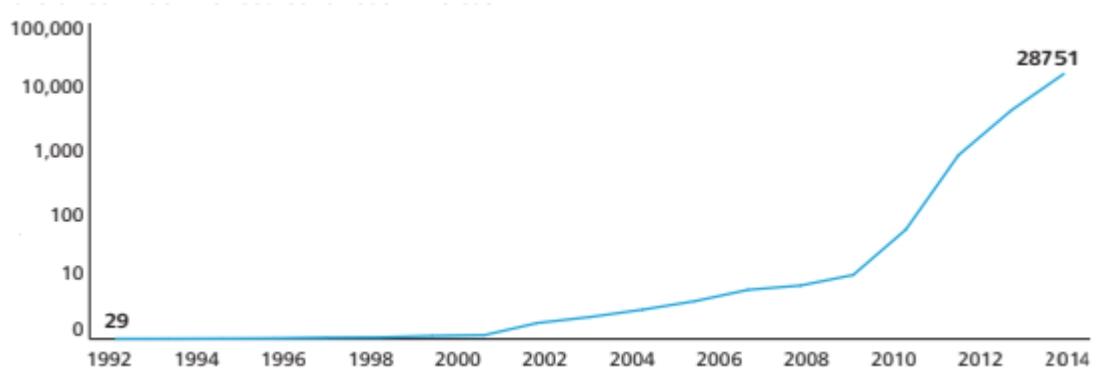


Рисунок 3.3 – Зростання потужності датчиків, виміряна у мільйонах Герц

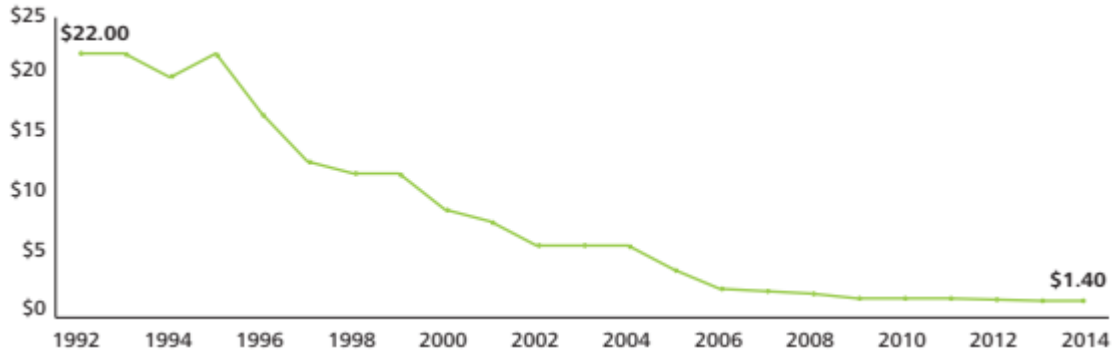


Рисунок 3.4 – Зменшення вартості датчиків за попередні 25 років

Сервери та сховища. З точки зору архітектури, сервери в середовищі IoT мають декілька ролей. Сервери необхідні для процесів починаючи від запуску програмного коду до управління необхідними програмними додатками IoT. Пристрій IoT може потребувати різних програм для виконання того, що він призначений. Сервер додатків може бути або апаратним. Однією з ключових цілей серверів є керування та обробка даних датчиків. Термін “великі дані” часто згадується в цьому контексті. Додатки та аналіз великих даних описані у наступному пункті. Управління оновленнями для різних частин в середовищі IoT також є життєво важливим. Середовище IoT складається з різних апаратних модулів, включаючи власні прошивки в кожному модулі. Ці модулі повинні бути оновлені протягом життєвого циклу пристрою IoT, і, отже, спеціальний сервер оновлення може бути встановлений у середовищі IoT. Це також актуально і для всіх програмних модулів. Сервери необхідні для зберігання та управління необробленими даними, що генеруються різними датчиками. Кількість даних датчиків може бути великою; отже, зберігання даних лише на сервері не є актуальним, і тому має сенс зберігати дані на окремому дисковому сховищі. Система зберігання даних може бути локальною дисковою пам’яттю на основі підключення по оптоволоконному каналу. Одним з можливих варіантів також є використання хмарної системи зберігання даних від відомого постачальника хмари. Однією з ключових ролей з сервером є автентифікація користувача, щоб гарантувати доступ до

додатків IoT і керування даними IoT тільки чинним користувачам. Існує декілька варіантів керування автентифікацією користувача. Одна з можливостей полягає в тому, щоб керувати користувачами та можливими ключами безпеки локально в самому пристрої IoT або використовувати спеціальний сервер керування або додаток для цих цілей. Можливості віддаленого доступу та автентифікації користувачів також повинні оброблятися в межах серверу керування користувачами та програмами.

Великі дані та аналітичні програми. Однією з основних складових в архітектурі IoT є додатки для обробки великих даних та аналітики. На даний момент існують різні постачальники, які пропонують програми для управління великою кількістю даних і маніпулювання даними таким чином, щоб вони були більш читабельними для людини. Обсяг даних, що генеруються пристроями IoT, величезний. Не має значення, чи дані генеруються датчиком або камерою спостереження або будь-яким іншим пристроєм IoT. Величезна кількість даних в основному не має ніякого значення, поки вона не була проаналізована і адаптована таким чином, що людина зможе її зрозуміти. У найгіршому випадку згенеровані дані датчика є лише текстом без будь-яких формулювань. Нижче на рисунку наведено приклад базових даних датчиків без будь-яких перетворень.

```
29.7
1001.7
35.3
28.3
1001.7
36.1
27.2
1001.6
39.0
27.4
1001.6
40.2
30.8
1001.5
39.9
33.1
1001.5
37.7
35.0
1001.4
35.3
37.5
1001.5
33.7
```

Рисунок 3.5 – Дані датчиків: температура, тиск та вологість повітря

Наведені вище дані генеруються датчиками температури і повітряного тиску. Як видно, вищенаведені цифри нічого не ілюструють; вони – лише купа чисел. Для візуалізації цих чисел потрібні великі дані та аналітичні програми. Сьогодні ринок додатків для великих даних і аналітичних інструментів величезний. Деякі програми зосереджені лише на одній області, такі як великі дані або аналітика; однак, деякі постачальники надають повний набір програм для покриття всіх великих даних і аналітичних потреб в одному пакеті. На рисунку 3.6 наведено уявлення про доступність додатків на ринку.

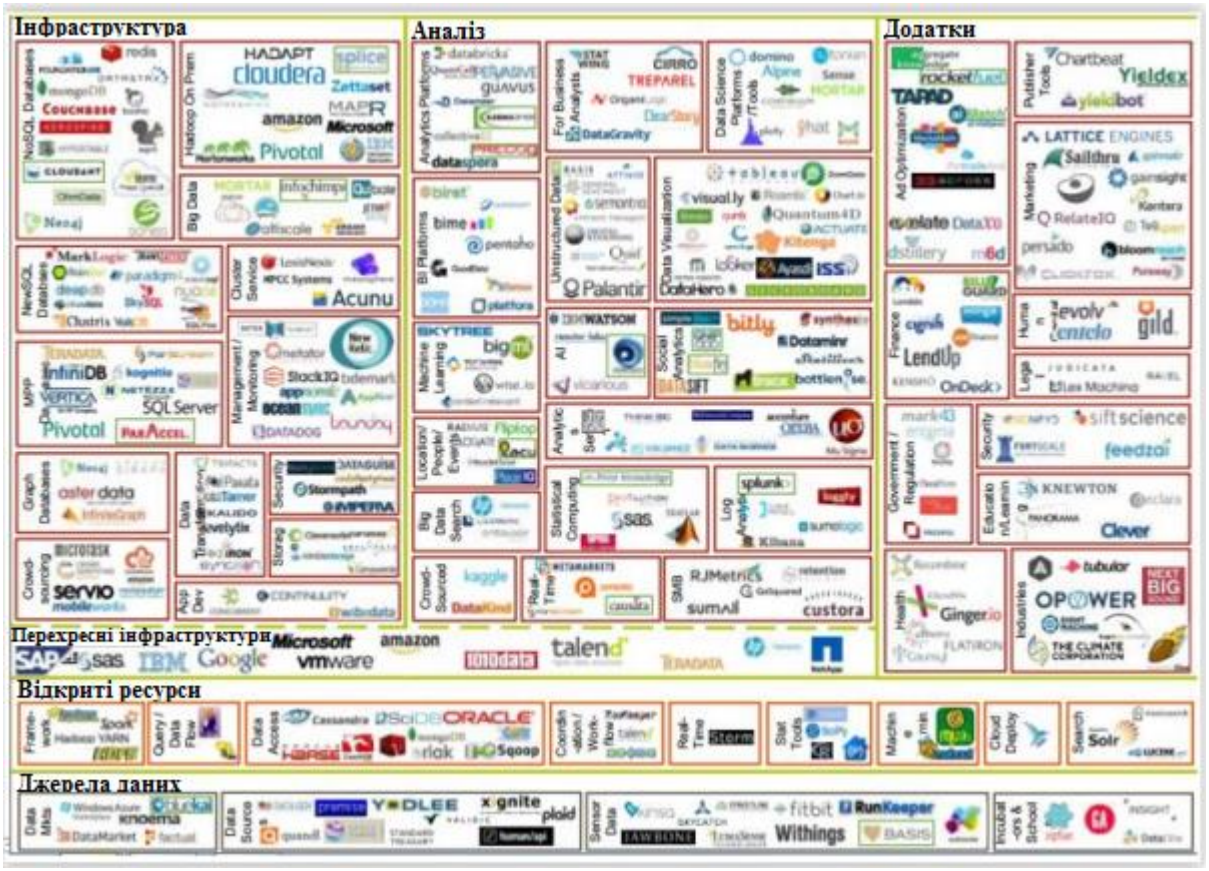


Рисунок 3.6 – Додатки для обробки великих даних та аналітики, представлені на ринку

Завдання програм для великих даних полягає в тому, щоб допомогти користувачам зрозуміти, що за дані там знаходяться, і що більш важливо, дати зрозуміти які дані є важливими для задоволення потреб організації. Можна сказати, що дані без будь-якого аналізу практично не мають толку. Одна з ключових ролей у великих інструментах даних також є можливість зберігати дані та тримати їх у безпеці. На рисунку 3.7 представлено процес переходу потоку даних від сенсора до програми аналітики, включаючи проміжні етапи.

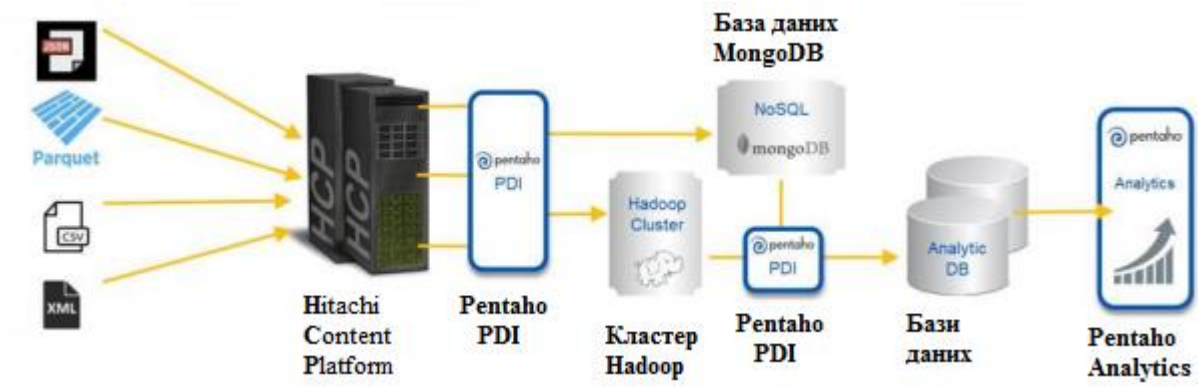


Рисунок 3.7 – Процес переходу даних

Наведений вище приклад показує типовий потік даних від датчиків і прикладних модулів, необхідних для аналізу даних. Датчики та мережні модулі виключені з цього прикладу. Цей приклад взято з рішення на 2017 рік компанією Hitachi Vantara для обробки великих даних та аналітики. Потік даних зліва направо. Неопрацьовані дані датчиків або будь-які неструктуровані або напівструктуровані дані збираються з різних місць в одне велике місце для зберігання, в цьому випадку Hitachi Content Platform, HCP. Після збору дані змінюються таким чином, що вони можуть використовуватися з інструментами Pentaho PDI. Pentaho PDI передає новостворені дані до кластера Hadoop і для бази даних MongoDB для зберігання. Інструменти аналітики Pentaho отримують дані і змінюють і формулюють її таким чином, щоб вони були доступними для читання, у такому вигляді як графіки чи графи. (Hitachi Vantara Big Data Analytics 2017)[49].

Технології та протоколи. З огляду на те, що Інтернет речей складається з безлічі різних існуючих технологій, в цьому розділі дається загальна довідкова інформація про те, що таке IoT, а також висвітлюються деякі загальні проблеми, пов’язані з його впровадженням; детальніше пояснено, чому безпека IoT настільки важлива. Крім того, будуть представлені деякі ключові технології, а також загальні протоколи, які були розроблені і використані промисловістю і науковим співтовариством.

Передбачається, що Інтернет речей зробить революцію у взаємодії окремих осіб і корпорації з цифровим і фізичним світом. В майбутньому IoT стане частиною повсякденного життя кожної людини, розширивши комунікаційні та мережеві можливості фізичних об'єктів або інтелектуальних пристроїв.

Однак тільки з недавнім розвитком і прийняттям технологій, таких як радіочастотна ідентифікація (RFID) і бездротові сенсорні мережі (WSN), технологія IoT стала можливою і доступною. Як правило, Інтернет речей дозволяє фізичним об'єктам віртуально присутнім постійний обмін інформацією через інтернет, головним чином з метою взаємодії один з одним для виконання або генерування корисної дії. Тому IoT можна розглядати як розширення IT у всіх сферах нашого життя; перетворення ізольованих в даний час мереж в нові мережі для формування глобальної взаємозалежної гетерогенної мережі інтелектуальних об'єктів або речей.

З огляду на все це, середовище IoT буде складатися з безлічі різнорідних технологій і пристроїв ; кожен з них зроблений для різних цілей, створений різними постачальниками, з різними можливостями, складнощами і швидкістю передачі даних. Незалежно від цих відмінностей, пристрої IoT зазвичай називають інтелектуальними пристроями, хоча не всі вони рівні, деякі з них більш потужні, ніж інші. Простіше кажучи, середа IoT – це обмежене середовище, що складається з будь-якого пристрою, який в даний час підключено до Інтернету, а також побутових об'єктів, встановлених з вбудованим пристроєм. Крім того, інтелектуальний пристрій, є пристроєм/вузлом, яке має наступні характеристики:

- фізичну присутність;
- засоби зв'язку;
- можуть бути однозначно ідентифіковані;
- володіють деякими базовими обчислювальними можливостями;
- можуть взаємодіяти з навколишнім середовищем.

Використання технології IoT означає, що ми будемо надавати безпрецедентний доступ і збір інформації про наше особисте і професійне життя. Таким чином, аспект безпеки в IoT є надзвичайно важливим, та об'єднує цілий ряд існуючих технологій і пристроїв. Тому для забезпечення безпеки середовищ IoT кожна з базових технологій, які інтегруються, повинна бути захищена сама по собі, оскільки будь-які проблеми безпеки, з якими вони стикаються, будуть, очевидно, успадковуватися середовищами IoT.

Крім того, інтеграція різних технологій сама по собі може призвести до появи нових вразливостей, яких не було в автономних системах. Наприклад, візьмемо технологію NFC – зазвичай мається на увазі, що технологія розгорнута в закритій системі, де зчитувач вважається безкомпромісним і має безпечне з'єднання з сервером, з яким він спілкується. Типовим прикладом цього є кредитна карта NFC, яка використовує захищений платіжний термінал/зчитувач NFC для оплати послуг. У цій ситуації зчитувач платежів NFC, як очікується, буде відокремленим пристроєм і буде надійно завантажений. Однак в сценарії IoT пристроєм зчитування/терміналом може бути будь-який пристрій з підтримкою NFC. Таким чином, це може бути мобільний телефон, і хоча ці пристрої самі по собі не є небезпечними, існує ймовірність того, що їх користувачі випадково встановили на нього шкідливе програмне забезпечення, яке зробило б пристрій вразливим. Тому в сценарії IoT ми більше не можемо припускати, що такі термінали завжди захищені, оскільки інші небезпечні пристрої, такі як мобільні телефони, можуть використовуватися в якості терміналу.

Інша проблема полягає в тому, що пристрої IoT не завжди будуть використовуватися в безпечному та контрольованому середовищі, наприклад, вдома або офісі. Тому розгортання в середовищах з жорсткими і неконтрольованими умовами збільшує ризик виникнення несправностей, а також фізичного саботажу і маніпуляцій.

Однак одна з найбільших проблем в розробці безпечної системи для IoT пов’язана з обмеженим характером пристроїв IoT. З огляду на обмежену пам’ять, енергію, пропускну здатність і можливості обробки пристроїв IoT, вони не можуть безпосередньо реалізувати існуючі існуючі механізми безпеки, які використовуються в Інтернеті. Наприклад, загальний метод забезпечення узгодженості інформації полягає в використанні криптографії, але більшість криптографічних механізмів вимагають значної кількості ресурсів з точки зору обчислювальної потужності та енергії. Це досить складне питання, яке необхідно подолати і яким приділяється велика увага в академічній спільноті.

Незважаючи на це, багато областей життя людей можуть отримати вигоду від цієї технології, оскільки вона дозволяє в режимі реального часу відслідковувати, контролювати і збирати дані. Області, які найбільше виграють від цієї технології – це транспорт, охорона здоров’я і моніторинг навколишнього середовища.

IoT можна використовувати і у персональному медичному пристрої, який відстежує стан пацієнта в режимі реального часу. Це дозволяє пацієнтам, особливо літнім, залишатися незалежними протягом більш тривалого періоду часу, без спеціалізованої медичної допомоги. Іншим прикладом є розумний будинок, в якому мережа датчиків може використовуватися для управління і контролю безпеки будинку. Крім того, за допомогою детекторів руху, власник будинку може отримати сигнал та негайно перейти до відеотрансляції в разі, якщо в будинку хтось виявлений, у той момент коли в ньому не мав би знаходитись ніхто . Крім того, власник будинку може дозволити функцію розпізнавання осіб для того, щоб дозволити системі автоматично регулювати такі функції як яскравість світла, температура кімнати і налаштування музики, коли користувач входить і виходить з кімнати, відповідно до переваг жителів будинку. Існує досить велика кількість досліджень, що охоплюють деякі з корисних і винахідливих способів реалізації технології IoT, і у всіх випадках безпека є

важливим чинником. В середовищі IoT все буде пов’язано; це означає, що кожна людина і об’єкт у фізичному світі можуть бути зчитані завдяки їх віртуальній присутності в Інтернеті.

Безліч непомітних засобів, за допомогою яких пристрої IoT збирають і обробляють конфіденційну інформацію, дозволяють віртуальному світу безпосередньо впливати на фізичний світ, що ще раз підкреслює важливість безпеки для Інтернету речей.

Інтернет речей можна розглядати як інтеграцію пасивного сенсорного зв’язку та вбудованих пристроїв з Інтернетом. Таким чином, в цьому розділі ми коротко представимо три ключові технології для IoT. Це інтернет-протокол версії 6 (IPv6) [50], технології радіочастотної ідентифікації (RFID) і бездротові сенсорні мережі (WSN). Одразу відзначимо, що це не повний список технологій, які охоплюють IoT, і є частиною Інтернету речей, це такі як: інтелектуальні сенсорні пристрої, зв’язок ближнього поля (NFC), хмарні обчислення системи глобального позиціонування (GPS), сервіс-орієнтовані архітектури (SOA), географічні інформаційні системи (ГІС) і мобільні стільникові пристрої.

Інтернет-протокол версії 6. Інтернет-протокол версії 6 або IPv6 був розроблений через вичерпання доступних в даний час IP-адрес, що використовуються за схемою IPv4[51]. Схема IPv6 забезпечує доступність 2128 IP-адрес в порівнянні з 232 IP-адресами за схемою IPv4, що є значною різницею. Цей аспект є дуже важливим для IoT через те, що число інтелектуальних пристроїв і датчиків, які, як передбачається, будуть підключені до Інтернету, легко витратять запас адресного простору доступний за схемою IPv4.

Ідентифікація радіочастоти. Радіочастотна ідентифікація є однією з ключових технологій Інтернету речей. Незважаючи на те, що його розгортання в комерційному і приватному секторах було досить недавнім, його вперше використали для ідентифікації дружніх літаків під час Другої світової війни; хоча тоді це було не так портативно і енергоефективно.

Зазвичай RFID-технологія складається з двох пристроїв: RFID-міток і RFID-зчитувачів. RFID-мітка – це пристрій, прикріплений до об’єкта, який ми хочемо відстежувати або збирати інформацію, а RFID-зчитувач – це пристрій, який може розпізнавати/виявляти присутність RFID-мітки і може зчитувати інформацію, що зберігається на ній. Крім того, технологія RFID дозволяє отримувати інформацію з помічених об’єктів по бездротовій мережі за допомогою радіохвиль.

Мітки RFID зазвичай можна розділити на три категорії: пасивні, напівактивні і активні мітки. Пасивні мітки RFID – це пристрої без власного джерела живлення. Таким чином, вони отримують свою потужність шляхом зміни електромагнітної радіохвилі, яку RFID-зчитувач посилає при запиті інформації. Напівактивна мітка має невелике джерело живлення, але також отримує енергію, подібно до пасивних міток, на додаток до свого обмеженого джерела живлення, в той час як активні мітки RFID мають власний вбудований джерело живлення для зарядження мікрочіпа і датчиків.

Хоча активні мітки є важливими з точки зору IoT, ми повинні пам’ятати, що інтелектуальні пристрої повинні працювати протягом тривалих періодів часу без втручання користувача. Тому енергоефективна реалізація, яка отримує енергію від інших джерел, таких як пасивні пристрої, є більш ідеальною для середовищ IoT.

RFID-мітки можуть мати датчики і механізми для збору інформації. Крім того, мітки RFID досить обмежені з точки зору пам’яті, енергії, обчислювальної потужності і пропускної здатності [52].

Також технологія RFID зазвичай працює, коли зчитувач RFID передає радіочастотний (RF) сигнал, який мітка отримує і перетворює в енергію для живлення свого чіпа. Потім мітка відправляє свою ідентифікацію назад читачеві; як видно на рисунку 3.6. Ось як, в основному працює технологія RFID (хоча в деяких випадках є відмінності, наприклад, деякі мітки можуть зашифровувати повідомлення, які вони відправляють при спілкуванні з

зчитувачем, а деякі можуть навіть ігнорувати зчитувачі, які не надають відповідний пароль):

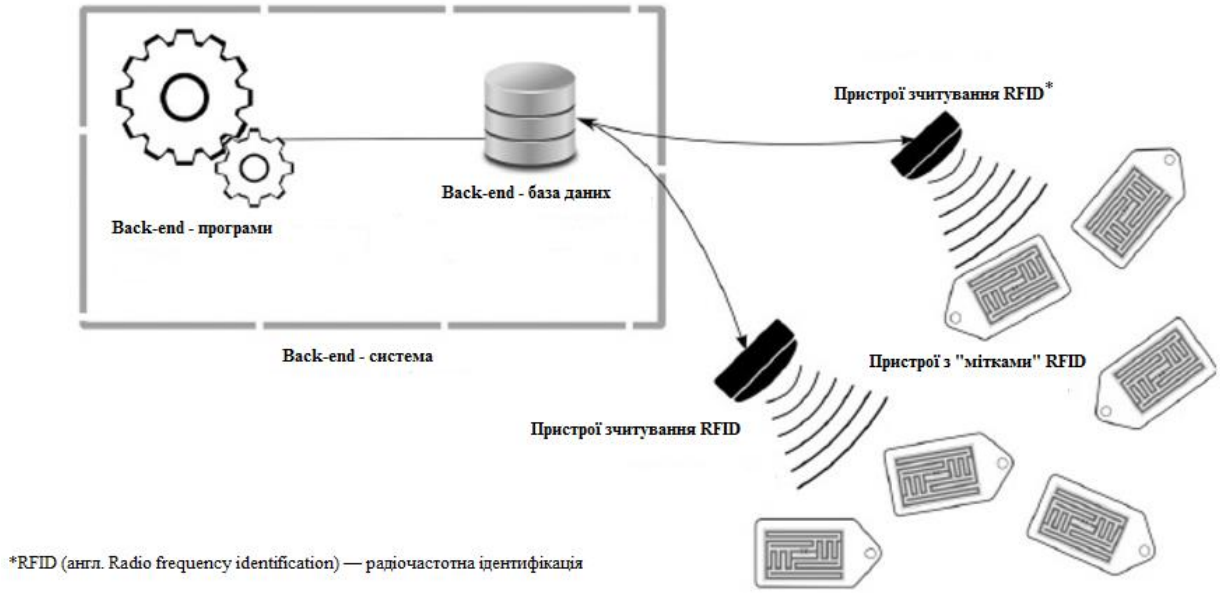


Рисунок 3.8 – Приклад системи RFID

Бездротові сенсорні мережі. Як правило, бездротові сенсорні мережі (WSN) складаються з групи сенсорних пристроїв, розкиданих в певній галузі, яка збирає і передає дані в центральний приймальний пристрій; який потім відправляє дані в сховище даних для обробки. Ці приймальні пристрої зазвичай більш потужні, ніж сенсорні пристрої, оскільки вони необхідні для обробки всієї вхідної інформації, можливо, виконують деяку обробку інформації і відправляють інформацію в серверну систему. Ця ідея зображена в WSN – мережах, традиційно побудованих з однорідних пристроїв з обмеженими можливостями. Однак, як і RFID, існують різні типи WSN; наприклад, в деяких сенсорних мережах маршрутизатори та приймальні пристрої доступні тільки в певний час, в той час як інші не мають таких обмежень. Незважаючи на це, всі варіанти WSN складаються з пристроїв з обмеженнями на їх ємність, обчислювальну потужність, канали зв’язку і діапазон датчиків.

Крім того, оскільки сенсорні пристрої мають обмежений діапазон зв’язку, вони не завжди можуть відправляти/повідомляти інформацію

безпосередньо в вузол приймача. Таким чином, WSN зазвичай передають інформацію через інші сенсорні вузли до тих пір, поки вона не досягне приймального вузла [53].

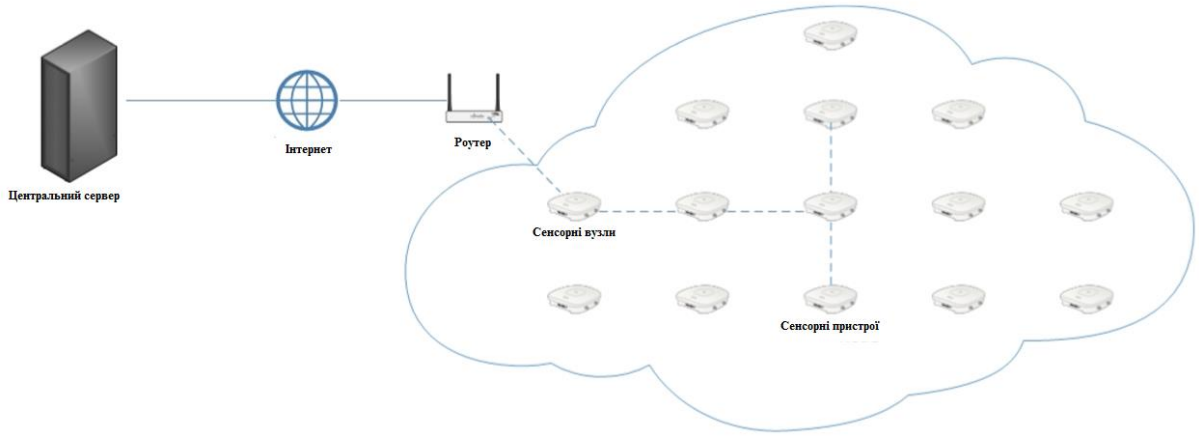


Рисунок 3.9 – Просте налаштування WSN

IoT-протоколи. З огляду на те, що Інтернет є однією з ключових технологій, необхідних для функціонування IoT, стек протоколів TCP/IP, аналогічний стеку, доступному для Інтернету, також може бути визначений для середовищ IoT. Тому в цьому розділі будуть описані деякі стандартні протоколи, призначені для Інтернету речей. На малюнку нижче показаний стек протоколів, який ми розробили при вивченні літератури, хоча він і не є вичерпним: це показує, що в області IoT була проведена велика робота.

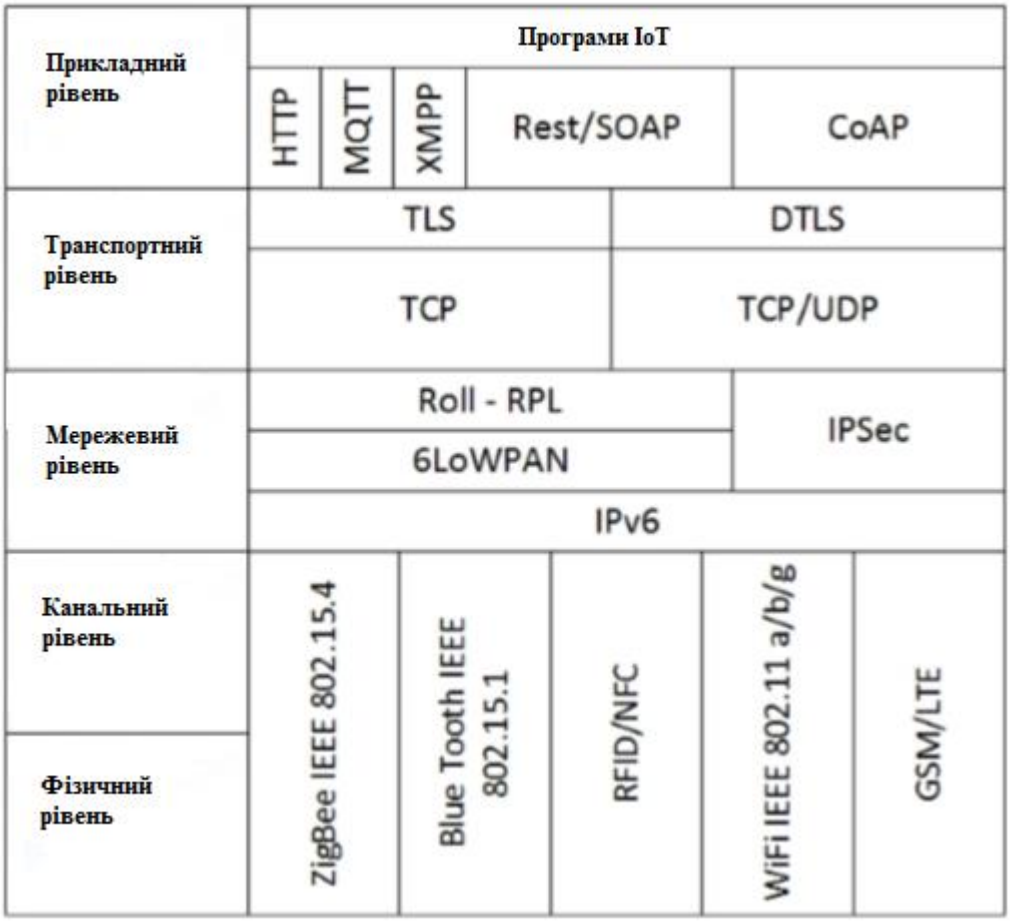


Рисунок 3.10 – IoT стек протоколів

Нижче будуть розглянуті деякі з найбільш часто використовуваних протоколів, що зустрічаються при проведенні огляду літератури [54].

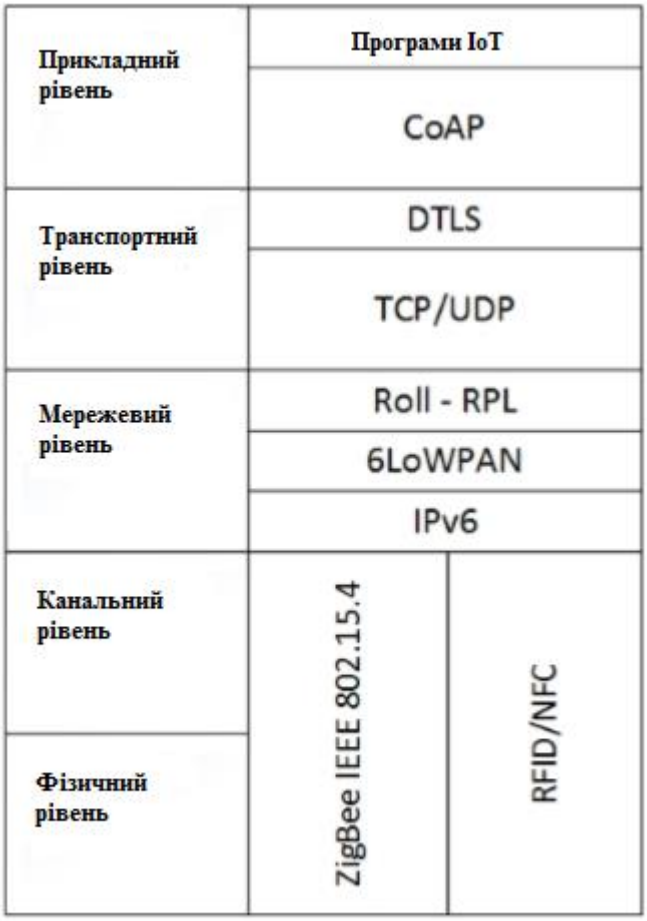


Рисунок 3.11 – Елементи IoT стеку, що є найбільш використовуваними

Слід зазначити, що на рисунку показаний найбільш розповсюджений набір протоколів, що використовується науковими колами при проведенні досліджень безпеки в IoT.

Протоколи прикладного рівня. Нижче описані деякі протоколи прикладного рівня і їх функції. Короткий опис можна знайти в таблиці

Таблиця 3.2 – Загальні прикладні протоколи для IoT

Прикладні протоколи	Транспортні протоколи	QoS*	Модель зв'язку	Безпека
CoAP	UDP	Yes	Request/respond Publish/subscribe	DTLS
MQTT	TCP	Yes	Publish/subscribe	TLS/SSL
XMPP	TCP	No	Request/respond Publish/subscribe	TLS/SSL

*QoS (англ. Quality of service) - якість обслуговування

Хоча й існує кілька протоколів прикладного рівня, але протокол CoAP є найбільш часто використовуваним [55]. Перш за все тому, що він дуже легкий, так як працює по протоколу UDP. Додатковим фактором є те, що протокол CoAP допускає як одноадресний, так і багатоадресний зв'язок.

Протокол обмеженого застосування. Протокол обмеженого застосування (CoAP) є спеціалізованим протоколом прикладного рівня, призначеним для використання обмеженими пристроями. Він дозволяє використовувати функції HTTP, а також модель взаємодії клієнт/сервер (запит/відповідь). Крім того, як і HTTP, CoAP використовує універсальні ідентифікатори ресурсів (URI) для доступу до ресурсів на конкретному вузлі або пристрої. Це дозволяє легко взаємодіяти з протоколом HTTP, оскільки саме він сьогодні використовується в Інтернеті.

Основна перевага протоколу CoAP полягає в тому, що він забезпечує низькі витрати, враховуючи, що він працює по протоколу UDP замість TCP. Крім того, він підтримує багатоадресний і одноадресний зв'язок, а також вбудовану функцію виявлення пристроїв. У нього також є механізми для забезпечення якості обслуговування, що важливо, тому що він працює по ненадійному протоколу UDP.

Однак, незважаючи на те, що він був спеціально розроблений для пристроїв з обмеженими можливостями, протокол CoAP не має вбудованих функцій безпеки. Подібно протоколу HTTP, який для забезпечення безпеки використовує протокол TLS, протокол CoAP для забезпечення безпеки використовує протокол DTLS, відповідно до пропозиції Інженерної робочої групи по Інтернету (IETF). Іншим можливим протоколом безпеки для CoAP є протокол IPSec, але на відміну від DTLS, протокол IPSec не був схвалений для використання в поєднанні з протоколом CoAP IETF.

Спрощений мережевий протокол. Спрощений мережевий протокол (MQTT) був розроблений IBM для полегшення міжмашинних комунікацій. Він працює поверх протоколу TCP для реалізації моделі взаємодії

“публікація/підписка”. Ця модель була обрана тому, що клієнтські пристрої не мають спеціально запитувати оновлення; що фактично зменшило б споживання ресурсів на вузлах IoT.

Що стосується безпеки, протокол MQTT використовує свій брокерський пристрій, який може забезпечувати автентифікацію через протокол SSL/TLS.

Відкритий мережевий протокол для швидкого обміну повідомленнями. Відкритий мережевий протокол для швидкого обміну повідомленнями та інформацією про присутність між користувачами мережі Інтернет (XMPP) – це протокол, розроблений для зв’язку в реальному часі і працює по протоколу TCP. Він враховує моделі взаємодії “публікація/підписка” та “запит/відповідь” і націлений на низьку затримку і невеликий обсяг повідомлень [56]. Однак він не підтримує якість обслуговування, і витрати, пов’язані з розглядом XML-повідомлень, тому вони можуть бути досить високими.

Як і попередні два прикладних протоколи, для забезпечення безпеки XMPP використовує інший рівень; зокрема, транспортний рівень в рамках SSL/TLS.

Протоколи транспортного рівня. Цей рівень використовує протоколи TCP і UDP. Найбільш часто використовуваний протокол безпеки, що реалізується цим рівнем, - це протокол безпеки транспортного рівня (TLS) для Інтернету та розподіленої безпеки транспортного рівня (DTLS) для обмежених пристроїв IoT. Ці два протоколи коротко описані нижче.

Безпека транспортного рівня. TLS – це протокол, розроблений для забезпечення безпеки надійних транспортних протоколів; як протокол TCP. Як такий, він забезпечує автентифікацію, конфіденційність і цілісність на транспортному рівні, гарантуючи, що атаки викрадення і підробки повідомлень не можуть відбутися. Як правило, TLS дозволяє двом пристроям в Інтернеті порівнювати загальний ключ, який потім використовується для створення безпечного каналу зв’язку. Однак, оскільки

цей протокол є досить ресурсномістким, пристрої IoT з обмеженими можливостями не можуть запустити цей протокол. Інша причина, по якій цей протокол не підходить для середовищ IoT, полягає в тому, що TLS призначений для роботи по надійному каналу зв'язку[57]. Отже, в разі втрати пакета або повідомлень, що з'являються не по порядку, протокол розірве з'єднання. З огляду на те, що пристрої IoT працюють по ненадійному каналу, це може призвести до розриву великої кількості з'єднань.

DTLS – це протокол, який призначений для імітації TLS по ненадійному каналу зв'язку, наприклад, за протоколом UDP. Це в основному просто TLS з декількома додатковими функціями; наприклад, DTLS не допускає потокові шифри, так як його ненадійний канал не запобігає втрати повідомлень і повідомлення, отримані не по порядку.

Однак ключовим недоліком протоколу DTLS є те, що він не був розроблений спеціально для пристроїв IoT. В результаті він не підтримує багатоадресний зв'язок. Крім того, передбачається, що пристрої IoT на основі CoAP вже мають довгострокові ключі для роботи цього протоколу . Іншим недоліком протоколу DTLS є те, що процес "handshake" має можливість допустити виконання атаки вичерпання ресурсів (Resource exhaustion attack) на обмеженому пристрої. Проте, DTLS швидший, ніж традиційний TLS, оскільки він працює по UDP.

Протокол мережевого рівня. Тепер ми в загальних рисах розглянемо протоколи IPv6 для бездротових персональних мереж з низьким енергоспоживанням (6LoWPAN), протокол маршрутизації IPv6 для мереж з низьким енергоспоживанням і втратами (RPL) і протоколи безпеки протоколу Інтернету (IPSec), які знаходяться на мережевому рівні [58].

6LoWPAN. Протокол 6LoWPAN був розроблений IETF для роботи над IPv6, щоб дозволити інтегрувати технології різнорідного канального рівня. Крім того, це основний мережевий протокол, який використовується IoT, і простіше кажучи, він дозволяє обмеженим пристроям, які не можуть

обробляти традиційний стек IP, що використовується Інтернетом, функціонувати і підключатися до пристроїв в Інтернеті.

Цей протокол дозволяє обмеженим пристроям поводитися як будь-який інший пристрій, підключений до Інтернету, з деякими застереженнями. Таким чином, це дозволило б обмеженим пристроям і будь-яким іншим, підключеним до Інтернету, створювати наскрізне з'єднання. Крім того, він використовує механізми стиснення і інкапсуляції заголовків пакетів для зменшення навантаження на канал зв'язку. Однак цей протокол жодним чином не забезпечує безпеку; перекладаючи це завдання на інші протоколи, такі як протоколи IPSec і DTLS.

Крім того, маршрутизація на цьому рівні може бути виконана через протокол RPL, а безпека може бути встановлена через протокол IPSec.

RPL. RPL – це протокол, розроблений IETF для маршрутизації в середовищах IoT, і використовує механізми векторів відстаней для маршрутизації в середовищах IPv6 . Цей протокол був розроблений для мереж з низьким енергоспоживанням і з втратами (LLN), тому він економить ресурси, бідно генеруючи керуючий трафік і обмежуючи його по відношенню до трафіку даних. RPL підтримує три категорії потоків трафіку: точка-точка, точка-точка і точка-точка. Саме з цих причин цей протокол краще існуючих протоколів маршрутизації, таких як OSPF, IS-IS і OLSR[59].

IPSec. IPSec – це протокол, який використовується для забезпечення конфіденційності, цілісності та автентичності між двома клієнтами по небезпечному каналу. Основна перевага IPSec в порівнянні з TLS і DTLS полягає в тому, що він забезпечує прозорість безпеки для програми. Як правило, протокол IPSec має дві фази роботи: фаза асоціації безпеки і робоча фаза [60].

Фаза асоціації безпеки зазвичай використовує протокол IKEv2 для генерації асоціацій безпеки між об'єктами. Після цього результуючий ключ, згенерований на попередньому етапі, буде використовуватися для

забезпечення безпечного каналу між двома об’єктами. Слід зазначити, що на цьому етапі протокол IPSec може працювати в різних режимах; це режими заголовка автентифікації (AH) або інкапсуляції корисного навантаження (ESP). AH може використовуватися для забезпечення цілісності та автентичності IP-пакета, але він не гарантує конфіденційність інформації; це те, що дозволяє ESP. Однак ESP не гарантує справжність заголовка, як AH, тому що зовнішній IP-рівень незахищений цілісністю. Незважаючи на це, ESP є кращим режимом, використовуваним в порівнянні з AH, оскільки на нього не впливають NAT і, що більш важливо, він шифрує корисне навантаження повідомлень для забезпечення конфіденційності. ESP також забезпечує виявлення повторних атак.

Крім того, з огляду на додаткові витрати для цього протоколу в порівнянні з DTLS, в поєднанні з тим фактом, що не всі вузли IoT здатні використовувати протокол IPSec, робить протокол DTLS найкращим засобом забезпечення безпеки. Однак протокол IPSec може використовуватися в залежності від настройки IoT.

Блокчейн у вирішенні проблем безпеки Інтернету речей. Сам термін Blockchain частково характеризує його завдання і призначення. Частина “Block” – це блоки, “chain” – це “ланцюжок”. Виходить, що Blockchain – це ланцюжок блоків. Причому не просто ланцюжок. У ньому витримується строга послідовність [61].

Що це за блоки і що за ланцюжок? Блоки – це дані про транзакції, угодах і контрактах всередині системи, представлені в криптографічного формі. Спочатку блокчейн був (і залишається досі) основою криптовалюта Bitcoin. Всі блоки збудовані в ланцюжок, тобто пов’язані між собою. Для запису нового блоку, необхідно послідовне зчитування інформації про старі блоки.

Всі дані в блокчейн накопичуються і постійно доповнюють сформовану базу даних. З цієї бази даних неможливо нічого видалити або провести заміну/підміну блоку. І вона “безмежна” – туди може бути

записана нескінченна кількість транзакцій. Це одна з головних особливостей блокчейна.

Технологія Blockchain збільшила свій вплив на Інтернет речей, за рахунок посилення безпеки та можливості включення в екосистему все більшого числа пристроїв. Удосконалення в області безпеки пристроїв IoT сприяють більш швидкому впровадженню цієї революційної інновації і відкривають широкий спектр можливостей для підприємств найближчим часом. Рішення IoT, що використовують Blockchain, можуть бути створені для підтримки постійно зростаючого списку записів даних з криптографічним захистом від зміни і модифікації. Blockchain може допомогти скоротити витрати і непередбачуваність роботи периферійних пристроїв або підключених серверів. Схвалення цієї зростаючої інновації свідчить про неймовірні перспективи в сфері IoT і всередині підприємства.

Блокчейн набирає обертів в якості інструменту безпеки IoT. У той час, як галузь очікує регулювання та шукає шляхи для вирішення самих проблем, блокчейн стає потенційною допомогою; впровадження цієї технології зросло з одного 9% до 19% за останні 12 місяців. Більш того, чверть (23%) респондентів вважають, що технологія блокчейна була б ідеальним рішенням для захисту пристроїв IoT, при цьому дев’ять з десяти (91%) організацій, які в даний час не впроваджують технологію, ймовірно, розглянуть її в майбутньому.

Та поки технологія поступово знаходить своє місце в захисті IoT-пристроїв, підприємства продовжують використовувати інші методи для захисту від кіберзлочинів. У централізованому середовищі обробки транзакцій кожна транзакція повинна бути підтверджена за допомогою централізованої довіреної сторону (наприклад, банківську систему), що призводить до збільшення вартості і зменшення продуктивності в централізованій точці. Що ж стосується старої децентралізованої моделі IoT, то при застосуванні технології блокчейн – третя сторона більше не

потрібна. Для підтримки цілісності і узгодженості даних в блокчейні використовуються консенсусні алгоритми.

Блокчейн використовує асиметричну криптографічну техніку для захисту всієї мережі. Асиметрична криптографія або криптографія з відкритим ключем містить 2 ключа: один відкритий ключ і другий закритий ключ. Відкритий ключ використовується вузлом для адресації в мережі блокчейна, а закритий ключ використовується вузлом для підписання транзакції, яку він ініціює. Інші вузли використовують свій відкритий ключ і порівнюють його після хешування зі своїм підписом для перевірки ідентифікації вузла ініціатора. Блокчейн – це однорангова мережа, в якій всі вузли мають однакову копію записів.

Тільки 19% компаній в даний час використовують блокчейн, а планують використовувати 23% (Рис. 3.12). Близько трьох з десяти (29%) використовують біометрію, а 38 % надають перевагу двофакторній автентифікації.

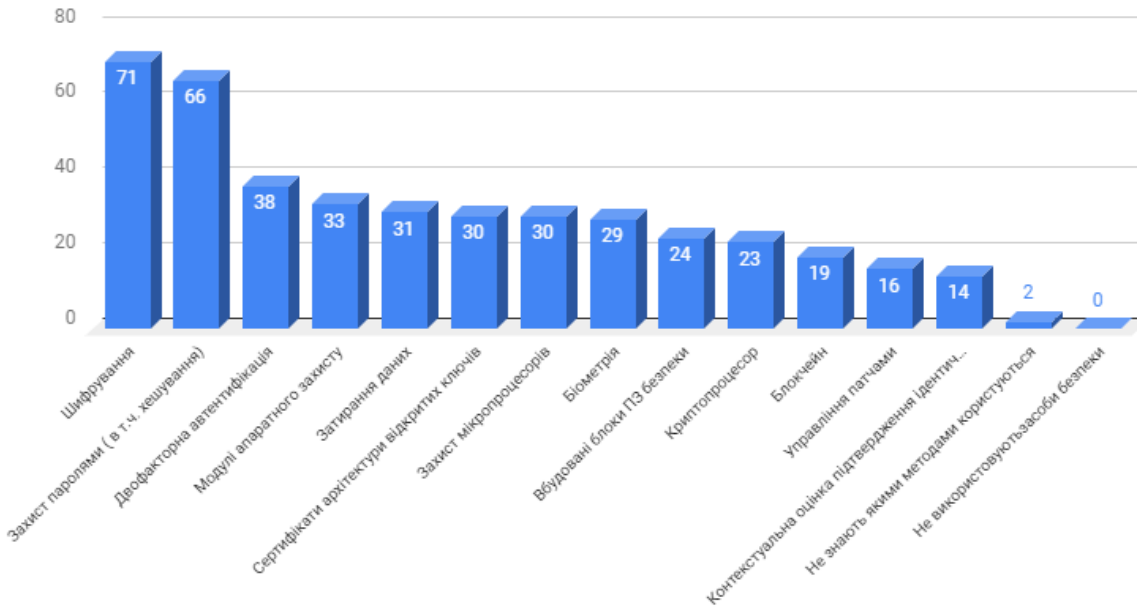


Рисунок 3.12 – Технології, що використовуються організаціями для захисту даних/послуг/пристроїв IoT

Блокчейн в IoT представляє собою найбільший технологічний прорив з моменту інтеграційних обчислювальних систем і систем обробки

транзакцій. Завдяки значному прогресу в області інновацій та програмного забезпечення, передача та обробка транзакцій пристроями в усіх областях стала можливою сьогодні Досі існують серйозні проблеми з адаптивністю, пов’язані з впровадженням децентралізованих систем, а також з безпекою, координацією, управлінням інтелектуальною власністю, ідентифікацією та конфіденційністю, тому багато установ і приватних осіб активно працюють над вирішенням цих питань, що прогнозує позитивний результат у покращенні безпеки засобів IoT.

Роль біометрії у питанні безпеки IoT. Термін “біометричний” – це “грецьке слово”, “біо” означає “життя”, а “метрика” означає “виміряти”. Вона в першу чергу визначається як єдина характеристика, що містить різні риси людського тіла, для ідентифікації ідентичності людини. Біометричні підходи віднедавна є найефективнішими методами для розпізнавання людей, як заміна перевірки індивіда та надають їм доступ до динамічних або віртуальних доменів на основі буквено-цифрових паролів, PIN-кодів, смарт-карт, жетонів, ключів і т.д. Біометричні технології застосовуються насамперед для автоматичного розпізнавання людей на основі їх фізіологічних ознак або поведінкових характеристик. “Паролі, ключі, і жетони” можуть не використовуватись, або бути підроблені/зламані, тоді як біометрична техніка – це унікальна і бездоганна техніка фізичної безпеки, яка використовується для перевірки окремої особи.

Рисунок 3.13 – Приклад біометричних ознак людського тіла

Для цілей автентифікації, перевірки та ідентифікації, біометрична безпека виявляється найсучаснішою технологією, яка дозволяє клієнтам підтверджувати свою діяльність в режимі онлайн через програмне забезпечення за допомогою відбитків пальців або розпізнавання голосу, відомі до прикладу банками для надання онлайн-доступу клієнтам доїх рахунків. П’ять інтегрованих компонентів, які повинні міститися в характерній біометричній системі:

1. Датчик може збирати дані і перетворювати їх в цифровий формат.
2. Алгоритм обробки сигналів для виконання процедур перевірки якості та створення біометричних шаблонів.
3. Елемент зберігання даних, який зберігає дані, які пізніше будуть зрівняні зі свіжими біометричними шаблонами.
4. Система підбору, необхідна для перевірки відповідності нових біометричних шаблонів з кількома шаблонами, що зберігаються в сховищі даних.
5. Система прийняття рішень, яка використовує результати, отримані алгоритмом узгодження, щоб виконати рішення на рівні системи.

Біометрична безпека в основному застосовується в середовищі з серйозними фізичними умовами безпеки або у місцях, які надзвичайно схильні до крадіжки особистих даних. Біометричні системи безпеки містять особливості людського тіла, які не змінюються протягом життя людини. Особисті риси тіла попередньо зберігаються в біометричній системі безпеки або сканері, який може бути вилучений лише спеціальним персоналом. Як тільки зроблено крок у приміщенні або відбулась спроба отримати допуск до системи, біометричний сканер одразу аналізує нові тілесні риси,і перевіряє з існуючими записами. Якщо результат відповідає заявленому, то фізичній особі надається доступ .

Користь біометрії для безпеки мережі. Біометричні дані або використання тілесних особливостей для доступу до захищених систем – це рішення наступного покоління для посилення інформації та розташування. Біометрія знаходиться на крок попереду від паролів та в двох кроках від традиційних замків з ключами, це реальне, зручне багаторівневе рішення для безпеки , яке не під силу навіть хорошим хакерам.

Нижче наведено основні аргументи, які свідчать про те, що біометрія є безпечним методом для перевірки ідентичності людини.

- Унікальність: біометричні характеристики, тобто фізичні або логічні, постійно є унікальними для кожної людини. Ймовірність того, що 2 особи, що мають повністю ідентичні біометричні дані, майже дорівнює нулю. Численні біометричні системи були створені за допомогою унікальних фізичних характеристикам осіб.
- Не можна зробити копію: оскільки біометричний актив є вродженою властивістю особистості, його надзвичайно важко скопіювати. Особа ніяким чином не може надати комусь іншому репліку свого обличчя або руки для того, щоб обійти процес перевірки особи. Таким чином, біометричними рисами ніколи не можна поділитись з іншими.
- Не можна підробити: Біометричні особливості окремої людини майже неможливо підробити або скомпрометувати, в розпал численних нових технологій, які розпізнають та перевіряють біометричні дані, які належать живій людині.
- Не можуть бути втрачені: оскільки біометричні ознаки є вродженими та унікальними активами індивідуума і на відміну від паролів, PIN-кодів, квитків тощо, вони не можуть бути втрачені. Біометричний актив особи може бути зіпсований чи пошкоджений лише у випадку серйозної аварії.
- Більш ефективні: біометрична верифікація є ефективним методом перевірки ідентичності людини, оскільки біометрія окремих людей не може бути імітованою. Trusted Execution Environment (безпечене

середовище виконання) входить до біометричних пристроїв, які відокремлюють управління біометричною інформацією від операційної системи пристрою. Це робить практично неможливим для хакерів фальсифікацію процесу автентифікації, оскільки не існує способу використання шкідливих програм та інших вірусів для маніпулювання кінцевими результатами. Існують різні способи біометрії, які можна використовувати в процесі автентифікації людської ідентичності.

Цей метод в основному реалізується за допомогою таких людських активів, як відбитки пальців, текстури очей, голос, моделі рук, розпізнавання облич і так далі. Хоча, серед усіх доступних способів біометрії, автентифікація за відбитками пальців була найбільш широко використовуваним методом для ідентифікації людей і була добре прийнята в країнах, що розвиваються, але все ще використання відбитків пальців для цілей автентифікації не є прийнятним в умовах, коли люди не мають пальця, або його було сильно пошкоджено; ситуації, коли ідентифікацію необхідно зробити моментально через обмеження по часу. Тому з метою безпеки в інтернеті речей буде розглянуто ще й система розпізнавання облич для підтвердження автентифікації користувача і забезпечення доступу до приватної інформації. Зображення обличчя користувача спочатку фіксується і зберігається в базі даних, і потім шифрується, щоб не було змоги підробити інформацію. Коли користувач подає запит на онлайн-доступ до персональної інформації, в той момент, обличчя сканується та проходить перевірку на відповідність з зображенням, що вже зберігається в базі даних. Якщо обидва зображення точно співпадають, то доступ користувачеві дозволений, в іншому ж випадку доступ заборонений.

Система розпізнавання облич. Людське обличчя є найпростішою особливістю, яка може бути використана в системі безпеки на основі біометрії, для розпізнавання людини. Технологія розпізнавання облич, надзвичайно відома і прийнята більш широко, оскільки не існує ніяких

вимог щодо фізичного контакту між користувачами та обладнанням. Камери спочатку переглядають обличчя користувача, а потім підбирають його зі збереженої бази даних для автентифікації. Крім того, обладнання досить просто встановити і немає необхідності вигадувати ще щось додатково. Ця технологія широко застосовується в різноманітних схемах безпеки, таких як контроль корпоративного доступу або облікові записи користувачів комп'ютера. Розпізнавання обличчя в основному визначається як завдання розпізнавання раніше виявленого обличчя як відомого або навпаки. Система, що передбачає розпізнавання облич, призначена для точного та постійного режиму ідентифікації обличчя окремої людини. Вона має справу з автоматичним розпізнаванням або перевіркою особи по цифровому зображенню/відео, зіставляючи конкретні риси обличчя. Це свого роду управління доступом до особистості та контроль доступу. Більше того, ця стратегія розглядається як пасивна, що без втручань ідентифікує та визнання людей. Хоча існують додаткові методи ідентифікації, такі як PIN-код (персональний ідентифікаційний номер), пароль, підпис, відбитки пальців, райдужна оболонка, відбиток пальців, рука та ін. ідентифікувати один одного. Біометричні системи розпізнавання осіб спочатку збирають дані з обличчя користувачів і зберігають їх у базі даних для швидкого використання. Потім вимірюється повний контур людського обличчя, розташування та кількісна характеристика певних ознак на обличчі користувача, таких як відстань між очима, носом, вухами, ротом, розміром очей та іншими. Приклади зазвичай включають посмішку, плач і зморшки на обличчі. Існують дві цілі для розпізнавання обличчя, які називаються перевіркою та ідентифікацією. Зображення обличчя надається системі ідентифікації обличчя, щоб визначити приблизний стан людини, а після цього йде перевірка обличчя з урахуванням всіх умов. Нижче на малюнку показані етапи розпізнавання обличчя.

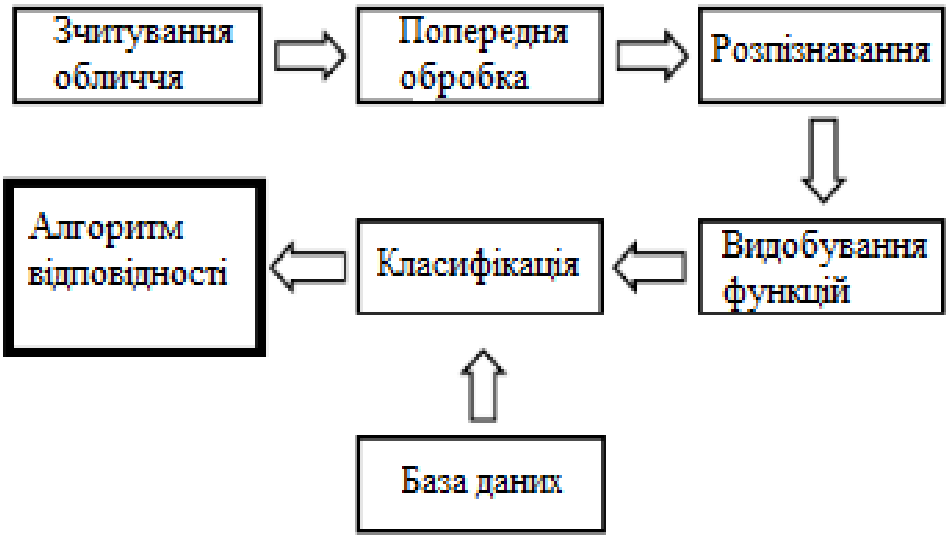


Рисунок 3.14 – Загальна система розпізнавання облич

Етапи розпізнавання облич.

Попередня обробка зображення. На цьому етапі зображення обличчя спочатку попередньо обробляються та розширюються для покращення якості зображення шляхом видалення шумів та надмірностей з вхідного зображення. Цей етап видалення шумів з зображення розглядається як найважливіше завдання у всьому процесі, оскільки шумне зображення може вплинути на точність розпізнавання облич і також впливає на загальну продуктивність системи. Попередня обробка виконується для наступних двох цілей:

- зменшити шум та можливі його наслідки
- змінити зображення в різних варіаціях для полегшення експлуатації системи в майбутньому.

Розпізнавання облич. Виявлення обличчя в деяких зображеннях може бути простим процесом для людини, але не для ПК, який використовує пікселі зображення як частину обличчя. У паспорті на фото застосовано певні обмеження, такі як освітлення, фон, положення голови, що значно спрощують процес розпізнавання обличчя, проте в реальному житті це не так. Ця процедура є процесом вилучення обличчя за допомогою вхідного

зображення. Вона є дуже корисною для ідентифікації людини при рухах, в різних позах і т.д.

Видобування функцій. Видобування функцій обличчя – це процес перетворення вхідних даних у певний набір функцій. Особливі точки, такі як очі, ніс, рот, витягуються, а потім використовуються як вхідні дані до програми. Як тільки обличчя буде доступне для системи, відбудеться вилучення ознаки з обличчя. У вилученні ознак створюється математична ілюстрація, що називається біометричним шаблоном або біометричним посиланням, яка зберігається в базі даних, і це стане основою будь-якої задачі розпізнавання. Виділеними ознаками можуть бути деякі області кутів нахилу, мірки, отримані з обличчя людиною. Унікальність вилучених наборів ознак прямо пропорційна швидкості розпізнавання.

Вилучення ознак може допомогти скоротити величезну кількість даних до відносно невеликого набору, який швидше обчислюється. На нього впливають багато ускладнень, наприклад, різниця в різних зображеннях одного і того ж виразу обличчя, світлових напрямків візуалізації, різноманітних поз, розміру і кута. Першочерговим завданням методів вилучення об’єктів є вилучення точних характеристик з зображення обличчя.

Безпосередньо з використанням людського обличчя шаблони, які витягуються з зображень, для розпізнавання особи мають кілька недоліків. Перш за все, кожен патч часто охоплює понад 1000 пікселів, що є досить великим розміром для побудови жорсткої системи розпізнавання. По-друге, обличчя може бути візуально видозмінено за рахунок різних факторів.

Таким чином, виконується вилучення ознак, щоб уникнути цих недоліків, а також виконується компонування інформації, зменшення розмірів, вилучення відмінностей і очищення шуму. Вилучення ознак також називається зменшенням розмірності і часто здійснюється за допомогою принципу аналізу компонентів (PCA).

Класифікація. Після завершення вилучення ознак наступним кроком є вибір підмножини вилучених ознак, що, як правило, здійснюється методом класифікації. На цьому етапі розглядається вся можлива підмножина витягнутих ознак і вибирається та, яка виконує функцію критерію. На цьому етапі зображення класифікується за допомогою відповідного класифікатора. Наявність алгоритмів розпізнавання облич використовує широкий спектр методів класифікації. Іноді два або більше класифікаторів об'єднуються для досягнення кращих результатів. З іншого боку, більшість алгоритмів на основі моделей відповідають зразкам з моделлю або шаблоном. Потім, метод навчання може бути використаний для поліпшення алгоритму. Як правило, алгоритм класифікації має декілька видів навчання, а саме, без вчителя і з вчителем. Іноді нове придбання міток може бути неможливим. Таким чином, необхідне напів-контрольоване навчання. Остаточний результат після класифікації потім узгоджується з шаблоном або зображенням, що зберігається в базі даних, за допомогою алгоритму зіставлення. Алгоритм відповідності порівнює новий біометричний шаблон з одним або кількома шаблонами, що зберігаються в базі даних. Нарешті, процес прийняття рішення (або автоматизований, або з участю людини) використовує результати з відповідного модуля для прийняття рішень на рівні системи. Якщо збіг підтверджено, то особі надається доступ.

Модель архітектури IoT

Вище була представлена архітектура рівнів IoT, яка є найбільш поширеною. Нижче приведена покращена модель архітектури системи IoT (Рис.3.15) з описом особливостей кожного з них [62].

Перш за все, зазначимо, що наша модель складатиметься з шести шарів, а саме:

1. Рівень кодування;
2. Рівень обробки;
3. Мережевий рівень;
4. Рівень проміжного ПЗ;
5. Рівень додатків;
6. Рівень бізнес-логіки.

Рисунок 3.15 – Рівні архітектури IoT

1. Рівень кодування.

Рівень кодування є першим шаром в моделі архітектури IoT і забезпечує процес ідентифікації для кожного його інтелектуального елементу. Кожному пристрою присвоюється унікальний ідентифікатор, який відрізняє кожен пристрій.

2. Рівень обробки.

Основним обладнанням на рівні обробки є радіочастотний ідентифікаційний пристрій (RFID), бездротова мережа датчиків (WSN), всі види датчиків, GPS, Bluetooth і т.д. . Основними функціями шару обробки є

збір даних з різних фізичних пристроїв і перетворення даних в цифровий сигнал. Потім рівень обробки передає дані на мережевий рівень.

3. Мережевий рівень.

Основним обладнанням цього рівня є мережа мобільного зв'язку, Інтернет та будь-який інший спосіб зв'язку. Цей шар отримує всю інформацію з шару обробки і передає дані до шару проміжного ПЗ через середовища передачі, такі як Wi-Fi, Bluetooth, WiMAX, ZigBee, GSM, 3G і 4G, використовуючи протоколи зв'язку, такі як IPv4, IPv6, MQTT і DDS . Мережевий рівень відповідає за обробку, управління та обслуговування даних.

4. Рівень проміжного ПЗ.

Рівень проміжного програмного забезпечення отримує величезну кількість інформації з мережевого рівня і обробляє дані, використовуючи деякі інтелектуальні системи обробки, такі як хмарні обчислення, щоб забезпечити прямий доступ до бази даних та зберігання всієї інформації в хмарі. Функціонування цього рівня базується на сервісно-орієнтованій архітектурі (Service Oriented Architecture, SOA) – шаблон програмного забезпечення, модульний підхід до розробки програмного забезпечення, заснований на використанні розподілених, слабко пов'язаних замінних компонентів, оснащених стандартизованими інтерфейсами для взаємодії за стандартизованими протоколами. Головна функція програмного забезпечення на цьому етапі полягає в тому, щоб доставити всі функції системи до кінцевих користувачів. Процес створення сервісу надає функції кожному смарт-об'єкту і управляє ними. Процес абстракції об'єктів відповідає за обмін інформацією між різними об'єктами "спільною для них мовою". Для захисту обмінюваних даних використовується процес управління довірою, конфіденційністю та безпекою.

5. Рівень додатків.

Прикладний рівень використовує оброблені дані для подальшої роботи багатьох програм. Програмні додатки IoT базуються на потребах

користувачів в таких областях як промисловість, освіта, медичний сектор та комунікації. Прикладний рівень використовує різну кількість протоколів, такі як протокол обмеженого застосування (CoAP), спрощений мережевий протокол, що працює на TCP/IP (MQTT), відкритий стандарт протоколу прикладного рівня для проміжного програмного забезпечення, орієнтованого на обробку повідомлень (AMQP), а також протокол XMPP - відкритий мережевий протокол для швидкого обміну повідомленнями та інформацією про присутність між користувачами мережі Інтернет.

6. Бізнес-рівень.

Бізнес-рівень – це останній шар архітектури IoT. Він відповідає за управління додатками та послугами системи IoT. Бізнес-шар використовується для створення різних моделей, які використовуються для задоволення різних потреб.

3.2 Класифікація рівнів архітектури та відповідних засобів безпеки IoT

Архітектура безпеки IoT складається з трьох основних шарів, які можна класифікувати за рівнями обробки, мережі та прикладного рівнів. Кожен шар має свої компоненти, стандарти зв’язку та протоколи. Шари безпеки IoT забезпечують різні протоколи безпеки, послуги та механізми безпеки для посилення загального захисту системи IoT. Наступний рисунок показує архітектуру шару безпеки IoT. У наступних розділах відображаються компоненти, функції, загальні атаки, проблеми та міра безпеки кожного шару безпеки. Тому ми сформулюємо проблеми, різні типи атак і деякі рішення безпеки кожного шару IoT. На рисунку 3.16 представлені атаки і контрзаходи на кожному шарі безпеки IoT.

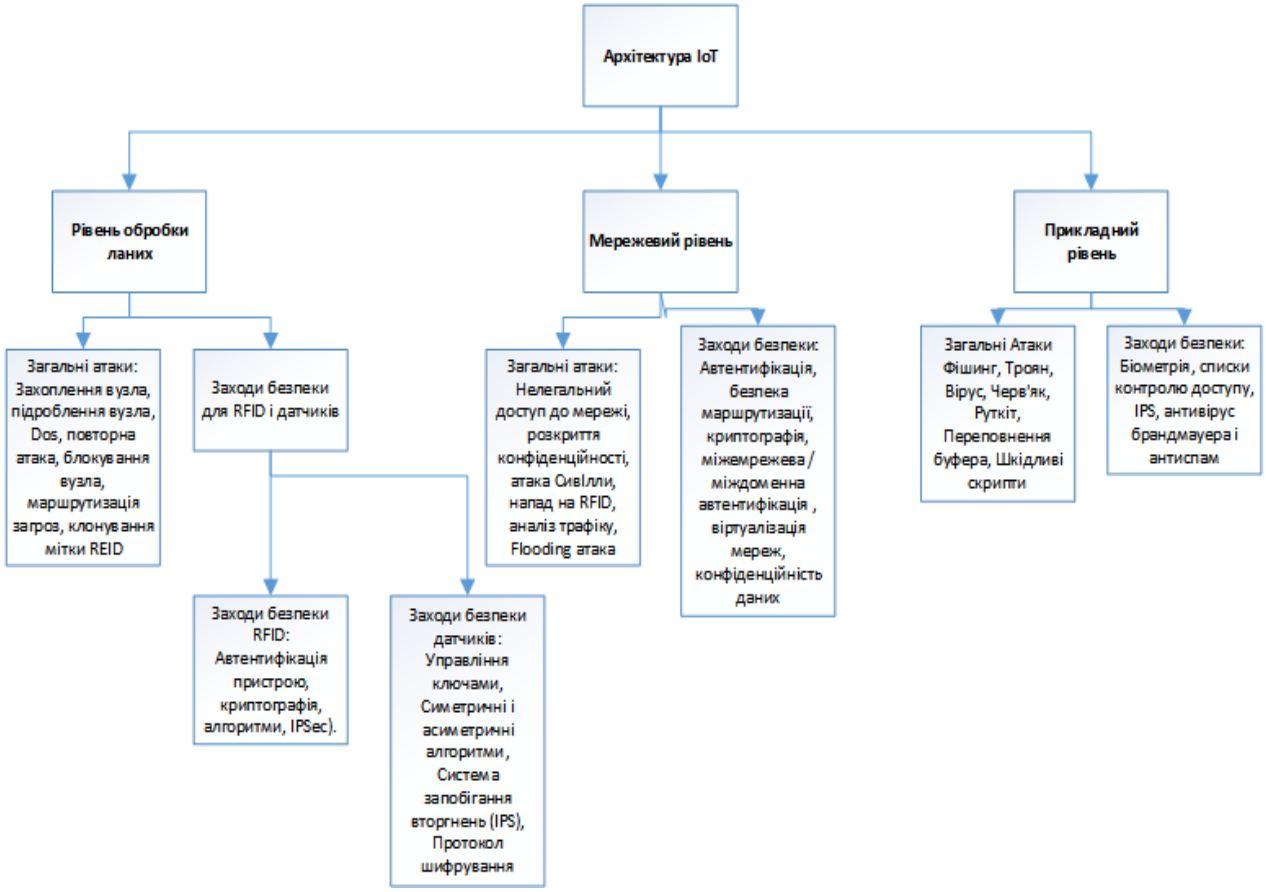


Рисунок 3.16 – Атаки та заходи безпеки на кожному шарі безпеки IoT

Рисунок показує компонент і функції кожного шару безпеки IoT. Він відображає атаки, проблеми та вимоги безпеки, які потрібні для кожного шару. Більш того, таблиця ілюструє багато методів безпеки для вирішення проблем безпеки в системі IoT.

Що стосується вимог безпеки, вони гарантують високий рівень системи для мережі IoT і підвищують продуктивність мережі. Далі будуть розглянути атаки та найпоширеніші категорії проблем для кожного шару та описана необхідна міра безпеки.

Таблиця 3.3. Специфіка основних рівнів безпеки та методи їх захисту

Рівень	Компоненти	Функції	Атаки/проблеми/ слабкі місця	Методи/Механізми безпеки
Рівень обробки	Усі типи датчиків,	Використову-ється для	Захоплення вузлів, підробка	Алгоритми хешування, криптографічні алгоритми,

даних	RFID, GPS, Bluetooth	зв’язку різних смарт-пристроїв в IoT, збору інформації та передачі даних на мережевий рівень	вузлів, відмова в обслуговуванні (Dos), Replay Attack, блокування вузлів, загрози маршрутизації, клонування міток RFID тощо	контроль доступу, IPSec, Керування ключами (PKI), система запобігання вторгнень, протокол шифрування, оцінка ризиків
Мережевий рівень	Стільниковий зв’язок та Інтернет	Він використовується для передачі інформації	Атаки: викрадення сеансів, Sybil, RFID Spoofing, аналіз трафіку та Flooding-атаки. Проблеми: сумісність, безпека кластерів, незаконна мережа доступу та розкриття конфіденційності	End to End authentication (автентифікація від одного кінця до іншого) безпечна маршрутизація, алгоритми криптографії, автентифікація між мережами/доменами, технологія мережевої віртуалізації, конфіденційність даних і цілісність для виправлення та контролю помилок.
Прикладний рівень	Розумний зв’язок (правильно підібраний тип зв’язку)	Він використову-ється для надання багатьох послуг та аналізу інформації	Дозвіл на доступ до даних/Захист і відновлення даних/Можливість виправлення вразливостей програмного забезпечення	Біометрія, списки контролю доступу (ACL), IPS, Антивіруси, Антиспами і Firewall.

Рівень обробки даних

Отже, дані збираються з різних пристроїв і передаються через бездротову мережу. Вони перетворюються на сигнали, які піддаються багатьом видам загроз. Зловмисники можуть легко отримати доступ, контролювати та знищувати дані або обладнання.

Типи атак на рівні обробки. Як згадувалося вище, основними компонентами шару обробки є RFID і WSN, тому далі у цьому пункті увага буде зосереджена на спільних атаках у WSN, RFID і деяких ефективних атаках на цьому рівні, як показано на рисунку 3.16.

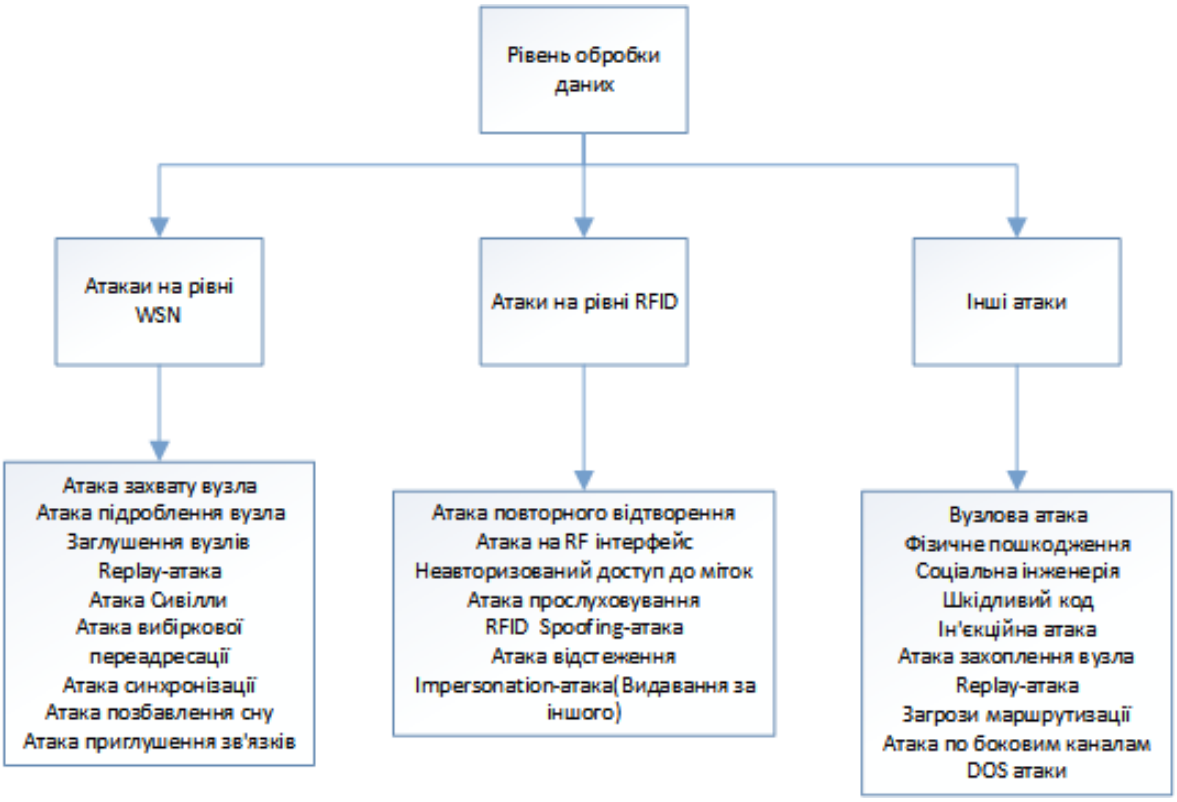


Рисунок 3.16 – Атаки рівня обробки даних

Напади і загрози рівня обробки можуть бути класифіковані на атаки WSN, атаки RFID і решта розповсюджених атак цього шару.

- Атака захоплення вузла. Цей тип атаки може знищити WSN або сенсорний вузол, посилаючи або отримуючи дані для доступу та змінюючи конфіденційну інформацію. Атаки такого типу можуть керувати ключовими вузлами або шлюзовими вузлами. Ця атака може призвести до витоку інформації і тим самим створити загрозу для всієї мережі.
- Fake Node Attack. Зловмисник додає або впроваджує до існуючого підроблений вузол до системи IoT. Тоді зловмисник додає фальшивий

код або дані в мережу IoT. Цей тип атаки може зупинити передачу даних або взагалі знищити мережу.

- Атака Сивілли (Sybil attack). Це відома атака в WSN. Вид атаки в одноранговій мережі, в результаті якої жертва підключається тільки до вузлів, контрольованих зловмисником.
- Повторна атака. Мета цієї атаки – розірвати процес автентифікації для дійсного користувача. Сценарій цієї атаки полягає в тому, що зловмисник посилає велику кількість повідомлень, які були отримані хостом призначення. Таким чином, зловмисник може змінювати або відтворювати вузол, підробляючи інформацію користувачів.
- Dropping Attack. Це найнебезпечніша атака в WSN, яка використовує два способи; вибіркова переадресація та синхронізація атак. Що стосується селективної атаки переадресації, зловмисник вибирає деякі пакети і пересилає їх в мережу зловмисників і видаляє інші пакети для досягнення своєї зловмисної мети. Таким чином, деякі вузли не можуть пересилати пакети. Що стосується атак синхронізації, “атаки синхронізації мають намір розширити свої слоти протоколів MAC і поширити їх на інші вузли”. Атака “Позбавлення сну”. У цій атаці зловмисник споживає енергію роботи вузла датчика, що робить його увесь час недоступним. Ця атака впливає на роботу системи і послуг IoT.
- Атака приглушення зв’язків (Link Layer Jamming Attack) Мета цієї атаки – передбачити отримані пакети за допомогою протоколу MAC у WSN. Ця атака фокусується на сигналі передачі вузлів WSN.
- RF-інтерфейс для атаки на RFID. Ця атака залежить від атаки DoS, щоб використовувати шумовий сигнал і передати його через радіочастотний сигнал. Це призводить до припинення обміну повідомленнями між пристроями.

• Несанкціонований доступ до атаки міток.

Метою несанкціонованого доступу до атаки тегів є розрив процесу автентифікації, для отримання доступ до мітки RFID. Зловмисник може читати, змінювати або видаляти дані.

Атаки клонування міток. Зловмисник може створити клоновану мітку, щоб користувач не міг розрізняти оригінальну мітку від підробленої. Згодом користувач може надсилати або отримувати фальшиву інформацію, а зловмисник може отримати справжню, щоб бути автентифікованим користувачем.

Повторна атака. Метою цієї атаки є те, що зловмисник може отримувати дані і записувати дані на карту атаки за допомогою мікропроцесорів. У цьому випадку зловмисник увійти до системи доступу. Потім зловмисник стає авторизованим користувачем і отримує доступ до даних або змінює їх.

Атака прослуховування RFID. Зловмисник може легко підслуховувати дані від мітки до користувача або навпаки, щоб порушити конфіденційність і отримати всю інформацію. Характеристики атаки підслуховування RFID такі ж, що і у WSN-атаки підслуховування, оскільки RFID має ті ж характеристики, що і WSN.

RFID Spoofing Attack. Ідея цієї атаки полягає в тому, що зловмисник може поширювати неправильні дані до системи RFID, а остання вважатиме що це оригінальні дані. Відправник і приймач мають справу з неправильними даними, тому зловмисник може отримати доступ до даних і керувати мережею.

Атака відстеження. Це небезпечна атака, оскільки зловмисник може зчитати мітки RFID або особисту інформацію. Метою відстеження атаки є збір інформації про мережу IoT за допомогою інструментів сканування портів.

Атака підміни (Impersonation Attack). Зловмисник може виявити пристрій у мережі та видати себе за особу користувача. Тоді зловмисник генерує пакети, які містять конфіденційну інформацію або характеристики

пристрою. Мета цієї атаки - змінити інформацію RFID. Цей процес відомий як перехоплення або фальшива законна ідентичність. Така атака призводить до розкриття інформації.

Атака на вузол. Цей тип атаки може пошкодити датчик вузла, посилаючи і отримуючи дані в або з системи IoT, щоб отримати доступ і контролювати всю важливу інформацію.

Атака ін'єкції шкідливого коду. Зловмисник може виконувати свої завдання за допомогою атаки MIM (Man in the middle) і впровадити себе між двома вузлами. Зловмисник може ввести шкідливий код у вузол, щоб отримати доступ до системи та керувати або пошкодити дані.

Атака фізичного ушкодження. Метою цієї атаки є пошкодження та знищення мережі IoT. Зловмисник може маніпулювати та використовувати пристрої мережі IoT, щоб пошкодити систему безпеки та службу.

Атака соціальної інженерії. Зловмисник використовує користувачів мережі IoT для отримання приватної інформації за допомогою інструментів підслуховування.

Атака шифрування. Існує три типи атак шифрування, які можна класифікувати як атаку тимчасової атаки і атаку бічного каналу.

Timing-атака. Може бути реалізований шляхом аналізу часу алгоритму шифрування, необхідного для реалізації механізму шифрування. Мета цієї атаки - отримати шифрування ключа.

Атака по стороннім каналам. Атака сторінніми каналами використовує інформацію про фізичні процеси у пристрої, які не розглядаються у теоретичному описі криптографічного алгоритму. Деякі атаки сторонніми каналами вимагають знання внутрішніх дій системи на якій втілено алгоритм, інші, такі як диференційний аналіз енерговикористання, дієві як атаки на чорний ящик. Найпотужніші атаки сторонніми каналами покладаються на статистичні методи Пола Кохера. Серйозними наслідками цього нападу є витрачання часу та енергії, а також витік інформації.

Загрози маршрутизації. Вони реалізуються шляхом повторної передачі інформації про маршрут даних і створення петлі маршрутизації.

Ця атака викликає наступні пошкодження:

1. Контроль і блокування передачі мережі.

2. За рахунок збільшення помилки повідомлень буде розширюватись шлях мережі.

3. Збільшення затримки з кінця до кінця.

• DoS-атака. Це широковідома загроза не лише в мережі IoT, що призводить до втрати мережевих ресурсів або послуг і займає пропускну здатність. Атака DoS була детально розглянута в попередньому розділі.

Заходи безпеки рівня обробки

У попередньому розділі обговорювалися різні типи загроз і атак в WSN, RFID і найпоширеніші атаки на рівні обробки. Заходи безпеки необхідні для підвищення рівня безпеки системи IoT. Міри безпеки повинні гарантувати низьке енергоспоживання та швидкодію. Міра безпеки для шару обробки даних поділяється на дві частини: заходи безпеки для WSN і заходи безпеки для RFID. Таблиці 4.2 і 4.3 показують порівняння між заходами безпеки для WSN і RFID, для того, щоб зробити логічний висновок і вибрати найбільш підходящий механізм безпеки для них. У таблицях 4.2 і 4.3 представлено, що кожен механізм безпеки реалізує необхідні вимоги безпеки і запобігає атакам. Крім того, в наступній таблиці показано переваги та недоліки методів безпеки.

Таблиця 3.4 – Методи безпеки для WSN

Методи безпеки WSN	**Корисність використання**	**Тип атаки, якої можна уникнути таким способом**	**Переваги**	**Недоліки**

Управління ключами	Він використовується для забезпечення генерування ключів та оновлення алгоритмів безпечного використанням розподілу ключів, наприклад інфраструктура відкритого ключа (PKI), яка створює відкриті ключі цифрової сертифікації.	Модифікація даних, атака Сивілли, прослуховування and spoofing атаки	Ці механізми безпеки легко реалізувати	Цей метод потребує значних витрат часу.
Алгоритми захисту ключів	Для системи IoT використовуються алгоритми симетричних і асиметричних ключів. Існує багато симетричних алгоритмів, таких як RC5 і асиметричні алгоритми, такі як AES.	Атака повторення, прослуховування, аналіз трафіку, spoofing.	Алгоритми симетричних ключів забезпечують менше споживання енергії, вартість і час роботи вузлів.	Алгоритми асиметричного ключа споживають більше енергії та часу
Протокол безпеки маршрутизації	Існує багато алгоритмів маршрутизації безпеки, таких як поєднання даних, багаторівнева маршрутизація механізми шифрування.. Протокол безпечного шифрування мереж (SNEP) широко використовується для WSN, який забезпечує мультиточкову широкомовну автентифікацію.	Загрози маршрутизації	SNEP потребує менше витрат часу.	Більшість алгоритмів протоколу безпеки маршрутизації потребують енергії та часу.

Автентифікація та контроль доступу	Метод автентифікації заснований на технології відкритого ключа, тобто використовується спільний ключ і хеш-функція. Контроль доступу заснований на асиметричній і симетричній криптосистемі. Необхідно забезпечити високу швидкість процесора і пам’ять	Атака захоплення вузла, Сивілли, прослуховування	Легка технологія автентифікації відкритого ключа споживає менше енергії	Традиційні механізми автентифікації та контролю доступу не застосовуються до системи IoT
Система виявлення та попередження вторгнень IDS/IPS	є технологією запобігання загрози мережі, яка аналізує мережевий трафік потоки для виявлення і запобігання експлойтів вразливості. Вона використовується для виявлення і запобігання більшості підозрілих користувачів і атак	Більшість атак та загроз	IPS використовується для виявлення та запобігання атак і загроз. IDS використовується для автоматичної зупинки атак	IDS вимагає визначення політики безпеки, щоб гарантувати, що загрози та атаки обробляються відповідно до рекомендацій корпоративної політики безпеки

Методи безпеки для RFID. Другим важливим пристроєм в шарі сприйняття є RFID. Заходи безпеки RFID є найважливішим питанням для забезпечення конфіденційності, цілісності, доступності, приватності та

автентифікації. Таблиця 3.4 показує заходи безпеки для RFID разом з перевагами та недоліками.

Таблиця 3.5 – Заходи безпеки для RFID

Метод безпеки для RFID	**Корисність використання**	**Тип атаки, якої можна уникнути таким способом**	**Переваги**	**Недоліки**
Контроль доступу	Він використовується для захисту конфіденційних даних користувачів і захисту всієї інформації з міток RFID. Він використовується для прогнозування несанкціонованого доступу до тегів.	Прослуховування, неавторизований доступ до міток, spoofing, підробка даних	Цей спосіб є корисним для захисту датчиків і аналізу антен.	Контроль доступу може витрачати більше часу
Шифрування даних	Це найбільш істотний метод шифрування сигналу RFID і даних RFID.	RF interface on RFID, replay, RFID прослуховування та spoofing атака	Він використовує менше обчислювальної потужності і досягає високого рівня безпеки	Шифрування даних може витрачати більше часу
Безпека IP	Він пропонує два	Прослуховуван	Він	IPSec може

механізму (IPSec)	рівні техніки безпеки, які є механізмами автентифікації та шифрування. Механізм автентифікації: він використовується для ідентифікації ідентифікації користувача. Механізм шифрування: він використовується для шифрування даних і сигналу RFID.	ня, spoofing, підробка даних та атака клонування міток	гарантує більш безпечні дані і сигнали RFID .	витрачати більше часу та потужностей
Технологія криптографії	Він заснований на хеш-функції та алгоритмах шифрування. Він використовується для захисту сигналу RFID	RFID-прослуховування, RFID-spoofing, клонування міток, RF interface on RFID і атаки маршрутизації	Вона захищає протоколи зв'язку	IPSec може витрачати більше часу та потужностей

Таблиці 3.4 і 3.5 показують порівняння між механізмами безпеки WSN і RFID для вибору відповідних заходів безпеки для передачі даних і сигналів для забезпечення конфіденційності, автентифікації та цілісності. Ці таблиці використовуються для вибору алгоритмів безпеки, які гарантують безпечну передачу даних і шифрують сигнали з низьким споживанням енергії і часу. Кожен метод передачі WSN і RFID забезпечує вимоги безпеки для

отримання високої продуктивності. Крім того, в таблицях 3.4 і 3.5 показано переваги і недоліки заходів безпеки для розробки механізмів безпеки. Більш того, в цих таблицях пояснюється, яким атакам можна запобігти застосовуючи той чи інший метод.

Існують також інші способи захисту для рівня оброки, які описано нижче.

Безпечне завантаження. Криптографічні хеш-алгоритми використовуються для перевірки пристроїв і програмного забезпечення Інтернету за допомогою цифрового підпису. Цей механізм безпеки не підходить для системи IoT, оскільки потребує значної потужності та часу.

Анонімність (Anonymity)

Анонімність є найкращим рішенням для мережі IoT для захисту особистої інформації користувачів. Недоліком анонімності є те, що воно потребує значно більшої обробної потужності.

Оцінка ризиків.

Це важливий метод захисту мережі IoT і запобігання багатьом загрозам і атакам. Оцінка ризику є найважливішим методом для мережі IoT, оскільки вона здатна виявити будь-які помилки в системі безпеки. Вона має можливість виявляти будь-які загрози та атаки в пристроях IoT з використанням багатьох методів, таких як IPS. Оцінка ризиків передбачає багато механізмів безпеки, які є відповідними методами для природи середовища IoT. Механізми безпеки повинні забезпечувати низьке споживання енергії і часу для досягнення високої продуктивності мережі IoT. Отже, методи безпеки повинні модифікуватися, поліпшуватися і вдосконалюватися, щоб бути зручними алгоритмами для інтелектуальних об’єктів системи IoT.

Мережевий рівень. Як згадувалось раніше, основним обладнанням мережевого рівня є мережа стільникового зв’язку та Інтернет. Мережевий рівень має справу з даними, середовищами передачі і протоколами зв’язку. Він є “підходящим полем” для багатьох загроз, атак і проблем.

Атаки і проблеми мережевого рівня. На мережевому рівні зловмисник намагається отримати доступ до інформації, що передається, середах передачі і протоколам зв'язку. Мета зловмисника – знищити конфіденційність і цілісність. У наступних розділах будуть пояснені проблеми мережевого рівня. На рисунку 3.17 показані класифікація атак і проблем мережевого рівня.

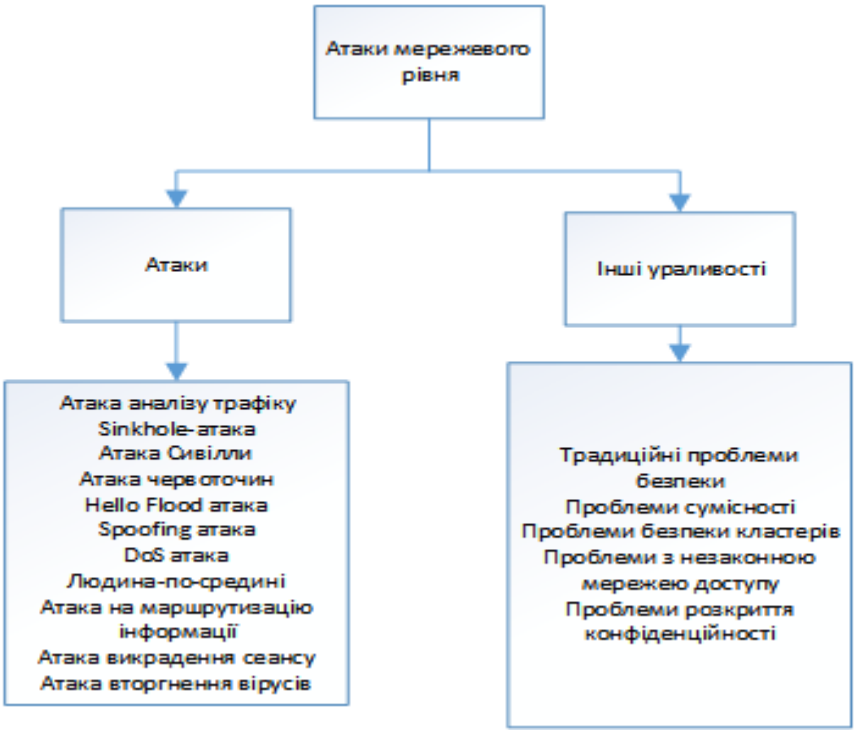


Рисунок 3.17 – Класифікація атак і проблем мережевого рівня

Цей пункт поділено на дві частини: атаки мережевого рівня і проблеми мережевого рівня.

1. Атаки мережевого рівня.

На мережевому рівні існує безліч атак, які завдають шкоди переданих даним, середах передачі і протоколам. У наступних розділах показані різні типи атак.

- Атака аналізу трафіку. Сценарій цієї атаки полягає в тому, що зловмисник намагається отримати більше інформації про користувачів і мережу за допомогою деяких інструментів, таких як сканування портів і атаки з використанням сніффінгу.

- Атака воронки. Атакуючий використовує будь-який слабкий вузол і контролює його. У такий спосіб можна заборонити передавати будь-які пакети і зупинити передачу даних. Таким чином, атака може призвести до відмови в онлайн службах, але використовувати енергію і час. Цей вид атаки призводить до DoS-атаки, яка є дуже небезпечною для IoT.
- Атака Сивілли. Цей тип атаки дуже небезпечний, особливо для WSN. вид атаки в одноранговій мережі, в результаті якої жертва підключається тільки до вузлів, контрольованих зловмисником.
- Атака червоточини (Wormhole Attack). Ця атака імітує маршрут, коротший, ніж справжній; це може збити з пантелику механізми маршрутизації, засновані на знанні відстані між вузлами. •Зазвичай має один або кілька шкідливих вузлів і тунель між ними. Атакуючий вузол захоплює пакети з одного пункту і передає їх іншому віддаленому вузлу, який розподіляє їх локально. Атака червоточини може бути легко запущена зловмисником без знання мережі або злому будь-яких законних вузлів та криптографічних механізмів.
- Hello Flood Attack- дуже ризикована атака в мережі IoT. Деякі протоколи маршрутизації в WSN вимагають, щоб вузли передавали Hello-запити, щоб оголосити себе своїм “сусідами”. Зловмисник може відправити велику кількість повідомлень від шкідливого вузла на безліч вузлів в мережі IoT. Ця атака викликає заклинювання трафіку і блокує канал зв’язку.
- Підтвердження спуфінгової атаки. Атака з підміною підтвердження використовується для атаки з селективної переадресацією для управління будь-яким вузлом в мережі IoT для досягнення мети зловмисників. Таким чином відбувається втрата великої кількості пакетів.
- DOS атаки. Зловмисник відправляє велику кількість повідомлень або пакетів в мережу, щоб зробити мережеві ресурси і служби

недоступними. Це також призводить до завантаження смуги пропускання, перевантаження системи і запобігання більшості законних запитів від автентифікованих і авторизованих користувачів.

- Атака сховища. Всі користувачі в системі IoT мають змогу зберігати свою особисту інформацію на різних пристроях або в хмарах. Тому багато атак використовують ці пристрої для отримання доступу і контролю даних.
- Впровадження атаки підробки інформації. У цій атаці зловмисник може маніпулювати одним вузлом в WSN і впроваджувати шкідливу інформацію в мережу IoT. Отже, зловмисник може отримати доступ до мережі і отримати повний контроль над мережею IoT.
- Атака “Людина посередині”. Як згадувалося вище, зловмисник поміщає себе між двома сенсорними вузлами і підслуховує всю інформацію, щоб отримати доступ до інформації з двох сенсорних вузлів. Метою цього нападу є використання каналу зв’язку або протоколу для порушення конфіденційності і приватності.
- Інформаційна атака маршрутизації. Мета інформаційної атаки маршрутизації полягає в тому, щоб підробити і змінити інформацію маршрутизації. Ця атака викликає багато проблем, таких як відправка помилкових повідомлень, відкидання мережевого трафіку і створення помилкової петлі маршрутизації, щоб пошкодити мережу IoT.
- Атака викрадення сесії.Зловмисник намагається вкрасти сеанс між двома вузлами, щоб отримати доступ і контролювати всю інформацію користувачів і мережі.
- RFID спуфінг атака.Ця атака завдає шкоди RFID-сигналам. Зловмисник перехоплює дані, що передаються, використовуючи неправдиві RFID-сигнали, і перевіряє їх справжність. Зловмисник використовує ці сигнали для передачі шкідливих даних, які вважаються надійними.

2. Проблеми мережевого рівня.

Мережевий рівень страждає від багатьох проблем, які викликають псування трафіку, перевантаження мережі і розкриття конфіденційності

- Звичайні проблеми безпеки. Мережа IoT страждає від загальних проблем безпеки, таких як перехоплення, DoS, “людина посередині”, перехоплення сеансів, вторгнення вірусів і незаконного доступ до мережі, які завдають шкоди конфіденційності і цілісності.
- Проблема сумісності. Як згадано вище, IoT включає в себе пристрої різного роду, тому існують методи множинного доступу. Через цю неоднорідність природи система безпеки і мережі є слабкою. Ця проблема призводить до того, що мережа IoT схильна до безлічі різних атак і вразливостей.
- Розкриття конфіденційності. Розкриття конфіденційності є найбільшою проблемою в системі IoT. Зловмисник може захопити або вкрасти особисті дані користувачів (напр. IP-адреса, місце розташування і т.д.) За допомогою соціальної інженерії, прослуховування і сніфінгу.
- Проблема безпеки кластера. Проблема безпеки кластера є основною проблемою на мережевому рівні, оскільки в мережі IoT є велика кількість пристроїв. Кожен пристрій генерує дані. Таким чином, всі пристрої відправляють величезну кількість даних. Це призводить до використання великого обсягу трафіку даних, який спричиняє перевантаження мережі і блокує мережевий трафік.
- Заходи безпеки мережевого рівня

Заходи безпеки мережевого рівня концентруються на досягненні двох основних вимог безпеки – конфіденційності і цілісності даних. Заходи безпеки мережевого рівня вказують на відповідні механізми безпеки для досягнення вимог безпеки і запобігання атак. У таблиці 3.6 наведені різні методи безпеки мережевого рівня.

Таблиця 3.6 – Методи безпеки мережевого рівня

Метод безпеки	**Корисність використання**	**Тип атаки, якої можна уникнути таким способом**	**Переваги**	**Недоліки методу**
Наскрізне шифрування та управління ключами.	Всі вузли в мережі IoT повинні проходити перевірку автентичності з використанням механізму перевірки достовірності, інфраструктури відкритих ключів та наскрізного шифрування.	Нелегальний доступ до вузлів, DoS і атаки в Sinkhole.	Він забезпечує наскрізну автентифікацію і шифрування.	Це важкий метод безпеки.
Безпека маршрутизації. (Security Aware and Routing).	Наступним кроком заходів безпеки мережевого рівня є безпечна маршрутизація, яка відбувається після процесу автентифікації. Механізми безпеки маршрутизації важливі для захисту даних і збереження конфіденційності даних.	Більшість загроз і атак.	Він забезпечує багатопроменеве поширення для маршрутизації даних і розширює можливості системи по виявленню будь-яких помилок в системі.	Цей метод потребує значної кількості часу опрацювання.
Система криптографії	Вона використовується для перевірки передачі даних через інші вузли і виявлення будь-якої помилки в мережі.	Запобігає підроблення даних на прийнятому вузлі.	Вона може виявити мережеву помилку і перевірити дані. Криптографія з симетричним ключем	Асиметрична криптографія потребує потужність і час.

			потребує мало енергії і часу.	
Автентифікація крос-мережі та домену	Для захисту протоколів використовується автентифікація між двома мережами. Для захисту DNS використовується автентифікація між доменами.	Загрози маршрутизації.	Використовується для захисту мережевих протоколів.	Він потребує більше енергії.
Технологія віртуалізації мережі	1. Це процес об’єднання апаратних і програмних ресурсів і мережевих функцій в одну або віртуальну мережу. 2. Існує два типи віртуальної мережі: зовнішня і внутрішня віртуалізація. 3. Зовнішня віртуалізація об’єднує безліч мережевих частин у віртуальний пристрій – LAN для підвищення точності мережі і ефективності даних. 4. Внутрішня віртуалізація забезпечує мережеву функціональність програмного забезпечення на одному мережевому сервері.	Більшість мережевих атак.	Вона використовується для зменшення складності управління мережею	Цей метод потребує значної кількості часу опрацювання.
Метод перевірки цілісності та	Він використовується для виявлення і контролю будь-якої	Незаконний доступ і підробка	Він використовується для	Цей метод потребує

конфіденційності даних	помилки, яка відбувається в мережі. Цілісність даних використовує алгоритми шифрування для перевірки вихідних даних, які відправляються на сторону одержувача.	(спуфінг)	перевірки вихідних даних	значної кількості часу опрацювання.
Виявлення флуду (Flooding)	Ідея цього методу полягає в тому, що відправник надсилає hello-запит одержувачу, яке використовується для перевірки якості сигналу. Якщо цей сигнал схожий на поодинокі в діапазоні радіо, приймач приймає повідомлення	Флуд атака	Використовує для перевірки справжності сигналу.	Потребує затрат часу

Поширені проблеми і атаки прикладного рівня

Далі будуть представлені різні атаки і проблеми прикладного рівня.

- Права доступу до даних. Існує велика кількість користувачів, що використовують різні додатки. Тому існує безліч дірок для вразливостей програмного забезпечення, таких як атаки шифрування, спам і шкідливі програми.
- Захист і відновлення даних. Механізми захисту та обробки даних недостатні для запобігання втрати і пошкодження даних. Тому мережі IoT потрібна система управління вузлами.
- Здатність працювати з великою кількістю даних і вразливим прикладним програмним забезпеченням. Існують перерви в роботі

мережі і втрата даних через великої кількості вузлів, величезного обсягу передачі даних і складного середовища.

- Вразливості прикладного програмного забезпечення. Існує багато вразливостей програмного забезпечення, таких як фішинг, трояни, віруси, черв'яки, руткіти, переповнення буфера, шкідливі скрипти.

Заходи безпеки на рівні додатків

Існують дві основні методи безпеки прикладного рівня: біометрія і списки контролю доступу (ACL). Біометрія забезпечує захист інформації і запобігає внутрішнім і зовнішнім атакам (більш детально було описано в попередніх розділах роботи). Списки ACL можуть встановлювати ролі, щоб пропускати запити автентифікованих і авторизованих користувачів і отримати доступ до мережі. ACL можуть відстежувати і контролювати мережевий трафік. Інструментами заходів безпеки є IPS, антивірус і антиспам і брандмауер.

З проведеного вище аналізу по реалізації безпеки рівнів архітектури IoT ми можемо визначити рішення з безпеки для IoT, яке коротко викладено нижче:

1. Безпека мережі IoT з використанням брандмауера, IPS і т.д.
2. Автентифікація з використанням цифрового підпису і біометрії.
3. Захист зв'язку з використанням автентифікації і шифрування PKI.
4. Реалізація безпеки виконання коду з використанням криптографічних алгоритмів і програмних засобів.
5. Забезпечення належного зберігання даних з використанням шифрування та авторизації.
6. Підвищення обізнаності про безпеку.

Повертаючись до попередніх порівнянь, представленим в цьому дослідженні, тепер можна зібрати запропоновану модель управління безпекою для мережі IoT.

3.3. Проектування нової моделі архітектури IoT

Метою створення моделі є представлення системи управління безпекою мережі IoT, для зменшення часу обробки даних і та за допомогою невеликих потужностей забезпечити відповідні механізми достатні для кожного з рівнів безпеки IoT. Запропонована модель допомагає дослідникам і розробникам вибирати зручні протоколи і механізми безпеки кожного рівня безпеки для захисту даних і інтелектуальних об’єктів. Така модель використовується для максимального запобігання або зменшення атак, загроз і проблем. Цілі запропонованої моделі можуть бути представлені таким чином:

У ній представлено уточнююче дослідження щодо вибору відповідних механізмів безпеки для необхідних рівнів безпеки IoT і роз’яснюються переваги і недоліки методів безпеки.

Модель забезпечує вимоги безпеки, такі як контроль доступу, управління маршрутизацією, автентифікація, конфіденційність і цілісність для кожного рівня безпеки.

Гарантує безпеку декількох додатків.

Вона забезпечує надійні функції для кожного смарт-об’єкта в IoT, IDS/IPS і відновленні безпеки.

Представлена далі модель виявляє і запобігає більшості загроз і атак; захищає особисту інформацію користувачів; виявляє будь-яку помилку при передачі даних.

У запропонованій моделі ми використовуємо платформу Things Board, яка надає безліч механізмів безпеки. Ми можемо управляти стратегією

вибору алгоритмів безпеки для досягнення високого рівня вимог безпеки і зниження енергоспоживання і часу.

Наша модель складається з трьох частин.

Перша частина – це рівні безпеки IoT, які представляють собою рівні обробки, мережі і додатків.

На другій частині представлені протоколи безпеки і механізми рівня безпеки IoT.

Третя частина містить сервери баз даних, які використовуються для кожного рівня безпеки IoT для зберігання всієї інформації про механізми безпеки. Сервери баз даних корисні для адміністратора і користувачів для збереження лог-файлів методів безпеки і користувачів.

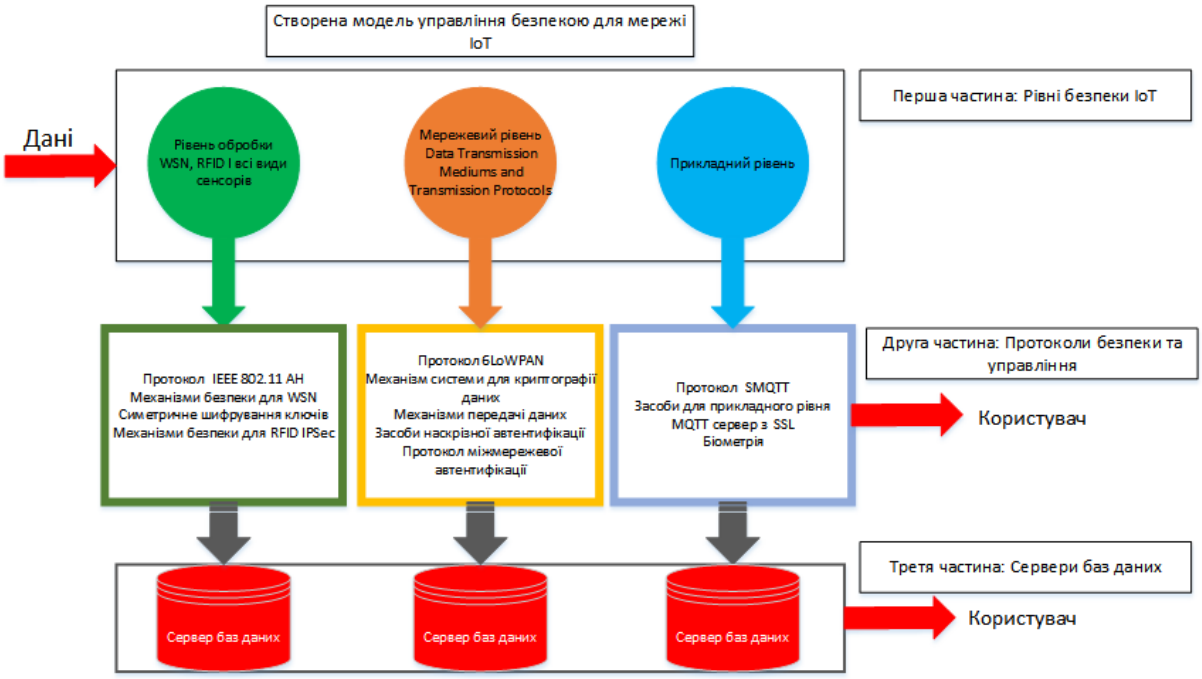


Рисунок 3.18 – Створена модель системи управління безпекою для мережі IoT

Перша частина запропонованої моделі

Перша частина запропонованої моделі вже був обговорений в попередніх розділах, тому далі ми зосередимося на другій і третій частинах.

Друга частина запропонованої моделі.

Другий етап складається з трьох основних розділів. У цих розділах описуються використовувані протоколи і механізми безпеки рівнів безпеки IoT відповідно.

Третя фаза запропонованої моделі – це сервери баз даних, які зберігають всю інформацію і параметри механізмів безпеки для кожного рівня безпеки, профілі користувачів, помилки механізмів безпеки, log-файли системи IoT і списки контролю доступу. Третій етап може допомогти адміністратору і користувачам управляти всією інформацією про мережу IoT і користувачів.

3.4 Протоколи і механізми безпеки рівнів архітектури за моделлю OSI

Протоколи і механізми безпеки рівня обробки даних. Найбільш прийнятним протоколом для рівня обробки є IEEE 802.11 AH, оскільки він підходить для бездротового зв’язку. Це легкий протокол, що споживає мало енергії і часу. У той же час це зменшує накладні витрати. Він забезпечує ефективний двонаправлений обмінний пакет, що дозволяє датчику економити більше енергії, використовуючи зв’язок по висхідній і низхідній лініях між датчиками. Датчик посилає дані і переходить в сплячий режим, коли той завершує свою місію. Він має короткий MAC-адрес, який використовується для збільшення часу очікування та економії енергії. IEEE 802.11 AH використовує алгоритм шифрування для забезпечення конфіденційності і приватності.

Зручні механізми безпеки рівня сприйняття можуть бути ідентифіковані відповідно до попереднього огляду механізмів безпеки, які були пояснені в попередніх таблицях. У них показані переваги і недоліки кожного з механізмів безпеки для забезпечення відповідних механізмів безпеки обираючи для WSN. і RFID. Відповідними механізмами безпеки WSN є Key Management (PKI) і алгоритми безпечного ключа, що

використовують алгоритми симетричного шифрування ключа, що забезпечують низьке енергоспоживання.

IPSec. Механізм використовується для RFID, тому що він забезпечує алгоритми автентифікації і шифрування.

Для алгоритмів автентифікації токен доступу використовується для надання односторонньої хеш-функції. Одностороння хеш-функція дозволяє користувачам вводити імена користувачів і паролі, щоб отримати токен доступу для отримання певного ресурсу без використання імені користувача і пароля. Після того як користувач отримає токен доступу, він може відобразити його, щоб отримати доступ до певного ресурсу на певний період часу для віддаленого сайту. Клієнт повинен вказати токен доступу як частина URL-адреси запиту або як ім'я користувача. Токен доступу на основі алгоритму автентифікації забезпечує авторизацію, контроль доступу, доступність і конфіденційність.

Для алгоритму шифрування симетричне шифрування використовується для досягнення полегшеного алгоритму шифрування, щоб витрачати малу потужність і час. Оцінка анонімності і ризику використовується для всіх типів датчиків для захисту приватної інформації користувачів і виявлення мережевих помилок.

Протоколи і механізми безпеки мережевого рівня

Найбільш прийнятним протоколом мережевого рівня є 6LowPAN, який використовується для інкапсуляції IPV6. IPV6 забезпечує довгий заголовок в невеликих пакетах. 6LowPAN має низьку пропускну здатність, невелике енергоспоживання, невелику вартість, мобільність, масштабованість мережі та та довгий час очікування, і може зменшити проблему передачі.

Відповідні механізми безпеки мережевого рівня можуть бути класифіковані по мірі безпеки передачі даних, середовища і протоколу передачі.

Система криптографії використовується для забезпечення безпеки передачі даних з використанням алгоритму криптографії з симетричним ключем. Він потребує мало енергії і часу виконання.

Наскрізний алгоритм (End-to-End) з використанням автентифікації на основі сертифікатів X.509 використовується для середовищ передачі. Він використовує двостороннє з'єднання Socket Secure Layer (SSL) для генерації сертифіката на стороні клієнта і підключення до сервера. Він використовує механізм PKI, оскільки немає необхідності поширювати відкриті ключі або перевіряти відбитки пальців при створенні або оновленні пар ключів. Такий метод є добре масштабованим, оскільки не потрібно довіряти окремим об'єктам, для цього потрібен лише один сертифікат автентифікації (CA) або якась обмежена їх кількість. Він забезпечує перевірку особистості за допомогою секретних приватних ключів.

Механізм міжмережевої автентифікації використовується для захисту протоколу передачі протоколів IoT. Він використовується для зменшення складності управління мережею.

Третя частина запропонованої моделі - протоколи і механізми безпеки прикладного рівня

На сьогодні, для зв'язку між пристроями, досі найбільш поширено використовується HTTP протокол. Проте раніше ми вже визначили, що існують й інші протоколи, що можуть бути використані для IoT, це такі як MQTT, XMPP та COAP. Попередньо описавши можливості кожного з них, слід обрати протокол MQTT.

Щоб показати доцільність і переваги саме цього протоколу в порівнянні з HTTP, ми вивчили характеристики кожного з них, і зібравши показники часу відгуку та розміру пакета при передачі ідентичного навантаження через MQTT і HTTP, ми знайшли відмінності між двома протоколами.

Щоб провести справедливе порівняння між двома протоколами, необхідно взяти до уваги всі етапи процесу автентифікації (рукостискання). Для

випадку MQTT це означає, що повідомлення про підключення і відключення вимірюються послідовно з повідомленнями фактичних даних. Спершу ми виміряли час відповіді для відправки 1, 100 і 1000 повідомлень через MQTT по одному циклу з'єднання, а також захопили розміри пакетів, які були надіслані по дроту, а потім час відповіді для відправки одного повідомлення з 1, 10 та 100 полями властивостей по одному циклу підключення, а потім захопили відправлений розмір пакета. Далі ми виміряли середній час відгуку для відправки корисного навантаження по HTTP з 1, 10 та 100 полями властивостей, а потім зафіксували розмір пакета по дроту.

Нижче наведені результати передачі пакетів через HTTP і MQTT тільки з одним імітованим користувачем. Передане повідомлення являє собою простий об'єкт, що містить одну пару ключ-значення.

Таблиця 3.7 - Вплив зміни кількості повідомлень на час

Кількість повідомлень за один цикл з'єднання	**Середній час відповіді для циклу з'єднання (мс)**	**Середній час відповіді на повідомлення (мс)**
1	113	113
100	4724	47
1000	40366	43

Таблиця 3.8 - Вплив зміни розміру корисного навантаження на час

Кількість полів властивостей у кожному повідомленні	Середній час відповіді для циклу з'єднання (мс)	Середній час відповіді на поле властивості (мс)
1	207	207
10	212	21
100	191	2

Таблиця 3.9 - Час відповіді HTTP

Кількість полів властивостей у повідомленні	Середній час відповіді (мс)	Середній час відповіді на поле властивості (мс)
1	289	289
10	280	28
100	247	3

Результати захоплення розміру пакета

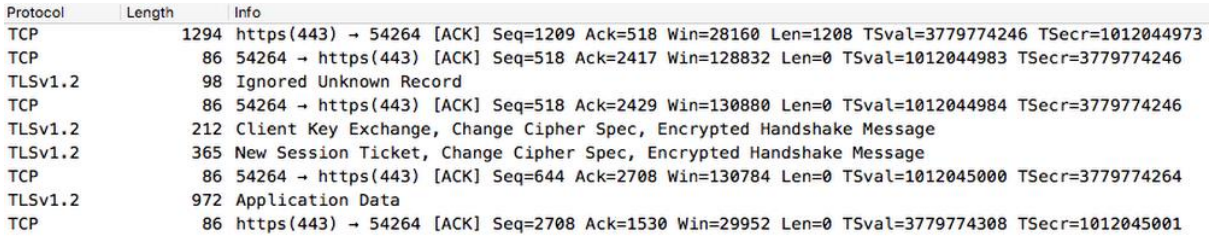
Щоб отримати більш точне уявлення про те, які пакети насправді надсилаються через дріт, ми використовували Wireshark для захоплення всіх пакетів, переданих з і до TCP-порту. Розміри кожного пакета були також записані.

Журнал логів показує процес рукостискання, який встановлює тунель TLS для зв'язку MQTT. Основна частина цього процесу полягає в обміні та перевірці як сертифікатів, так і відкритого ключа.

Рис. MQTT через протокол підключення TLS

Принцип роботи такий, що журнал логів показує, що по циклу передачі одного повідомлення, MQTT відправляє повідомлення від клієнта до сервера, MQTT відправляє ACK повідомлення назад до клієнта, плюс клієнт так само відправляє назад TCP ACK для прийнятого MQTT ACK.

Процедура ініціалізації для налаштування тунелю TLS для випадку HTTP така ж сама, як для випадку MQTT, і тепер встановлений захищений тунель повторно використовується всіма наступними запитами.



Protocol	Length	Info
TCP	1294	https(443) → 54264 [ACK] Seq=1209 Ack=518 Win=28160 Len=1208 TSval=3779774246 TSecr=1012044973
TCP	86	54264 → https(443) [ACK] Seq=518 Ack=2417 Win=128832 Len=0 TSval=1012044983 TSecr=3779774246
TLSv1.2	98	Ignored Unknown Record
TCP	86	54264 → https(443) [ACK] Seq=518 Ack=2429 Win=130880 Len=0 TSval=1012044984 TSecr=3779774246
TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
TLSv1.2	365	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
TCP	86	54264 → https(443) [ACK] Seq=644 Ack=2708 Win=130784 Len=0 TSval=1012045000 TSecr=3779774264
TLSv1.2	972	Application Data
TCP	86	https(443) → 54264 [ACK] Seq=2708 Ack=1530 Win=29952 Len=0 TSval=3779774308 TSecr=1012045001

Протокол HTTP не використовує з'єднання, тобто токен JWT, що використовується для автентифікації, відправляється в заголовку для кожного запиту.

У наведеній нижче таблиці підсумовується розмір пакета, надісланий під час кожного стану передачі для MQTT і HTTP:

Таблиця 3.10 – Сума розміру переданих пакетів

(байт)	MQTT	HTTP
Встановлення з'єднання	5572	2261
На опублікування повідомлення	388	3285
На роз'єднання	376	0
Сума	6336	5546

Рис. Розмір пакетів надісланих протягом кожного циклу передачі повідомлення

Наведена нижче таблиця показує як зміна розміру корисного навантаження на розмір пакету у мережі.

Таблиця 3.11 – Вплив зміни розміру корисного навантаження на розмір пакету

Корисне навантаження (Payload)	MQTT 1	MQTT 10	MQTT 100	HTTP 1	HTTP 10	HTTP 100
Розмір пакета, що передається по дроту (байт)	388	686	3788	1982	2332	6683
Співвідношення розмірів пакету в порівнянні з одним полем	1	1.77	9.76	1	1.18	3.37

Таблиця 3.12 - Результуюча таблиця (кількість витрачених байт):

(байт)	MQTT	HTTP
Встановлення з'єднання	5572	2261

На опублікування повідомлення	388	3285
На роз'єднання	376	0
Сума	6336	5546

Дивлячись на результат, який порівнює час відгуку за один цикл з'єднання для MQTT, ми ясно бачимо, що початкова налаштування з'єднання збільшує час відгуку для відправки окремих повідомлень до рівня, який дорівнює часу відгуку відправки одного повідомлення по HTTP, що в нашому випадок округлено дорівнює 120 мс на повідомлення. Вплив кількості даних (навантаження), що відправляються, має ще більше значення для MQTT, в якому близько 6300 байтів відправляється для одного повідомлення, що є більшим значенням, ніж для HTTP, у якого результуюче значення дорівнює 5600 байтів. Переглядаючи журнал трафіку пакетів, ми бачимо, що більша частина - понад 90% переданих даних - призначена для встановлення і розірвання з'єднання.

Реальна перевага MQTT над HTTP спостерігається, коли ми повторно використовуємо єдине підключення для відправлення декількох повідомлень, в яких середня відповідь на повідомлення досягає приблизно 40 мс, а обсяг даних на повідомлення досягає приблизно 400 байт. Слід зауважити, що у випадку HTTP ці скорочення просто неможливі.

Висновок, який ми можемо зробити, полягає в тому, що, вибираючи між MQTT та HTTP, дуже важливо якомога більше повторно використовувати те ж саме з'єднання. Якщо з’єднання часто встановлюються і розриваються для надсилання окремих повідомлень, ефективність не є суттєвою у порівнянні з HTTP.

Найбільше підвищення ефективності може бути досягнуто за рахунок збільшення MQTT в щільності інформації для кожного повідомлення корисного навантаження.

Таким чином складемо загальну таблицю (табл. 3.13) з основними характеристиками по двом протоколам.

Таблиця 3.13 – Основні характеристики протоколу MQTT та HTTP

	MQTT	HTTP
Повна назва	Message Queue Telemetry Transport - спрощений мережевий протокол	Hyper Text Transfer Protocol - протокол передачі гіпер-текстових документів
Архітектура	Публікація-підписка [62]	Клієнт-серверна
Протокол, на якому працює	TCP	TCP и UDP
Розмір повідомлень	Маленький	Великий
Формат повідомлень	Двійковий з заголовком 2байта	ASCII формат
Розподіл даних	Від 1 до 0/1 / N	Лише «один до одного»
Безпека даних	Так, він використовує SSL / TLS для безпеки передачі даних	Сам по собі HHTP не надає безпечну передачу, для цього використовується HTTPS
Складність	Простий протокол	Більш складний через використання ASCII парсеру
Шифрування	Він шифрує корисне навантаження	Дані не шифруються перед передачею
Коли використовувати	Якщо потрібно холодильнику зв’язатись з термометром для адаптації насоса двигуна, то цей варіант значно кращий.	Якщо мета зібрати якомога більше інформації, то достатньо HTTP.

Використовуваний протокол – це протокол MQTT, який використовує шифрування на основі полегшених алгоритмів шифрування для досягнення низької потужності і часу. Сервер MQTT через SSL є основою безпеки мережі IoT, яка захищає конфіденційну інформацію в мережі IoT. SSL захищає додатки IoT з використанням алгоритмів шифрування для захисту конфіденційної інформації, автентифікації, критичної безпеки і цілісності даних для інтерфейсу програми та особистої інформації про користувачів. Біометрія є підходящою мірою безпеки для рівня додатків, оскільки саме

вона може запобігати внутрішнім і зовнішнім атаки, і захищати всі дані між рівнем додатків і користувачами. Біометрія є новою темою в області досліджень, і дослідники намагаються знайти підходящі алгоритми безпеки для мережі IoT, щоб зменшити споживання енергії і час обробки. У додаток до вище перерахованих механізмів, важливими елементами в мережі IoT для моніторингу, управління і контролю мережевого трафіку є списки контролю доступу.

Реалізація запропонованої моделі і її варіації, підходять для різних мережевих платформ IoT, що можна використати як основу майбутньої роботи, та визначити вплив нашої моделі на алгоритми безпеки і енергоспоживання.

3.5 Рекомендації по захисту інформаційних ресурсів в IoT

Системи IoT бувають дуже складними, їм потрібні комплексні заходи захисту, що покривають рівні хмар і підключень, також необхідна підтримка пристроїв IoT з обмеженими обчислювальними ресурсами, яких недостатньо для підтримки традиційних рішень безпеки. Простого універсального рішення не існує, і для забезпечення безпеки недостатньо замкнути двері, залишивши вікна відкритими. Безпека повинна бути всебічною, інакше атакуючі просто скористаються найслабшою ланкою системи. Звичайно, традиційні IT-системи, як правило, передають і обробляють дані з систем IoT, але самі системи IoT володіють своїми унікальними потребами в захисті. [63]

Передові практики розгортання IoT повинні враховувати широкий спектр проблем до, під час і після створення систем. Що говорить про наявність великої кількості місць, де все може піти не так. Давайте визначимо деякі кращі практики для успішного розгортання IoT:

Стратегічне планування може бути найбільш важливим кроком на шляху до успіху. Тут встановлюються цілі, визначаються метрики, збираються команди, виявляються варіанти використання, проводиться інвентаризація і оцінюються бізнес-процеси. Це може і фактично має бути

найбільш трудомісткою частиною розгортання IoT, тому що саме тут відбуваються фундаментальні рішення, які мають значущий вплив на кожен наступний крок.

Детально вивчіть управління кінцевими точками і пристроями в мережі. Традиційно інструментам управління мережею пропонувалося визначити, чи включені пристрої і системи, працюють вони чи не працюють. Але для розгортання IoT ви враховувати більш глибокий аналіз поведінки кінцевих точок і працездатності мережі. Крім простого визначення часу безвідмовної роботи і доступності, системи IoT повинні миттєво визначити, чи працюють системи і пристрої на необхідному рівні для досягнення мети.

Безпека має першочергове значення. Плануйте та дійте відповідно. Пам’ятайте про те, що ви вже підключили безліч пристроїв, віртуальних або хмарних мереж. І ми говоримо не тільки про потреби кінцевих точок, таких як автомобілі або холодильники. Основні компоненти, такі як динамічні апарати, системи лінійного підключення та датчики різного роду,мають найбільш невтішну ситуацію. Ваші системи повинні бути готові не тільки до появи нових видів кінцевих точок, але й до миттєвого аналізу їх законності, доступу та привілеїв у відповідності з політиками безпеки і управлінням ідентифікації.Ваші системи мають бути в змозі точно визначати, що вони можуть і не можуть робити для використання ваших систем, додатків та даних.

Великий потенціал IoT створить навантаження на успадковану інфраструктуру, тому будьте готові робити стратегічні інвестиції в інфраструктуру, особливо в області мереж і з'єднань. Зрештою, обсяг, різноманітність і швидкість передачі даних як по провідний, так і по бездротовій мережі різко зростають, і кінця цьому не видно.Необхідно переконатися, наприклад, що ви модернізували фізичні мережеві комутатори та інструменти управління, щоб забезпечити безперебійний потік інформації, і що ваша бездротова мережа готова до останньої версії, будь то 802.11ac або щось, що планується бути випущеним. Постійний, надійний і всебічний потік всіх даних - структурованих і неструктурованих - необхідний для аналітики, яка стане критично важливим компонентом в розгортанні і використанні IoT, і ви не зможете зробити це без надійної, безпечної та масштабованої інфраструктури.

Успішне впровадження IoT має кілька загальних характеристик, включаючи детальне планування, обережне виконання і ретельний моніторинг прогресу в досягненні цілей.

Отже, короткий чек-ліст по безпечному розгортанню IoT системи матиме наступний вигляд:

- Додавайте пристрої IoT в «окрему, захищену брандмауером мережу», як в гостьових мережах. «Це дозволяє вам обмежувати вхідний трафік, запобігати переходам в вашу базову мережу і моніторити трафік для виявлення аномалій».
- Вимкніть речі, які не використовуються. Це може здаватись очевидним, але контрольний список також контролює «фізичне блокування / закриття портів, камер і мікрофонів».
- Переконайтеся, що люди не мають фізичного доступу до смарт-пристроїв IoT для скидання паролів і т.і.
- Увімкніть шифрування, коли це можливо, і розгляньте можливість підключення до ваших мереж тільки пристроїв, які підтримують шифрування. Якщо це неможливо, «розгляньте можливість використання VPN або інших засобів для обмеження доступу до даних».
- Постійно оновлюйте прошивку і програмне забезпечення (через автоматичні оновлення або щомісячні перевірки). Уникайте продуктів, які не можуть бути оновлені, стежте за життєвим циклом всіх пристроїв і видаляйте їх з експлуатації, коли вони перестають бути поновлюваними або безпечними.
- Безпека IoT продовжує розвиватися, і відмітка кожного елемента в списку OTA не забезпечить повний захист. Але це прості передові практики, які можуть допомогти знизити ризик. Ігнорувати їх на свій страх і ризик.

Висновки за розділом 3

Отже IoT має ряд серйозних недоліків. Складність такої системи є найважливішою проблемою, оскільки операції з IoT є комплексними і не існує гнучкої інтеграції між пристроями. Система складається з різних пристроїв з різною архітектурою, впровадженням та обслуговуванням, тому будь-яка вразливість програмного або апаратного забезпечення одного із пристроїв може мати серйозні наслідки для багатьох інших пристроїв

мережі. Мережа Інтернету речей страждає від проблем з автентифікацією та контролем доступу, оскільки розумні об’єкти є пристроями різних типів, які базуються на різних платформах (апаратних засобах та мережах). Крім того, всі пристрої повинні взаємодіяти один з одним через різні мережі. Таким чином, проблема безпеки є найбільшою проблемою, оскільки всі пристрої та дані піддаються різним видам загроз і атак. Існують найрізноманітніші загрози та атаки, які можуть спричинити серйозні катастрофи в мережі. Крім того, всі персональні дані всіх користувачів піддаються найнебезпечнішим атакам. Також IoT не має норм та правил, які б пояснювали, як захищати пристрої та дані. Саме тому четвертий розділ цієї магістерської роботи присвячений запропонованій моделі, яка може бути використана для побудови системи управління безпекою мережі IoT для реалізації відповідних механізмів безпеки різних рівнів архітектури IoT.

ВИСНОВКИ

Інтернет речей став ще одним значним нововведенням в світі і покладає великі надії своїми можливостями для поліпшення нашого життя. У той же час IoT стикається з багатьма проблемами. Найбільші з них – це проблеми безпеки, а саме конфіденційності і цілісності.

Основна мета полягала в тому, щоб визначити вимоги безпеки, які можуть поліпшити продуктивність мережі IoT. Тому тут коротко представлено загальну інформацію про IoT, включаючи історію, компоненти, з'єднання і додатки IoT.

Було обговорено ряд питань проблеми безпеки IoT, а також можливі варіанти рішень проблем безпеки IoT для запобігання внутрішніх і зовнішніх атак.

Ми визначили, що найбільш значиму роль в розробці рішень безпеки і управлінні мережею IoT відіграють вимоги до безпеки датчиків, та каналів передачі і обробки даних. Одним з найбільш важливих питань безпеки, які можна отримати з проведеного дослідження, є розуміння значення кожного типу загроз, атак, проблем і вразливостей, для того ,щоб уникнути їх,потрібно використовувати відповідні методи безпеки.

Мета роботи була зосереджена на рівнях створеної моделі архітектури з детальним описом кожного з них і сформованими можливостями для вирішення проблем безпеки IoT, а також проведене порівняння механізмів безпеки для кожного з рівнів моделі архітектури IoT, з врахуванням потужності і часу обробки інформації, як два основних критерія.

Крім того підкреслено необхідність розробки та застосування стандартів безпеки, а також надані рекомендації по впровадженню систем IoT.