НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Інститут телекомунікаційних систем

Кафедра Інформаційно-телекомунікаційних мереж

До захисту допущено:

Завідувач кафедри

_____ Лариса ГЛОБА

«___»_____2021 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Інформаційно-комунікаційні технології»

спеціальності 172 «Телекомунікації та радіотехніка»

на тему: «Модифікований метод захисту інформації в мережі Інернету речей»

Виконав:
студент IV курсу, групи ТІ-71
Петров Олександр Сергійович _____

Керівник:
Асистент кафедри ІТМ ІТС
Курдеча Василь Васильович _____

Рецензент:
Зав. кафедри промислової електроніки
Ямненко Юлія Сергіївна _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____

Київ – 2021 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Інститут телекомунікаційних систем
Кафедра Інформаційно-телекомунікаційних мереж

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 «Телекомунікації та радіотехніка»

Освітньо-професійна програма «Інформаційно-комунікаційні технології»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Лариса ГЛОБА
«___»_____2021 р.

ЗАВДАННЯ
на дипломну роботу студенту
Петрову Олександру Сергійовичу

1. Тема роботи «Модифікований метод захисту інформації в мережі Інернету речей», керівник роботи асистент кафедри інформаційно-телекомунікаційних мереж ІТС Курдеча Василь Васильович, затверджені наказом по університету від «14» квітня 2021 р. № 1007-с
2. Термін подання студентом роботи 7 червня 2021 р.
3. Вихідні дані до роботи
    1. Існуючі моделі Internet of Things
    2. Blockchain
4. Зміст роботи
    1. Проаналізувати проблеми безпеки та визначити можливі ризики IoT.
    2. Дослідити існуючі методи забезпечення інформаційної безпеки.
    3. Модифікувати метод захисту інформації в мережі IoT за допомогою використання Blockchain технології.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо)

Плакат №1 (слайд) Тема дослідження;
Плакат №2 (слайд) Об’єкт, предмет та методи дослідження;
Плакат №3 (слайд) Мета дослідження. Основні задачі дослідження;
Плакат №4 (слайд) Актуальність дослідження;
Плакат №5 (слайд) Проблеми IoT;

Плакат №6 (слайд) Методи боротьби з проблемами IoT;
Плакат №7 (слайд) Модифікований метод;
Плакат №8 (слайд) Протокол перевірки отриманої інформації;
Плакат №9 (слайд) Порівняння запропонованого методу з існуючими;
Плакат №10 (слайд) Висновки.
Плакат №11 (слайд) Публікації;

6. Дата видачі завдання 05.09.2020

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1.	Отримання завдання	05.09.2020	виконано
2.	Збір інформації	01.01.2021	виконано
3.	Розгляд технології Internet of Things	15.02.2021	виконано
4.	Огляд нормативно-правових актів пов'язаних з поняттям конфіденційності	01.03.2021	виконано
5.	Поглиблене вивчення проблеми вразливості мережі IoT	14.03.2021	виконано
6.	Огляд технології Blockchain	28.03.2021	виконано
7.	Дослідження модифікованих методів захисту інформації в мережі Інернету речей	15.04.2021	виконано
8.	Оформлення дипломної роботи	25.05.2021	виконано
9.	Отримання допуску до захисту	01.06.2021	виконано

Студент Олександр ПЕТРОВ

Керівник Василь КУРДЕЧА

РЕФЕРАТ

Дипломна робота «Модифікований метод захисту інформації в мережі Інернету речей» складається з переліку умовних скорочень, вступу, основної частини, що містить 3 розділи, висновків і списку використаних джерел. Загальний обсяг роботи – 67 сторінок. Робота містить 6 рисунків та 3 таблицю. Список використаних джерел включає 23 одиниць.

Мета роботи: Підвищити рівень інформаційної безпеки в IoT мережах за допомогою модифікації методу захисту інформації.

В даній роботі було розглянуто модель мережі Internet of Things і визначено її проблеми інформаційної безбеки.

Проаналізовано методи вирішення вразливостей IoT.

Запропоновано та проаналізовано модель IoT з впровадженням блокчейн технології.

Ключові слова: IoT, конфіденційність, інформаційна безпека, Blockchain, захист інформації.

ABSTRACT

Thesis " Modified method of data protection in the IoT network " consists of a list of abbreviations, introduction, main part, containing 3 sections, conclusions and a list of sources used. The total volume of the work is 67 pages.
The work contains 6 figures and 3 table. The list of used sources includes 23 units.

Purpose: To increase the level of information security in IoT networks by modifying existing methods.

In this paper the model of the Internet of Things network is considered and its problems of information security are defined.

Methods for solving IoT vulnerabilities are analyzed.

The IoT model with the introduction of blockchain technologies is proposed and analyzed.

Keywords: IoT, privacy, information security, Blockchain, data protection.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

AI	(Artificial intelligence) – штучний інтелект
API	(Application Programming Interface) – інтерфейс програмного додатку
chal	запит на верифікацію (скор. *Challenge* – виклик)
CRSC	(Challenge Receiving Smart Contract) – Виклик отримання смарт-контракту
CSP	(Cloud Service Provider) – Провайдер хмарних послуг
COVID-19	(coronavirus disease 2019) - коронавірусна хвороба 2019
DCD	(Data Consumer Device) – Прилад – користувач даних
DOD	(Data Owner Device) – Прилад – власник даних
DoS	(Denial of Service) - відмова в обслуговуванні
HSSC	(HVTs Storage Smart Contract) – Смарт-контракт на зберігання HVT
HVT	(homomorphic verifiable tags) – гомоморфні теги перевірки
IIoT	(Industrial Internet of Things) – промисловий інтернет речей
IoT	(Internet of Things) - Інтернет речей
IP	(Internet Protocol) – інтернет протокол
IVSC	(Integrity Verification Smart Contract) – Смарт-контракт для перевірки доброчесності
NAS	(Network Attached Storage) – сховище файлового рівня
P2P	(peer-to-peer) – вузол до вузла
QOS	(Quality of Service) – якість обслуговування
SAN	(Storage Area Network) – сховище блочного зберігання
TCP	(Transmission Control Protocol) – протокол керування передачею
UDP	(User Datagram Protocol) – протокол датаграм користувача
ІКТ	Інформаційно-комунікаційні технології
ПЗ	програмне забезпечення

ВСТУП

На сьогоднішній день людство уже «кількісно» програло приладам. Відповідно до останніх досліджень число гаджетів на Землі перевищило число усіх людей. Причому щосекунди на планеті стає на дві людини більше, річний приріст населення рівняється приблизно 1,2%, натомість приріст тільки мобільних девайсів перевищує ці показники як мінімум в 5 разів.

Таке поширення приладів привело до появи технології, з величезним потенціалом і властивостями масштабування та розширення – Internet of Things. Що в свою чергу принесло низку нових можливостей і якісні зміни в буденному житті. Актуальність цих змін особливо помітна в сьогоднішній ситуації світової пандемії. Коли уряди більшості країн закликають громадян залишатися вдома, коли офісні будівлі спорожнілі стоять уже не перший день. Доводиться переосмислювати відношення людина-людина, людина-будівля і людина-пристрій/додаток, щоб забезпечити нове нормальне функціонування суспільства.

Таким чином, ***об'єктом досліджень*** є захист інформації в Internet of Things.

Предмет досліджень – є метод захисту інформації в мережі Internet of Things.

Мета досліджень – підвищити рівень інформаційної безпеки в IoT мережах за допомогою модифікації уже існуючих методів.

Задачі:

1) Проаналізувати проблеми безпеки та визначити можливі ризики IoT.

2) Дослідити існуючі методи забезпечення інформаційної безпеки.

3) Модифікувати метод захисту інформації в мережі IoT за допомогою використання Blockchain технології.

Наукова новизна дослідження – аналіз застосування модифікованого методу захисту інформації і протидії атакам в середовищі IoT.

РОЗДІЛ 1.
ПОНЯТТЯ ТА СТРУКТУРНА СУТНІСТЬ ТЕХНОЛОГІЇ INTERNET OF THINGS, ПРОБЛЕМА ПРИВАТНОСТІ

1.1. Прикладне використання Internet of Things

Найперший і найшвидше впроваджує нові концепції великий бізнес, адже для нього не використана можливість це великі фінансові втрати. Гроші крутять колесо економіки, а економіка формує життя усіх нас: і підприємців ,не важливо чи великих, чи малих, і звичайних громадян і цілих держав і їхніх урядів.

Будівлі є другим фактором за затратністю для компаній після зарплат працівникам. Моніторинг та розуміння завантаженості будівель не лише допомагає заощадити гроші бізнесу, але також може забезпечити, щоб працівники максимально використали свій час в офісі. Оскільки світ роботи переходить від щоденних поїздок на роботу до роботи частково або повністю віддалено, Інтернет речей відіграватиме вирішальну роль в оптимізації робочих процесів і забезпеченні відповідності будівель протидії COVID-19.

Тому вони повинні бути розумнішими, гнучкішими та, що найважливіше, захищеними від біологічних загроз. В центрі цієї зміни буде IoT-моніторинг температури тіла та підрахунок людей, контроль якості повітря та споживання енергії, а також мережа розумних підключених пристроїв, які допоможуть урядам та компаніям не лише відстежувати COVID-19, але також приймають розумніші рішення щодо транспортної та офісної інфраструктури. І коли ми спільно працюємо над створенням нової норми, ці рішення Інтернету речей також допоможуть нам досягти цілей з нульовим рівнем викидів вуглецю.

У лондонській штаб-квартирі Vodafone цей метод вже реалізується. Інтелектуальне рішення для управління IIoT в будівлі використовує безліч підключених датчиків для відстеження споживання енергії та управління заповненням робочого столу. Це все подається в систему управління будівлею,

яка допомагає виявити зайняті райони та забезпечити соціальне дистанціювання. Ця технологія допоможе безпечно та контрольовано управляти поверненням до роботи, одночасно забезпечуючи дані, необхідні для постійної адаптації та вдосконалення її роботи.

Виявлення тепла - ще один приклад. Коли офіси знову почнуть відкриватися, співробітники будуть розраховувати на те, що їхні компанії будуть у безпеці. Камера детектора тепла Vodafone Business швидко та непомітно перевіряє людей, щоб перевірити наявність підвищеної температури тіла, що є потенційною ознакою зараження COVID-19, і дозволяє компаніям вжити відповідних заходів. Послуга повністю управляється та захищена, виявлення надсилаються на захищену центральну консоль. Аналіз даних проводиться в локальній системі організації, тут є цілодобова технічна підтримка та ремонт на наступний день[1].

Поряд з цим стільникові з'єднання IoT, що забезпечуються зростанням 5G дозволить нам будувати впроваджувати ці методи де раніше це було не можливо.

Згідно з дослідженнями, проведеними у звіті IoT Spotlight від травня 2020 року, 84% компаній вважали, що IoT забезпечив їм безперервність бізнесу під час пандемії, а 95% побачили позитивну рентабельність інвестицій. Ще до пандемії ера Інтернету речей була досить тривалою, і кожен третій бізнес використовував цю технологію. Розгортання 5G дозволило більшій кількості пристроїв підключитися до мережі. Але в розпал глобальної охорони здоров’я та економічної кризи багато підприємств намагаються сформулювати переваги прийняття того, що часто сприймається як складні нові технології. Дослідження фірми цифрової безпеки Gemalto показують, що 48 відсотків підприємств намагаються виявити порушення безпеки Інтернету речей у своїй мережі. Половина організацій заявила, що вартість впровадження також є основною перешкодою, тоді як підтримка та інтеграція застарілих технологій також є ключовими проблемами.

Багато розчарувань, які відчувають підприємства, які впровадили або намагалися впровадити технології IoT, можна вирішити, застосовуючи більш цілісний підхід з рішеннями, які є модульними, масштабованими та здатними підключитись до застарілих систем. Наявність фізичної мережі та інфраструктури управління та контролю для реалізації переваг IoT є ключовим фактором, як і спільно створені індивідуальні рішення, які дозволяють будь-якому бізнесу, який хоче зробити правильний вибір, отримати доступ до широкого спектру знань та технологій.

У довгостроковій перспективі технології IIoT допоможуть компаніям не тільки збирати більше даних безпечним та сумісним способом, але і вчитися на цих даних та вносити важливі зміни, які приносять користь їхнім працівникам та навколишньому середовищу, яке ми всі ділимо. Створені спільно рішення Інтернету речей допоможуть організаціям мінімізувати ризик та відновити довіру співробітників та споживачів. А те, що працює для однієї будівлі, можна масштабувати до цілого міста, де розумні датчики, підключені до еластичних та надшвидких мереж 5G, можуть допомогти чиновникам контролювати інфраструктуру та краще розуміти мінливий спосіб взаємодії та переміщення по міських просторах.

Нова технологія надає користувачам можливість перевірити стан своєї домашньої безпеки зі своїх смартфонів, завести машину за допомогою програми для мобільного телефону та дистанційно відкрити та закрити свої гаражні ворота з будь-якої точки світу. Ці технології стають частиною IoT. В основному розумінні IoT відноситься до підключення повсякденних предметів (наприклад, телевізорів, побутової техніки чи тренажерів) до Інтернету. Це дозволяє здійснювати моніторинг у режимі реального часу та широкий збір даних про власність, людей, рослин та тварин[1].

По-перше, розумні будинки та офіси стали частиною IoT. Зокрема, ці розумні будинки та офіси надають доступ до вимикачів світла, дверей, вікон, жалюзей та температури та можливість керувати ними дистанційно.

Наприклад, WeMo дозволяє користувачам контролювати потужність (наприклад, споживання енергії), домашню електроніку та побутову техніку, воду та Wi-Fi за допомогою смартфона. HomeKit від Apple, ще один розумний домашній продукт, полегшує управління сигналізацією, спостереження системи, ліхтарі та двері, серед інших предметів, через IPhone або IPad. Інші доступні технології дозволяють користувачам контролювати свої будинки та офіси за допомогою браслетів. Наприклад, браслети Reemo дозволяють користувачам контролювати медіа (такі як, телефони, відеоігри, стереосистеми та телевізори), безпеку (наприклад, сигналізації та спостереження), клімат (включачи, термостати, каміни, розумні вентилятори та теплі підлоги) та потужність (наприклад, розетки, вимикачі та регулятори яскравості) у своєму будинку, використовуючи жести руками. Такі типи пристроїв здійснюють обробку в режимі реального часу моніторинг майна, а також переміщення та діяльність людей вдома та в офісі.

По-друге, були розроблені мобільні пристрої, які можуть контролювати діяльність людей та життєво важливі показники. Fitbit - це фітнес-пристрій, який відстежує та займається в режимі реального часу моніторинг пройденої відстані користувачем, зроблених ним кроків, піднімань по сходах, спалених калорій та якості сну, цілодобово. Hexoskin- це одяг, який контролює дихання частоту серцевих скорочень, і навіть відстежує режим сну користувач. Є інші пристрої, що носяться, вони обіцяють відстежувати звички сну новонародженого, збираючи дані, про те спить він на спині чи на животі, частоту дихання, температуру шкіри, ... і навіть, в деяких випадках, рівень кисню в крові та частоту серцевих скорочень. Ці пристрої дозволяють спостерігати в реальному часі, за людьми, внутрішньою роботою їх тіла, а також за їхніми рухами та діяльністю.

1.2 Структура Internet of Things

Варто зазначити, що не існує єдиної узгодженої архітектури IoT. Вони різняться за складністю та кількістю архітектурних шарів залежно від конкретного бізнес-завдання.

Наприклад, прикладна модель, представлена в 2014 році компаніями Cisco, IBM та Intel на Всесвітньому форумі IoT 2014, має цілих сім рівнів. Згідно з офіційним прес-релізом ведучого форуму Cisco, мета цієї архітектури – «допомогти навчати IT-директорів, IT-відділи та розробників щодо розгортання проектів IoT та пришвидшити прийняття IoT»[2].

Рис.1.1: Рівнева модель IoT

Але незалежно від варіанту використання та кількості шарів, ключові будівельні блоки будь-якої структури IoT завжди однакові, а саме:

- розумні речі
- мережі та шлюзи, що дозволяють пристроям з низьким енергоспоживанням (що часто трапляється в IoT) входити у великий Інтернет
- платформи проміжного програмного забезпечення або IoT, що забезпечують місця для зберігання даних та вдосконалені обчислювальні машини, а також аналітичні можливості

- додатки, що дозволяють кінцевим користувачам отримувати вигоди від IoT та керувати фізичним світом

Рис. 1.2: Базова структурна архітектура IoT

Ці елементи складають основу будь-якої системи IoT, на основі якої може бути розроблена ефективна багатошарова архітектура. Найчастіше це такі шари:

- рівень сприйняття, що розміщує розумні речі
- рівень зв'язку або транспортний рівень, що передає дані з фізичного рівня в хмару і навпаки через мережі та шлюзи
- рівень обробки, що використовує платформи IoT для накопичення та управління всіма потоками даних
- прикладний рівень, що забезпечує такі рішення, як аналітика, звітування та управління пристроями, для кінцевих користувачів.

Окрім найважливіших компонентів, можуть бути додаткові шари:

- обчислювальний шар краю або туману, що виконує попередню обробку даних близько до краю, де речі IoT збирають нову інформацію. Як правило, різкі обчислення відбуваються на шлюзах;
- діловий рівень, де бізнес приймає рішення на основі даних;
- рівень захисту, що охоплює всі інші рівні.

Часто розглядаються як необов’язкові, ці додаткові компоненти тим не менше роблять проект IoT чудово підходить для сучасних потреб бізнесу[2].

Рівень сприйняття: перетворення аналогових сигналів у цифрові дані і навпаки

Початковий етап будь-якої системи IoT охоплює широкий спектр «речей» або пристроїв кінцевих точок, які діють як місток між реальним та цифровим світами. Вони різняться за формою та розмірами - від крихітних силіконових чіпів до великих транспортних засобів. За своїми функціями речі IoT можна розділити на такі великі групи.

Такі датчики, як зонди, датчики, лічильники збирають фізичні параметри, такі як температура або вологість, перетворюють їх на електричні сигнали та передають в систему IoT. Сенсори IoT, як правило, невеликі і споживають мало енергії.

Пускачі перетворюють електричні сигнали із системи IoT у фізичні дії. Пускачі використовуються в контролерах двигунів, лазерах, роботизованих зброях.

Машини та пристрої, підключені до датчиків та виконавчих механізмів або мають їх невід'ємними частинами.

Важливо зауважити, що архітектура не обмежує сферу застосування її компонентів або їх розташування. Крайовий шар може включати лише кілька «речей», фізично розміщених в одній кімнаті, або безліч датчиків та пристроїв, розподілених по всьому світу.

Рівень підключення: забезпечення передачі даних

Другий рівень відповідає за всі комунікації між пристроями, мережами та хмарними службами, що складають інфраструктуру IoT. Зв'язок між фізичним рівнем та хмарою досягається двома шляхами:

- безпосередньо, використовуючи стек TCP або UDP/IP;

- через шлюзи - апаратні або програмні модулі, що виконують трансляцію між різними протоколами, а також шифрування та дешифрування даних IoT.

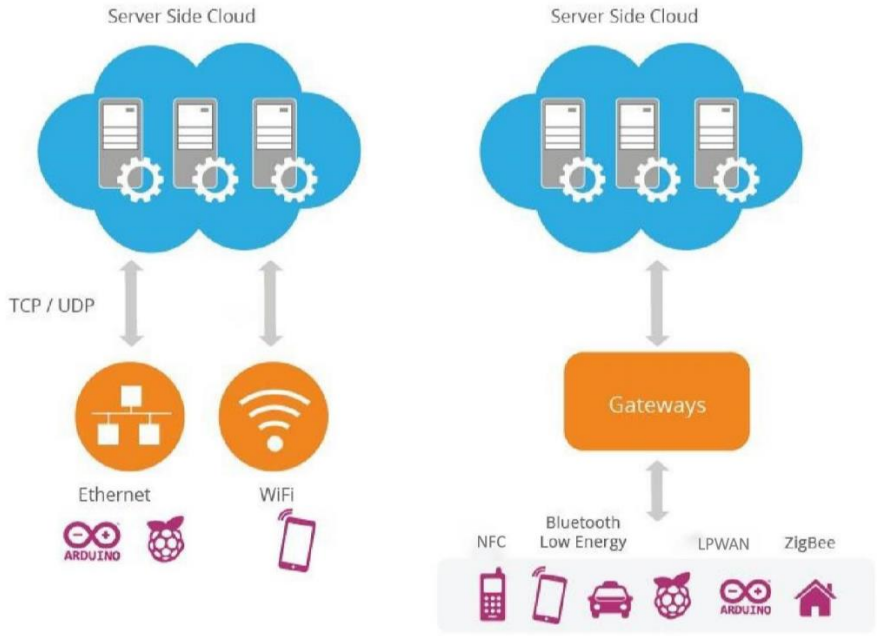

Рис. 1.3: Зв'язок між фізичним рівнем та хмарою

Зв'язок між пристроями та хмарними службами або шлюзами включає різні мережеві технології.

Ethernet підключає стаціонарні або стаціонарні пристрої IoT, такі як охоронні та відеокамери, постійно встановлене промислове обладнання та ігрові консолі.

WiFi, найпопулярніша технологія бездротових мереж, чудово підходить для рішень з великою кількістю даних IoT, які легко заряджати і працювати на невеликій території. Хороший приклад використання - це розумні домашні пристрої, підключені до електричної мережі.

NFC (Near Field Communication) забезпечує простий і безпечний обмін даними між двома пристроями на відстані 10 см або менше.

Bluetooth широко використовується носими пристроями для зв'язку на малій дальності. Для задоволення потреб малопотужних пристроїв IoT був

розроблений стандарт Bluetooth Low-Energy (BLE). Він передає лише невеликі порції даних і не працює для великих файлів.

LPWAN (малопотужна широкосмугова мережа) була створена спеціально для пристроїв IoT. Він забезпечує бездротове бездротове підключення на великому діапазоні при низькому споживанні енергії та тривалість автономної роботи 10+ років. Надсилаючи дані періодично невеликими порціями, технологія відповідає вимогам розумних міст, розумних будівель та розумного сільського господарства (моніторинг на місцях).

ZigBee - це бездротова бездротова мережа для передачі невеликих пакетів даних на невеликі відстані. Найвидатнішим у ZigBee є те, що він може обробляти до 65000 вузлів. Створений спеціально для домашньої автоматизації, він також працює для малопотужних пристроїв на промислових, наукових та медичних сайтах.

Стільникові мережі пропонують надійну передачу даних та майже глобальне покриття. Є два стільникові стандарти, розроблені спеціально для речей IoT. LTE-M (Long Term Evolution for Machines) дозволяє пристроям здійснювати прямий зв'язок із хмарою та обмінюватися великими обсягами даних. NB-IoT або вузькосмуговий IoT використовує низькочастотні канали для передачі невеликих пакетів даних[2].

Табл. 1.1: Технології, які використовуються при побудові мережі IoT

Мережа	Підключення	Особливості	Використання
Ethernet	Провідне, Ближньої дії	✓ Висока швидкість ✓ Захищеність	Стаціонарний IoT: відео, камери, ігрові консолі, зафіксовані прилади

		× Дальність дії залежить від довжини лінії × Обмежена мобільність	
Wifi	Безпровідне, ближньої дії	✓ Висока швидкість, ✓ Шикока сумісність × Обмежена дальність дії × Високе споживання енергії	Розумні будинки, девайси, які можуть легко підзаряджатись
NFC	Безпровідне, Ультраблизької дії	✓ Надійність ✓ Низьке споживання енергії × Обмежена дальність дії × Відсутність доступності	Системи оплати, розумні будинки
Bluetooth Low-Energy	Безпровідне, Ближньої дії	✓ Висока швидкість ✓ Низьке споживання енергії × Обмежена дальність дії × Низька пропускна здатність	Невеликі домашні девайси, маяки, чіпи

Продовження таблиці 1.1

LPWAN	Безпровідне, дальньої дії	✓ Висока дальність дії ✓ Низьке споживання енергії × Низька пропускна здатність × Висока затримка	Розумні будинки, розумні міста, розумна агрокультура(моніторинг полів)
ZigBee	Безпровідне, ближньої дії	✓ Низьке споживання енергії ✓ Масштабованість × Обмежена дальність дії × Проблеми відповідності	Домашня автоматизація, охорона здоров'я, індустріальні сайти
Стільникові мережі	Безпровідне, дальньої дії	✓ Майже глобальне покриття ✓ Висока швидкість ✓ Надійність × Висока ціна × Високе споживання енергії	Зв'язок з мобільними «речами», дронами

Як тільки частини рішення IoT з'єднані в мережу, їм все ще потрібні протоколи обміну повідомленнями для обміну даними між пристроями та з хмарою. Найпопулярнішими протоколами, що використовуються в екосистемах IoT, є:

DDS (Служба розподілу даних), яка безпосередньо пов’язує речі IoT між собою та із програмами, що відповідають вимогам систем реального часу;

AMQP (розширений протокол черги повідомлень), спрямований на одноранговий обмін даними між серверами;

CoAP (Протокол обмежених додатків), програмний протокол, призначений для обмежених пристроїв - кінцевих вузлів, обмежених в пам'яті та потужності (наприклад, бездротові датчики). Це схоже на HTTP, але використовує менше ресурсів;

MQTT (Message Queue Telemetry Transport), полегшений протокол обміну повідомленнями, побудований поверх стеку TCP / IP для централізованого збору даних з малопотужних пристроїв.

Обчислювальний рівень хмари: зменшення затримки системи

Цей рівень необхідний для того, щоб системи IoT могли відповідати вимогам до швидкості, безпеки та масштабу мобільної мережі 5-го покоління або 5G. Новий стандарт бездротового зв'язку обіцяє більш високу швидкість, меншу затримку та можливість обробляти набагато більше підключених пристроїв, ніж поточний стандарт 4G.

Ідея обчислень краю або туману полягає в тому, щоб обробляти та зберігати інформацію якомога раніше і якомога ближче до її джерел. Цей підхід дозволяє аналізувати та трансформувати великі обсяги даних у реальному часі локально, на межі мереж. Таким чином, ви економите час та інші ресурси, які інакше були б потрібні для надсилання всіх даних до хмарних служб. Результатом є зменшена затримка системи, що призводить до реакцій у режимі реального часу та підвищення продуктивності.

Обчислення краю здійснюються на шлюзах, локальних серверах або інших крайових вузлах, розкиданих по мережі. На цьому рівні дані можуть бути:

- оцінюються, щоб визначити, чи потрібна подальша обробка на більш високих рівнях
- відформатовані для подальшої обробки
- розшифровані
- відфільтровані
- перенаправлені на додатковий пункт призначення

Підводячи підсумок, перші три шари бачать дані в русі, оскільки вони постійно рухаються та змінюються. Лише після досягнення наступного рівня дані остаточно перебувають у стані спокою та доступні для використання споживчими програмами.

Рівень обробки: зробити необроблені дані корисними

Шар обробки накопичує, зберігає та обробляє дані, що надходять із попереднього шару. Всі ці завдання зазвичай виконуються на платформах IoT і включають два основні етапи.

Етап накопичення даних

Дані в режимі реального часу фіксуються за допомогою API і перебувають у стані спокою, щоб задовольнити вимоги програм, що не в реальному часі. Етап компонента накопичення даних працює як транзитний вузол між генерацією даних на основі подій та споживанням даних на основі запитів.

Крім усього іншого, етап визначає, чи дані відповідають вимогам бізнесу та де їх слід розміщувати. Він зберігає дані в широкому діапазоні рішень для зберігання даних, від озер даних, здатних утримувати неструктуровані дані, такі як зображення та відеопотоки, до сховищ подій та телеметричних баз

даних. Загальна мета - відібрати велику кількість різноманітних даних та зберегти їх найбільш ефективним способом.

Етап абстракції даних

Тут підготовка даних завершена, щоб споживчі програми могли використовувати їх для отримання статистичних даних. Весь процес передбачає такі кроки:

- поєднання даних з різних джерел, як IoT, так і не IoT, включаючи ERM, ERP та CRM системи
- узгодження декількох форматів даних
- агрегування даних в одному місці або надання їм доступу незалежно від їх розташування за допомогою віртуалізації даних
- Подібним чином, дані, зібрані на рівні програми, тут переформатовуються для надсилання на фізичний рівень, щоб пристрої могли це «зрозуміти»

Разом етапи накопичення та абстрагування даних завуальовують деталі апаратного забезпечення, покращуючи взаємодію смарт-пристроїв. Більше того, вони дозволяють розробникам програмного забезпечення зосередитись на вирішенні певних бізнес-завдань, а не на заглибленні в технічні характеристики пристроїв різних постачальників.

Прикладний рівень: задоволення бізнес-вимог

На цьому рівні інформація аналізується програмним забезпеченням, щоб дати відповіді на ключові ділові питання. Існують сотні програм IoT, які відрізняються за складністю та функцією, використовуючи різні технологічні стеки та операційні системи. Деякі приклади:

- програмне забезпечення для контролю та управління пристроєм
- мобільні програми для простої взаємодії
- служби ділової розвідки

- аналітичні рішення з використанням машинного навчання

В даний час додатки можна будувати прямо на платформах IoT, які пропонують інфраструктуру розробки програмного забезпечення з готовими до використання інструментами для видобутку даних, вдосконаленою аналітикою та візуалізацією даних. В іншому випадку програми IoT використовують API для інтеграції з проміжним програмним забезпеченням.

Бізнес-рівень: впровадження рішень, керованих даними

Інформація, сформована на попередніх рівнях, приносить цінність, якщо лише вона призводить до вирішення проблем та досягнення бізнес-цілей. Нові дані повинні ініціювати співпрацю між зацікавленими сторонами, які, в свою чергу, запроваджують нові процеси для підвищення продуктивності.

У прийнятті рішень зазвичай бере участь більше однієї людини, яка працює з кількома програмними рішеннями. З цієї причини бізнес-рівень визначається як окремий етап, що перевищує рівень окремого додатка.

Рівень безпеки: запобігання порушенням даних

Само собою зрозуміло, що повинен бути рівень захисту, що охоплює всі вищезазначені шари. Безпека IoT - це широка тема, яка заслуговує на окрему статтю. Тут буде вказано основні особливості безпечної архітектури на різних рівнях.

Безпека пристрою. Сучасні виробники пристроїв IoT зазвичай інтегрують функції захисту як в апаратне забезпечення, так і в прошивку, встановлену на ньому. Це включає:

- вбудовані мікросхеми TPM (Trusted Platform Module) з криптографічними ключами для автентифікації та захисту пристроїв кінцевих точок
- безпечний процес завантаження, який запобігає запуску несанкціонованого коду на включеному пристрої

- регулярне оновлення виправлень безпеки
- фізичний захист, як металеві щити, щоб заблокувати фізичний доступ до пристрою

Безпека з'єднання

Незалежно від того, чи дані надсилаються через пристрої, мережі чи програми, вони повинні бути зашифровані. В іншому випадку конфіденційну інформацію може прочитати кожен, хто перехоплює інформацію під час передачі. IoT-орієнтовані протоколи обміну повідомленнями, такі як MQTT, AMQP та DDS, можуть використовувати стандартний криптографічний протокол Transport Layer Security (TSL) для забезпечення наскрізного захисту даних.

Хмарна безпека

Дані у стані спокою, що зберігаються в хмарі, також повинні бути зашифровані, щоб зменшити ризик викриття конфіденційної інформації зловмисникам. Хмарна безпека також передбачає механізми автентифікації та авторизації для обмеження доступу до програм IoT. Іншим важливим методом безпеки є управління ідентифікацією пристрою, щоб перевірити надійність пристрою, перш ніж дозволити йому підключатися до хмари.

Хороша новина полягає в тому, що рішення IoT від великих провайдерів, таких як Microsoft, AWS або Cisco, постачаються із заздалегідь побудованими заходами захисту, включаючи наскрізне шифрування даних, аутентифікацію пристрою та контроль доступу. Однак завжди варто платити за те, щоб безпека була на всіх рівнях - від найменших пристроїв до складних аналітичних систем.

1.3 Поняття приватності та конфіденційності

Інформація — це валюта технологій. Конфіденційність в Інтернеті залежить від можливості контролювати як обсяг особистої інформації, яку ви надаєте, так і осіб, які мають доступ до такої інформації.

Зростання Інтернету та технологічних розробок призвели до вибуху даних створені споживачами та про них. Пристрої та датчики постійно ввімкнені і мають доступ до мережі, тому ще більше посилюють цю тенденцію. Тому необхідно забезпечити необхідні права користувачам незважаючи на постійний зріст загроз, а для цього необхідно визначитись з цілями.

Право на приватність та захист даних є ключовими елементами для розуміння того, як дані стали центральним елементом багатьох змін в людських взаємовідносинах і взаємодіях, нові бізнес-моделі та технологічний розвиток все більше звязують світ мережею. В так званій *економіці, керованій даними*, принципи, концепції та правові основи обробки даних принципово важливі для розробки загальної правової концепції власності[3].

Право на приватність завжди було темою бурхливих дискусі. Воно висвітлювалось під заголовками, як право залишатися наодинці, як гарантія особистого життя, розвиток сімейного життя і як невід'ємна частина формування особистості. Але нові технології змінили контекст цього права.

Наприклад, Інтернет змінив спосіб, людського спілкування і відношення один до одного, адже тепер всі виробляють і споживають інформацію. Люди перестали бути лише одержувачами, а стали виробниками контенту, і завдяки цьому сформувався великий обсяг інформації. Інші типи технологій, такі як смартфони та діджиталізація надали доступ до інформації, зробили його легшим, так що сьогодні, навіть, дитина без проблем може «загуглити» те що її цікавить. Тим самим відкривши простір для ще більшого і швидшого поновлення і створення інформації.

Це означає що із величезним збільшенням обсягу всієї інформації, масово зростають об'єми обігу персональних даних. Що змушує, в свою чергу, переглянути традиційне значення конфіденційності або ж пробуджує бажання контролю та прозорості політики поводження з даними.

Конфіденційність - це концепція, яка постійно змінюється. Раніше приватність розглядалась як право бути залишеним наодицні. Тоді не обговорювались проблеми, які можуть створити нові технології для прав особистості.

Можна зазначити, що поняття конфіденційності в зародку стосувалось лише охорони проти втручання третіх сторін. Але в даний час, в економікі, що зумовлена переробкою персональних даних, конфіденційність набула зв'язку з контролем персональних даних.

Європейська система прав людини ще з самого свого зародження розглядала конфіденційність та приватне життя за Конвенцією еластичним, широким терміном, який охоплював як негативні, так і позитивні зобов'язання. Поняття, що таке право охоплює не лише можливість залишитись наодинці, а також будувати власну особистість та стосунки з іншими людьми і світом було дуже скоро визнано. Воно швидко вийшло на перший план і стало однією з основних опор, що лежать в основі цілого виміру.

В широкому змісті конфіденційність розглядається як охоплення захисту багатьох аспектів людини, фізичної та соціальної ідентичності.

Як можна зазначити, право на приватність дозріло для розвитку в Інтернаціональній система. Проте захист даних ще не розвинувся як самостійна концепці. Розвиток нових технологій, швидше за все, поставить під сумнів сферу захисту конфіденційності даних.

Системі доведеться визначити рівень прозорості та доступу до інформації, які матимуть різні особи. Мінімальна основа для інформаційної

безпеки та гарантії пов’язані з біометричними та конфіденційними даними є також важливими темами, які, ймовірно, з’являться.

Оскільки конфіденційність та захист даних набувають все більшого значення для світу, необхідно розробляти концепцію враховуючи або робючись з культурними, економічними та правовими ландшафтами.

На сьогодні поняття «конфіденційність інформації» утвердилось у властивості інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і (або) процесом. Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею.

У всьому світі вже існують усталені закони про захист даних та конфіденційність, вони застосовуються до мобільних операторів роками. GSMA(об'єднання мобільних операторів та інших компаній мобільного зв'язку з усього світу) вважає, що можна застосувати наявні дані правила та принципи захисту щодо задоволення потреб у приватному житті в контексті послуг IoT та інших технологій[4].

Однак послуги IoT, як правило, залучають більше сторін, ніж просто мобільні оператори, такі як виробники пристроїв, онлайн-платформи і навіть державний сектор. Важливо, щоб існували нормативні акти, чіткість та юридична визначеність щодо послуг IoT, а також норми конфіденційності та захисту даних застосовували послідовно для всіх постачальників і користувачів Інтернету речей у нейтральному відношенні до послуг та технологій.

Регулятори повинні підтримувати та заохочувати заходи, за допомогою яких галузь може визначити та пом'якшити ситуацію, ризики для конфіденційності та за допомогою яких вони можуть продемонструвати відповідальність, наприклад через конфіденційність, вдосконалення

технологій та інструментів, які допомагають споживачам керувати своєю приватністю та контролювати, як використовуються їх дані.

Практики захисту даних та безпеки, розроблені для певної послуги IoT, повинні відображати загальний ризик для приватного життя особи та контекст, в якому знаходяться дані про неї , які збирали, розповсюджували та використовували. Будь-які регуляторні втручання повинні обмежуватися областями, де виникають виявлені ризики, а існуючих заходів недостатньо для їх вирішення.

GSMA та її члени спираються на свій великий досвід у вирішенні питань конфіденційності та безпеки проблеми та працюють спільно зі своїми партнерами IoT, такими як виробники пристроїв та постачальники послуг з освіти, щоб вбудувати конфіденційність та безпеку в технології IoT та загальний споживчий досвід. Ця тривала співпраця забезпечить можливість партнерам IoT галузі виявити та пом'якшити відповідні ризики конфіденційності споживачів у контексті послуг, що надаються[4].

1.4 Проблеми захищеності інформації в IoT

IoT пропонує значні можливості та потенціал для керування даними, інновації для досягнення цілей економічної, соціальної та державної політики та покращення повсякденного життя людей. Наприклад, IoT забезпечить безліч нових додатків та послуг, розширюючи можливості споживачів стежити за своїм здоров’ям чи керувати споживанням енергії свого житла незалежно від місце знаходження, «розумні» рішення для дому та міста, що ведуть до зниження рівня забруднення, кращого управління дорожнім рухом тощо[21].

Багато служб IoT будуть призначені для створення, збору або обміну даними. Деякі з цих даних (наприклад, дані про стан автомобілів чи фізичний стан користувача) вважаються «особистими даними» або впливають на

конфіденційність споживача, а отже, підлягають під закони про захист особистості та приватне життя[22].

Однак багато служб IoT включають дані про окремих споживачів і підпорядковуються загальним законам про телекомунікації. Якщо послуги IoT надають мобільні оператори, вони також підпорядковуватимуться телекомунікаційним правилам конфіденційності та безпеки. IoT для споживачів послуг, ймовірно, включатиме генерацію, розповсюдження та використання детальних даних, які можуть вплинути на приватність осіб. Наприклад, від висновків про їх здоров’я до розвитку цифрового потенційного клієнта на основі їхніх звичок покупок та місцезнаходження. У міру набуття популярності послуг споживання IoT, буде створено більше даних про споживачів, проаналізовано в режимі реального часу та передано між різними сторонами через національні кордони[3].

Справа в тому, що якщо IoT стане вездесущим - усі (приватні особи та підприємства) будуть потенційно вразливими. Зв'язування об'єктів пропонує нові можливості впливу та обміну. Це призводить до безлічі нових (а також уже відомих) потенційних ризиків, що стосуються інформаційної безпеки, конфіденційності та захисту даних, що необхідно враховувати. Тяжкість і ймовірність кожного ризику залежатиме від обставини, за яких розгортається кожна програма / система IoT.

Існують такі особливості Інтернету речей:

- Чотири ключові технологічні галузі забезпечують основу IoT: всеохоплююча ідентифікація та адресація, обробка, створення мереж та зондування
- Зв'язок відбуватиметься від об'єкта до об'єкта та від об'єкта до людини
- Обсяг даних, що збираються та обробляються фізичними особами, суттєво збільшиться і буде надходити з різних (нових) джерел

- Більшість комунікацій відбуватимуться автоматично - об’єкти вирішать обмінюватися даними зі своїми навколишнього середовища, можливо, без того, щоб користувач про це знав
- Об’єкти неоднорідні, можуть забезпечувати різні функціональні можливості в залежності від їх контексту

Спираючись на ознаки, визначені вище, можна визначити деякі основні виклики та проблеми, що стосуються конфіденційності, захисту даних та інформаційної безпеки.

Конфіденційність, захист даних та інформаційна безпека доповнюють один одного. Інформаційна безпека розглядається як збереження конфіденційності, цілісносності та доступності інформації.

Інформаційна безпека сприймається як основна вимога у наданні послуг IoT для галузі, як з метою забезпечення безпеки для самої організації та створення вигоди й для громадян.

Можна сказати, що до інформаційної безпеки мають застосовуватися загальні вимоги щодо безпеки, оскільки IoT - це особливий випадок і скоріше треба розглядати концепцію підходу, а не конкретну технологію, звісно ще складно правильно визначити всі вимоги[5]. Відповідно до різних досліджень з виявлення потенційних ризиків у таких сильно взаємопов'язаних середовищах, можна зазначити наступні відкриті питання.

Забезпечення безперервності та доступності у наданні послуг на основі Інтернету речей

Дуже важлива проблема і полягає у забезпеченні доступності та безперервності надання послуг та уникненні будь-якої можливості операційного збою чи перебою зв'язку. Це безпосередньо стосується архітектурної моделі, структура якої залежить від послуг, що плануються надаватись: централізована чи децентралізована.

Слід також розглядати не лише дані, що стосуються ідентифікованої особи, як особисті дані, але це також відноситься до даних, що стосуються осіб, соціальна ідентичність яких(ім’я, адреса, ...) не є безпосередньо відомою, але може бути розкрита наприклад за допомогою ідентифікації конкретного об'єкта або співставлення даних з різних джерел.

Проектування технологій IoT

Інформаційна безпека, конфіденційність та захист даних повинні систематично вирішуватись на стадії проектування. На жаль, у багатьох випадках вони додаються згодом ,а не передбачаються і дана функціональність планується на місці. Це не тільки обмежує ефективність додаткової інформації, заходів безпеки та конфіденційності, але також є менш ефективним з точки зору витрат на їх впровадження. Більше того, об'єкти IoT не завжди мають достатньо обчислювальної потужності для реалізації всіх відповідних рівнів безпеки чи не мають такі функціональні можливості взагалі. Неоднорідність об'єктів стає дуже складною в цьому контексті. Подібним чином необхідно враховувати неоднорідність політики конфіденційності.

Ризики мають контекстний та ситуативний характер

Чим більше людей залучено до процесу, тим більше міркувань та політик щодо конфіденційності стають контекстними та ситуативними, а отже, більш складним стає виявити та оцінити потенційні загрози. Що стосується виявлення конфіденційності, захисту даних та ризиків безпеки, це залежить від контексту та призначення об’єктів, що розглядаються (наприклад: здоров’я, геолокація…).

Простежуваність / профілювання / незаконна обробка

Збільшений збір даних може викликати проблеми автентифікації та довіри до об’єктів. Крім того, слід також зазначити, що за допомогою зібраної

інформації з кількох об’єктів, пов’язаних з однією людиною, ця особа може бути легше ідентифікована і пізнана.

Повторне використання даних підвищується в середовищі

Завдяки розповсюдження збільшеного обсягу даних в середовищі IoT існує проблема того як будуть дані використання для додаткових цілей або інших цілей, які не були вказані спочатку. Переназначення даних може бути ще до початку збору даних, наприклад правоохоронні органи або спецслужби можуть вимагати доступу до даних, зібраних іншими особами для зазначених цілей. Це не тільки стосується порушення особистих прав на приватне життя, але також може вплинути на широкі соціальні та громадські інтереси.

Реалізація прав на захист даних для фізичних осіб та дотримання законодавства для організацій

Необхідно розглянути наслідки впровадження IoT для суб’єктів даних та їх прав на захист даних та питання щодо того, як застосовувати принципи захисту даних у цій галузі. За допомогою IoT додатків, що працюють у фоновому режимі, можуть використовуватись персональні дані, а користувачі навіть не знати про будь-яку їх обробку.

Втрата / порушення конфіденційності особи та захисту даних - природна характеристика IoT

Навколишнє середовище – це поширеність пристроїв, датчиків, зчитувачів та додатків, які потенційно можуть збирати безліч типів даних про людей, коли вони рухаються в таких середовищах. Можливості автоматичної ідентифікація об'єктів може призвести до автоматичної ідентифікації осіб, які не мають не бажають втручання в їхній простір і не мають ніякого відношення до проведення цільової операції.

Інформація, зібрана на основі ідентифікаторів об'єктів, даних датчиків та можливостей зв'язку

Таким чином, системи IoT можуть розкривати інформацію про людей, їх звички, місцезнаходження, інтереси та інше. Особиста інформація та інші уподобання зберігаються для подальшого використання в системах. У поєднанні з даними доступних з інших служб або джерел, діяльність з видобутку даних може навіть створити нові знання про осіб, які можуть не виявитись шляхом окремого вивчення базових наборів даних. Посилення занепокоєння стосуються відмови електронної ідентифікації та ідентифікації крадіжки. Прикладом цієї проблеми може бути те, що в безконтактних кредитних картках можна прочитати ім’я та номер картки без будь-якої автентифікації. За допомогою цих даних зловмисники можуть придбати товари з ідентифікацією та отримати доступ до банківського рахунку власника картки.

Реалізація шкідливих атак на пристрої та системи IoT

Компрометація систем IoT через невідповідний або неадекватний контроль за інформаційною безпекою є дуже важливим ризиком, оскільки це може призводити до подальших ризиків, деякі з них вже були згадані. Завдання зловмисника полягає у визначенні засобів контролю систем IoT, для яких ще не відомо, яке саме поширення вони мають. Це також залежить від остаточної архітектури IoT (розподілена або централізована). Однак, оскільки очікується, що більше даних буде передаватися, ніж у традиційних архітектурах, існує підвищений ризик реалізації атак та отримання несанкціонованого доступу до даних передається.

Блокування користувачів

Як у випадку з існуючими додатками та технологіями (наприклад, хмарні обчислення та соціальні програми мережа) існує підвищений ризик замикання споживачів на певному постачальнику послуг IoT, їм важко

переходити від одного постачальника до іншого та зменшувати свою портативність даних. Така залежність буде шкідливою для користувачів, які мають контроль над своїми даними та право вибору постачальників.

Наслідки, пов’язані зі здоров’ям

Швидкий розвиток ІКТ призвів до збільшення кількості портативних пристрої та датчиків (Інтернет речей), які забезпечують різні сценарії електронного контролю здоров’я, такі як віддалений моніторинг пацієнта. Очікується, що «Інтернет речей» створить значний вплив на подальше надання послуг охорони здоров'я. Однак невисока надійність технологій IoT в e-Health створює небезпеку та ризики конфіденційності. Зокрема, існують ризики щодо ідентифікації пацієнта та надійності зібраної інформації. Більше того, сучасні рішення електронної охорони здоров’я, засновані на IoT базуються на відкритих, взаємопов’язаних середовищ, які збирають та швидко обмінюються конфіденційними даними, роблячи проблему ще важчою. Крім того, в деяких випадках фізична цілісність людини (причина смерті тощо) може бути під загрозою.

Наприклад, це може бути випадок активних або пасивних функцій безпеки, що використовуються в автомобілі (наприклад, гальмо автоматично гальмує за певних обставин) або «речах», що використовуються у секторі охорони здоров’я (наприклад, якщо це може бути кардіостимулятор запрограмований дистанційно піддає людину ризику). Додаток також може виявити, що людина страждає на певні захворювання, і цим можна скористатися для фізичного нападу на цю людину.

Втрата контролю користувача / труднощі з прийняттям

Безумовно, автоматизовані рішення створять не тільки сприйняття втрати контролю, але можуть також призвести до фактичної втрати контролю, оскільки одна з головних цілей IoT - це надання деякої автономії об’єктам та

автоматизація прийняття рішень. І сприйняття, і фактична втрата контролю може мати серйозний вплив на багато аспектів повсякденного життя людини.

З іншого боку, IoT може допомогти людям похилого віку або інвалідам довше залишатися вдома та контролювати свої справи, власне життя, тоді як контроль над певними «детальними рішеннями» може бути обмежений.

Рішення, що приймаються пристроями чи програмами автоматично на основі цього величезного набору даних, що сприймаються, можуть не бути прозорими для суб'єктів даних ,а отже створюють відчуття втрати контролю. До того ж ці рішення буде важко зрозуміти людеям, оскільки особливо часто інформація, яка збирається за допомогою датчиків, підсвідомо розпізнається лише окремими людьми.

Право

З огляду на глобальний характер IoT, інша проблема полягає в тому, що приватні особи та компанії стикаються з низкою національних / регіональних законів про захист даних, що забезпечують різні рівні захисту.

Коли контролери даних систем IoT та особи, на яких впливають ці системи, знаходяться в різних країнах, це потенційно може призвести до багатьох різних проблем з законами.

Згідно з вищевикладеним, основними цілями має бути ефективний захист персональних даних, що тягне за собою застосування правових принципів, а також ефективної інформаційної безпеки (конфіденційність, цілісність, доступність) послуг, з метою надання кращих послуг IoT для громадян.

Іншим цікавим елементом є питання універсальності захисту персональних даних, яке буде дуже важливим і актуальним в середовищі IoT. Окрім очевидних юридичних проблем, питання сфери вибору користувачів і переносимість даних також потрібно враховувати.

Через глобальний характер IoT важливо підвищити рівень гармонізації законодавства про захист даних та забезпечити високого рівня правозастосування[6]. Обґрунтовано можна зазначити, що якщо IoT має відповідати відповідним вимогам:

- право на видалення
- право забути
- переносимість даних
- конфіденційність
- принципи захисту даних.

Висновки:

В цьому розділі було розглянуто концепцію Internet of Things загалом. Також було наведено приклади актуальності його використання. Також було визначено проблеми конфіденційності за допомогою розгляду її зі сторони технічного забезпечення і з боку правового поняття. Виділення проблем IoT дає змогу покращити систему шляхом їх аналізу і подальшого вирішення.

РОЗДІЛ 2.
РІШЕННЯ ВИЗНАЧЕНИХ ВРАЗЛИВОСТЕЙ

2.1 Стратегії і підходи вирішення проблем інформаційної безпеки

При формуванні політики IoT слід ретельно враховувати два загальних принципи[7]:

- IoT не повинен порушувати людську ідентичність, цілісність людини, права людини, конфіденційність особи, громадські свободи.
- Особи залишаються під контролем своїх персональних даних, що генеруються або обробляються в IoT, за винятком випадків, коли це суперечить попередньому принципу.

Є низка критичних аспектів, які прямо або вторинно впливають на інформаційну безпеку в IoT. Найперше – це організаційні заходи, такі як:

- створення і впровадження єдиної політики інформаційної безпеки підприємства з урахуванням всіх додатків і систем,
- розробка правил безпечного використання IoT-приладів і мереж,
- вдосконалення законодавчого забезпечення недоторканності приватного життя та особистої, державної та інших таємниць,
- державна і приватна стандартизація і сертифікація пристроїв, каналів передачі, сховищ інформації та прикладного ПО з обробки та аналізу даних.

Технічні інструменти захисту даних від витоків, втрат і перехоплення, управління, використання також потребують переконфігурації, де це необхідно. Має бути реалізація шифрування та/або інших криптографічних методів, персоналізація IoT-пристроїв з використанням унікальних ідентифікаторів ID, MAC-адрес, ключів і сертифікатів, що забезпечують досить високий рівень кібербезпеки без додаткових витрат, гнучкі політики управління доступом з багатофакторною авторизацією, резервування,

реплікація, організація захищеного периметра і інші засоби інформаційної безпеки[7].

Обладнання, яке використовується в IoT мережах не завжди відповідає необхідним критеріям. Виробник повинен нести відповідальність зі своєї сторони за продукцію і її цілеспрямленість. Для повної відповідності вимогам мають використовуватись сучасні і надійні інструменти програмної розробки (API, бібліотеки, фреймворки, протоколи…) і апаратні рішення (плати, контролери та ін.). Бажано скоротити кількість компонентів, необхідних для роботи обладнання, оскільки кожен додатковий елемент є потенційним джерелом вразливостей і фізичних поломок. Девайси мають реалізувати безпечну аутентифікацію, узгодження зашифрованих сеансів і перевірку автентичності користувачів. Для того, щоб як найдовше зберігати надійність і актуальність складових систем виробник повинен забезпечити регулярний випуск оновлень ПО для усунення знайдених і потенційно можливих вразливостей[8].

Незважаючи на те, що дана область діяльності непідконтрольна окремому користувачеві IoT-системи, а регулюється галузевими гігантами або цілими державами, вона дуже важлива для кінцевого клієнта - підприємства або фізичної особи. Тому необхідно повноцінно ввести стандарт, адже він регулює довіреність інформаційної та фізичної компонентів IoT-систем: надійність, функціональну безпеку, інформаційну безпеку, безпеку персональних даних, стійке функціонування в умовах атаки. Тому за останні роки державні і міжнародні організації провели низку заходів для стандартизації і регламентування. Однак, питання кібербезпеки інтернету речей хвилюють не тільки державних чиновників. Питаннями сертифікації IoT-систем займаються і приватні компанії, а також незалежні експертні співтовариства. На жаль, сьогодні сертифікація ще не діє повноцінно[23]. Навіть наявність сертифікатів, що підтверджують відповідність IoT-системи вимогам приватних програм, громадських ініціатив або міжнародних

стандартів інформаційної безпеки не гарантує 100% -вий захист Інтернету речей. Також варто відзначити деякі негативні наслідки заходів щодо підвищення рівня захисту інтернету речей від злому і втрати даних :

- багатофакторні системи аутентифікації вводять додаткові і часто незручні дії для користувачів, що викликає їх роздратування;
- складні криптографічні операції і необхідність безпечного зберігання даних значно збільшують вартість мікросхем;
- роботи по забезпеченню кібербезпеки істотно збільшують терміни і вартість створення кожного компоненти IoT-системи.

Для підтримки тенденції захищеності даних в мережі Інтернету речей, відносно нової технології, не достатньо розглянути її зі сторони самостійної концепції та методів її реалізації. Ефективним буде використання симбіозу недавно створених технологій та реалізація нових на основі існуючих[9].

2.2 Методи захисту інформації і протидії атакам в IoT

Хмарне зберігання

Постійне зростання зберігання зібраних даних в IoT системах зумовлює швидкий розвиток усього ринку сховищ. Із зростанням Інтернету речей (IoT) їх кількість пристроїв зондування інформації, підключених до Інтернету збільшується, щоб усвідомити взаємозв'язок між людьми, пристроїв та „речей“. Новий прогноз IDC оцінює що буде 41,6 мільярда пристроїв Інтернету речей у 2025 році, які будуть генерувати 79,4 зеттабайт даних. Забезпечуючи зберігання та управління даними, система хмарного зберігання стає необхідною частиною нової екосистеми. В даний час уряди, підприємства та окремі користувачі активно переносять свої дані до хмари. Така величезна кількість даних несе велику цінність. Однак це збільшує можливий ризик,

наприклад, несанкціонований доступ, витік даних, розкриття конфіденційної інформації.

Хмарне сховище - це, по суті, система хмарних обчислень, яка дозволяє користувачам зберігати та обмінюватися даними в мережі[10]. Переваги хмарного зберігання включають необмежений обсяг даних простору, зручної, безпечної та ефективної доступності файлів і стороннє резервне копіювання та низьку вартість використання. Хмарні сховища можуть бути розділені на п'ять категорій у практичному застосуванні:

- загальнодоступне хмарне сховище,
- особисте хмарне сховище,
- приватне хмара зберігання,
- гібридне хмарне сховище,
- хмарне сховище спільноти.

У публічній хмарі підприємства передають бізнес із зберігання даних на аутсорсинг постачальникам хмарних сховищ (наприклад, AWS та Alibaba Cloud) без розгортання інфраструктури та обслуговування серверів. Доступ до даних може мати лише уповноважений користувач. Такі переваги публічної хмари, як гнучкість, масштабованість та економія коштів, приваблюють велику кількість малих та середніх компаній підприємств. Персональна хмара, також відома як мобільна хмара зберігання, є по суті галуззю загальнодоступної хмари, але відрізняються з публічної хмари, вона надає послуги загальнодоступного хмарного зберігання для окремих користувачів. У приватній хмарі підприємствам це потрібно розгортати інфраструктури хмарного сховища та організовувати професійних персонал для управління та обслуговування серверів. Це гарантує, що приватна хмара має вищий рівень безпеки, ніж загальнодоступна та контроль даних знаходиться в руках самого підприємства. Але вартість різко зростає. Ця модель зберігання більше підходить для великих підприємств з великою кількістю дорогих та

конфіденційні дані. Гібридна хмара - це поєднання загальнодоступних хмара та приватна хмара, яка успадковує всі переваги обох. Підприємства можуть зберігати дорогі та конфіденційні дані у приватній хмарі та інші дані у публічній хмарі. Апеляція цієї моделі зберігання продовжує зростати. Як нова хмара режим зберігання в останні роки, хмара спільноти дуже підходить для медичної та фінансової промисловості. Хмара спільноти надає хмарні послуги для декількох підприємств у певному громада. Зазвичай у цих підприємств однакові проблеми або потрібно спільно працювати над деякими проектами. Інфраструктурою та управлінням серверами можуть спільно займатися члени хмари спільноти або передавати їх на третю сторону. З точки зору архітектури зберігання, в основному хмарні платформи зазвичай пропонують три широкі класи зберігання: блочне зберігання, зберігання файлів та зберігання об’єктів.

1) Блочне зберігання реалізується SAN, по суті забезпечує віртуальну мережу сховищ із забезпеченням логічного управління обсягом за допомогою спрощеного інтерфейсу веб-служб.

2) Зберігання файлів, як правило, асоціюється за технологією NAS. Разом з файловою системою, менеджери зберігання файлів управляють спільним використанням даних і доступом до даних, що зберігаються. Це є більш гнучким, ніж блокове зберігання. Масові дані створюють для підприємств низку проблем, таких як розширення сховища, обмін даними, ефективна передача, вартість та безпека даних. Коли зберігання даних досягає рівня PB, обмеження NAS та SAN безпосередньо веде до збільшення вартості технічного обслуговування обладнання в подальшому періоді. Вони не можуть повністю задовольнити вимоги підприємства щодо надійності, доступності, безпеки та інших показників даних масового зберігання в цьому об'єкті зберігання є більш критичним.

3) Зберігання об’єктів, наприклад AWS S3, оптимізовано для зберігання великих обсягів неструктурованих даних. Хмарне сховище базується на інфраструктурі віртуалізації та схоже на хмарні обчислення з точки зору

доступних інтерфейсів, масштабованості та ресурсів вимірювання. Воно складається з чотирьох шарів , які можна узагальнити наступним чином: 1) Складовий шар, основна частина хмарного сховища, зроблений з пристроїв зберігання даних та уніфікованого управління запам'ятовуючими пристроями. 2) Первинний рівень управління - це ядро, а також найскладніша частина хмарного сховища. 3) Рівень інтерфейсу програми – це найбільш гнучка частина хмарного сховища. 4) Останнє – це рівень доступу. З цієї точки зору, хмарне сховище постачає послуги доступу до даних, включаючи зберігання даних, обчислення даних, автентифікація та контроль доступу. Завдяки характеристикам хмарного зберігання, проблеми із захистом даних та конфіденційністю неминуче породжується.

Шифрування - це ефективна техніка захисту даних. Суть шифрування даних полягає у перетворенні оригінального файлу відкритого тексту або даних у рядок нечитабельного коду за деякими алгоритмами, який зазвичай називають зашифрованим текстом. Навіть якщо хтось перехоплює спотворений код, він / вона не може використовувати спотворений код, щоб отримати оригінальний вміст, який ефективно захищає конфіденційність даних та заважає їм від фальсифікації. Користувачі, яким надано доступ може розшифрувати файл за допомогою відповідного закритого ключа та потім оновити, змінити зашифрований текст. Шифрування поділяється на симетричне шифрування та асиметричне шифрування. Симетричне шифрування використовує секретний ключ для шифрування та дешифрування даних. Однак перед використанням симетричного шифрування користувачі потребують визначити ключ консенсусу, що дуже незручно для спільного користування файлами. Для порівняння, асиметричний шифрування, також відоме як шифрування відкритим ключем, - це більше зручно. Шифрування відкритого ключа містить пару ключів. Відкритий ключ, який можна розкрити іншим для шифрування файлів, тоді як приватний ключ використовується для розшифрування зашифрованого тексту.

Тому очевидно, що при використанні хмарного зберігання в мережі IoT уникаються ризики перифірійних вузлів, але виникають нові ризика вразливості хмарного сховища. Частково їх вирішує концепція Fog Computing.

Тумані обчислення

Концепція Fog Computing, розроблялася з орієнтацією на додатки IoT, хоча не виключаються й інші застосування Fog-систем, наприклад, в мережах зв'язку 5G.

Однак незважаючи на те, що розвиток Cloud-систем є необхідною умовою для успіху IoT, в деяких випадках, одні лише системи Cloud не можуть задовольнити вимогам швидшого аналізу і зростаючого обсягу даних від пристроїв IoT. Тому, все більше вимог пред'являється до попередньої обробки Edge Computing, яка є місцем розташування Fog-систем.

Це, призвело до створення концепції обробки даних на основі обчислень в хмарі Cloud. Така концепція отримала назву Mobile Edge Computing (MEC).

Основна мета Fog Computing - перемістити обчислення ближче до кордону мережі, знижуючи тим самим, необхідність віддалених комунікацій через центральне хмара Cloud і пов'язані з цим затримки і перевантаження смуги пропускання ядра мережі[11].

Зробивши вибір в сторону туманних обчислення очевидно можна отримати низку переваг. Вторгнення зловмисника до локальних служб виявляються вузлами туману при взаємодії з ними. Туманні обчислення дають гнучкість у виявленні і захисті даних, особливо, коли це стосується конфіденційної інформації. При передачі дані шифруються, що в свою чергу підвищує безпеку на кожній транзакції і обчислювальне навантаження не грає таку критичну роль як на перифірії. Дана технологія дозволяє зберігати дані в різних агрегатних станах, що підвищує подальшу швидкодію і енергоефективність.

Водяні знаки

IoT і хмарні технології отримали значну підтримку від урядів та науково-дослідні інститутів по всьому світу. Дані переміщуються у вигляді аудіо, відео, зображень та текст. Перевірка власності та захист авторських прав даних є складним завданням. Дані є вирішальним елементом в розумних міста, які підтримують інфраструктуру даних та допомагають людям отримати доступ до цифрового вмісту. Цифровий водяний знак забезпечує рішення для захисту авторських прав на цифровий вміст та перевірки права власності – секретне повідомлення, що розміщене всередині цифрового вмісту без шкоди для цінних даних. Ця секретна інформація згодом використовується для ідентифікації. Цифрові водяні знаки класифікуються: текстові водяні знаки, водяні знаки зображення, звукові водяні знаки та відео водяні знаки. Більшість досліджень зосереджена на зображеннях, аудіо та відео. В даний час текстовий водяний знак має отримав популярність завдяки великій кількості документів[12].

Машинне навчання

Штучні нейронні мережі - один з найбільш популярних алгоритмів машинного навчання. Він задовольняє безліч переваг, таких як відмовостійкість, адаптивне навчання і узагальнення. Отримані значення різних характеристик таких як відбиток пальця, силует і біфуркація, використовуються в якості вхідних даних в нейромережі для цілей навчання з використанням алгоритму зворотного поширення. Перевірка відбитка пальця виконується на основі попередніх експериментальних значень, що зберігаються в базі даних.

Машина опорних векторів - це навчальний алгоритм для нелінійних і лінійних класифікацій, аналізу головних компонентів, категоризації тексту, ідентифікації мовця і регресії. Це максимізує розрив між кордоном прийняття рішення і схемами навчання. Вектор ознак будується на основі значень

пікселів відбитка пальця і використовується для навчання SVM. Відбувається аналіз різних шаблонів відбитка, а потім виконується його зіставлення на основі ідентифікованих шаблонів.

Фундаментальна потреба в IoT - забезпечити безпеку всіх систем і пристроїв, підключених до мережі. Роль машинного навчання полягає у використанні та навчанні алгоритмів для виявлення аномалій в пристроях IoT або для виявлення будь-яких небажаних дій, що відбуваються в системі IoT, для запобігання втрати даних або інших проблем. Таким чином, машинне навчання являє собою платформу з високим потенціалом для подолання ризиків вразливості IoT[13].

Застосування машинного навчання допомагає уникнути Dos-атак шляхом підвищення точності дедукції, підслуховування шляхом використання стратегій розгрузки на основах одного з навчань, спуфінгу шляхом підвищення точності визначення і точності класифікації, витоку даних шляхом використання алгоритмів цілосності[14].

2.3 Розгляд технології Blockchain

Блокчейн - пов'язаний ланцюжок блоків даних, який дозволяє створювати записи транзакцій. На основі протоколу розподіленого консенсусу, керованого учасниками (тобто вузлами мережі), в яких відсутнє центральне керування. За побудовою ланцюжок записів є незмінним; тобто жоден вузол не може змінювати вміст раніше узгоджених блоків. Іншими словами, дозволені тільки вставки або агрегації нових транзакцій, оскільки неможливо видалити або змінити існуючі.

Властивість незмінності доповнюється додатковими характеристиками. По-перше, повинна існувати можливість отримання зведеної інформації про стан всього ланцюга в будь-який момент часу, щоб в разі маніпуляції з будь-яким блоком ланцюга можна було виявити таку маніпуляцію. По-друге, було

б бажано мати доступ до простого способу перевірки того, чи була транзакція включена в блокчейн чи ні. Нарешті, сторонам, які беруть участь в транзакції, які повинні бути включені в будь-який з блоків, має бути дозволено робити це анонімно.

Зв'язок блокчейн ланцюгу базується на хеші. Хеш-функції можна визначити як функції, які здатні перетворювати будь-який блок двійкових даних в інший двійковий блок фіксованого розміру. Результат такого перетворення називається хешем або дайджестом.

Хеш-функції

З математичної точки зору хеш-функції створюються з використанням концепції односторонніх функцій Trapdoor (TOWF), які представляють собою функції, визначені між наборами X і Y

$$f: X \to Y, f(x) = y$$

f – одностороння функція, отже, з точки зору обчислень, її повинно бути легко обчислити,

$f(x) = y$ для всіх елементів $x \in X$, але в той же час має бути важко отримати $x = f^{-1}(y)$ для значень $y \in Y$.

Якщо додаткова функція відома, то має бути можливим вичислити за поліноміальний час елемент $x \in X$ щоб $f(x) = y$.

Таким чином, хеш-функція - це одностороння функція, яка застосовується до повідомлення m змінного розміру, де повідомлення належить певному набору повідомлень M, і надає дайджест повідомлення з фіксованим, заздалегідь визначеним розміром в бітах, n. Отже, хеш-функції можна описати наступним чином:

$$h: M \to \{0,1\}^n, h(m) = \widehat{m}$$

Оскільки хеш-функції перетворять повідомлення будь-якої довжини в набір з *n* бітів, кількість можливих хешів набагато менша, ніж кількість різних вхідних повідомлень. Отже, завжди будуть різні повідомлення, дайджести яких збігаються.

Властивості:

1. Бітова залежність: хеш повідомлення $h(m) = \hat{m}$, має бути складною функцією, яка залежить від усіх бітів повідомлення, так щоб при зміні біту повідомлення його хеш має змінюватись приблизно наполовину.
2. Супротив прообразу: має бути важко обчислити повідомлення m з відомого хешу $\hat{m}$, так щоб $h(m) = \hat{m}$. Тобто будь-яку хеш функцію має бути важко обрахувати.
3. Супротив другому прообразу: Взявши повідомлення m_1, має бути важко знайти інше повідомлення m_1, $m_1 \neq m_2$ з одного хешу. Тобто не має бути можливості виявити інше повідомлення, таке що $h(m_1) = h(m_2)$.
4. Супротив зіткненням: пошук двох повідомлень повинен бути обчислювально важким m_1 і m_2, $m_1 \neq m_2$, а також $h(m_1) = h(m_2)$.

Властивість 1 дозволяє гарантувати цілісність інформації, так як при зміні будь-якої кількості біт результат функції покаже велику різницю між вихідним хешем і новим хешем, тому атаки методом проб і помилок неможливі[15].

З іншого боку, варто згадати, що, незважаючи на схожість, останні два властивості насправді різні. Властивість 3 вважає, що одне з повідомлень відомо, і намагається знайти інше повідомлення з тим же хешем. Для порівняння, у властивості 4 до повідомлень не накладаються ніякі умови. Виходячи з парадоксу дня народження, опір зіткнення є більш слабким умовою, ніж опір другого прообразу. Якщо хеш-функція вразлива для опору зіткнень, її використання більше не рекомендується.

Відповідність вищевказаним властивостям гарантує, по крайней мере, на початковому етапі, що функції, які їх виконують, чи не уразливі і запобігають то, що, приймаючи в якості вхідних даних хеш повідомлення, вміст повідомлення може бути вилучено і що ніхто не зможе знайти ще одне повідомлення з таким же хешем.

Використання

Протягом деякого часу найбільш широко використовуваної хеш-функцією була MD5 (Message Digest 5), запропонована Ривестом, яка генерує хеш-значення довжиною 128 біт. Однак функція MD5 перестала використовуватися, коли в 2005 р були опубліковані деякі уразливості. Фактично, навіть незважаючи на те, що він все ще використовується в незахищених контекстах, таких як перевірка цілісності завантажених файлів, в середовищах, де безпека є критичним аспектом, його використання заборонено.

Функція SHA-1 (Secure Hash Algorithm-1), яка генерує 160-бітові хеші, була прийнята Національним інститутом стандартів і технологій (NIST) в 1995 році. SHA-1 продовжує використовуватися досить часто сьогодні, хоча колізії були виявлені. Як і у випадку з MD5, його використання категорично відкидається більшістю міжнародних організацій і установ у сфері захищених додатків. Інша функція, яка надає 160-бітові хеші і досі використовується в деяких сценаріях, - це функція RIPEMD-160 (дайджест повідомлення оцінки примітивів цілісності RACE).

Сімейство хеш-функцій SHA-2 є наступником функції SHA-1. Специфікація SHA-2 включає функції SHA-224, SHA-256, SHA-384 і SHA-512, які забезпечують хеш-значення 224, 256, 384 і 512 біт відповідно, де SHA-224 і SHA-384 є усічені версії функцій SHA -256 і SHA-512 відповідно. Цей діапазон розмірів хеша значно підвищує безпеку в порівнянні з довжиною виведення MD5 і SHA-1.

У листопаді 2007 року NIST оголосив конкурс SHA-3 Cryptographic Hash Algorithm Competition, щоб вибрати стандартну хеш-функцію, що відповідає новим вимогам ефективності і безпеки. Оголошення про виграшною функції цього конкурсу було оприлюднено в жовтні 2012 року, і вибір припав на Keccak, який згодом був використаний в якості ядра сімейства функцій SHA-3. Версії Keccak 256 і 512 були прийняті в якості хеш-функції в ланцюжку блоків Ethereum.

2.4 Впровадження Blockchain в IoT мережу

Незважаючи на численні переваги, введені системою IoT у багатьох сферах, централізована архітектура IoT, яка пов’язує усі об'єкти IoT через центральний сервер, стикається з багатьма проблемами. Ці виклики є перешкодою для подальшого розвитку додатків IoT. Наприклад, одна точка відмови – якщо сервер виходить з ладу, всі програми та послуги IoT, пов'язані з ним, будуть відмовляти. Це впливає на доступність і якість обслуговування, що забезпечується системою IoT. Крім того, централізований сервер зберігає всі дані, створені з різних пристроїв IoT, в одному місці (центральний сервер), що робить його бажаною метою для багатьох зловмисників. Крім того, збереження конфіденційності даних видається сумнівним, оскільки всі дані IoT, які включають конфіденційну та особисту інформацію, зберігаються в одному місці на віддаленому сервері під повним контролем стороннього постачальника. Масштабованість централізованої архітектури - ще одна проблема, яка, можливо, не є практичним рішенням для системи IoT, яка щороку збільшується на мільярди одиниць.

З огляду на проблеми, що виникають внаслідок централізованої архітектури IoT, правильним вибором може бути переміщення IoT до архітектури з розподіленим реєстром. Серед поширених і популярних видів технологій розподіленої книги є блокчейн. По суті, це розподілена, децентралізована, спільна та незмінна книга, яка зберігає інформацію про різні

транзакції, які коли-небудь відбувались у певній одноранговій мережі (P2P). Було зібрано групу транзакцій, яким було призначено блок у книзі. Кожен блок має позначку часу та хеш-функцію, які використовуються для зв’язку поточного блоку з попереднім блоком. Це створює ланцюжки блоків, саме тому його називають блокчейном.

Щоб зберегти транзакцію в розподіленій книзі, більшість вузлів у мережі блокчейнів повинні записати свою згоду. Технологія Blockchain сприяє обміну інформацією, в якій усі користувачі / вузли, що надають участь у мережі blockchain, мають копію золотої / оригінальної книги, щоб усі користувачі отримували оновлення з нещодавно доданими транзакціями або блоками. Тому можна виділити низку критичних переваг використання блокчейну:

- Децентралізація: блокчейн - це, як правило, децентралізоване та розподілене середовище, яке базується на комунікації P2P між вузлами зв'язку. Децентралізація дозволяє використовувати обчислювальну потужність усіх користувачів, що надають участь, що зменшує затримку та усуває єдину точку відмови. Ця функція долає єдину точку несправності.
- Прозорість: на відміну від централізованої моделі, де центральний сервер має лише повний контроль і доступ до всіх даних, блокчейн пропонує хороший рівень прозорості, при якому всі вузли мають доступ до всіх деталей транзакцій, які коли-небудь відбувалися в їх мережі. Крім того, кожен вузол має копію розподіленої книги, щоб постійно оновлюватись із змінами. В додатку відсутність третьої сторони збільшує доброзичливість та довіру до бізнесу.
- Незмінність: серед найважливіших характеристик блокчейну є здатність гарантувати цілісність транзакцій шляхом створення незмінних книг. На відміну від централізованої моделі, де цілісність даних управляється і зберігається лише через центральний орган, що може бути загрозою, блокчейн використовує хеш-функції, які не

мають зіткнень, щоб зв’язати кожен блок з попереднім блоком, який підтримує цілісність блоку вмісту. Крім того, блоки, що зберігаються в книзі, ніколи не можуть бути змінені, лише якщо більшість користувачів підтверджують цю зміну.

- Покращена безпека: серед переваг технології блокчейн є те, що вона забезпечує кращий захист у порівнянні з існуючими рішеннями. Застосовуючи інфраструктуру відкритих ключів, блокчейн забезпечує безпечне середовище від різного роду атак. Крім того, механізм консенсусу забезпечує надійний метод, який покращує безпеку блокчейну. Більше того, відсутність єдиної точки відмови в технології блокчейну, яка може вплинути на цілі системи, забезпечує кращий захист над централізованою моделлю.
- Анонімність: незважаючи на те, що блокчейн використовує книгу, яка розподіляється між усіма користувачами, блокчейн забезпечує анонімну ідентифікацію для захисту конфіденційності вузлів. Функція анонімності може бути використана для забезпечення безпечної та приватної системи голосування.
- Зниження витрат: на відміну від централізованої архітектури, в якій для побудови централізованого сервера потрібна вдосконалена і повна апаратно-програмна система, технологія блокчейн зменшує витрати, пов’язані з установкою та підтримкою великих централізованих серверів, оскільки використовує обробну потужність зв'язку пристроїв.
- Автономність: здатність приймати автономні рішення є однією з функцій, яку може надати технологія блокчейн. Це дозволяє виробляти нові пристрої, здатні приймати розумні та автономні рішення. Наприклад, функції блокчейну, включаючи захист від несанкціонованого доступу та кращу безпеку, можуть бути

використані для створення кращих та безпечних автономних транспортних засобів.

Табл.2.1.: Порівняння показників IoT та Blockchain

Показник	IoT	Blockchain
Конфіденційність	Відсутність конфіденційності	Забезпечує конфіденційність вузла-учасника
Пропускна здатність	IoT девайси мають обмежені ресурси і пропускну здатність	Широка смуга пропускання
Структура	Централізована	Децентралізована
Масштабованість	IoT містить велику кількість пристроїв	Масштабується при великій мережі
Ресурси	Обмежені	Ресурсоємна система
Затримка	Вимагають низької затримки	Виявлення блоків займає багато часу
Безпека	Відкрите питання	Має кращий захист

Висновки:

Даний розділ був присвячений розгляду стратегій і методів рішення вразливостей мережі IoT. Було розглянуто зв’язки IoT з іншими технологіями. За допомогою перерахування можливих рішень було аналітично вирішено найоптимальніші з них. Завдяки цьому можна виявити найшвидший і найдієвіший спосіб реалізації підвищення інформаційної безпеки в IoT.

РОЗДІЛ 3:
ІНТЕГРАЦІЯ BLOKCHAIN В IOT СТРУКТУРУ

3.1 Модифікований метод захисту за допомогою блокчейну

В попередньому розділі окремо будо розглянуто рішення з використанням блокчейну для подолання низки пролем IoT. В цьому розділі буде запропоновано модель IoT з впровадженням блокчейну і наведено доведенняїї ефективності.

Проста архітектура IoT-блокчейн складається з чотирьох шарів. Блокчейн додається як окремий шар між мережевим та прикладним рівнями.

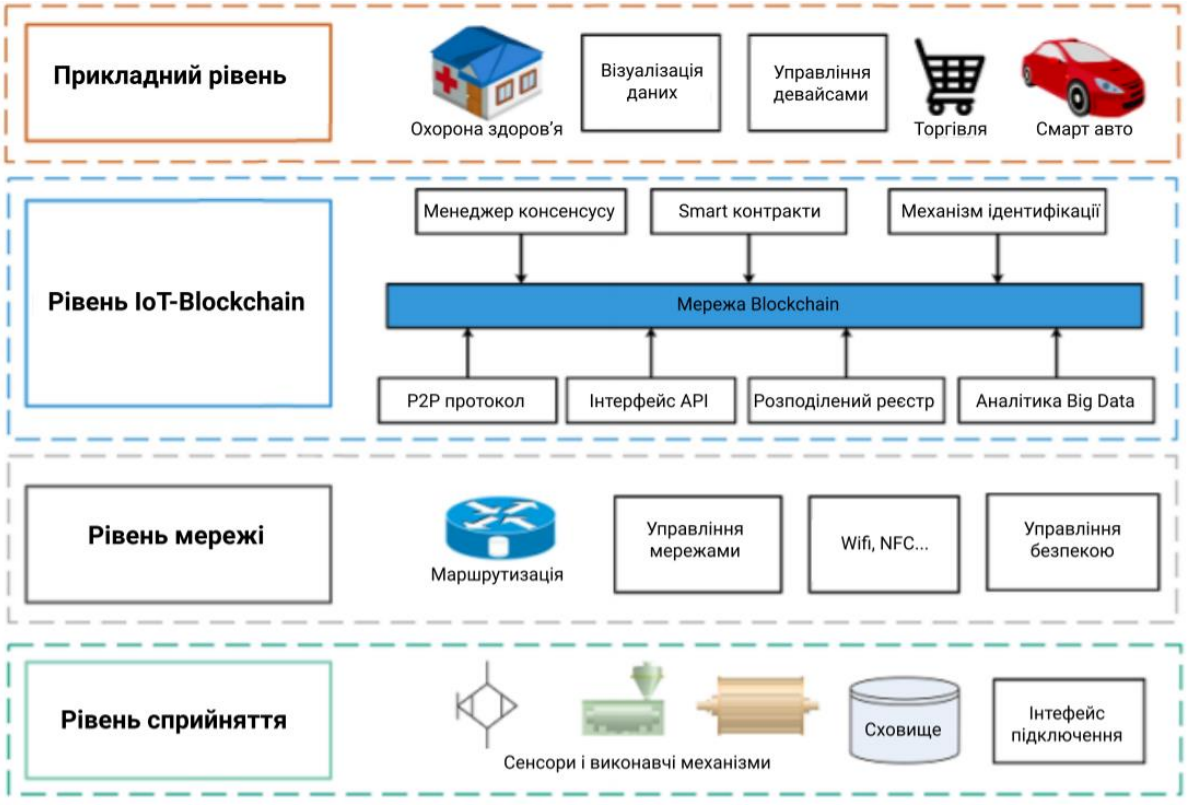

Рис.3.1: Рівнева модель IoT з використанням Blockchain

Перший рівень - це рівень сприйняття, який містить речі і предмети IoT, такі як датчики та виконавчі механізми, які використовуються для сприйняття навколишнього середовища та збору відповідних даних, які можуть допомогти зрозуміти оточення. Потім мережевий рівень, який здійснює управління

мережею та маршрутизацією, він дозволяє зв’язувати всі об’єкти Інтернету речей та взаємодіяти через Інтернет. Цей рівень включає в себе мережеві та захисні пристрої, які забезпечують зв'язок та управління безпекою.

Доданий рівень включає всі модулі, що дозволяють реалізувати різні функції технології blockchain в системі IoT. Ці особливості включають зв'язок P2P, розподілену книгу, смарт-контракти, API, аналіз великих даних, управління консенсусом та управління ідентифікацією. Протоколи P2P необхідні для забезпечення децентралізованого зв'язку між різними об'єктами IoT. Крім того, розподілений журнал є однією з важливих функцій, на котрі кожен пристрій IoT може мати копію, щоб його можна було оновлювати за кілька хвилин або навіть секунд у мережі IoT. Книга може бути створена як з дозволу, так і без нього. Тип книги буде сильно залежати від контексту та кількості вузлів у мережі IoT.

Модуль аналізу великих даних дозволяє блокчейну забезпечити ефективне онлайн-зберігання та обробку даних, оскільки система IoT створює величезні обсяги даних, які неможливо обробити за допомогою традиційних методів. Крім того, багато операцій депонуються в структурованих формах книг, що вимагатиме подальшого аналізу даних. Розумні контракти також є однією з важливих частин технології блокчейну, яка застосовується для автоматизованих рішень на основі заздалегідь визначених умов.

Як правило, смарт-контракт - це програмний код, який запускається за допомогою блокчейну для виконання набору дій, коли заздалегідь визначені умови виконуються або перевіряються.

Управління консенсусом також є однією з основних функцій, необхідних для інтеграції блокчейну з IoT. Він діє як центральний сервер, який підтримує довіру між комунікаційними вузлами в мережі.

Управління ідентифікацією використовується для контролю та ідентифікації різних вузлів у мережі IoT. Крім того, інтерфейс API дозволяє

додаткам IoT отримувати доступ до послуг блокчейну. Рівень додатків - це верхній рівень, який включає різні програми IoT та забезпечує завдання візуалізації даних, які створюють численні оцифровані служби та допомагають особам, що приймають рішення, приймати точні та точні рішення на основі зібраних даних з фізичних пристроїв IoT[16].

Традиційні методи перевірки цілісності даних зазвичай використовують методи шифрування для захисту даних у хмарі, покладаючись на довірених сторонніх аудиторів (TPA). Схеми цілісності даних, засновані на блокчейні, можуть успішно уникнути проблеми довіри TPA, однак їм доводиться стикатися з проблемами великих обчислювальних та комунікаційних накладних витрат. Для вирішення вищезазначених питань пропонується схема цілісності даних (BB-DIS) на основі блокчейну та білінейного картографування для великомасштабних даних IoT. У BB-DIS дані IoT нарізані на фрагменти та генеруються гомоморфні теги (HVT) для перевірки вибірки. Цілісність даних може бути досягнута відповідно до характеристик білінійного зіставлення у вигляді транзакцій блокчейну[18].

3.2 Представлення математичної моделі

Запропонована модель є децентралізованою для вирішення проблеми єдиної точки довіри в традиційній моделі служби аудиту даних колективної довіри. Протокол дозволяє користувачам відстежувати історію своїх даних. Таким чином, більшість існуючих методів перевірки цілісності даних, заснованих на технології блокчейну, зосереджуються на проблемі довіри, а не на розмірі даних. Більш помітним питанням є те, що дані IoT, що зберігаються в хмарі, потрібно оновлювати в режимі реального часу, щоб задовольнити найновіші вимоги різних додатків. Тому необхідно запропонувати динамічне рішення на основі блокчейну, спрямоване на оновлення даних для перевірки цілісності даних.

Технологія Blockchain реалізує децентралізовані однорангові транзакції, координацію та співпрацю без потреби довіри за допомогою шифрування даних, відмітки часу та розподіленого консенсусу. Це може вирішити проблему високої вартості, неефективності та небезпечного зберігання даних централізованих систем[17].

Табл.3.1: Структурні елементи моделі

Позначення	Пояснення
DOD	Прилад – власник даних
DCD	Прилад – користувач даних
CSP	Провайдер хмарних послуг
HSSC	Смарт-контракт на зберігання HVT
CRSC	Виклик отримання смарт-контракту
IVSC	Смарт-контракт для перевірки доброчесності

Структура моделі в основному включає чотири типи об'єктів, тобто смарт-контракти, пристрої, що володіють даними (DOD), споживачі даних (DCD) та постачальники хмарних послуг (CSP). Для досягнення різних функцій існує три види смарт-контрактів, тобто смарт-контракт на зберігання HVT (HSSC), інтелектуальний контракт на отримання виклику (CRSC) та інтелектуальний контракт для перевірки цілісності (IVSC). Усі ці сутності можуть діяти як вузли блокчейну в мережі блокчейнів. Насправді перевірка цілісності даних залучає декількох власників даних та споживачів даних. Перевірка цілісності виконується за допомогою смарт-контрактів у системі блокчейнів. Користувачі з вимогами цілісності можуть запускати клієнтів блокчейну на своїх вузлових пристроях або виходити з мережі блокчейн. CSP також служить вузлом у мережі блокчейнів, що робить вузли повністю розпорошеними, а перевірку цілісності більш ефективною.

DOD і DCD слід додавати до мережі блокчейнів, коли система блокчейнів ініціалізується для створення пари ключів. Власник даних повинен заплатити за взаємодію зі смарт-контрактом та хмарною службою зберігання. CSP може виступати як майнер-вузол у мережі блокчейнів, який кваліфікований для надання послуг через майнінг та отримання відповідної винагороди. Споживач даних просить використовувати дані, що зберігаються на хмарному сервері, і оплачує відповідні витрати за це. У цій структурі CSP забезпечує загальну послугу зберігання даних для власників даних, тоді як нехмарні дані можуть передаватися через міжвузольну мережу P2P.

Протокол верифікації

Процес верифікації цієї схеми показаний на рисунку 3.2, а транзакції між різними смарт-контрактами та всіма учасниками перелічені в таблиці 2 детально. Протокол розділений на три етапи: етап кроку, етап виклику та етап перевірки. Розумний контракт та CSP виконують роль перевіряючого та постачальника доказів відповідно.

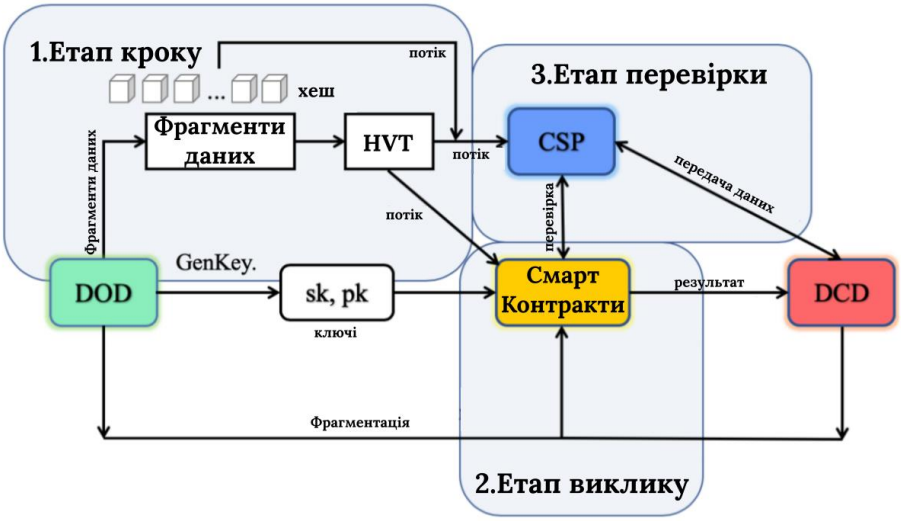

Рис.3.2: Протокол перевірки отриманих даних

Етап кроку: DOD встановлює двобічне відображення, вибирає хеш-функцію короткого підпису, випадково вибирає приватний ключ і обчислює відповідний відкритий ключ із закритого ключа. Потім DOD нарізає файл

даних на набір з декількох фрагментів даних однакової довжини. Після хешування DOD обчислює HVT кожного фрагменту даних, щоб сформувати набір метаданих аутентифікації, що зменшує накладні витрати на зв'язок, підтримуючи публічний аудит. DOD завантажує набір фрагментів даних і метадані на сервер хмарного сховища. Набір метаданих надсилається HSSC через мережу блокчейнів у формі транзакції. DOD видаляє файл даних локально.

Етап виклику: DOD витягує c-елементи з HSSC для побудови випадково встановленого індексу фрагментів даних і надсилає ряд випадкових значень разом із індексом фрагменту даних, заданому CSP та CRSC у вигляді *chal*, запиту на виклик.

Етап перевірки: IVSC отримує HVT та *chal* від HSSC та CRSC відповідно. Отримавши запит на виклик, CSP обчислює доказ {R, μ, η} і відправляє його в IVSC. IVSC перевіряє, чи є підтвердження правильним. Якщо це правильно, дані, що зберігаються в хмарі, інтегруються, і IVSC повертає результат до DOD.

Алгоритм верифікації

DCD також може ініціювати запит на перевірку збережених даних. DCD, що подає запит на службу перевірки цілісності, може брати участь у етапі виклику та етапі перевірки. Коли цілісність даних підтверджується, CSP надсилає дані з серверів відповідному клієну через мережу P2P.

Необхідно використати інтелектуальні контракти в процесі перевірки та алгоритм перевірки відповідно до протоколу перевірки для верифікації метаданих аутентифікації. Поетапне застосування алгоритму перевірки:

Етап кроку: G_1 - циклічна група додавання q-порядку, P - один з його генераторів. G_2 - циклічна мультиплікативна група порядку Q. Z_q означає ціле кільце моди q. По-перше, DOD має встановити двобічне відображення:

$$e: G_1 \times G_2 \to G_2$$

і хеш-функцію захисту короткого підпису:

$$H: \{0,1\}^* \to \{0,1\}^\lambda$$

Маємо: $\varphi(i,j)$: $Z_q^* \times \{1,2,\dots,n\} \to \{1,2,\dots,n\}$ є псевдовипадковою функцією, де $k_0 \in Z_q^*$ та $|q| \geq \lambda \geq 160$.

DOD вибирає приватний ключ $\alpha \leftarrow Z_q^*$ випадковим чином відповідним відкритим ключем $Y = \alpha P$. Відкритий ключ *pk* має значення *Y*, а закритий ключ *sk* - значення α. Не можливо розрахувати приватний ключ із відкритого ключа.

DOD ділить файл даних F на фрагменти даних однакової довжини: $\{m_1, m_2, m_3, \dots, m_n\}$, і генерує HVT для кожного фрагменту даних m_i:

Існує колекція метаданих: $\Phi = \{\delta_1, \delta_2, \dots, \delta_n\}$

Нарешті, DOD завантажує набір фрагментів даних на сервер хмарного сховища та відправляє набір метаданих Φ до HSSC. DOD видаляє файл даних локально.

Етап виклику: DOD витягує c-елементи випадковим чином для побудови індексу фрагменту даних набору $I = \{s_1, s_2, \dots, s_c\}$, $c \in [1, n]$, і генерує псевдовипадкове число для кожного $i \in I$. DOD надсилає випадкове значення та індекс фрагменту даних, встановлені на CSP та CRSC, у вигляді запиту виклику *chal* = $\{(i, v_i)\}$, $s_1 < i < s_c$.

Етап перевірки: Як постачальник доказів, після отримання chal запиту, CSP обчислює:

$$R = \sum_{i=s_1}^{s_c} v_i Y$$

$$\mu = \sum_{i=s_1}^{s_c} v_i H(m_i) P$$

$$\eta = P - P^2 \sum_{i=s_1}^{s_c} \frac{v_i}{\delta_i}$$

CSP повертає *{R, μ, η}* як доказ IVSC.

Після отримання доказу {R, μ, η} IVSC обчислює, чи інтегровані дані на сервері хмарного сховища: $e(\eta, P) \cdot e(\mu + R, P) = e(P, P)$. Якщо рівняння відповідає дійсності, дані цілі. Розумний контракт повертає результат перевірки запитувачу послуги.

Виконання верифікації

Відповідно до наведеної вище схеми, якщо дані, що зберігаються CSP, не порушені, доказ, надісланий CSP, є правильним. Наступний розрахунок доводить правильність схеми.

$$e(\eta, P) \cdot e(\mu + R, P) = e\left(P - P^2 \sum_{i=s_1}^{s_c} \frac{v_i}{\delta_i}, P\right) \cdot e\left(\sum_{i=s_1}^{s_c} v_i H(m_i) P + \sum_{i=s_1}^{s_c} v_i Y, P\right)$$

$$= e\left(P - P^2 \sum_{i=s_1}^{s_c} \frac{v_i H(m_i) + \alpha}{P}, P\right) \cdot e\left(\sum_{i=s_1}^{s_c} v_i H(m_i + \alpha) P, P\right)$$

$$= e\left(-\sum_{i=s_1}^{s_c} v_i H(m_i + \alpha) P, P\right) \cdot e(P, P) \cdot \left(\sum_{i=s_1}^{s_c} v_i H(m_i + \alpha) P, P\right)$$

$$= e(P, P)$$

З рівняння видно, що алгоритм перевірки здійсненний.

Припустимо, що є деякі зловмисники, хочуть пройти перевірку смарт-контракту, тоді їм потрібно побудувати підпис $\delta_j^* = \frac{1}{H(m_j^*) + \alpha}$ щоб зробити:

$$\mu^* = e\left(\sum_{i=s_1}^{s_c} v_i H(m_i) P + v_i H(m_j^*) P\right)$$

Маємо:

$$\eta^* = P - \left(P^2 \sum_{i=s_1, i \neq j}^{s_c} \frac{v_i}{\delta_i} \right) - P^2 \frac{v_i}{\delta_i}$$

$$e(\eta^*, P) \cdot e(\mu^* + R, P) = e(P, P)$$

Однак зловмисник не знає закритого ключа α, тому підробити m_j^* неможливо

$$\frac{1}{H(m_j) + \alpha} P = \frac{1}{H(m_j^*) + \alpha} P$$

і доказ не може бути зміненим.

Якщо зловмисники будуть намагатись видалити дані m_j^* на сервері хмарного сховища, подібно до аналізу вище, це буде неможливо реалізувати m_j^*, оскільки приватний ключ α невідомий.

З наведеного вище аналізу можна зробити висновок, що алгоритм перевірки може протистояти зловмисним атакам.

Динамічність

Операція динамічного оновлення даних, що підтримується схемою, завершується алгоритмом запиту на оновлення UpdateReq() та алгоритмом виконання оновлення UpdateExec(). Відповідні операції включають додавання фрагменту даних, модифікацію фрагменту даних та видалення фрагменту даних.

UpdateReq(): Алгоритм працює на DOD, вимагає оновлення копії переданого файлу, що зберігається у віддаленому CSP, і вихідним запитом є оновлення.

DOD надсилає запит на оновлення до хмари у вигляді $\langle BlockOp, Ind, m_i', \delta_i' \rangle$ де BlockOp - це відповідна операція фрагмента даних, Ind представляє індекс оновленого фрагмента даних, m_i', δ_i' - оновлений фрагмента даних та оновлені метадані відповідно.

UpdateExec (): Алгоритм виконується на CSP сервер. Вхідним параметром є запит на оновлення DOD, а вихідним - нова копія файлуF' та нові метадані δ_i'. Після кожного оновлення, щоб переконатись у правильності операції хмарного оновлення, DOD виконує угоду про виклик.

Операція додавання: DOD вставляє новий фрагмент даних у позицію j. Якщо спочатку є n фрагментів даних, після операції, що додається, буде n + 1 фрагментів даних. Якщо сформований запит виклику містить блок даних m_n+ 1, перевірку все ще можна завершити, оскільки набір метаданих оновлено.

Операція видалення: Під час видалення фрагмента даних усі наступні фрагменти даних будуть випереджати одну позицію. Якщо певний фрагмент даних зі значенням індексу j буде видалений, DOD надсилає запит на видалення $\langle Delete, j, null, null \rangle$до CSP. Отримавши запит на видалення, CSP видаляє фрагмент даних, позиція індексу якого j у резервних копіях.

Доведення

Щоб довести ефективність запропонованої схеми цілісності даних (BB-DIS), використано моделювання MathLab. Для порівняльного аналізу взято мережу блокчейнів для безпосереднього зберігання результатів хешування – B-DIS[18]. Мережу, в якій фрагменти даних на основі блокчейну хешуються кілька разів відповідно до структури дерева Меркле – BM-DIS[19]. І структуру методу B-DAM[20] з механізмом аудиту даних на основі блокчейну. Дані в експерименті були взяті в середньому за 30 тестів.

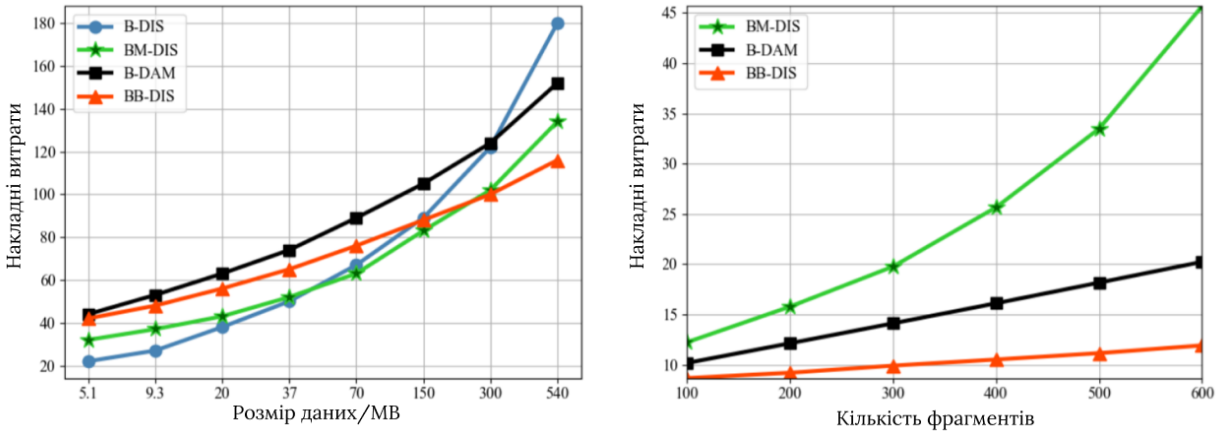

Рис.3.2.: Порівняння накладних витрат

На рисунку 3.2 показані витрати на перевірку цілісності за різними шкалами даних IoT. Підтримувалась постійна загальна кількість фрагментів і їх розмір. З рисунку 3.2 видно, що коли обсяг даних перевищує 150 Мб, запропонована схема стає більш ефективною. Тобто досягається довіра та значно покращується швидкість перевірки великомасштабних даних. Як видно, коли розмір фрагментів даних фіксований (20 КБ), BB-DIS приймає менше обчислювальних витрат, ніж BM-DIS та B-DAM.

Висновки:

В даному розділі було детально розглянуто запропоновану модель захисту даних в мережі IoT з впровадженням блокчейну. Разом з попереднім розділом був проведений загальний розбір технології Blockchain і її можливість його прикладного використання. За допомогою математичної моделі було доведено переваги запропонованого методу. Використана концепція протидіє враженню даних в мережі IoT, а також полегшує проблему маштабованості.

ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ

В даній роботі було проведено розгляд технології Internet of Things. Відповідно до визначених задач:

1. Було проаналізовано проблеми IoT такі як - конфіденційність та інформаційна безпека та за рахунок структуризації ризиків стало можливо проаналзувати методи їх розв"язку
2. Досліджено існуючі методи захисту інформації, що дозволило вибрати прототип та підтвердити можливість застосування технологіїї Blockchain в мережах IoT.
3. Модифіковано метод захисту інформації на основі впровадження Blockchain в мережі IoT і використання смарт-контактів для побудови децентралізованої моделі довіри.
4. Математичним моделюванням було доведено ефективність запропонованого рішення. Результати моделювання показали, що запропонований метод має високий потенціал протидії і низькі показники затрат.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. “How the internet of things can help create a better new normal” – Режим доступу до ресурсу: https://www.wired.co.uk/article/bc/vodafone-iot

2. “IoT Architecture: the Pathway from Physical Signals to Business Decisions” – Режим доступу до ресурсу: https://www.altexsoft.com/blog/iot-architecture-layers-components/

3. “Internet of Things: security and privacy implications” – Режим доступу до ресурсу: https://www.researchgate.net/publication/275228804_Internet_of_Things_security_and_privacy_implications

4. “Privacy” – Режим доступу до ресурсу: https://www.gsma.com/aboutus/legal/privacy

5. “RFID and Inclusive Model for the Internet of Things” – Режим доступу до ресурсу: https://docbox.etsi.org/zArchive/TISPAN/Open/IoT/low%20resolution/www.rfidglobal.eu%20CASAGRAS%20IoT%20Final%20Report%20low%20resolution.pdf

6. “IoT Privacy and Security: Challenges and Solutions” ” – Режим доступу до ресурсу: https://www.mdpi.com/2076-3417/10/12/4102/pdf

7. “7 design principles for IoT” – Режим доступу до ресурсу: https://futurice.com/blog/7-design-principles-for-iot

8. “Особенности защиты информации в Интернете вещей” – International Journal of Open Information Technologies ISSN: 2307-8162 vol. 6, no.10, 2018

9. V. Hassija et al.: Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures – Режим доступу до ресурсу: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8742551

10. P. Yang et al.: Data Security and Privacy Protection for Cloud Storage: A Survey – Режим доступу до ресурсу: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9142202

11. S. Aljanabi, A. Chalechale: Improving IoT Services Using an HFCO – Режим доступу до ресурсу: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9328240

12. U. Khadam et al.: Digital Watermarking Technique for Text Document Protection Using Data Mining Analysis – Режим доступу до ресурсу: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8713871

13. M. BinJubier et al.: Comprehensive Survey on Big Data Privacy Protection – Режим доступу до ресурсу: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8943156

14. Towards Secured Online Monitoring for Digitalized GIS Against Cyber-Attacks Based on IoT and Machine Learning – Режим доступу до ресурсу: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9440436

15. Analysis of the Cryptographic Tools for Bockchain and Bitcoin – Режим доступу до ресурсу: https://www.mdpi.com/2227-7390/8/1/131/htm

16. A Review of Blockchain in Internet of Things and AI Big Data Cogn. Comput., 2020 Licensee MDPI, Basel, Switzerland

17. “ H. Wang, J. Zhang: Blockchain Based Data Integrity Verification” – Режим доступу до ресурсу: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8895808

18. B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, “Blockchain based data integrity service framework for IoT data, in Proc. ICWS”, Jun. 2017.” – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/8029796

19. D. Yue, R. Li, Y. Zhang, W. Tian, and C. Peng, “Blockchain based data integrity verification in P2P cloud storage,in Proc. ICPADS”, Dec. 2018 – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/8644863

20. C. Wang, S. Chen, Z. Feng, Y. Jiang, and X. Xue, “Block chain-based data audit and access control mechanism in service collaboration, in Proc. ICWS”, Jul. 2019– Режим доступу до ресурсу: https://ieeexplore.ieee.org/abstract/document/8818439

21. XIII Міжнародна науково-технічна конференція студентів та аспірантів "Перспективи розвитку інформаційно-телекомунікаційних технологій та систем" (ПРІТС-2020) **«ІНФОРМАЦІЙНА БЕЗПЕКА INTERNET OF THINGS»** Режим доступу до ресурсу: http://conferenc.its.kpi.ua/2020/paper/view/20784/10840

22. XIII Міжнародна науково-технічна конференція студентів та аспірантів "Перспективи розвитку інформаційно-телекомунікаційних технологій та систем" (ПРІТС-2021) **«ПРОБЛЕМИ ЗАХИСТУ ДАНИХ В МЕРЕЖІ INTERNET OF THINGS»** Режим доступу до ресурсу: http://conferenc.its.kpi.ua/2021/paper/view/23215/12586

23. XV Міжнародна науково-технічна конференція "Перспективи телекомунікацій 2021" (ПТ-2021) **«АНАЛІЗ МЕТОДІВ ЗАХИСТУ ДАНИХ В МЕРЕЖІ INTERNET OF THINGS»** Режим доступу до ресурсу: http://conferenc.its.kpi.ua/2021/paper/view/23277/12581