НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

До захисту допущено

Завідувач кафедри

_____ **Дмитро ЛАНДЕ**

«_____»_____2024 р.

Дипломна робота

на здобуття ступеня магістра

зі спеціальності: 125 Кібербезпека

на тему:
Безпека віддалених морських взаємодій на основі принципів туманної обробки даних

Виконав (-ла): здобувач вищої освіти ІІ курсу, групи ФБ-з21мп
(шифр групи)

Петренко Кирил_Миколайович___
(прізвище, ім'я, по батькові) (підпис)

Науковий керівник к.т.н. Стьопочкіна Ірина Валеріївна
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Рецензент _____

(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2024 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою
Спеціальність (спеціалізація) – 125 Кібербезпека «Системи, технології та математичні методи кібербезпеки»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Дмитро ЛАНДЕ
(підпис)
«___»_____2024 р.

ЗАВДАННЯ
на магістерську дисертацію здобувачу ступеня магістра

Петренку Кирилу Миколайовичу
(прізвище, ім'я, по батькові)

1. Тема дисертації
Безпека віддалених морських взаємодій на основі принципів туманної обробки даних
науковий керівник дисертації ,
к.т.н. Стьопочкіна Ірина Валеріївна ,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «06» листопада 2023 р. № 5147-с

2. Термін подання студентом дисертації 10 січня 2024 р.

3. Об'єкт дослідження кіберфізичні системи суден

4. Вихідні дані технічна документація, теоретичні дані, науково-дослідницькі роботи, програмно-апаратне забезпечення Orange Pi

5. Перелік завдань, які потрібно розробити
1) Аналіз існуючих рішень в області керування доступом
2) Вивчення переваг і недоліків рішень, аналіз існуючих засобів вирішення недоліків
3) Пропозиція вирішення виявлених проблем за допомогою власно розробленої моделі

4) Реалізація концепту рішення, порівняння та ідентифікація вирішених проблем

6. Орієнтовний перелік ілюстративного матеріалу
16 ілюстрацій, 24 таблиць

7. Орієнтовний перелік публікацій
Petrenko K., Styopochkina I. Maritime security and cyber security: current challenges and threats // Maritime security of the baltic-black sea region: challenges and threats, December 23, 2021 Volume 1, P.333-337.

8. Дата видачі завдання 10.01.2023

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Вибір тематики	01.11.2022 - 01.01.2023	Виконано
2	Огляд наукової літератури за темою	01.01.2023 - 01.05.2023	Виконано
3	Написання першого розділу дисертації	01.05.2023 - 01.06.2023	Виконано
4	Розробка архітектурної моделі	01.06.2023 - 01.08.2023	Виконано
5	Здійснення перевірки працездатності рішень	01.08.2023 - 01.09.2023	Виконано
6	Проходження переддипломної практики	01.09.2023 - 29.10.2023	Виконано
7	Проведення аналізу, написання другого та третього розділів	16.10.2023 - 15.12.2023	Виконано
8	Створення стартап-проекту	16.12.2023 - 21.12.2023	Виконано
9	Створення презентації для доповіді	22.12.2023 - 30.12.2023	Виконано
10	Передзахист магістерської дисертації	10.01.2024 - 10.01.2024	Виконано
11	Перевірка на плагіат, проходження рецензування	11.01.2024 - 15.01.2024	Виконано
12	Захист магістерської дисертації	17.01.2024	Виконано

Студент _____ _____
(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ _____
(підпис) (ініціали, прізвище)

РЕФЕРАТ

Обсяг роботи 66 сторінок, 16 ілюстрацій, 24 таблиці та 12 джерел літератури.

Об'єктом дослідження є кіберфізичні системи суден.

Предметом дослідження є безпека обробки даних у кіберфізичних системах суден на основі туманних обчислень.

Мета роботи - розробка архітектури обробки даних на основі принципів туманних обчислень з урахуванням політики безпеки.

Методи дослідження - порівняльний аналіз за літературними джерелами, аналіз і синтез, комп’ютерний експеримент, емуляція.

Новизна роботи: запропоновано нову архітектурну модель туманної обробки даних на основі сучасних пристроїв типу Orange Pi.

Результати роботи викладені у третьому розділі, що демонструє працездатність запропонованої архітектурної моделі.

Результати роботи можуть бути використані для покращення конфіденційності, цілісності та доступності інфраструктур обробки даних в морських комунікаціях, що експлуатують системи управління суднами.

Ключові слова: морська безпека, кібербезпека систем управління судноплавством, туманна обробка даних.

ABSTRACT

The thesis contains 66 pages, 16 illustrations, 24 tables and 12 sources of literature.

The object of research is the cyber-physical systems of ships.

The subject of research is the security of data processing in cyber-physical systems of ships based on fog computing.

The purpose of the work is to develop a data processing architecture based on the principles of fog computing, taking into account the security policy.

Research methods - comparative analysis based on literary sources, analysis and synthesis, computer experiment, emulation.

The novelty of the work: a new architectural model of foggy data processing based on modern Orange Pi-type devices is proposed.

The results of the work are presented in the third section, which demonstrates the workability of the proposed architectural model.

The results of the work can be used to improve the confidentiality, integrity and availability of data processing infrastructures in maritime communications operating ship control systems.

Keywords: maritime security, cyber security of shipping management systems, foggy data processing.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

SAR—Search and rescue

GMDSS—Global Maritime Distress and Safety System

NAVTEX—NAVigational TEleX

MSSIS—Maritime Safety and Security Information System

ВСТУП

Актуальність роботи.

Важливість та корисність туманних обчислень наразі є беззаперечним фактом. Однак, більшість установ орієнтуються на використання централізованих, хмарних обчислень, оскільки це є більш традиційною формою зберігання та обробки даних. В деяких областях, зокрема, в морській кібербезпеці, важливо запроваджувати туманну обробку інформації, хоча б тому, що зв’язок із центром може бути втрачений, або можуть статись затримки у передачі даних непереборного характеру [5]. Тому, актуальним залишається розробка моделей архітектур безпечної туманної обробки даних, зокрема, в області морської безпеки.

Об’єкт дослідження: кіберфізичні системи суден.

Предмет дослідження: безпека обробки даних у кіберфізичних системах суден на основі туманних обчислень.

Мета роботи: розробка архітектури обробки даних на основі принципів туманних обчислень з урахуванням політики безпеки

Задачі дослідження:

1. Проаналізувати переваги туманної обробки даних.
2. Виявити системи суден, в яких може бути корисною туманна обробка даних.
3. Запропонувати архітектурні рішення та політику безпеки на основі принципів туманної обробки даних.
4. Запропонувати механізми безпеки, які можуть бути впроваджені щодо даних архітектурних рішень.
5. Запропонувати склад програмно-апаратних засобів, які можуть бути використані для реалізації обробки даних на борту суден.
6. Здійснити експеримент, який показує працездатність рішень.

Новизна роботи: запропоновано нову архітектурну модель туманної обробки даних на основі сучасних пристроїв типу Orange Pi.

Апробація роботи: Роботу апробовано на міжнародній конференції Морська безпека балтійсько-чорноморського регіону: виклики та загрози. [5]

РОЗДІЛ 1. Аналіз механізмів комунікацій у судноплавстві та можливостей використання туманної обробки даних

1.1. Огляд сучасних методів комунікацій у судноплавстві

За період розвитку судноплавства системи комунікації між суднами подолали шлях від жестів та азбуки Морзе до складних систем попередження про небезпеки по різним каналам зв’язку.

Перш за все слід поділити методи комунікації за типами:

- Радіозв'язок;
- Супутниковий зв'язок;
- Системи зв'язку на коротких хвилях;
- Інтернет-зв'язок;
- Бездротові мережі.

В даній області переважає радіозв’язок як самий простий спосіб передачі інформації у даному середовищі [5].

На даний момент можна виділити основні системи комунікації які широко використовуються на прийняті як стандарт у судноплавстві:

- Автоматична система ідентифікації AIS;
- Глобальна морська система оперативного сповіщення та забезпечення безпеки GMDSS;
- NAVigational TEleX.

GMDSS (Глобальна система забезпечення морської безпеки та аварійного зв'язку) – це міжнародна система, яка використовує сучасні радіозв'язкові системи на суші, супутники та суднові системи для забезпечення безпеки та зв'язку у разі аварійних ситуацій. Вона була розроблена Міжнародною Морською

Організацією (IMO) і представляє значне покращення у способах аварійного зв'язку. Усі судна, які підпадають під Міжнародну Конвенцію про безпеку життя на морі, мають повністю відповідати вимогам GMDSS. Це набір процедур, обладнання та комунікаційних протоколів, що використовуються для забезпечення безпеки та проведення рятувальних операцій на транспортних засобах, таких як кораблі, човни та літаки у разі лиха. Він доповнює Міжнародну конвенцію з пошуку та порятунку на морі (ICMSaR) та є основою для обміну інформацією.
GMDSS складається з кількох систем, які виконують такі функції: оповіщення (включаючи визначення місцезнаходження транспортного засобу в небезпеці) для суден та берегової влади поблизу, координація пошуково-рятувальних операцій, визначення місцезнаходження (навігація), забезпечення безпеки на морі, інформаційне повідомлення про події, загальний зв'язок та зв'язок “bridge-to-bridge”. Система також надає резервні засоби оповіщення про небезпеку та аварійні джерела живлення.

GMDSS включає в себе наступні системи:

- Navtex - це система міжнародного автоматичного розповсюдження інформації про безпеку на морі (MSI), що включає навігаційні попередження, прогнози погоди, попередження про погоду, повідомлення про пошук та рятування та іншу інформацію для суден. Navtex призначений для надання доступних, зручних та автоматизованих способів отримання цієї інформації на суднах, що знаходяться у морі на відстані близько 370 км (200 морських миль) від берега. Невеликий, доступний за ціною і автономний "розумний" радіоприймач з установкою на містку або в іншому місці, звідки здійснюється керування кораблем, перевіряє кожне отримане повідомлення на те, чи було воно отримано раніше, чи належить до категорії нецікавих для капітана судна. Частота передачі цих повідомлень англійською мовою становить 518 кГц(MF діапазон), а для передачі місцевою мовою іноді використовується частота 490 кГц(MF діапазон). Повідомлення кодуються заголовками з використанням літер алфавіту для

позначення радіомовних станцій та типів повідомлень. Потім слідує двозначний серійний номер повідомлення.

- International Cospas-Sarsat Programme – це міжнародна програма, яка займається пошуком та порятунком за допомогою супутникових систем (SAR). Вона створена як некомерційна міжурядова ініціатива, яка об'єднує 45 країн та агенцій. Мета програми полягає у виявленні та визначенні розташування радіобуїв, які були активовані людьми, авіаційними або морськими суднами в тяжкому стані, а також передачі цієї інформації про тривогу відповідним службам для організації рятувальних операцій. Учасники програми здійснюють перехоплення сигналів лиха за допомогою близько 65 супутників на орбіті Землі, які оснащені транспондерами та процесорами сигналів. Ці системи здатні виявити радіобуй у будь-якій точці планети та передати інформацію на частоті Cospas-Sarsat 406 МГц.
- Пошуково-рятувальний транспондер: Установка GMDSS на судах включає використання спеціального пристрою, відомого як пошуково-рятувальні транслокатори радіолокації. Вони служать для виявлення рятувальних засобів або суден, що перебувають у тяжкому стані. За допомогою цих транспондерів створюється серія точок на радарному дисплеї рятувального корабля діаметром близько 3 см. Дальність виявлення між цими пристроями та суднами залежить від висоти радарної щогли та пошуково-рятувального пристрою і зазвичай становить близько 15 км (8 морських миль). Коли пошуково-рятувальний пристрій виявляє щось на радарі, він подає візуальний та звуковий сигнал людям, які потребують допомоги.[11]

Інформаційна система для забезпечення безпеки та захисту на морі (MSSIS) - це публічна та відкрита мережа, яка збирає та розповсюджує дані практично в режимі реального часу. Країни-учасниці обмінюються інформацією з автоматичної системи ідентифікації (AIS), берегових радарів та інших морських систем. MSSIS об'єднує дані від учасників до одного потоку даних, який передається через захищені сервери в Інтернеті. Уряди

мають можливість переглядати дані AIS з усього світу в режимі реального часу за допомогою різних способів графічного представлення, таких як текст, фотографії та електронні карти.[12]

1.2. Основні принципи та переваги туманних обчислень

Термін "туманні обчислення" був вперше запропонований компанією CISCO у 2002 році та визначений як "розширення хмарних обчислень, яке забезпечує надання обчислювальних, мережевих та сховищ даних ресурсів між кінцевими пристроями та хмарними центрами обчислень" [9]. У 2015 році було створено консорціум OpenFog - об'єднання компаній та академічних організацій, таких як Cisco, Dell, Intel та Microsoft Corp, а також Прінстонський університет, який займається стандартизацією технології туманних обчислень (18 грудня 2018 року консорціум OpenFog став частиною The Industrial Internet Consortium). У 2018 році Національний інститут стандартів і технологій США визначив поняття “туманні обчислення”: Туманні обчислення – це модель багаторівневої організації, яка забезпечує широкий доступ до масштабованих обчислювальних ресурсів. складається з туманних вузлів (фізичних або віртуальних), які знаходяться між інтелектуальними кінцевими пристроями та централізованими (хмарними) сервісами.Туманні вузли контекстно-залежні та підтримують єдину систему управління даними та організацію комунікацій. горизонтальні структури (для підтримки федерації сервісів) або бути пов'язаними мережевою близькістю до інтелектуальних кінцевих пристроїв.

Туманні обчислення скорочують час відгуку мережевих додатків і дозволяють кінцевим пристроям використовувати локальні обчислювальні ресурси, і навіть підключатися до централізованим сервісів за необхідності. Розширення області застосування туманних обчислень за рахунок виконання обчислень, зберігання та управління даними на проміжних вузлах допомагає скоротити розрив між хмарою та кінцевими пристроями . Це дозволяє використовувати туманні обчислення в

нових областях, таких як IoT, транспортні засоби , “розумне” місто, охорона здоров'я , “розумна” доставка (включаючи використання безпілотних автомобілів), реальний час підземна зйомка , відеоспостереження та інші.

У 2017 році консорціум OpenFog представив стандартну архітектуру туманних обчислень, що ґрунтується на восьми ключових принципах: можливість програмування, ієрархічна структура, гнучкість, надійність обслуговування (Reliability, availability and serviceability —
RAS), доступність, надійність, автономність, відкритість та безпека.[9]

1.3. Переваги туманних обчислень

Розглянемо докладніше основні аспекти туманних обчислень:

1. Локалізація обчислень:

- Туманні обчислення передбачають використання розподіленого обчислення, при якому обробка даних відбувається ближче до джерела їхнього виникнення. Це дозволяє знизити затримки та збільшити ефективність обчислень.

Локалізація обчислень в туманних обчисленнях — це ключовий принцип, що визначає їхню ефективність та практичність. Подивимося докладніше на основні аспекти цього принципу:

1.1. Мінімізація Затримок:

- Основна ідея локалізації обчислень полягає в тому, щоб обробка даних відбувалася якнайближче до місця їхнього виникнення. Це дозволяє значно знизити затримки, оскільки дані не мають подолати велику відстань для обробки.

1.2. Розподілене Обчислення:

- Системи туманних обчислень використовують розподілені обчислення, що означає, що обробка відбувається на різних вузлах мережі, а не централізовано. Це забезпечує більш рівномірне та швидке розподілення завдань.

1.3. Оптимізація Ресурсів:

- Локалізовані обчислення дозволяють краще використовувати обчислювальні ресурси. Вузли можуть працювати з обмеженими обчислювальними можливостями, спеціалізованими апаратними засобами або обробляти конкретний тип даних.

1.4. Надійність та Доступність:

- Локальна обробка даних також забезпечує високу доступність та надійність системи. Якщо один вузол виходить з ладу, інші можуть продовжити роботу. Це важливо в сценаріях, де безперебійна робота критично важлива.

1.5. Масштабованість:

- Завдяки локальній обробці, системи туманних обчислень легко масштабуються. Додавання нових вузлів до мережі дозволяє підвищити загальну продуктивність та обчислювальну потужність.

1.6. Зменшення Трафіку в Мережі:

- Локальна обробка даних дозволяє зменшити кількість даних, які потрібно передавати через мережу до центральної точки обробки. Це може знизити витрати на передачу даних та робить мережу більш ефективною.

1.7. Сприяння Концепції "Краю Мережі" (Edge Computing):

- Локалізація обчислень сходиться з концепцією "краю мережі", де обчислення відбуваються на периферійних пристроях, ближче до користувача чи джерела даних. Це особливо важливо в застосуваннях IoT та системах в реальному часі.

1.8. Швидкість та Реакція в Реальному Часі:

- Локальна обробка дозволяє системі оперативно реагувати на події в реальному часі, що важливо для вимогливих до швидкості застосувань, таких як системи моніторингу або автоматизоване керування.

1.9. Збереження Приватності:

- Оскільки дані обробляються локально, зменшується ризик витоку чутливої інформації через великі мережі. Це важливо для застосувань, де збереження приватності даних є критично важливою.

Локалізація обчислень у туманних обчисленнях створює ефективну та гнучку інфраструктуру для обробки даних, забезпечуючи швидкість, надійність та збереження ресурсів.

2. Інтеграція з хмарними обчисленнями:

- Туманні обчислення існують в доповнення до хмарних обчислень, створюючи розподілену систему обчислень, що охоплює хмару та кінцеві пристрої.

Основна ідея полягає у створенні комплексного середовища, яке поєднує хмарні та туманні ресурси. Основні аспекти цієї інтеграції:

2.1. Розподілене управління ресурсами:

Хмарні обчислення надають централізоване управління ресурсами, але туманні обчислення дозволяють локальним вузлам самостійно управляти частиною цих ресурсів.

2.2. Локальна обробка даних:

Туманні обчислення дозволяють обробляти дані на місці на локальних вузлах, що знижує навантаження на централізовані сервери у хмарі та дозволяє ефективно працювати з великими обсягами даних.

2.3. Зниження затримок:

Інтеграція туманних та хмарних обчислень має перевагу у зниженні затримок передачі даних. Там, де хмарні обчислення можуть викликати великі затримки, туманні обчислення виконуються ближче до місця виникнення даних.

2.4. Гнучкість розгортання:

Інтеграція надає гнучкість при розгортанні обчислювальних середовищ. Різні компоненти системи можуть використовувати як хмарні, і туманні ресурси залежно від потреб.

2.5. Ефективне використання мережі:

Туманні обчислення дозволяють виконувати обробку даних дома, що знижує необхідність передачі великих обсягів даних через мережу. Це особливо корисно в умовах обмеженої пропускної спроможності мережі.

2.6. Інтеграція з інтернетом речей (IoT):

Інтернет речей часто використовується разом із туманними обчисленнями, де датчики та пристрої збирають дані, а туманні ресурси надають можливість їх обробки безпосередньо на місці.

2.7 Безпека та збереження конфіденційності:

Інтеграція дозволяє використовувати більш детальні стратегії безпеки, оскільки деякі обчислення можуть бути виконані на місці, де розміщені інформаційні ресурси [3].

2.8 Гнучкі розподілені обчислення:

Комбінування туманних та хмарних обчислень дозволяє створювати розподілені обчислювальні середовища, які ефективно адаптуються до різних завдань та обсягів даних.
Інтеграція туманних та хмарних обчислень розширює можливості комп'ютерних систем та надає комплексний підхід до обробки даних у режимі реального часу.

3. Обробка в реальному часі:

- Деякі застосування, як от IoT (Інтернет речей) та системи в реальному часі, потребують швидкої обробки даних. Туманні обчислення дозволяють виконувати обчислення навіть у вузлах мережі, що допомагає забезпечити реальний час реакції.

Обробка даних як реального часу одна із головних аспектів туманних обчислень. Ця функція відіграє важливу роль у багатьох ситуаціях, де потрібна швидка обробка та аналіз даних. Основні аспекти обробки даних у режимі реального часу в контексті туманних обчислень:

3.1 Затримки:

Туманні обчислення дозволяють виконувати обчислення на локальних вузлах мережі, що значно скорочує час затримки порівняно із звичайними хмарними обчисленнями. Це особливо корисно для систем, які потребують миттєвої відповіді.

3.2 Інтернет речей (IoT) та системи реального часу:

В області IoT та систем реального часу, туманні обчислення можуть обробляти дані та надавати відповіді негайно без необхідності передачі на центральний сервер.

3.3 Аналіз та прийняття змін:

В областях, де необхідно враховувати швидкозмінні дані або управління, обробка даних у режимі реального часу дозволяє системам миттєво відреагувати на нові умови та зміни у навколишньому середовищі.

3.4 Медичні додатки:

У медичних системах туманні обчислення можуть забезпечувати швидку аналітичну обробку медичних даних, таких як вимірювання у режимі реального часу або моніторинг стану пацієнтів.

3.5 Автоматизоване керування:

Системи автоматизованого керування, такі як керування промисловими процесами або транспортними системами, можуть використовувати можливість миттєвої обробки даних на рівні туманних вузлів для прийняття точних та оперативних рішень.

3.6 Застосування у фінансовій сфері:

Швидка реакція на фінансові та економічні зміни може мати ключове значення у фінансовій сфері. Туманні обчислення мають потенціал застосування у реальному часі для аналізу даних ринків та прийняття оперативних фінансових рішень.

3.7 Машинне навчання та штучний інтелект [6]:

Обробка даних у режимі реального часу в туманних обчисленнях відіграє важливу роль у додатках машинного навчання та штучного інтелекту, де швидка аналітика може суттєво покращити роботу моделей.

Ефективна обробка даних у туманних обчисленнях у режимі реального часу є ключовим фактором для безлічі промислових та наукових додатків, де швидкість та ефективність обробки інформації визначають успіх системи чи технологічного рішення.

4. Мобільність та гнучкість:

- Туманні обчислення підтримують мобільність та гнучкість, що робить їх ефективними для розподілених та змінних середовищ.

4.1 Мобільність:

Туманні обчислення дозволяють забезпечити підтримку пересування даних та їх обробки. Це означає, що системи, засновані на туманних обчисленнях, можуть працювати рухомих об'єктах, таких як автомобілі, безпілотні апарати, мобільні пристрої та інші. Замість того, щоб покладатися на централізований центр хмари, дані можуть бути оброблені ближче до джерела інформації, що підвищує ефективність і знижує затримки при передачі даних.

4.2 Гнучкість:

Туманні обчислення відрізняються своєю здатністю адаптуватися до різних ситуацій та умов. Системи, які використовують туманні обчислення, можуть легко масштабуватися залежно від потреб, що змінюються. Це особливо важливо в динамічних оточеннях, де потрібна швидка реакція на зміни. Гнучкість також проявляється у можливості легкого інтегрування туманних обчислень у різні пристрої та системи для досягнення високої адаптивності.

1.4. Приклади застосування туманних обчислень

Приклади застосування:

Транспортні засоби: У автомобілях, поїздах або безпілотних транспортних засобах туманні обчислення можуть обробляти дані про стан дороги, координати та інші параметри безпосередньо на місці, що підвищує безпеку та навігацію систем.

Медичні пристрої: У медичних моніторах та пристроях для збору інформації про здоров'я пацієнтів туманні обчислення дозволяють обробляти та аналізувати дані на самому пристрої, що може бути важливим при реагуванні на надзвичайні ситуації та моніторинг пацієнтів у режимі реального часу.

Мобільні пристрої смартфони та інші портативні пристрої можуть використовувати туманні обчислення для локальної обробки даних, що підвищує продуктивність програм та знижує залежність від хмарних серверів.
Гнучкість та рухливість технології розподілених обчислень роблять її невід'ємною частиною різноманітних ситуацій, де необхідне швидке, адаптивне та ефективне оброблення даних безпосередньо на місці їх виникнення.

1.5. Перспективи туманних обчислень з точки зору безпеки

Розглянемо перспективи туманних обчислень в контексті кібербезпеки [4,6].
Безпека та приватність:

- Децентралізована архітектура туманних обчислень може знизити загрози для безпеки, оскільки обчислення та обробка даних відбуваються більш локально.

Безпека:
Туманні обчислення відкривають нові можливості для забезпечення безпеки даних. Важливо приділити увагу локалізації обробки інформації, щоб знизити

вразливість. Системи туманних обчислень дозволяють проводити всі обчислення та обробку даних поблизу джерела, що ускладнює доступ зловмисників.

Крім того, завдяки децентралізованій архітектурі туманні обчислення підвищують стійкість до кібератак [2]. Якщо один із вузлів системи піддається атаці, інші вузли продовжують працювати нормально. Це робить систему більш надійною та захищеною від збоїв та зловмисних дій.

Шифрування даних легко реалізується на рівні вузлів туманної мережі, що гарантує конфіденційність інформації, що передається. Крім того, використання туманних обчислень дозволяє проводити аутентифікацію та авторизацію на нижчому рівні для підвищення безпеки системи загалом.

Приватність:

З погляду приватності, туманні обчислення поважають принцип локальної обробки даних, що сприяє захисту особистої інформації кінцевих користувачів. Чутливі дані не залишають локальні вузли, що знижує ризик несанкціонованого доступу [3].

Крім того, можливість управління доступом та розподілу повноважень на рівні вузлів дозволяє гнучко контролювати доступ до інформації. Це особливо важливо у випадках, коли різні вузли обробляють інформацію різного рівня конфіденційності.

Загалом туманні обчислення надають ефективні механізми для забезпечення безпеки та приватності, що робить їх привабливими при виборі рішень для систем з високими вимогами до захисту даних [1].

Інтеграція з IoT:

- Застосування туманних обчислень в IoT дозволяє ефективно обробляти великі обсяги даних, які генеруються датчиками та пристроями IoT.

Туманні обчислення тісно пов'язані з концепцією Інтернету речей (IoT) та пропонують ефективні методи обробки даних, які генеруються безліччю сенсорів та пристроїв IoT. Основні аспекти інтеграції включають:

Ефективна обробка даних: Туманні обчислення дозволяють обробляти дані ближче до джерел, що допомагає знизити затримки та підвищити загальну ефективність систем IoT. Це особливо корисно для програм, що вимагають оперативної реакції на дані від датчиків.

Масштабованість: Системи туманних обчислень легко масштабуються до роботи з великим обсягом даних, які генеруються безліччю пристроїв IoT. Це дозволяє ефективно керувати динамічними навантаженнями та змінами в обсязі даних.

Безпека: Децентралізована обробка даних у туманних обчисленнях може підвищити рівень безпеки систем IoT. Чутливі дані обробляються локально, що допомагає зменшити ризики їхньої компрометації під час передачі через мережу.

Локальне прийняття рішень: Туманні обчислення дозволяють пристроям IoT приймати рішення на основі оброблених даних на самому пристрої, мінімізуючи необхідність передачі даних на центральні сервери для прийняття рішень. Це скорочує затримки та підвищує чуйність системи.

Енергоефективність: Обробка даних ближче до джерела дозволяє знизити обсяг даних, що передаються по мережі, що може допомогти в економії енергії в пристроях IoT, особливо в тих, які працюють від обмежених джерел енергії.

Інтеграція з хмарними обчисленнями: Туманні обчислення інтегруються з хмарними рішеннями, надаючи баланс між локальною та хмарною обробкою даних.

Це дозволяє ефективно використовувати обчислювальні ресурси відповідно до конкретних потреб та завдань Інтернету речей.

Інтеграція туманних обчислень з Інтернетом речей покращує загальну продуктивність, ефективність та безпеку розподілених систем, що є важливим аспектом у сучасному цифровому світі.

Управління ресурсами:

- Системи туманних обчислень можуть автоматично реагувати на зміни в завданнях та обчислювальних ресурсах для оптимізації продуктивності.

Туманні обчислення відрізняються здатністю динамічного управління обчислювальними ресурсами в режимі реального часу, що робить їх ефективними для завдань зі змінним навантаженням і вимогами, що змінюються. Основні аспекти управління ресурсами у контексті туманних обчислень:

Автоматична адаптація: Системи туманних обчислень мають механізми автоматичної адаптації до змін умов. Це включає моніторинг завантаження ресурсів, виявлення вузьких місць та динамічний розподіл обчислювальних завдань для оптимізації продуктивності.

Оптимізація енергоспоживання: Управління ресурсами також включає вивчення та використання методів, спрямованих на економію енергії. Зокрема, у туманних обчисленнях можливе відключення чи перерозподіл обчислювальних вузлів для мінімізації енергоспоживання у періоди низької активності.

Динамічне масштабування: Системи туманних обчислень здатні змінювати масштабування в режимі реального часу в залежності від поточного навантаження. Це дозволяє ефективно використовувати ресурси за несподіваних періодів підвищеної активності, таких як пікові навантаження на обчислення.

Забезпечення високої доступності: управління ресурсами також включає стратегії забезпечення безперервної роботи системи. Це досягається через розподіл навантаження та резервування додаткових ресурсів для компенсації збоїв.

Оптимізація мережевої взаємодії: Управління ресурсами у туманних обчисленнях також включає оптимізацію передачі даних через мережу. Локальна обробка даних може зменшити обсяг трафіку, зменшити затримки та підвищити ефективність мережної взаємодії.

Застосування штучного інтелекту для управління: У туманних обчисленнях використовуються алгоритми та методи штучного інтелекту для прогнозування та оптимізації використання ресурсів. Це включає машинне навчання для виявлення патернів використання та прийняття рішень.

Грунтуючись на даних про навантаження, системи туманних обчислень пропонують гнучкі стратегії управління ресурсами, які можуть бути адаптовані під конкретні вимоги додатків. Це включає можливість динамічного перерозподілу ресурсів у відповідь на зміни пріоритетів та терміновості завдань.

Стандартизація:

- Для розвитку та уніфікації технологій туманних обчислень були створені ініціативи та консорціуми, такі як OpenFog Consortium.

Стандартизація:

У сфері туманних обчислень стандартизація відіграє важливу роль, забезпечуючи сумісність та інтеграцію різних компонентів та рішень. Проекти зі стандартизації спрямовані на встановлення загальних правил та протоколів, які гарантують узгоджену взаємодію між пристроями та системами у туманному середовищі.

OpenFog Consortium: Це некомерційне об'єднання, яке розробляє стандарти для туманних обчислень. OpenFog створює рекомендації та специфікації для архітектур, протоколів та сервісів у туманному середовищі. Стандарти OpenFog охоплюють такі аспекти як безпека, управління ресурсами, архітектура мережі та інші.

IEEE P1934: Робоча група IEEE P1934 також займається стандартизацією туманних обчислень. Їхня робота спрямована на визначення стандартів для архітектури, інтерфейсів та протоколів у галузі туманних обчислень. Це сприяє одноманітності та спрощенню застосування туманних обчислень у різних галузях.

Стандарти безпеки: Розробка норм та правил безпеки є важливим аспектом стандартизації у сфері туманних обчислень. Це включає заходи захисту даних, шифрування, автентифікації та управління доступом. Стандарти безпеки створюють основу для надійного та стійкого функціонування туманних обчислень.

Вплив на промисловість: Прийняття стандартів у галузі туманних обчислень сприяє широкому використанню цієї технології промисловістю. Загальні стандарти роблять рішення більш сумісними, покращуючи їх інтеграцію та знижуючи витрати на розробку та впровадження.

Гнучкість і динамічність: Стандарти для туманних обчислень повинні бути достатньо гнучкими, щоб враховувати різноманітні завдання та вимоги у різних сферах застосування.

Це надає технології динамічності, дозволяючи їй ефективно адаптуватися до різних ситуацій використання.

Процеси оновлення та розвитку: У галузі туманних обчислень також важливі процеси оновлення та розвитку. Стандарти повинні періодично переглядатися та оновлюватись відповідно до еволюції технологій та зміни потреб користувачів.

Стандартизація відіграє ключову роль у успішному впровадженні туманних обчислень, забезпечуючи однаковість, сумісність та безпеку у різних сценаріях використання.

Масштабованість:

- Туманні обчислення легко масштабуються в залежності від обсягу даних та обчислювальних завдань.

Однією з головних переваг туманних обчислень є їхня здатність масштабуватися. Це означає, що система може легко зростати і адаптуватися до обсягу даних і завдань, що збільшується, не сильно впливаючи на продуктивність і ефективність.

Коли йдеться про масштабованість, туманні обчислення дозволяють легко додавати нові вузли або ресурси до мережі для обробки додаткових завдань. Це особливо корисно в умовах зростання обсягів даних, які часто зустрічаються в різних виробничих і наукових областях.

Крім того, масштабованість туманних обчислень дозволяє ефективно використовувати обчислювальні ресурси навіть за зміни навантаження. Система автоматично адаптується до змін та розподіляє завдання між вузлами для оптимального використання ресурсів.

У випадках, коли потрібна обробка великої кількості даних на великій кількості вузлів, масштабування туманних обчислень дозволяє легко розширювати мережу, додаючи нові вузли без проблем.

Однією з важливих характеристик масштабованості є здатність системи обробляти великі обсяги даних та ефективно використовувати ресурси без втрати продуктивності та безперервності обчислень.

Загалом, масштабованість туманних обчислень робить їх ефективними для застосування в гнучких та масштабованих системах, таких як великі мережі Інтернету речей (IoT), промислові процеси та інші області, де обсяг даних постійно зростає.

10. Інтелектуальні алгоритми:

- Застосування алгоритмів штучного інтелекту та машинного навчання для обробки та аналізу даних.

Висновки до розділу 1

У цьому розділі було проаналізовано механізми комунікацій в судноплавстві. Також було досліджено основні переваги туманих обчислень та можливість застосування останніх для доповнення механізмів комунікацій у судноплавстві для покращення безпеки.

РОЗДІЛ 2. Розробка політик безпеки для взаємодій вузлів та підсистем суден

В даному розділі запропонуємо політики безпеки для взаємодій вузлів та підсистем суден. Тут можемо розділити політики безпеки для внутрішніх комунікацій у вузлі та зовнішніх комунікацій, за принципом, запропонованим у [7].

2.1 Забезпечення конфіденційності

Для забезпечення конфіденційності можна впровадити кілька основних правил [2]:

1) Будь-яка взаємодія з керуючим сервером або будь-яким вузлом у мережі Інтернет чи мережі суден повинна пройти процедуру шифрування. Це може включати в себе використання шифрування, яке вбудоване в протокол, або передачу даних по відомо безпечних каналах. Такі канали можуть включати в себе VPN-з'єднання або SSH-тунелі до власних серверів.

2) Водночас, шифрування не повинно бути занадто “важким” для того, щоби не уповільнювати процес взаємодій. Можна запропонувати використовувати “lightweight” протоколи, з яких найкращими для взаємодій між пристроями з обмеженою функціональністю (пристроями IoT). Приклади алгоритмів "легкої криптографії" (lightweight cryptography), яка використовується для задач безпеки пристроїв інтернету речей: 1) ASCON, автентифіковане шифрування на основі перестановок із пов’язаними даними (AEAD) і хеш-схема, яка була обрана як переважне полегшене автентифіковане рішення шифрування під час конкурсу NIST; 2) Elephant, схема AEAD на основі перестановок, яка дотримується методології побудови nonce-based encryptthen-MAC; 3) GIFT-COFB, схема AEAD,

заснована на блокових шифрах, з базовим блоковим шифром GIFT-128; 4) Xoodyak, AEAD на основі перестановок і схема хешування, яка спирається на фіксовану 384-бітну перестановку, що працює в режимі Cyclist.

3) В разі, якщо обмін даними здійснюється між достатньо потужними серверами, можна вдаватись і до інших видів шифрування.

4) Сховище даних, де зберігається та обробляється інформація, має бути повністю зашифроване. Операційні програми за замовчуванням повинні мати обмежений доступ лише до ресурсів, якими вони операційно володіють. Наприклад, програма має право на запис тільки у свою власну директорію або до пристроїв, датчиків та систем, над якими вона функціонує.

При дотриманні правил 1)-4) за умови коректних налаштувань безпеки відповідних прикладних та системних програм, можна забезпечити конфіденційність.

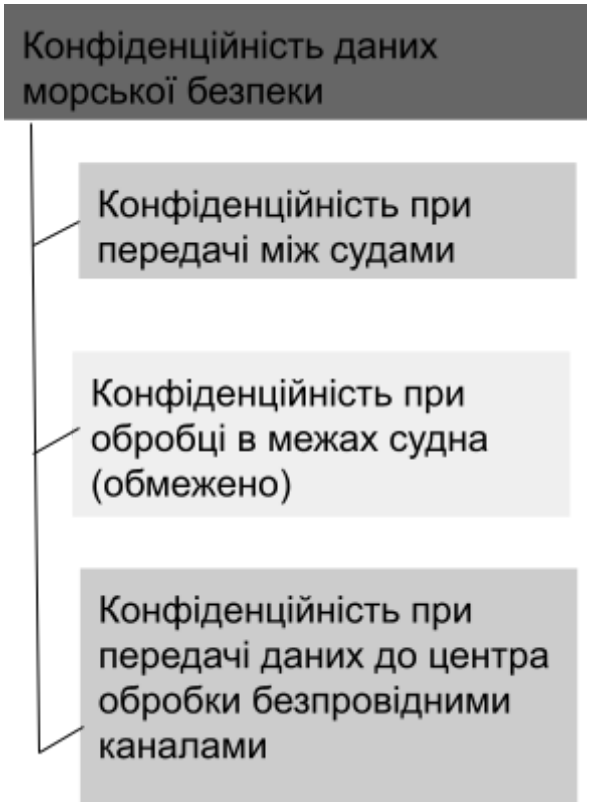


Рисунок 2.1 – Забезпечення конфіденційності

Рисунок 2.1 показує ланки забезпечення конфіденційності даних морської безпеки. Зокрема, конфіденційність даних, які не покидають межі судна, і обробляються за принципами туманної обробки даних - забезпечується в основному заходами фізичної безпеки.

2.2 Забезпечення цілісності

Для даних морської безпеки більше значення порівняно із конфіденційністю, відіграє є цілісність. Тому, забезпечення цілісності має бути здійснене на різних рівнях, включаючи протоколи, файлові системи та обробку даних. В операційній системі Linux (яка покладена в основу більшості операційних систем інтелектуальних кіберфізичних пристроїв, таких, як Raspberry Pi, Orange Pi та ін.) цілісність файлової системи забезпечується вбудованими механізмами та іншими програмними засобами, такими як Tripwire. Протоколи, такі як OpenVPN та SSH, забезпечують цілісність даних на рівні протоколів за допомогою вбудованих механізмів.

Встановлення базових правил для забезпечення цілісності включає:

1) Використання протоколів з механізмами цілісності для передачі даних (в деяких протоколах ці механізми можна увімкнути, використовуючи механізми сертифікатів, віддаленого обміну ключами та електронного підпису, що потребує певної інфраструктури відкритого ключа).
2) Регулярну перевірку файлової системи чи комплексу обробки даних на виявлення помилок. (Зазвичай операційна система слідкує за цим, за допомогою штатних вбудованих процедур самотестування).
3) Перевірку цілісності передаваних даних за допомогою хеш-суми файлу до та після передачі. Однак, за достатньої потужності обчислювальних пристроїв можна використовувати електронний підпис (бажано кваліфікований). Та/або алгоритми з п. 2.1, пункт 2).

2.3 Забезпечення доступності в системах управління судами

У даній області забезпечення доступності є одним з найважливіших умов. Доступність у даній моделі забезпечується за рахунок того що всі суда являються вузлами mesh мережі які можуть комунікувати між собою якщо інші канали комунікації стали недоступними [8]. Тобто кожен вузол являє собою додаткову точку відмови що дозволяє забезпечити доступність.

Також питання доступності тісно пов'язані із питаннями конфіденційності та цілісності в тому сенсі - що якщо є вибір обрати більш надійний алгоритм, але повільний (що може призвести до порушень доступності) - то обирають у випадку конфіденційності більш швидкий та менш надійний, а у випадку цілісності - помірковано надійний і достатньо швидкий (оскільки цілісність даних дуже важлива для інформації яка передається назовні від фізичних пристроїв). У випадку fog- обробки такі властивості можуть забезпечуватись елементарно шляхом впровадження заходів фізичної безпеки, унеможливлення доступу до пристроїв, які збирають та обробляють інформацію, невповноваженим персоналом судна.

2.4 Забезпечення автентичності даних

Будь-які дані, команди або пакети оновлення які впливають на детерміновану роботу системи повинні бути підписаними за допомогою КЕП (або в крайньому разі ЕП) для перевірки автентичності. Також для перевірки може використовуватись спосіб коли дані отримуються не тільки з центральних серверів, а й сусідніх вузлів які мають такі дані. У випадку оновлень ця вимога є обов'язковою.

2.5 Забезпечення спостережності

На кожному вузлі повинен бути механізм, який реазілує структуровані журнали та спеціальних окремий фізично захищений пристрій, у який можна

тільки додавати нові дані без можливості видалити попередні записи (чорний ящик). Вузли можуть передавати журнали тільки у транзитному режимі до центральних серверів які мають відповідні права на читання даних журналів. Для забезпечення ефективного моніторингу та полегшення виявлення помилок можна використовувати вбудований syslog. Цей інструмент можна налаштовувати для журналювання різних дій в системі, включаючи операції з журналами самої операційної системи Linux. Перш за все, для даної системи рекомендується журналювати:

1) Інформацію про авторизацію користувачів/вузлів, включаючи вдалі та невдалі спроби входу в систему, а також використані механізми аутентифікації. Ці дані можуть бути записані системою у відповідний файл, наприклад, /var/log/auth.log.
2) Помилки та системні критичні повідомлення, які мають мітки KERN_ERR та вище, в ядрі Linux. Ці події також слід фіксувати для подальшого аналізу.
3) Звіти вбудованого аудиту системи, що можуть містити важливу інформацію про події та дії в системі.

Такий підхід до журналювання дозволяє забезпечити вичерпний облік подій та полегшити виявлення можливих проблем у системі.

Також, традиційно на судах ведеться журнал (у паперовій формі) подій фізичної безпеки.

2.6. Розробка політик безпеки для систем управління суднами

Основні системи суден можна поділити на такі типи [10] :

1. **Системи навігації:** Включають GPS, гіроскопи, ехолоти та інші системи, які забезпечують точну навігацію та управління курсом судна.
2. **Системи безпеки та порятунку:** Включають системи контролю пожежі, шлюпки для порятунку, рятувальні жилети, радіобуї та інші засоби, які забезпечують безпеку пасажирів та екіпажу.

3. **Системи електроживлення та автоматизації:** Включають системи електроживлення, автоматичні системи керування двигунами, системи контролю витрати палива та інші системи, які забезпечують ефективне використання енергії та автоматизацію процесів на судні.
4. **Системи зв'язку:** Включають радіозв'язок, супутниковий зв'язок, системи радіолокації та інші технології, які забезпечують зв'язок з зовнішнім світом, а також зв'язок між судном та береговими станціями.
5. **Системи управління вантажем та баластні системи:** Включають системи управління вантажем, системи контролю ваги, баластні системи, які забезпечують ефективне завантаження та балансування судна.
6. **Системи опалення, вентиляції та кондиціювання повітря (ОВК):** Забезпечують комфортні умови для пасажирів та екіпажу на борту судна в різних кліматичних умовах.
7. **Системи очищення та утилізації відходів:** Включають системи очищення стічних вод, утилізації відходів, а також системи переробки та утилізації сміття, що допомагає дотримуватися екологічних стандартів та норм.
8. **Системи виявлення та запобігання аварій:** Включають радари, системи контролю близькості інших суден, системи попередження зіткнень та інші технології, які забезпечують безпечний рух судна та запобігають аваріям.
9. **Системи обслуговування пасажирів:** Включають системи обслуговування пасажирів, такі як бортові ресторани, розважальні системи, каюти та інші послуги, які забезпечують комфорт і задоволення потреб пасажирів під час плавання.
10. **Системи контролю забруднення та захисту навколишнього середовища:** Включають системи контролю викидів, системи очищення вихлопних газів, системи запобігання витоку палива та інші технології, які забезпечують дотримання стандартів з охорони навколишнього середовища.

Таблиця 2.1 Внутрішня політика безпеки систем судна

Тип системи	Послуги безпеки			
	Конфіденційність	Цілісність	Доступність	Спостережність
Системи навігації; Системи безпеки та порятунку; Системи електроживлення та автоматизації; Системи управління вантажем та баластні системи; Системи опалення, вентиляції та кондиціювання повітря (ОВК); Системи очищення та	-	+ Самотестування основних функцій при перезапуску; Контроль перепрошивання; Передача даних до керуючої системи без видозмін	+ Можливість контролю з боку керуючої системи та подібних пристроїв для синхронізації	+ Надсилання сигналів про збій до керуючої системи, які повинні логуватись у керуючій системі та/або хмарі

утилізації відходів; Системи виявлення та запобігання аварій; Системи обслуговування пасажирів; Системи контролю забруднення та захисту навколишнього середовища				
Системи зв'язку	+ Конфіденційність ключів для спілкування, які зберігаються на пристрої	+ Захист від сторонніх втручань у канал передачі	+ Можливість збору інформації з боку керуючої системи (доступність оцінюється методами надсилання пакетів про	+ Надсилання сигналів про нормальне функціонування, які повинні логуватись у керуючій системі та/або хмарі

			нормальне функціонування)	

Таблиця 2.2 Зовнішня політика безпеки судна

Тип пристрою	З ким спілкується шляхом безпровідного зв’язку, яка властивість інформації має забезпечуватись при обміні (Конфіденційність К, Цілісність Ц+Автентифікація А)				
	Хмара	Центр управління (сервери)	Портова інфраструктура	Судно	Окремі датчики у морі(радіобуй тощо)
Хмара	-	Довідкова /Синхронізуюча інформація (Ц+А+К)	Синхронізуюча інформація (Ц+А+К)	Довідкова /Синхронізуюча інформація (Ц+А+К)	Довідкова інформація (Ц)
Центр управління (сервери)	Довідкова /Синхронізуюча інформація (Ц+А+К)	Довідкова /Синхронізуюча інформація/ Керуючі сигнали (Ц+А+К)	Довідкова /Синхронізуюча інформація (Ц+А+К)	Довідкова /Синхронізуюча інформація/ Керуючі сигнали (Ц+А+К)	Довідкова інформація (Ц)

Портова інфраструктура	Довідкова /Синхроніз уюча інформація (Ц+А+К)	Довідкова /Синхроніз уюча інформація (Ц+А+К)	Довідкова /Синхроніз уюча інформація (Ц+А+К)	Довідкова /Синхроніз уюча інформація/ Керуючі сигнали (Ц+А+К)	Довідкова інформація (Ц)
Судно	Довідкова /Синхроніз уюча інформація (Ц+А+К)	Довідкова /Синхроніз уюча інформація (Ц+А+К)	Довідкова /Синхроніз уюча інформація (Ц+А+К)	Довідкова /Синхроніз уюча інформація (Ц+А+К)	Довідкова інформація (Ц)
Окремі датчики у морі(радіобуй тощо)	Синхронізуюча інформація, інформація про місцеположення (Ц)	Синхронізуюча інформація, інформація про місцеположення (Ц)	Синхронізуюча інформація, інформація про місцеположення (Ц)	Синхронізуюча інформація, інформація про місцеположення (Ц)	Довідкова інформація (Ц)

Висновки до розділу 3

Розглянуто основні системи управління суднами. Для них розроблені зовнішня та внутрішня політики з використанням туманної архітектури. Політики враховують такі аспекти як: конфіденційність, цілісність, доступність, автентичність, та спостережність (журналювання подій).

Показано доцільність та Linux - орієнтованої архітектури для поставленої задачі.

РОЗДІЛ 3. Перевірка працездатності запропонованих рішень

Для перевірки можливості налаштувань політик безпеки так, як наведено в Розділі 2, здійснено комп'ютерний експеримент на одноплатному комп'ютері OrangePi з Linux- подібною ОС ARMbian, встановленою на пристрої.

3.1 Перевірка можливості налаштувань конфіденційності

Запропонуємо спосіб забезпечення конфіденційності каналу передачі даних за допомогою OpenVPN. Такий вид конфіденційності може використовуватись при обміні між пристроями fog-рівня та віддаленими пристроями на берегу (в центрі обробки). Налаштуємо VPN point-to-Site з режимом аутентифікації по сертифікату. Даний спосіб відрізняється надійністю шифрування, автентифікації та забезпеченням цілісності даних, які передаються. Експеримент було здійснено із використанням підключення до мережі Інтернет 3G-модему, стільникового зв'язку та утиліти wvdial.

Здійснимо конфігурування серверу OpenVPN(Рис.3.1):

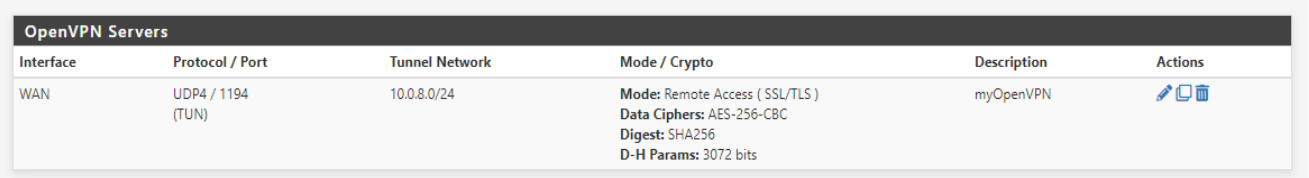


Рисунок 3.1 Характеристики OpenVPN

Здійснимо конфігурування клієнта:

Wvdial (Рис. 3.2):

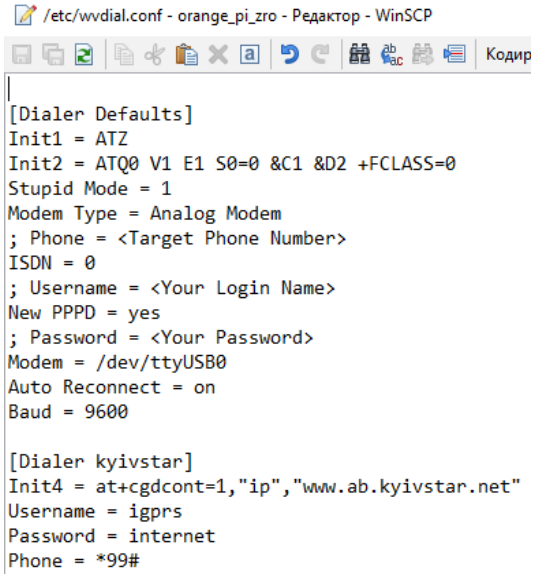


Рисунок 3.2 Конфігурація GSM

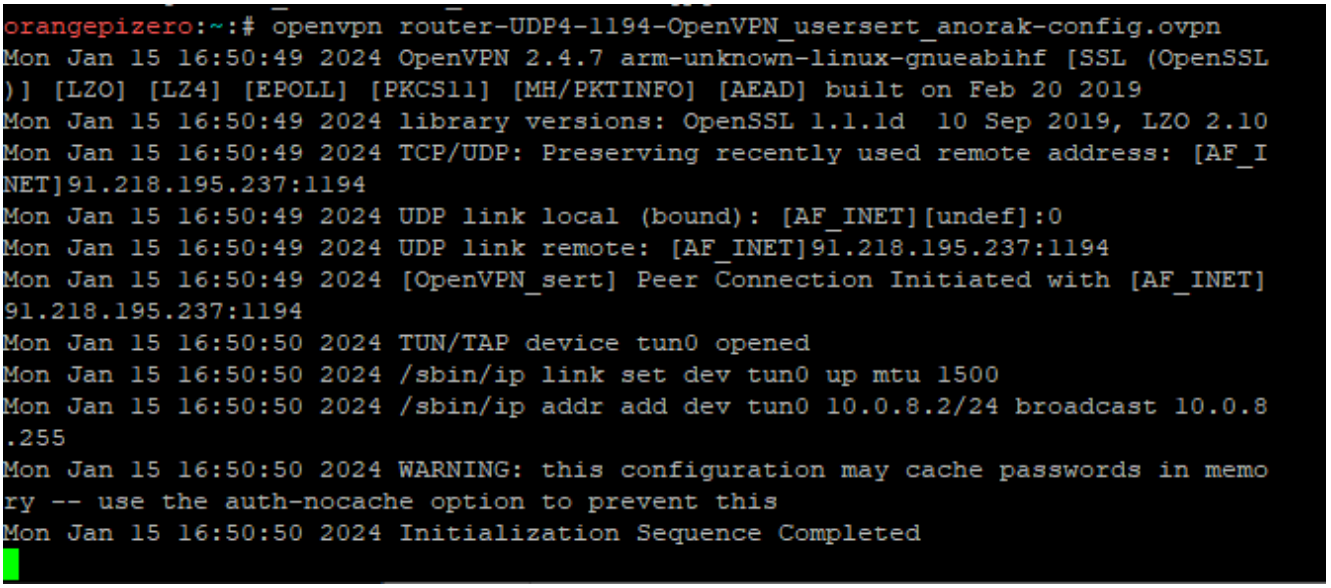
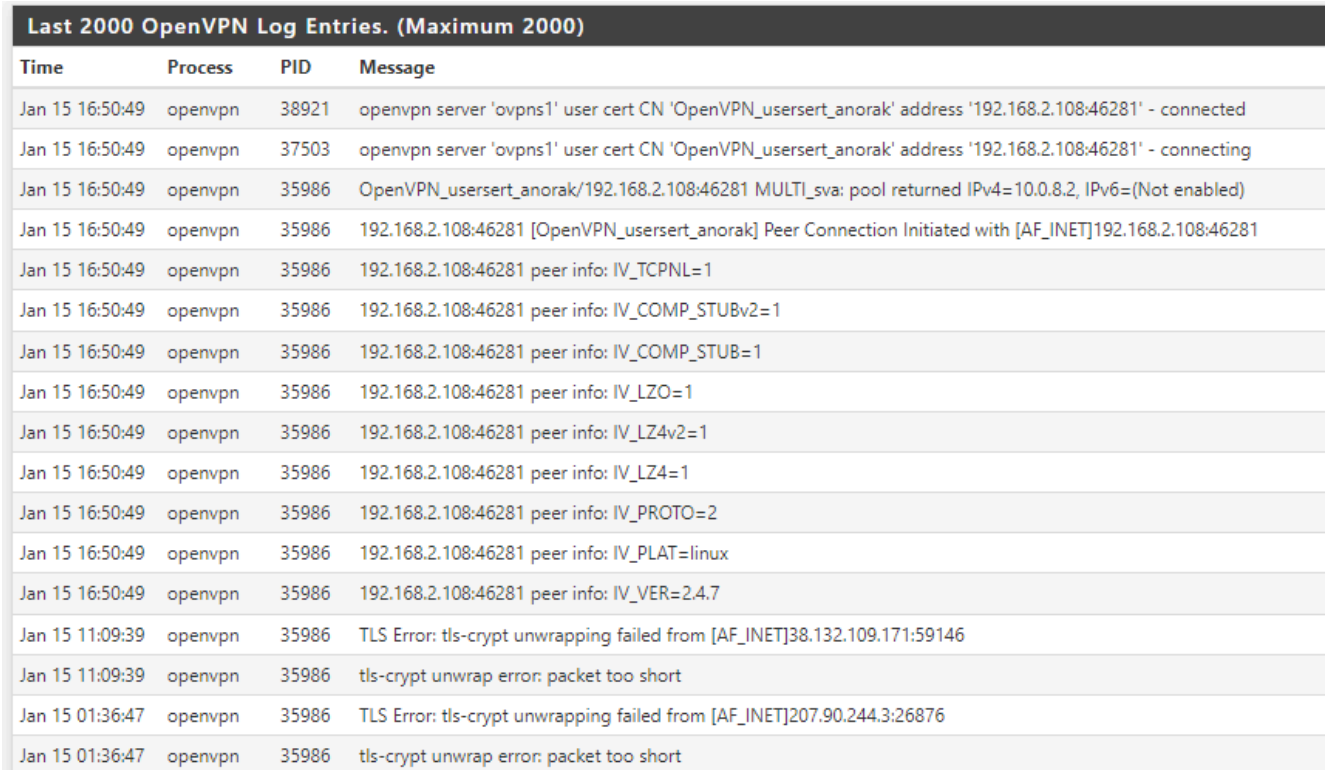


Рисунок 3.3. - Послідовність підключення до серверу OpenVPN

Виконаємо підключення до серверу за допомогою протокола OpenVPN(Рис. 3.3).

На Рис. 3.4 показано відображення цієї події.



Last 2000 OpenVPN Log Entries. (Maximum 2000)

Time	Process	PID	Message
Jan 15 16:50:49	openvpn	38921	openvpn server 'ovpns1' user cert CN 'OpenVPN_usersert_anorak' address '192.168.2.108:46281' - connected
Jan 15 16:50:49	openvpn	37503	openvpn server 'ovpns1' user cert CN 'OpenVPN_usersert_anorak' address '192.168.2.108:46281' - connecting
Jan 15 16:50:49	openvpn	35986	OpenVPN_usersert_anorak/192.168.2.108:46281 MULTI_sva: pool returned IPv4=10.0.8.2, IPv6=(Not enabled)
Jan 15 16:50:49	openvpn	35986	192.168.2.108:46281 [OpenVPN_usersert_anorak] Peer Connection Initiated with [AF_INET]192.168.2.108:46281
Jan 15 16:50:49	openvpn	35986	192.168.2.108:46281 peer info: IV_TCPNL=1
Jan 15 16:50:49	openvpn	35986	192.168.2.108:46281 peer info: IV_COMP_STUBv2=1
Jan 15 16:50:49	openvpn	35986	192.168.2.108:46281 peer info: IV_COMP_STUB=1
Jan 15 16:50:49	openvpn	35986	192.168.2.108:46281 peer info: IV_LZO=1
Jan 15 16:50:49	openvpn	35986	192.168.2.108:46281 peer info: IV_LZ4v2=1
Jan 15 16:50:49	openvpn	35986	192.168.2.108:46281 peer info: IV_LZ4=1
Jan 15 16:50:49	openvpn	35986	192.168.2.108:46281 peer info: IV_PROTO=2
Jan 15 16:50:49	openvpn	35986	192.168.2.108:46281 peer info: IV_PLAT=linux
Jan 15 16:50:49	openvpn	35986	192.168.2.108:46281 peer info: IV_VER=2.4.7
Jan 15 11:09:39	openvpn	35986	TLS Error: tls-crypt unwrapping failed from [AF_INET]38.132.109.171:59146
Jan 15 11:09:39	openvpn	35986	tls-crypt unwrap error: packet too short
Jan 15 01:36:47	openvpn	35986	TLS Error: tls-crypt unwrapping failed from [AF_INET]207.90.244.3:26876
Jan 15 01:36:47	openvpn	35986	tls-crypt unwrap error: packet too short

Рисунок 3.4 Журналювання підключення до серверу

Скріншот Рис. 3.5 ілюструє роботу програми GPG.

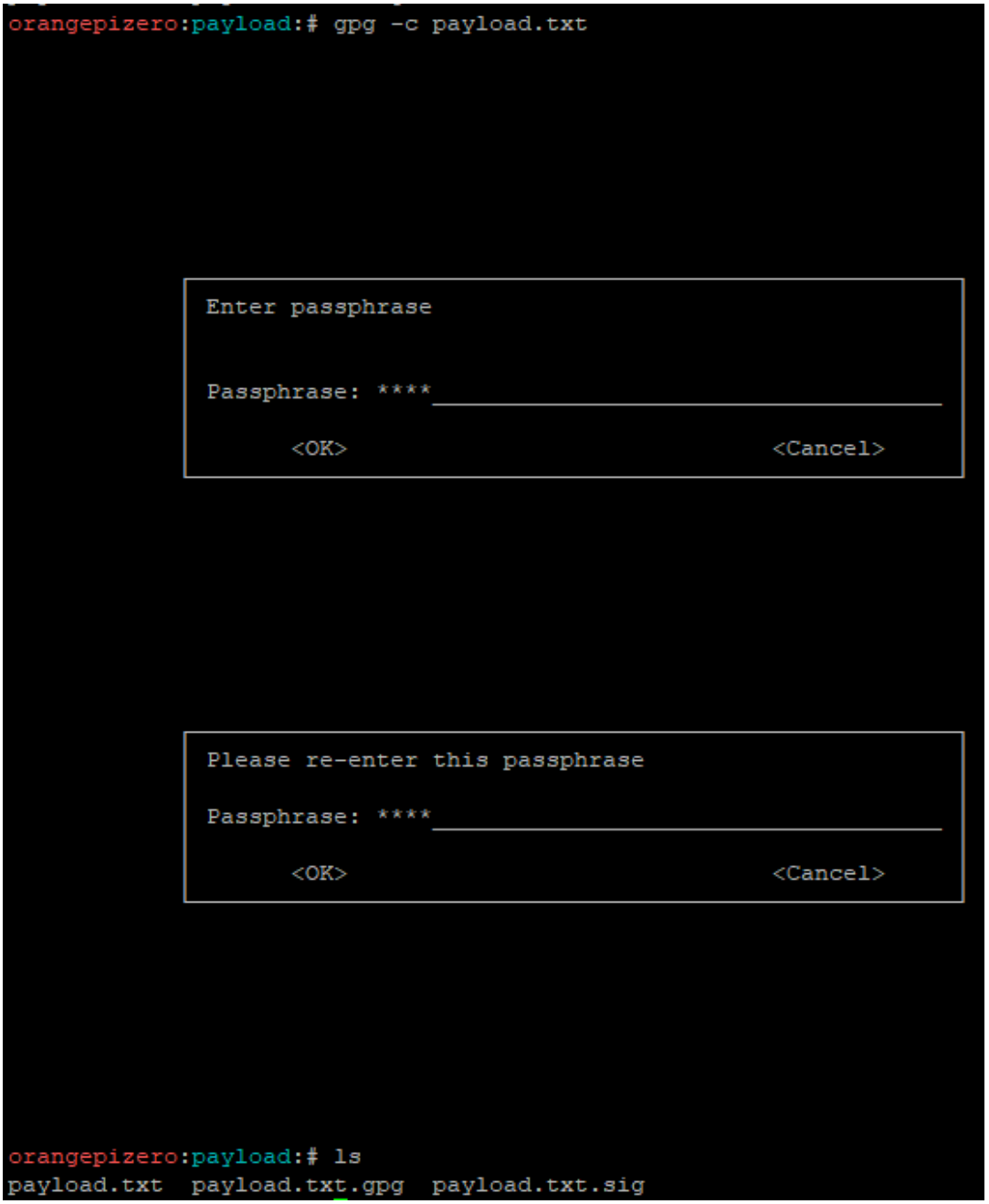


Рисунок 3.5 Шифрування GPG

Після виконная програми отримуємо файл з розширенням .gpg зашифрований алгоритмом AES-256. Алгоритми симетричної криптографії є цілком прийнятним рішенням для задач притаманних пристроям інтернету речей, в тому числі в складі кіберфізичних систем суден. На відмінність від алгоритмів асиметричної

криптографії, які треба використовувати з обачністю внаслідок їхньої потенційної ресурсовимогливості.

Процес розшифрування файлу наведено на Рис. 3.6.

```
orangepizero:payload:# gpg payload.txt.gpg
gpg: WARNING: no command supplied.  Trying to guess what you mean ...
gpg: AES256 encrypted data
gpg: encrypted with 1 passphrase
File 'payload.txt' exists. Overwrite? (y/N) y
orangepizero:payload:#
```

Рисунок 3.6 - Розшифрування файлу

Розшифрування та шифрування файлів може здійснюватись як на рівні пристроїв fog- рівня, так і на хмарному рівні. Тому, в разі використання симетричних алгоритмів - треба потурбуватись про обмін ключами. Це може відбуватись під час перебування судна у порті (де є можливість безпечно комунікувати із серверами хмарного рівня, в тому числі використовуючи алгоритм Діффі-Хеллмана), безпосередньо шляхом статичного впровадження відповідного таємного ключа до системи судна, переносом ключа на захищеному пристрої з сервера, який взаємодіяв по протоколу Діффі -Хеллмана із хмарним рівнем.

3.2 Перевірка наявності засобів забезпечення автентичності

Накладання ЕП будемо виконувати за допомогою програми GPG, на файли.

Рисунок 3.7 Створення ключа RSA-3072

```
orangepizero:~:# gpg --list-keys
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   2  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 2u
gpg: next trustdb check due at 2026-01-14
/root/.gnupg/pubring.kbx
------------------------
pub   rsa3072 2021-05-20 [SC] [expired: 2023-05-20]
      BCFC399ED58DA26790D74D90500AE03A7A426D0C
uid           [ expired] iotkey

pub   rsa3072 2024-01-15 [SC] [expires: 2026-01-14]
      581D46D011192CD1BE03C117B043F0BC46BEFC2C
uid           [ultimate] Kyryl
```

Створимо ключ, за замовчуванням створиться ключ RSA-3072(Рис. 3.7). Однак, слід зауважити, про те що в разі необхідності “полегшити” засоби ЕП, така можливість існує, за допомогою інтеграції прикладних бібліотек, які підтримують “lightweight” криптографію, яка не уповільнює обчислення,і придатна для малопотужних пристроїв в тому числі. Однак, пристрої типу Orange Pi успішно використовують асиметричну криптографію RSA.

Використовуючи створений ключ, підпишемо файл(Рис 3.8):

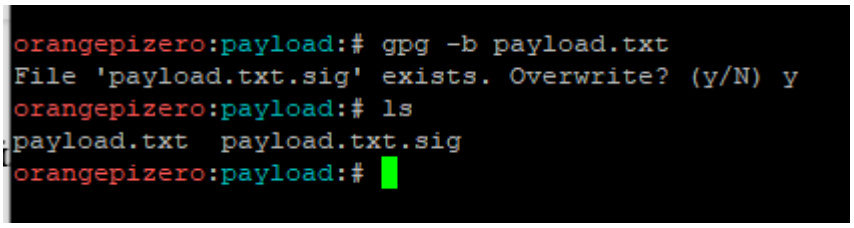


Рисунок 3.8 Накладання ЕП на файл

Далі, змінимо інформацію в файлі та виконаємо перевірку файла на автентичність (Рис. 3.9).

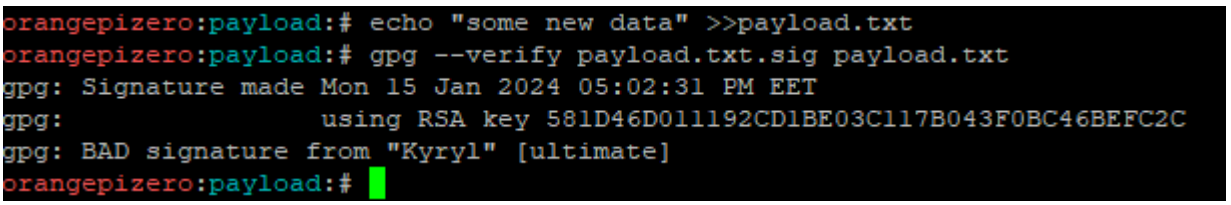


Рисунок 3.9 Скріншот з перевіркою автентичності

Скріншот показує наступне: перевірка ЕП відбулась успішно, в результаті встановлено, що даний ЕП не відповідає цьому файлу. Це означає порушення або цілісності, або автентичності. В даному випадку - автентичності.

3.3 Перевірка цілісності

Цілісність файлової системи в Linux-подібних системах перевіряється за допомогою використання штатної утиліти fsck. Цю утиліту буде правильно використовувати при кожному запуску операційної системи.

Панель налаштування утиліти з командного рядка показано на Рис 3.10.

```
orangepizero:~:# touch /forcefsck
orangepizero:~:# ls /
bin   dev  forcefsck  lib         media  opt   root  sbin     srv  tmp  var
boot  etc  home       lost+found  mnt    proc  run   selinux  sys  usr
orangepizero:~:#
```

Рисунок 3.10 Налаштування fsck

Як тільки ОС завантажена, необхідно виконати перевірку ФС(Рис 3.11):

```
Starting kernel ...

Loading, please wait...
Starting version 241
Begin: Loading essential drivers ... done.
Begin: Running /scripts/init-premount ... done.
Begin: Mounting root file system ... Begin: Running /scripts/local-top ... done.
Begin: Running /scripts/local-premount ... Scanning for Btrfs filesystems
done.
Begin: Will now check root file system ... fsck from util-linux 2.33.1
[/sbin/fsck.ext4 (1) -- /dev/mmcblk0p1] fsck.ext4 -a -C0 /dev/mmcblk0p1
/dev/mmcblk0p1: clean, 57314/2813120 files, 580024/7711744 blocks
done.
done.
Begin: Running /scripts/local-bottom ... done.
Begin: Running /scripts/init-bottom ... done.

Welcome to Debian GNU/Linux 10 (buster)!
```

Рисунок 3.11 Робота утиліти fsck

3.4 Перевірка можливостей спостережності

Форма з параметрами налаштування логів syslog-ng показана на Рис. 3.12.

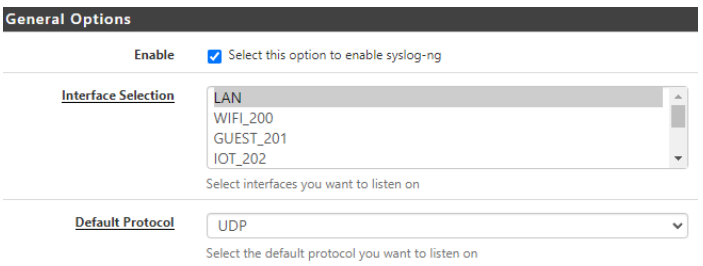


Рисунок 3.12 Налаштування syslog-ng серверу

Конфігурування клієнта для надсилання журналів на сервер показано на Рис. 3.13-3.14.

```
#
auth,authpriv.*                 /var/log/auth.log
*.*;auth,authpriv.none          -/var/log/syslog
#cron.*                         /var/log/cron.log
daemon.*                        -/var/log/daemon.log
kern.*                          -/var/log/kern.log
lpr.*                           -/var/log/lpr.log
mail.*                          -/var/log/mail.log
user.*                          -/var/log/user.log

#
# Logging for the mail system.  Split it up so that
# it is easy to write scripts to parse these files.
#
mail.info                       -/var/log/mail.info
mail.warn                       -/var/log/mail.warn
mail.err                        /var/log/mail.err

#
# Some "catch-all" log files.
#
*.=debug;\
        auth,authpriv.none;\
        news.none;mail.none     -/var/log/debug
*.=info;*.=notice;*.=warn;\
        auth,authpriv.none;\
        cron,daemon.none;\
        mail,news.none          -/var/log/messages

#
# Emergencies are sent to everybody logged in.
#
*.emerg                         :omusrmsg:*

*.info;mail.none;authpriv.none;cron.none @192.168.1.1:5140
```

Рисунок 3.13 Файл конфігурації syslog-ng

Showing 25 of 25 messages

Jan 15 18:07:06 router syslog-ng[57267]: syslog-ng starting up; version='4.2.0'
Jan 15 18:09:39 192.168.2.108 chronyd[817]: chronyd exiting
Jan 15 18:09:39 192.168.2.108 sshd[832]: Received signal 15; terminating.
Jan 15 18:09:39 192.168.2.108 systemd[1]: Closed Load/Save RF Kill Switch Status /dev/rfkill Watch.
Jan 15 18:09:39 192.168.2.108 systemd[1]: Condition check resulted in Show bootsplash on system halt, power off, reboot, or kexec being skipped.
Jan 15 18:09:39 192.168.2.108 systemd[1]: openvpn.service: Succeeded.
Jan 15 18:09:39 192.168.2.108 systemd[1]: Stopped OpenVPN service.
Jan 15 18:09:39 192.168.2.108 systemd[1]: Stopped target Graphical Interface.
Jan 15 18:09:39 192.168.2.108 systemd[1]: Stopped target Login Prompts.
Jan 15 18:09:39 192.168.2.108 systemd[1]: Stopped target Multi-User System.
Jan 15 18:09:39 192.168.2.108 systemd[1]: Stopping Authorization Manager...
Jan 15 18:09:39 192.168.2.108 systemd[1]: Stopping chrony, an NTP client/server...
Jan 15 18:09:39 192.168.2.108 systemd[1]: Stopping Getty on tty1...
Jan 15 18:09:39 192.168.2.108 systemd[1]: Stopping LSB: Advanced IEEE 802.11 management daemon...
Jan 15 18:09:39 192.168.2.108 systemd[1]: Stopping LSB: disk temperature monitoring daemon...
Jan 15 18:09:39 192.168.2.108 systemd[1]: Stopping LSB: RPi-Monitor sunxi-temp helper...
Jan 15 18:09:39 192.168.2.108 systemd[1]: Stopping OpenBSD Secure Shell server...

Рисунок 3.14 Лог утиліти syslog-ng

3.4 Схема розміщення пристроїв типу Orange Pi в складі кіберфізичної системи судна

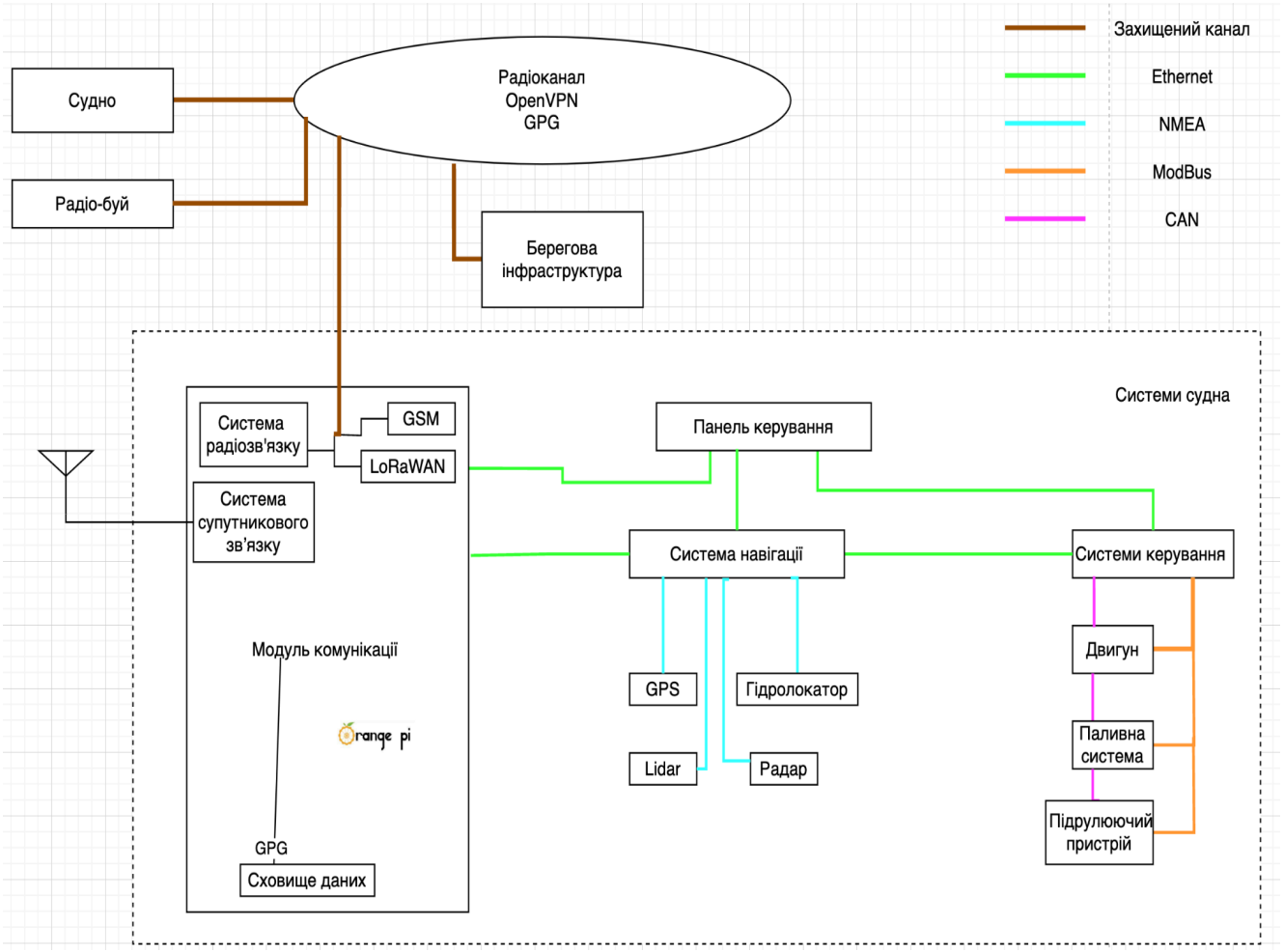


Рисунок 3.15 Схема взаємодії

Схему взаємодії пристроїв, які здійснюватимуть туманну обробку даних в складі кіберфізічної системи судна (Orange Pi) - показано на рис. 3.15.

Висновки до розділу 3

Було проаналізовано існуючі можливості Linux (і, в тому числі і ОС ARMbian як представника цього класу), в результаті чого визначено, що політики безпеки, представлені у табл. 3.1 , 3.2 можуть бути забезпечені засобами ОС та засобами відповідних протоколів комунікації (OpenVPN).

Це підтверджує можливість використання пристроїв Raspberry Pi для реалізації політик безпеки, спрямованих на конфіденційність, цілісність, доступність та спостережність даних кіберфізичних систем судна, на рівні fog.

РОЗДІЛ 4. Стартап

Для розробки стартапу, необхідно оцінити можливість впровадження запропонованої політики безпеки в умовах конкурентної глобальної економіки. Маркетинговий аналіз включає декілька кроків, якими ми плануємо зайнятися далі (пункти цього розділу).

4.1 Опис ідеї проекту

В цьому підрозділі буде здійснено аналіз змісту ідеї, що пропонується, можливі напрямки застосування, основні вигоди, що може отримати користувач товару (за кожним напрямком застосування) (таблиця 4.1) та відмінність від існуючих аналогів.

Таблиця 4.1 – Опис ідеї стартап-проекту

Зміст ідеї	Напрямки застосування	Вигоди для користувача
Розробка обчислювального комплексу пристроїв що використовують розроблену політику безпеки та/або інтеграцію в наявні апаратно-програмні комплекси	1. Адміністрування систем на суднах	Збільшення можливостей по налаштуванню та спрощення адміністрування

	2. Організації	Підвищення захисту апаратно-програмних комплексів на суднах

Після проведеного аналізу ринку, виявилось що готових рішень немає крім розробки ВМФ США для воєнних задач.[8]

4.2 Технологічний аудит ідеї проекту

В даному підрозділі будемо розглядати технології та методи які необхідні для реалізації проекту. В результаті аналізу було виявлено, що усі запропоновані технології є доступними та вільними у користуванні. В табл. 4.2 показано необхідні кроки при реалізації проекту та запропоновані методи і технології для їх вирішення.

Таблиця 4.2 – Технологічна здійсненність ідеї проекту

№	Ідея проекту	Технології її реалізації	Наявність технологій	Доступність технологій
1	Побудова системи комунікації	SSH OpenVPN	Наявна	Доступна
2	Впровадження запропонованої політики безпеки	Наявне програмне забезпечення у дистрибутивах Linux	Наявна	Доступна

4.3 Аналіз ринкових можливостей запуску стартап-проекту

Визначення ринкових можливостей, які можна використати під час ринкового впровадження проекту, та ринкових загроз, які можуть перешкодити реалізації проекту, дозволяє планувати напрями розвитку проекту з урахуванням стану ринкового середовища, потреб потенційних клієнтів та пропозицій проектів-конкурентів.

Першим кроком визначення ринкових можливостей є аналіз та попередня характеристика ринку стартап проекту, що зображено в Таблиці 5.3

Таблиця 4.3 – Попередня характеристика потенційного ринку стартап-проекту

№ п/п	Показники стану ринку (найменування)	Характеристика
1	Кількість головних гравців, од.	3
2	Загальний обсяг продаж, грн/ум.од	900 тис. ум.од.
3	Динаміка ринку (якісна оцінка)	Зростає
4	Наявність обмежень для входу (вказати характер обмежень)	Немає
5	Специфічні вимоги до стандартизації та сертифікації	Немає

6	Середня норма рентабельності в галузі (або по ринку), %	65%

Також необхідно розуміти цільову групу продукту і потреби які буде задовольняти продукт. Таким чином в таблиці 4.4 розглядаються характеристики потенційних клієнтів стартап-проекту.

Таблиця 4.4 – Характеристика потенційних клієнтів стартап-проекту

№ п/п	Потреба, що формує ринок	Цільова аудиторія (цільові сегменти ринку)	Відмінності у поведінці різних потенційних цільових груп клієнтів	Вимоги споживачів до товару
1.	Збільшення кількості кіберзагроз, застаріли підходи до побудови систем комунікацій	Компанії	–	Зручність використання, надійність, можливість використання в реальному часі, малий вплив на швидкодію пристрою

Після визначення цільової аудиторії проекту необхідно проаналізувати можливі фактори загроз, що можуть перешкоджати розвитку проекту, та фактори можливостей, що сприяють ринковому впровадженню (Табл. 4.5 та 4.6).

Таблиця 4.5 – Фактори загроз

№	Фактор	Зміст загрози	Можлива реакція компанії
1.	Малий стартовий капітал	Недостатня кількість грошей для реалізації ідеї та виходу на ринок	Інвестори або спроби пошуку дешевших варіантів реалізації ідеї
2.	Відсутність репутації	Немає статусу компанії, невідома якість продукту	Розробка документації та підготовка маркетингових рішень

Таблиця 4.6 – Фактори можливостей

№	Фактор	Зміст можливості	Можлива реакція компанії
1.	Низька кількість альтернатив	На ринку практично відсутні альтернативні продукти	Створення унікального, розширеного, функціоналу, що зробить це рішення привабливим за конкурентів

Таблиця 4.7 - Ступеневий аналіз конкуренції на ринку

Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)
1. Конкуренція – олігополія	Немає великих конкурентів – корпорацій, ринок ще є незаповненим	Можливість завоювати частину ринку за рахунок унікального функціоналу
2. Рівень конкурентної боротьби – світовий	Рішення доступно глобально	Необхідні додаткові дослідження та впровадження локалізації
3. За галузевою ознакою - міжгалузева	Не стосується певної галузі	Розширення сфери надання послуг
4. Конкуренція за видами товарів - товарно-видова	Цей товар є унікальним за рахунок своєї першопрохідності	

Після аналізу конкуренції проведено детальний аналіз умов конкуренції в галузі – за моделлю 5 сил М. Портера (таб. 4.8).

Таблиця 4.8 – Аналіз конкуренції в галузі за М. Портером

Складові аналізу	Прямі конкуренти в галузі	Потенційні конкуренти	Клієнти	Товари-замінники
	ВМФ США	Здешевлення продукту може призвести до появи	Організації які володіють великою кількістю кораблів	Організаційно-нормативні і суттєво інші технічні підходи для організацій
Висновки:	Конкурентна боротьба низька	Строки виходу на ринок від 1 до 2 років.	Клієнт має прямий вплив на подальший розвиток і вдосконалення	Обмежень немає

З огляду на конкурентну ситуацію можемо побачити, що продукт має

змогу вийти на ринок та бути конкурентоспроможним через 1-2 роки після початку розробки.

На основі аналізу конкуренції, проведеного в Таблиці 4.8, а також із урахуванням характеристик ідеї проекту (табл. 4.2), вимог споживачів до товару (табл. 4.5) та факторів маркетингового середовища (табл. 4.6-4.7) визначається та обґрунтовується перелік факторів конкурентоспроможності (табл. 4.10).

Таблиця 4.9 – Обґрунтування факторів конкурентоспроможності

№ п/п	Фактор конкурентоспроможності	Обґрунтування (наведення чинників, що роблять фактор для порівняння конкурентних проектів значущим)

1	Ціновий	Ціноутворення в даній сфері ще не затверджено
2	Відсутність прямих конкурентів	Відсутні рішення, що є прямою альтернативою за функціоналом продукту
3	Швидкодія	Продукт перевищує швидкодію інших архітектур

Таблиця 4.10 - Порівняльний аналіз сильних та слабких сторін продукту

№ п/п	Фактор конкурентоспроможності	Бали 1-20	Рейтинг товарів-конкурентів						
			–3	–2	–1	0	+1	+2	+3
1	Ціновий	17					+		
2	Технологічний	19							+
3	Технічний	9						+	
4	Ринковий	15						+	

Фінальним етапом ринкового аналізу можливостей впровадження проекту є складання SWOT-аналізу (матриці аналізу сильних (Strength) та слабких (Weak) сторін, загроз (Troubles) та можливостей (Opportunities) на основі виділених ринкових загроз та можливостей, та сильних і слабких сторін (табл. 4.11).

Таблиця 4.11 - SWOT-аналіз стартап-проекту

Сильні сторони: Використання в режимі реального часу; підвищення швидкодії	Слабкі сторони: необхідність попередніх досліджень і вимірів; низький маркетинговий рівень.
Можливості: співпраця з виробниками кораблів	Загрози: довгий строку виходу на ринок

З огляду на отримані результати SWOT аналізу було розроблено альтернативи ринкової поведінки при виходу стартап проекту на ринок.

Визначені альтернативи аналізуються з точки зору строків та ймовірності отримання ресурсів (табл. 4.12).

Таблиця 4.12 - Альтернативи впровадження стартап-проекту на ринку

№ п/п	Альтернатива (орієнтовний комплекс заходів) ринкової поведінки	Ймовірність отримання ресурсів	Строки реалізації
1	Розробка без інвестицій та команди	Мала ймовірність отримання ресурсів	3 роки
2	Розробка системи у партнерстві з крупним вендором	Висока ймовірність отримання ресурсів	2 рік
3	Пошук інвестицій на початковому етапі розробки	Середня ймовірність отримання ресурсів	2 рік

З означених альтернатив ринкового впровадження даного стартап-проекту було вирішено обрати розробку система у партнерстві з крупним вендором.

4.4 Розроблення ринкової стратегії проекту

Після детального аналізу ринкових можливостей та конкурентоспроможності продукту необхідно розробити стратегію виходу продукту на ринок. В таблиці 4.14 виявлено цільові групи потенційних споживачів даного стартап-проекту.

Таблиця 4.14 – Вибір цільових груп потенційних споживачів

№	Опис профілю цільової групи потенційних клієнтів	Готовність споживачів сприйняти продукт	Орієнтовний попит в межах цільової групи	Інтенсивність конкуренції в сегменті	Простота входу у сегмент
1	Користувачі Інтернет	Є потреба в підвищенні захисту окремих систем	Середній попит, пов’язаний з	Низька конкуренція, пов’язана з не заповненістю ринку і малою кількістю конкурентів	Висока, необхідний період попередніх досліджень

	мере жі		потребо ю		

В таблицях 4.15 та 4.16 визначимо базові стратегії розвитку та конкурентної поведінки продукту.

Таблиця 4.15 – Визначення базової стратегії розвитку

№	Обрана альтернатива розвитку	Стратегія охоплення ринку	Ключові конкурентноспроможні позиції відповідно до обраної альтернативи	Базова стратегія розвитку
1	Реалізація самостійної системи	Стратегія диференційованого маркетингу	Незалежність від сторонніх виробників	Стратегія диференціації
2	Інтеграція з виробниками суден	Стратегія спеціалізованого маркетингу	Тісна інтеграція з системами судна за рахунок прямої інтеграції просте поширення	Стратегія спеціалізації
3	Інтеграція з виробниками приладів керування та	Стратегія спеціалізованого маркетингу	Здешевлення кінцевого продукту	Стратегія спеціалізації

	моніторин гу			

Таблиця 4.16 – Визначення базової стратегії конкурентної поведінки

№	Чи є проект «першопрохідцем» на ринку?	Компанія шукатиме нових споживачів, або забиратиме існуючих у конкурентів?	Чи буде компанія копіювати основні характеристики товару конкурентів	Стратегія конкурентної поведінки
1	Так	Буде зацікавлювати як нових споживачів так і переманювати існуючих	Ні, так як використовує іншу технічний архітектуру	Стратегія диференціації

Таблиця 4.17 – Визначення стратегії ринкового позиціонування

№	Вимоги до товару цільової аудиторії	Базова стратегія розвитку	Ключові конкурентноспромож ні позиції власного стартап-проекту	Вибір асоціацій, які мають сформувати комплексну позицію

				власного проекту
1	Забезпечення захищеності суден	Стратегія диференціації	Застосування нової архітектури яка прискорює швидкодію	Туманні обчислення

4.5 Розроблення маркетингової програми стартап-проекту

Розробка маркетингової програми стартап проекту є важливою частиною запуску проекта. Складається з декількох етапів.

Таблиця 4.18 – Визначення ключових переваг концепції потенційного товару

№	Потреба	Вигода, яку пропонує товар	Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити
1	Нова модель комунікації яка забезпечує безпеку та швидкодію	Нову перспективну архітектуру і політику безпеки	Швидкодія, захищеність

Таблиця 4.20 – Визначення меж цін

№ п/п	Рівень цін на товари-замінники	Рівень цін на товари-аналоги	Рівень доходів цільової групи споживачів	Верхня та нижня межі встановлення ціни на товар/послугу
	Відсутній	300000-400000$	Від 500000$	Залежить від конфігурації

Таблиця 4.21 – Формування системи збуту

№	Специфіка закупівельної поведінки цільових клієнтів	Функції збуту, які має виконувати постачальник товару	Глибина каналу збуту	Оптимальна система збуту
1	Пошук систем туманих обчислень	Консультація, впровадження	Ринки оптової торгівлі	Продаж через дистриб'юторів

Таблиця 4.22 – Концепція маркетингових комунікацій

№	Специфіка поведінки цільових клієнтів	Канали комунікацій, якими користуються цільові клієнти	Ключові позиції, обрані для позиціонування	Завдання рекламного повідомлення	Концепція рекламного звернення

1	Пробне користування продукту	Усі можливі методи комунікацій в мережі Інтернет	Концетуально нових підхід в побудові взаємодій	Вказати на недоліки існуючих архітектур	Демонстрація швидкодії

Висновки до розділу 5

В розділі було розглянуті можливі перспективі стартап проекту, особливості, вимоги, яким має задовольняти продукт із огляду на маркетингові особливості, конкурентоспроможність, бар’єри входу на ринок та ін.

Запропоноване рішення має перспективи впровадження з огляду на актуальність ідеї та потребу потенційних клієнтів, незаповненість ринку та малу кількість конкурентів.

Для впровадження даного рішення було обрано розробити власний комплекс систем комунікацій, що є оптимальною можливістю з точки зору техніко-економічних можливостей, та допоможе виявити реальну потребу в даному продукті. Також можливим альтернативами є інтеграція з виробниками приладів керування та моніторингу та інтеграція з виробниками суден. Подальша розробка і дослідження проекту є доцільними.

Висновки

В результаті проведеної роботи було:

1) Проаналізовано переваги та сильні сторони туманної обробки даних, в тому числі з точки зору кібербезпеки.

2) Розроблено політики безпеки для пристроїв різних видів. Запропоновано архітектуру взаємодій на основі туманних обчислень.

Дані пристрої, якщо їхня функціональність заснована на лінукс-платформі, а не на контролерах чи мікроконтролерах, забезпечують всі вимоги, які висуваються до них політикою безпеки всередині пристрою та політикою безпеки по взаємодії з оточуючими пристроями. Функціональність системи при цьому не погіршиться і навпаки, стане ще більш гнучкою.

3) показано ефективність Лінукс-орієнтованих рішень для платформи пристроїв, які беруть участь у віддалених морських комунікаціях. Було проведено експеримент, для якого розгорнуто всі необхідні засоби, запропоновано послідовність заходів, які необхідно виконати, щоби налаштувати на платформі Лінукс-подібної ОС всі необхідні налаштування безпеки, які можуть знадобитись для різних видів систем обміну інформацією між судами та центральною системою навігації, а також всередині кіберфізичної системи судна.

Запропоновано спосіб безпечного обміну, який забезпечує необхідну в системі віддаленої морської комунікації автентифікацію, конфіденційність, не порушуючи швидкодії.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Maritime cyber security. Why cyber security is essential for your business. URL:https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/index.html .
2. ATT&CK for Industrial Control Systems. URL: https://collaborate.mitre.org/attackics/(дата звернення: 14.12.2021)
3. ICS Pentesting Tools. URL: https://github.com/kh4sh3i/ICS-Pentesting-Tools .
4. Meera M. S., Rao S. N. Comparative Analysis of IoT protocols for a Marine IoT System," 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2018. P. 2049-2053. DOI: 10.1109/ICACCI.2018.8554906.
5. Petrenko K., Styopochkina I. Maritime security and cyber security: current challenges and threats // Maritime security of the baltic-black sea region: challenges and threats, December 23, 2021 Volume 1, P.333-337.
6. J. Olivares et al. Artificial intelligence-based cybersecurity for connected and automated vehicles. DOI: 10.1561/9781638280613.
7. Петренко К. М. Безпека систем управління інтелектуальним транспортом на базі платформи Linux : дипломний проект. Київ, 2021. URL: https://ela.kpi.ua/handle/123456789/57064 (дата звернення: 01.10.2023).
8. The Abstracted Network for Enterprises and Internet of Things URL:https://meshdynamics.com/documents/ABSTRACTED-NETWORK-FOR-IOT.pdf
9. Fog computing [Електронний ресурс] URL: https://en.wikipedia.org/wiki/Fog_computing
10. Судовые системы [Електронний ресурс] URl: https://ru.wikipedia.org/wiki/%D0%A1%D1%83%D0%B4%D0%BE%D0%B2%D1%8B%D0%B5_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B
11. Global Maritime Distress and Safety System [Електронний ресурс] URL: https://en.wikipedia.org/wiki/Global_Maritime_Distress_and_Safety_System

12. Maritime Safety and Security Information System [Електронний ресурс] URL: https://en.wikipedia.org/wiki/Maritime_Safety_and_Security_Information_System