ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «БЕЗПЕКОВІ АСПЕКТИ ВПРОВАДЖЕННЯ ТЕХГОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ В ОХОРОННІ СИСТЕМИ»

на здобуття освітнього ступеня магістра

зі спеціальності: 126 Інформаційні системи та технології
(*код, найменування спеціальності*)

освітньо-професійної програми: Інформаційні системи та технології
(*назва*)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Кирил ПАВЛЕНКО
(*підпис*) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. ІСДМ–61

Кирил ПАВЛЕНКО
Ім'я, ПРІЗВИЩЕ

Керівник: Ірина СРІБНА
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ
д.т.н, доцент

Рецензент: _____
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут інформаційних технологій

Кафедра Інформаційні системи та технології

Ступінь вищої освіти Магістр

Спеціальність 126 Інформаційні системи та технології

Освітньо-професійна програма Інформаційні системи та технології

ЗАТВЕРДЖУЮ
Завідувач кафедрою
Інформаційних систем та технологій
_____ Каміла Сторчак
"____"_____ 2024 року

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

Павленко Кирилу Юрійовичу
(*прізвище, ім'я, по батькові здобувача*)

1. Тема роботи: «Безпекові аспекти впровадження технологій Інтернету речей в охоронні системи»

Керівник кваліфікаційної роботи Срібна Ірина Миколаївна професор кафедри, доктор технічних наук, доцент.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «15» жовтня 2024 р. № 320

2. Строк подання кваліфікаційної роботи «27» грудня 2024 р.

3. Вихідні дані до кваліфікаційної роботи: Сучасні методи захисту даних: шифрування, блокчейн, туманні та периферійні обчислення;
охоронні системи на базі технологій IoT;
стандарти та рекомендації щодо кібербезпеки IoT (IEC 62443, NISTIR 8259);
науково-технічна література з питань, пов'язаних з наукою про дані.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити).

1. Стан досліджень у сфері Інтернету речей та охоронних систем.
2. Методи та засоби захисту IoT-технологій в охоронних системах.
3. Практичні аспекти впровадження систем IoT в охоронні технології.
4. Актуальні виклики та майбутні напрями досліджень у сфері IoT-безпеки.

5. Перелік ілюстративного матеріалу: *презентації*

1. IoT в охоронних системах.
2. Джерела загроз на різних рівнях IoT-систем.
3. Методи захисту IoT-систем.
4. Практичний кейс: камера Swizoo G9 Pro з додатком Tuya Smart.
5. Приклад коду шифрування за допомогою алгоритму DES.
6. Запропоновані заходи безпеки.
7. Архітектура на основі штучного інтелекту та блокчейну.
8. Висновки, апробації.

6. Дата видачі завдання: «15» жовтня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури	15.10 – 21.10.24	Виконано
2	Аналіз досліджень Інтернету речей та охоронних систем.	25.10 – 30.10.24	Виконано
3	Методи захисту IoT-технологій в охоронних системах.	1.11 – 15.11.24	Виконано
4	Практичні аспекти впровадження систем IoT в охороні системи	20.11 – 29.11.24	Виконано
5	Оформлення роботи вступ, висновки, реферат	9.12 – 14.12.24	Виконано
6	Розробка демонстраційних матеріалів	15.12 – 20.12.24	Виконано
7	Попередній захист роботи	25.12.24	Виконано

Здобувач вищої освіти _____ Кирил ПАВЛЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Ірина СРІБНА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 78 с., 3 табл., 24 рис., 30 джерел.

Мета роботи - аналіз вразливостей та розробка методів і засобів забезпечення безпеки IoT-технологій, із застосуванням сучасних інноваційних підходів, шифрування, блокчейн, туманні та периферійні обчислення.

Об'єкт дослідження - технології Інтернету речей, що використовуються в охоронних системах.

Предмет дослідження - методи забезпечення безпеки IoT-технологій на різних рівнях інфраструктури, а також їх впровадження в охоронні системи.

Короткий зміст роботи: Під час виконання роботи визначено основні загрози безпеці IoT-технологій на різних рівнях інфраструктури. Проаналізовано вразливості охоронних систем, що базуються на IoT, та розглянуто сучасні методи їх усунення. На основі отриманих результатів розроблено рекомендації впровадження ефективних засобів захисту, включаючи шифрування даних, блокчейн-технології, туманні й периферійні обчислення. Проведено аналіз методів захисту для вибору оптимальних рішень залежно від вимог користувачів. Розглянуто практичний кейс з використанням камери Swizoo G9 Pro та платформи Tuya Smart, який дозволив виявити типові вразливості охоронних IoT-систем і перевірити ефективність запропонованих методів безпеки в реальних умовах. Запропонована методика підвищення безпеки IoT охоронних систем дозволяє забезпечити захист пристроїв, підвищити стійкість до кіберзагроз і покращити загальну ефективність управління системами безпеки.

КЛЮЧОВІ СЛОВА: IoT, ОХОРОННІ СИСТЕМИ, БЕЗПЕКА IOT, КІБЕРБЕЗПЕКА, ШИФРУВАННЯ ДАНИХ, БЛОКЧЕЙН, ТУМАННІ ОБЧИСЛЕННЯ, ПЕРИФЕРІЙНІ ОБЧИСЛЕННЯ, ВРАЗЛИВОСТІ IOT, TUYA SMART, SWIZOO G9 PRO

ABSTRACT

Text part of the master's qualification work:
78 pages, 24 pictures, 3 tables , 30 sources.

The purpose of the work is to analyze vulnerabilities and develop methods and tools for ensuring the security of IoT technologies, using modern innovative approaches, encryption, blockchain, fog and edge computing.

Object of research is Internet of Things technologies used in the field of security systems.

Subject of research is methods for ensuring the security of IoT technologies at different levels of infrastructure, as well as their implementation in security systems.

Summary of the work: During the work, the main threats to the security of IoT technologies at different levels of infrastructure were identified. The vulnerabilities of security systems based on IoT were analyzed in detail, and modern methods for eliminating them were considered. Based on the results obtained, recommendations were developed for the implementation of effective security measures, including data encryption, blockchain technologies, fog and edge computing. A comparative analysis of protection methods was conducted to select optimal solutions depending on user requirements. A practical case study using the Swizoo G9 Pro camera and the Tuya Smart platform allowed us to identify typical vulnerabilities of IoT security systems and verify the effectiveness of the proposed security methods in real conditions. The proposed methodology for improving IoT security in the field of security systems allows us to provide reliable protection of devices, increase resistance to cyber threats, and improve the overall efficiency of security system management.

KEY WORDS: IoT, SECURITY SYSTEMS, IOT SECURITY, CYBERSECURITY, DATA ENCRYPTION, BLOCKCHAIN, FOG COMPUTING, MOBILE EDGE COMPUTING, IOT VULNERABILITIES, TUYA SMART, SWIZOO G9 PRO

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

COAP	Constrained Application Protocol - протокол обмеженого застосування
SOAP	Simple Object Access Protocol - простий протокол доступу до об'єктів
SQL	Structured Query Language - мова структурованих запитів
DDOS	Distributed denial of service - розподілена відмова в обслуговуванні
GPS	Global Positioning System - глобальна система позиціонування
IoT	Internet of Things - Інтернет речей
M2M	Machine to Machine - машина до машини
MCC	Mobile Cloud Computing - мобільні хмарні обчислення
MEC	Mobile Edge Computing - мобільні периферійні обчислення
MQTT	Message Queuing Telemetry Transport - телеметричний транспорт черги повідомлень
NFC	Near Field Communication - комунікація ближнього поля
NFV	Network Function Virtualization - віртуалізація мережевих функцій
P2P	peer to peer
QoS	Quality of Service - якість обслуговування
RFID	Radio Frequency Identification - радіочастотна ідентифікація
SDN	Software-Defined Networking - програмно-визначена мережа
SHA	Secure Hash Algorithm - алгоритм безпечного хешування
SMQTT	Secure Message Queue Telemetry Transport - захищений телеметричний транспорт черги повідомлень
STD	Security Trust and Decentralization - довіра безпеки та децентралізація
WSN	Wireless Sensor Networks - бездротові сенсорні мережі
XMPP	Extensible Messaging and Presence Protocol - розширюваний протокол обміну повідомленнями та присутності
XSS	cross-site scripting - міжсайтовий скриптинг

ВСТУП

Сучасний розвиток Інтернету речей відкриває нові можливості для інтеграції розумних технологій у різні аспекти життя. Особливе значення IoT набуває у сфері охоронних систем, де надійність і захищеність є критичними для забезпечення безпеки користувачів, об'єктів та інформаційних систем. Збільшення кількості підключених пристроїв, таких як сенсори, камери відеоспостереження, та шлюзи, значно підвищує ризики, пов’язані із зовнішніми та внутрішніми кіберзагрозами. Ці ризики є особливо актуальними для України, де розбудова критичної інфраструктури на основі IoT потребує високого рівня захисту через підвищену загрозу кібератак.

Розробка та впровадження новітніх методів безпеки для IoT-технологій є необхідними для забезпечення довіри до розумних пристроїв та систем, що їх використовують. Проведення цієї роботи спрямоване на вирішення актуальних завдань захисту IoT у сфері охоронних систем, враховуючи сучасний рівень технологій та потреби вітчизняного ринку.

Метою дослідження аналіз вразливостей та використання інноваційних підходів, таких як блокчейн, шифрування даних, туманні й периферійні обчислення.

Для досягнення цієї мети поставлені наступні завдання:

- ✓ Провести аналіз вразливостей на різних рівнях IoT-інфраструктури.
- ✓ Вивчити сучасні методи захисту IoT, включаючи шифрування, блокчейн та інші технології.
- ✓ Розробити рекомендації щодо інтеграції IoT у сферу охоронних систем із підвищенням їх безпеки.
- ✓ Провести практичний аналіз функціонування камери Swizoo G9 Pro та оцінити ефективність існуючих засобів захисту.

Об'єктом дослідження є технології Інтернету речей, що використовуються в охоронних системах.

Предметом дослідження є методи забезпечення безпеки IoT-технологій на різних рівнях інфраструктури та в рамках їх практичного застосування.

У роботі використано комплексний підхід, який включає:

- аналіз літературних джерел з проблем безпеки IoT;
- порівняльний аналіз алгоритмів шифрування та методів захисту;
- моделювання і тестування вразливостей IoT-пристроїв на прикладі Swizoo G9 Pro;
- експериментальну оцінку ефективності інтегрованих методів захисту.

Наукова новизна роботи полягає у застосуванні блокчейн-технологій, туманних і периферійних обчислень для забезпечення багаторівневої безпеки IoT у сфері охоронних систем. Запропоновані підходи дозволяють покращити захист на сенсорному, мережевому та прикладному рівнях. Практична значущість полягає в можливості використання розроблених рекомендацій для захисту IoT-пристроїв у реальних умовах, що особливо важливо для підвищення безпеки на підприємствах і критичних об’єктах України.

Апробація результатів та публікації: Павленко К.Ю. «Безпекові аспекти застосування технологій інтернету речей в охоронних системах для інтелектуальних житлових та міських рішень». Тези доповіді на II Всеукраїнську науково-технічну конференцію «Технологічні горизонти: дослідження та застосування інформаційних технологій для технологічного прогресу України і світу». – Київ, 18 листопада 2024 р.

Павленко К.Ю. «Моделювання загроз безпеці в IoT-системах охорони: підходи до мінімізації ризиків». Тези доповіді на VII Всеукраїнська науково-технічна конференція «Комп'ютерні технології: інновації, проблеми, рішення». – Житомир, 2 грудня 2024 р.

Теоретична значущість полягає в тому що результати вносять значний внесок у розвиток теоретичних основ безпеки Інтернету речей, зокрема в сфері охоронних систем. У роботі систематизовано знання про загрози безпеці IoT на різних рівнях архітектури, включаючи сенсорний, мережевий, проміжний та прикладний рівні. Запропоновані рішення, зокрема використання туманних і периферійних

обчислень, адаптація блокчейн-технологій і сучасних алгоритмів шифрування, сприяють формуванню комплексного підходу до захисту IoT-систем. Це створює основу для подальших наукових досліджень у галузі кібербезпеки, пов’язаної з IoT.

Методична значущість роботи включає розробку алгоритмів і методів аналізу вразливостей IoT-пристроїв, побудови захищених каналів зв'язку та інтеграції багатоетапних рішень безпеки. Зокрема, у роботі:

- ✓ описано процес вибору оптимального алгоритму шифрування залежно від обмежень IoT-пристроїв (ресурси, швидкість роботи, енергоспоживання);
- ✓ розроблено методику інтеграції блокчейну для управління доступом до даних і забезпечення цілісності інформації;
- ✓ запропоновано підходи до тестування IoT-пристроїв на наявність кіберзагроз у реальних умовах експлуатації.

Ці методики можуть бути використані для підготовки спеціалістів у галузі IoT-безпеки та кіберзахисту, а також при розробці технічних регламентів для охоронних систем.

Практична значущість отриманих результатів полягає в можливості їх впровадження для підвищення рівня захисту IoT-систем у сфері охорони. Зокрема:

- Проведений аналіз кейсу камери Swizoo G9 Pro на базі Tuya Smart дозволяє виробникам IoT-пристроїв та розробникам програмного забезпечення враховувати типові вразливості та ефективно усувати їх.

- Запропоновані підходи до впровадження блокчейну, туманних і периферійних обчислень у реальних охоронних системах допоможуть підвищити стійкість систем до атак, знизити затримки при обробці даних та мінімізувати ризик втручання.

Результати дослідження можуть бути адаптовані для використання в критичних об’єктах інфраструктури України, таких як енергетика, транспорт, медицина, що особливо важливо в умовах зростання кіберзагроз.

1 СТАН ДОСЛІДЖЕНЬ У СФЕРІ ІНТЕРНЕТУ РЕЧЕЙ ТА ОХОРОННИХ СИСТЕМ

Пристрої Інтернету речей, також відомі як «розумні об’єкти», можуть варіюватися від простих пристроїв «розумного будинку», таких як розумні двері чи вікна, до переносних пристроїв, таких як розумні годинники та браслети із підтримкою RFID, до складного промислового обладнання та транспортних систем. Також можливо розробити «розумні міста», засновані на технологіях IoT.

IoT дозволяє цим «розумним пристроям» спілкуватися один з одним та з іншими пристроями з підтримкою Інтернету. Як смартфони та шлюзи, створюючи величезну мережу взаємопов’язаних пристроїв, які можуть обмінюватися даними та виконувати різні завдання автономно. Це може включати:

- моніторинг екологічної обстановки в господарствах
- керування транспортними потоками за допомогою розумних автомобілів та інших розумних автомобільних пристроїв
- керування машинами та процесами на заводах
- керування систем охорони
- відстеження товарних запасів і відправок на складах

Потенційні сфери застосування IoT величезні та різноманітні, і його вплив уже відчувається в багатьох галузях промисловості, включаючи виробництво, транспорт, охорону здоров’я та сільське господарство. Оскільки кількість пристроїв, підключених до Інтернету, продовжує зростати, IoT, ймовірно, відіграватиме дедалі важливішу роль у формуванні нашого світу. Зміна того, як ми живемо, працюємо та взаємодіємо одне з одним.

У корпоративному контексті пристрої IoT використовуються для моніторингу широкого діапазону параметрів, таких як температура, вологість, якість повітря, споживання енергії та продуктивність машини. Ці дані можна аналізувати в реальному часі, щоб виявити закономірності, тенденції та аномалії, які можуть допомогти компаніям оптимізувати свою діяльність і підвищити прибутковість.

Використовуючи пристрої IoT для автоматизації та оптимізації процесів, підприємства можуть підвищити ефективність. Наприклад, датчики IoT можна використовувати для моніторингу продуктивності обладнання та виявлення або навіть вирішення потенційних проблем зменшуючи витрати на обслуговування та покращуючи час ефективність роботи.

На рисунку 1.1 показано минулу, теперішню та майбутню архітектуру IoT. У майбутньому очікується, що пристрої не лише підключатимуться до Інтернету та інших локальних пристроїв, але й безпосередньо з іншими пристроями в Інтернеті.

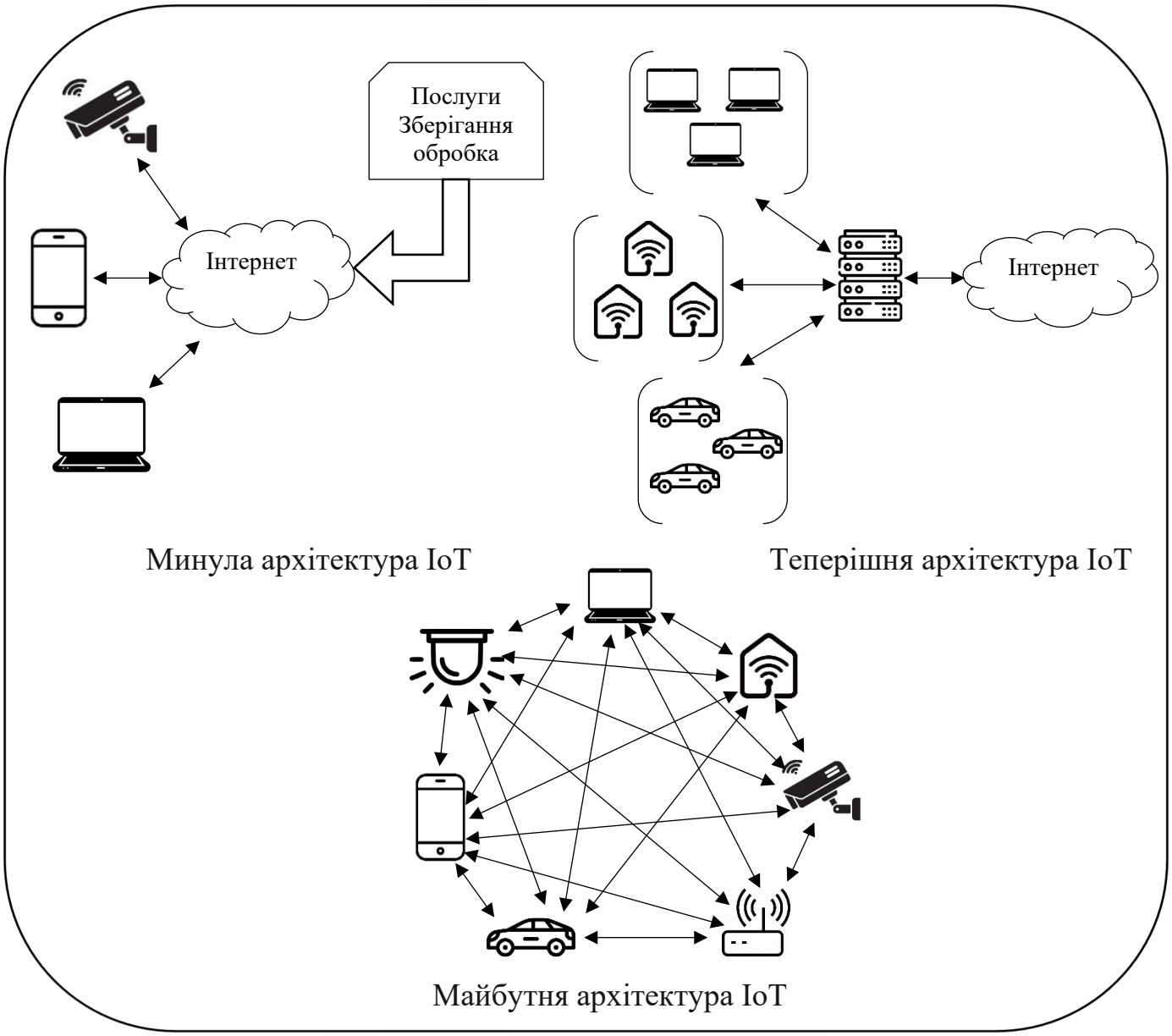


Рис. 1.1 Архітектури IoT

Майбутнє IoT багатообіцяюче, на горизонті багато захоплюючих подій для бізнесу. Ось деякі тенденції та прогнози щодо майбутнього IoT:

- **Зростання:** очікується, що кількість пристроїв IoT продовжуватиме швидко зростати, за оцінками, протягом наступних кількох років використовуватимуться десятки мільярдів пристроїв IoT. Це зростання відбуватиметься завдяки впровадження в галузях, а також розробці нових варіантів використання та програм.
- **Периферійні обчислення:** стають все більш важливими для IoT, оскільки дозволяють обробляти та аналізувати дані ближче до джерела даних, а не в централізованому центрі обробки даних. Це може покращити час відгуку, зменшити затримку та зменшити обсяг даних, які необхідно передати через мережі IoT.
- **Штучний інтелект і машинне навчання:** стають все більш важливими для IoT, оскільки вони можуть використовуватися для аналізу величезних обсягів даних, які генеруються пристроями IoT, і отримання значущої інформації. Це може допомогти підприємствам приймати більш обґрунтовані рішення та оптимізувати свою діяльність.
- **Blockchain:** технологія досліджується як спосіб покращення безпеки та конфіденційності в IoT. Цю технологію можна використовувати для створення захищених децентралізованих мереж для пристроїв Інтернету речей, що мінімізує вразливі місця в безпеці даних.
- **Стійкість:** стає дедалі важливішим фактором для IoT, оскільки підприємства шукають способи зменшити свій вплив на навколишнє середовище. IoT можна використовувати для оптимізації споживання енергії, зменшення відходів і підвищення стійкості в різних галузях.

1.1 Безпека, критичні сфери застосування IoT

Безпека є надзвичайно важливою для всіх систем IoT, які вже розроблені або знаходяться в процесі розробки. Системи IoT дуже швидко зростають і проникають

у більшість існуючих галузей. Хоча оператори підтримують ці додатки IoT за допомогою існуючих мережевих технологій, деякі з цих додатків потребують суворішої підтримки безпеки з боку технологій, які вони використовують.

Розумні міста: передбачають широке використання нових обчислювальних і комунікаційних ресурсів для підвищення загальної якості життя людей [1]. Це включає розумні будинки, розумне управління трафіком, розумне управління надзвичайними ситуаціями, розумні комунальні послуги тощо [2]. Хоча використання інтелектуальних програм має на меті покращити загальну якість життя громадян, воно створює загрозу конфіденційності громадян. Послуги смарт-карт, як правило, піддають ризику дані картки та купівельну поведінку громадян. Багато мобільних програм можуть без дозволу поширювати інформацію про місцезнаходження користувачів. Є програми, за допомогою яких батьки можуть стежити за своєю дитиною. Однак якщо такі програми будуть зламані, то безпека дитини може опинитися під загрозою.

Розумне середовище: включає різні додатки IoT, такі як виявлення пожеж у лісах, моніторинг рівня снігу у високогірних регіонах, запобігання зсувам, раннє виявлення землетрусів, моніторинг забруднення повітря тощо. Усі ці додатки IoT тісно пов’язані з життям людей і тварин у цих районах. Державні установи, які займаються такими сферами, також покладатимуться на інформацію з цих програм IoT.

Порушення безпеки та вразливість у будь-якій сфері, пов’язаній із такими програмами, можуть мати серйозні наслідки. У цьому контексті як помилково негативні, так і помилково позитивні результати можуть призвести до катастрофічних результатів для таких програм IoT. Наприклад, якщо програма починає помилково визначати землетруси, то це призведе до грошових втрат для уряду та бізнесу. З іншого боку, якщо програма не зможе передбачити землетрус, то це призведе до втрати як майна, так і життя. Тому додатки для інтелектуального середовища мають бути високоточними, і слід уникати порушень безпеки та фальсифікації даних.

Інтелектуальне вимірювання та розумні електромережі: розумне вимірювання включає програми, які пов’язані з різними вимірюваннями, моніторингом та керуванням. Найпоширенішим застосуванням інтелектуального обліку є інтелектуальні мережі, де споживання електроенергії вимірюється та контролюється. Інтелектуальний облік також може бути використаний для вирішення проблеми крадіжки електроенергії [3]. Інші застосування інтелектуального вимірювання включають моніторинг рівня води, нафти та газу в резервуарах для зберігання та цистернах. Інтелектуальні лічильники також використовуються для моніторингу та оптимізації продуктивності сонячних електростанцій шляхом динамічної зміни кута сонячних панелей для збору максимально можливої сонячної енергії. Існують також деякі додатки IoT, які використовують розумні лічильники для вимірювання тиску води в системах водного транспорту або для вимірювання ваги товарів.

Однак інтелектуальні системи вимірювання вразливі як до фізичних, так і до кібератак порівняно з аналоговими лічильниками, які можна підробити лише фізичними атаками. Крім того, інтелектуальні лічильники або вдосконалена інфраструктура вимірювання призначені для виконання функцій, окрім загального запису споживання енергії. У мережі інтелектуального будинку все електричне обладнання вдома підключено до інтелектуальних лічильників, і інформація, зібрана з цього обладнання, може використовуватися для керування навантаженням і витратами. Навмисне вторгнення в такі системи зв’язку споживачем або зловмисником може змінити зібрану інформацію, що призведе до грошових втрат для постачальників послуг або споживачів [4].

Безпека та надзвичайні ситуації: є ще однією важливою сферою, де розгортаються різноманітні системи IoT. Це включає в себе такі програми, як дозвіл лише авторизованим особам у зонах обмеженого доступу тощо. Іншим застосуванням у цій області є виявлення витоку небезпечних газів у промислових зонах або зонах навколо хімічних заводів.

Рівень радіації також можна виміряти в районах навколо ядерних реакторів або базових станцій стільникового зв’язку, а також створити сповіщення, коли рівень радіації високий. Існують різні будівлі, системи яких містять конфіденційні

дані або містять конфіденційні товари. Для захисту конфіденційних даних і товарів можна розгорнути програми безпеки. системи IoT, які виявляють різні рідини, також можна використовувати для запобігання корозії та поломок у таких чутливих будівлях. Порушення безпеки в таких програмах також можуть мати різні серйозні наслідки. Наприклад, злочинці можуть спробувати проникнути в зони обмеженого доступу, атакуючи вразливі місця в таких програмах. Крім того, помилкові сигнали про рівень радіації можуть мати серйозні негайні та довгострокові наслідки. Наприклад, якщо немовлята піддаються впливу високого рівня радіації, це може призвести до серйозних захворювань, що загрожують життю в довгостроковій перспективі.

Розумна роздрібна торгівля: системи IoT широко використовуються в секторі роздрібної торгівлі. Були розроблені різноманітні додатки для моніторингу умов зберігання товарів під час їх переміщення по ланцюжку поставок. IoT також використовується для контролю відстеження продуктів на складах, щоб можна було оптимально поповнювати запаси. Також розробляються різноманітні програми для інтелектуальних покупок, які допомагають клієнтам залежно від їхніх уподобань, звичок, алергії на певні компоненти тощо. Також були розроблені механізми надання досвіду онлайн-покупок офлайн-магазинам за допомогою методів доповненої реальності. Різні компанії в роздрібній торгівлі стикалися з проблемами безпеки під час розгортання та використання різноманітних додатків IoT. Деякі з цих компаній включають Apple, Home Depot, JP Morgan Chase і Sony [5].

Зловмисники можуть спробувати скомпрометувати додатки IoT, пов’язані з умовами зберігання товарів, і можуть спробувати надіслати неправильну інформацію про продукти користувачам, щоб збільшити продажі. Якщо функції безпеки не реалізовано в розумній роздрібній торгівлі, зловмисники можуть викрасти інформацію про дебетові та кредитні картки, номери телефонів, адреси електронної пошти тощо клієнтів, що може призвести до грошових втрат для клієнтів і роздрібних продавців.

Розумне сільське господарство та тваринництво: включає моніторинг вологості ґрунту, контроль мікроклімату, вибіркове зрошення в сухих зонах, а також

контроль вологості та температури. Використання таких передових функцій у сільському господарстві може допомогти досягти високої врожайності та позбавити фермерів від грошових втрат. Контроль рівня температури та вологості в різних зернових і овочевих виробництвах може допомогти запобігти грибку та іншим мікробним забрудненням. Контроль кліматичних умов також може допомогти підвищити врожайність і якість овочів і сільськогосподарських культур.

Подібно до моніторингу врожаю, існують додатки IoT для моніторингу активності та стану здоров'я сільськогосподарських тварин шляхом прикріплення датчиків до тварин. Якщо такі додатки скомпрометовані, це може призвести до крадіжки тварин із ферми, а зловмисники також можуть завдати шкоди посівам.

Домашня автоматизація: є однією з найбільш широко використовуваних і розгорнутих програм IoT. Це включає такі програми, як програми для дистанційного керування електроприладами для економії енергії, системи, встановлені на вікнах і дверях для виявлення зловмисників, тощо. Системи моніторингу застосовуються для відстеження споживання енергії та води, і користувачам рекомендується економити кошти та ресурси.

Вторгнення виявляються шляхом порівняння дій користувача в ключових місцях будинку зі звичайною поведінкою користувача в цих місцях. Однак зловмисники можуть отримати несанкціонований доступ до пристроїв IoT у домі та спробувати завдати шкоди користувачам. Наприклад, кількість випадків квартирних крадіжок стрімко зросла після впровадження різноманітних систем домашньої автоматизації [6]. У минулому також були різні випадки, коли зловмисники намагалися проаналізувати тип і обсяг Інтернет-трафіку до або з розумного дому, щоб оцінити поведінку та присутність мешканців.

IoT пропонує має багато переваг, але також створює кілька ризиків і проблем. Ось деякі найбільш значущі з них:

1 **Ризики для безпеки та конфіденційності:** оскільки пристрої IoT стають все більш поширеними, безпека та конфіденційність стають дедалі важливішими. Багато пристроїв IoT вразливі до хакерських атак та інших кіберзагроз, які мо-

жуть поставити під загрозу безпеку та конфіденційність даних. Пристрої IoT також можуть збирати величезні обсяги персональних даних, що викликає занепокоєння щодо конфіденційності та захисту даних.

2 **Проблеми сумісності:** пристрої IoT від різних виробників часто використовують різні стандарти та протоколи, що ускладнює для них виконання зв'язку «машина-машина». Це може призвести до проблем сумісності та створити накопичені дані, які важко інтегрувати та аналізувати.

3 **Перевантаження даних:** пристрої IoT генерують величезні обсяги даних, які можуть перевантажити підприємства, які не готові їх обробляти. Аналіз цих даних і отримання значущої інформації може бути серйозною проблемою, особливо для компаній, які не мають необхідних інструментів аналітики та досвіду.

4 **Вартість і складність:** впровадження системи IoT може бути дорогим і складним, вимагаючи значних інвестицій в апаратне забезпечення, програмне забезпечення та інфраструктуру. Управління та підтримка системи Інтернету речей також може бути складною справою, що вимагає спеціальних навичок і досвіду.

1.1.1 Джерела загрози безпеці в програмах IoT

Будь-яку програму IoT можна розділити на чотири рівні:

- рівень сприйняття;
- мережевий рівень;
- рівень проміжного ПЗ;
- прикладний рівень.

Кожен із цих рівнів у програмі IoT використовує різноманітні технології, які створюють низку проблем і загроз безпеці. На рисунку 1.2 показано різні технології, пристрої та програми на цих чотирьох рівнях. Далі будуть розглянуті різні можливі загрози безпеці в системах IoT для цих чотирьох рівнів.

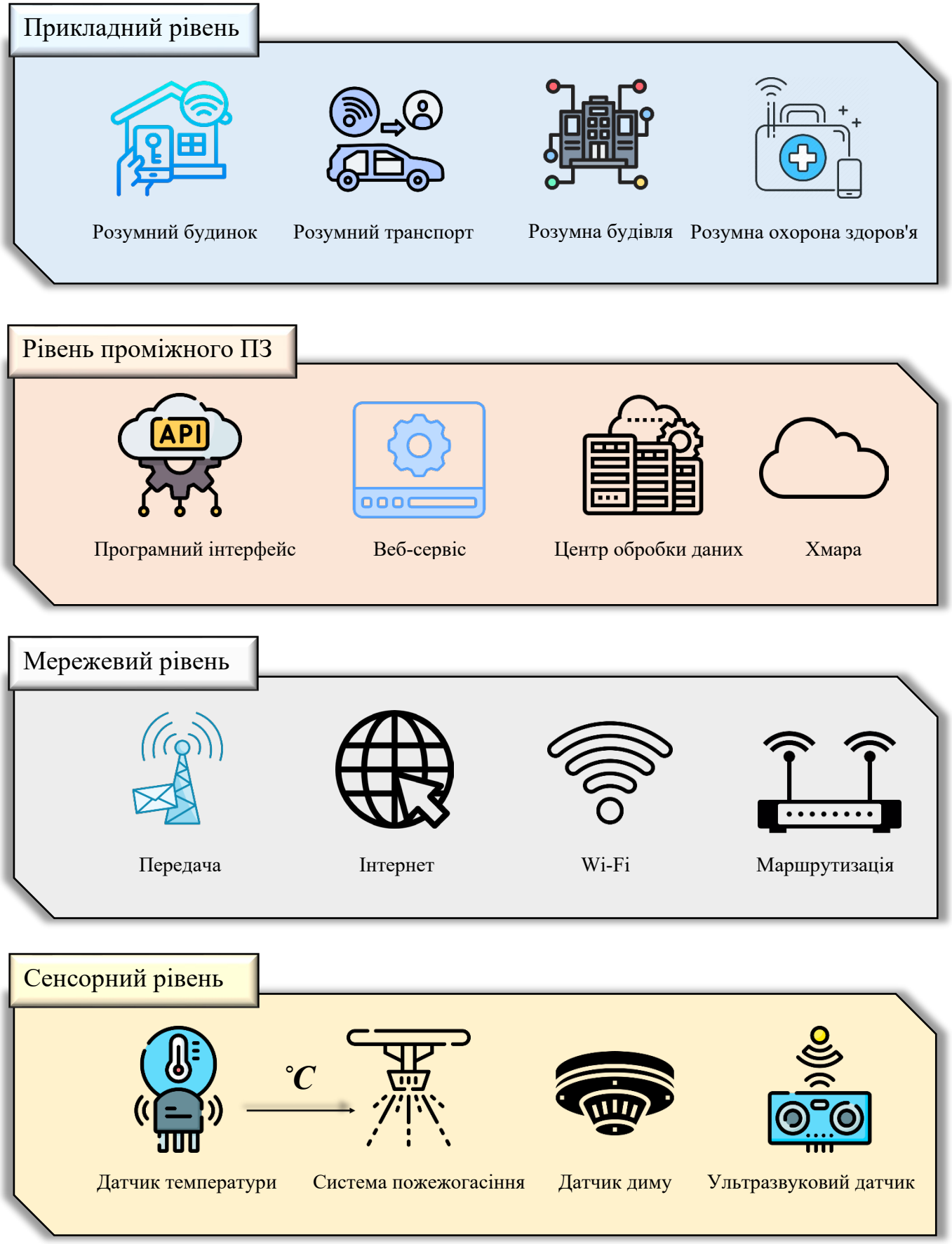


Рис. 1.2 Рівні в системі IoT

1.1.2 Проблеми безпеки на сенсорному рівні

Сенсорний рівень в основному працює з фізичними датчиками та приводами IoT. Датчики використовуються для запису та моніторингу процесів, а також обладнання шляхом вилучення даних та інформації. Приводи, з іншого боку, використовуються для автоматизації завдань на робочому місці, заощаджуючи людську працю.

Ці два компоненти працюють разом для розробки ефективних рішень IoT. Існують різні види датчиків для сприйняття різних типів даних, наприклад, ультразвукові датчики, датчики камери, датчики виявлення диму, датчики температури та вологості тощо. Існують механічні, електричні, електронні або хімічні датчики, які використовуються для визначення фізичного середовища.

Різні технології сенсорного рівня використовуються в різних додатках IoT, таких як RFID, GPS, WSN, RSN тощо [7].

Основні загрози безпеці, які можуть трапитися на рівні сприйняття такі:

1. **Захоплення вузлів:** системи IoT складаються з кількох вузлів малої потужності, таких як датчики та виконавчі механізми. Ці вузли вразливі до різноманітних атак. Наприклад можна спробувати захопити або замінити вузол у системі IoT шкідливим вузлом. Новий вузол може здаватися частиною системи, але не контролюватися власником. Це може призвести до порушення безпеки всієї системи IoT [8].
2. **Атака з впровадженням шкідливого коду:** під час атаки впроваджується шкідливий код у пам’ять вузла. Коли мікропрограмне забезпечення або програмне забезпечення вузлів IoT оновлюються це дає можливість для впровадження шкідливого коду. Використовуючи такий шкідливий код можна змусити вузли виконувати деякі небажані функції або навіть спробувати отримати доступ до всієї системи IoT.
3. **Атака з введенням помилкових даних:** коли вузол захоплено його можливо використати його для введення помилкових даних у систему IoT. Це може призвести до хибних результатів і призвести до неправильної роботи

програми IoT. Також можна використовувати цей метод, щоб викликати DDoS-атаку.

4. **Атаки через побічні канали (SCA):** окрім прямих атак на вузли, різноманітні атаки на побічні канали можуть призвести до витоку конфіденційних даних. Архітектура процесорів, електромагнітне випромінювання та споживана ними потужність розкривають конфіденційну інформацію. Атаки на побічних каналах можуть ґрунтуватися на споживанні електроенергії, лазерних атаках, атаках за часом або електромагнітних атаках. Сучасні мікросхеми забезпечують різноманітні заходи для запобігання цим атакам під час впровадження криптографічних модулів.
5. **Прослуховування та втручання:** системи IoT часто складаються з різних вузлів, розгорнутих у відкритих середовищах. Як наслідок, такі системи піддаються перехопленню. Зловмисники можуть підслуховувати та захоплювати дані на різних етапах, таких як передача даних або автентифікація [9].
6. **Атаки із затримкою сну:** під час таких атак зловмисники намагаються розрядити батарею малопотужних периферійних пристроїв IoT. Це призводить до відмови в обслуговуванні вузлів у системі IoT через розряджену батарею. Це можна зробити, запускаючи нескінченні цикли на периферійних пристроях за допомогою шкідливого коду або штучно збільшуючи енергоспоживання периферійних пристроїв.
7. **Атаки під час завантаження:** периферійні пристрої вразливі до різних атак під час процесу завантаження. Це пов’язано з тим, що на цьому етапі незадіяні вбудовані процеси безпеки. Зловмисники можуть скористатися цією вразливістю та спробувати атакувати пристрої вузла під час їх перезапуску. Оскільки периферійні пристрої, як правило, мають низьке енергоспоживання та іноді проходять цикли сну та пробудження, тому важливо забезпечити захист процесу завантаження на цих пристроях.

1.1.3 Проблеми безпеки на мережевому рівні

Ключовою функцією мережевого рівня є передача інформації, отриманої від сенсорного рівня, до обчислювального блоку для обробки. Нижче наведено основні проблеми безпеки, які виникають на мережевому рівні.

1. **Фішингові атаки на сайт:** фішингові атаки часто стосуються атак, під час яких кілька пристроїв Інтернету речей можуть стати мішенню за допомогою мінімальних зусиль зловмисника. Зловмисники очікують, що хоча б кілька пристроїв стануть жертвами атаки. Існує ймовірність натрапити на фішингові сайти під час відвідування користувачами веб-сторінок в Інтернеті. Після того, як обліковий запис і пароль користувача може бути зламано, усе середовище IoT, яке використовується, стає вразливим до кібератак. Мережевий рівень в IoT дуже вразливий до фішингових атак [10].
2. **Атака на доступ:** Атака на доступ також називається розширеною постійною загрозою. Це тип атаки, під час якої неавторизована особа або зловмисник отримує доступ до мережі IoT. Зловмисник може продовжувати залишатися в мережі непоміченим протягом тривалого часу. Метою або наміром такого роду атак є крадіжка цінних даних або інформації, а не завдання шкоди мережі. Системи IoT безперервно отримують і передають цінні дані, тому дуже вразливі до таких атак [11].
3. **DDoS/DoS-атака:** у цьому типі атак зловмисник заповнює цільові сервери великою кількістю небажаних запитів. Це виводить з ладу цільовий сервер, тим самим порушуючи роботу інших користувачів. Якщо зловмисник використовує кілька джерел для затоплення цільового сервера, то така атака називається DDoS або розподіленою атакою на відмову в обслуговуванні. Такі атаки не характерні для систем IoT, але через неоднорідність і складність мереж IoT мережевий рівень IoT схильний до таких атак. Багато пристроїв IoT у системах не налаштовані чітко, і тому вони стають легкими шлюзами для зловмисників для запуску DDoS-атак на цільові сервери [12].

4. **Атаки на передачу даних:** системи IoT мають справу з великим обсягом зберігання й обміну даними. Дані є цінними, тому вони завжди є мішенню хакерів та інших зловмисників. Дані, які зберігаються на локальних серверах або в хмарі, несуть загрозу безпеці, але дані які передаються або передаються з одного місця в інше, ще більш вразливі до кібератак. У системах IoT існує багато передач даних між датчиками, виконавчими механізмами, хмарою тощо. Для таких переміщень даних використовуються різні технології підключення, тому системи IoT сприйнятливі до порушень даних.
5. **Атаки маршрутизації:** під час таких атак шкідливі вузли в систему IoT можуть намагатися перенаправити шляхи маршрутизації під час передачі даних. Sinkhole атаки – це особливий вид атаки маршрутизації, під час якої зловмисник рекомендує системі штучний найкоротший шлях маршрутизації та залучає вузли для маршрутизації трафіку через нього. Worm-hole атаки — це ще одна атака, яка може стати серйозною загрозою безпеці, якщо її поєднати з іншими, такими як Sinkhole. Warm-hole — це поза смугове з'єднання між двома вузлами для швидкої передачі пакетів. Зловмисник може створити «теплу діру» між скомпрометованим вузлом і пристроєм в Інтернеті та спробувати обійти основні протоколи безпеки в системі IoT.

1.1.4 Проблеми безпеки на рівні проміжного програмного забезпечення

Роль проміжного програмного забезпечення в IoT полягає у створенні рівня абстракції між мережевим рівнем і рівнем додатків. Проміжне програмне забезпечення також може забезпечити потужні обчислювальні можливості та зберігання [13]. Рівень проміжного програмного забезпечення включає брокерів, постійні сховища даних, системи масового обслуговування, машинне навчання тощо. Хоча рівень проміжного програмного забезпечення корисний для забезпечення надійної системи IoT, він також сприйнятливий до різноманітних атак. Ці атаки можуть отримати контроль над усією системою шляхом зараження проміжного ПЗ. Безпека

бази даних і хмарна безпека є іншими основними проблемами безпеки на цьому рівні. Різні можливі атаки на рівні проміжного ПЗ наведені нижче:

1. **Атака Man-in-the-Middle:** протокол MQTT використовує модель публікації-підписки між клієнтами та передплатниками за допомогою брокера MQTT, який фактично діє як проксі. Це допомагає відокремити публікацію та підписаних клієнтів один від одного, і повідомлення можна надсилати без знання адресата. Якщо зловмисник може контролювати брокера і стати людиною посередині, то він/вона може отримати повний контроль над усією комунікацією без будь-якого відома клієнтів.
2. **Атака впровадження SQL:** програмне забезпечення також чутливе до атак впровадження SQL. У таких атаках зловмисник може вбудувати зловмисні оператори SQL у програму. Потім отримати особисті дані будь-якого користувача і навіть змінити записи в базі даних [14].
3. **Атака з обгортанням підпису:** у веб-службах, що використовуються в проміжному програмному забезпеченні, використовуються підписи XML [15]. Під час атаки з упаковкою підпису зловмисник порушує алгоритм підпису та може виконувати операції або змінювати підслухане повідомлення, використовуючи вразливі місця в SOAP [16].
4. **Атака за допомогою зловмисного програмного забезпечення в хмарі:** під час такої атаки зловмисник може отримати контроль, впровадити шкідливий код або віртуальну машину в хмару. Зловмисник видає себе за дійсну службу, намагаючись створити екземпляр віртуальної машини або шкідливий модуль служби. Таким чином зловмисник може отримати доступ до сервісних запитів служби та захопити конфіденційні дані, які можна змінювати залежно від конкретного випадку.
5. **Атака затоплення в хмарі:** ця атака працює майже так само, як атака DoS у хмарі, і впливає на якість обслуговування. Для виснаження хмарних ресурсів зловмисники постійно надсилають численні запити до служби. Ці атаки можуть мати великий вплив на хмарні системи, збільшуючи навантаження на хмарні сервери.

1.1.5 Проблеми безпеки на шлюзах

Шлюз — це широкий рівень, який відіграє важливу роль у з'єднанні кількох пристроїв, людей, речей і хмарних служб. Шлюзи також допомагають надавати апаратні та програмні рішення для пристроїв IoT. Шлюзи використовуються для дешифрування та шифрування даних IoT і перекладу протоколів для зв'язку між різними рівнями [17]. Сучасні системи IoT неоднорідні, включаючи стеки LoraWan, ZigBee, Z-Wave та TCP/IP із багатьма шлюзами між ними. Деякі проблеми безпеки для шлюзу IoT наведені нижче:

1. **Безпечне підключення:** коли в систему IoT встановлюється новий пристрій або датчик, необхідно захистити ключі шифрування. Шлюзи діють як посередники між новими пристроями та службами керування, і всі ключі проходять через шлюзи. Шлюзи чутливі до атак типу "людина посередині" та підслуховування з метою захоплення ключів шифрування, особливо під час процесу підключення.
2. **Додаткові інтерфейси:** мінімізація місць для потенційних атак є важливою стратегією, про яку слід пам'ятати під час встановлення пристроїв IoT [18]. Лише необхідні інтерфейси та протоколи повинні бути реалізовані виробником шлюзу IoT. Деякі служби та функції мають бути обмежені для кінцевих користувачів, щоб уникнути обхідної автентифікації або витоку інформації.
3. **Наскрізне шифрування:** для забезпечення конфіденційності даних потрібна справжня наскрізна безпека прикладного рівня [19]. Програма не повинна дозволяти нікому, крім унікального одержувача, розшифровувати зашифровані повідомлення. Хоча протоколи Zigbee і Zwave підтримують шифрування, це не наскрізне шифрування, оскільки для того, щоб перевести інформацію з одного протоколу в інший, шлюзи повинні розшифрувати та повторно зашифрувати повідомлення. Це розшифрування на рівні шлюзу робить дані вразливими до порушень даних.
4. **Оновлення мікропрограми:** більшість пристроїв IoT обмежені в ресурсах, тому вони не мають інтерфейсу користувача чи обчислювальної потужності

для завантаження та встановлення оновлень мікропрограми. Зазвичай шлюзи використовуються для завантаження та застосування оновлень мікропрограми. Слід записати поточну та нову версії мікропрограми, а також перевірити дійсність підписів для безпечного оновлення мікропрограми.

1.1.6 Проблеми безпеки на прикладному рівні

Прикладний рівень безпосередньо працює з кінцевими користувачами та надає їм послуги. Системи IoT, такі як розумні будинки, розумні лічильники, розумні міста, розумні мережі тощо, знаходяться на цьому рівні. Цей рівень має певні проблеми безпеки, яких немає на інших рівнях, наприклад проблеми з крадіжкою даних і конфіденційністю. Проблеми безпеки на цьому рівні також є специфічними для різних програм. Багато додатків IoT також складаються з підрівня між мережевим рівнем і рівнем додатків, який зазвичай називають рівнем підтримки додатків або рівнем проміжного програмного забезпечення. Рівень підтримки підтримує різні бізнес-послуги та допомагає в розумному розподілі ресурсів і обчисленнях. Основні проблеми безпеки, з якими стикається прикладний рівень, наведені нижче:

1. **Викрадення даних:** системи IoT мають справу з великою кількістю критичних і приватних даних. Дані, що передаються, ще більш вразливі до атак, ніж дані, що перебувають у стані спокою, а в програмах Інтернету речей передаються багато даних. Користувачі не бажають реєструвати свої особисті дані в системах IoT, якщо ті вразливі до атак викрадення даних. Шифрування даних, ізоляція даних, автентифікація користувача та мережі, керування конфіденційністю тощо – це деякі методи та протоколи, які використовуються для захисту програм IoT від викрадення даних.
2. **Атаки на контроль доступу:** контроль доступу – це механізм авторизації, який дозволяє користувачам або процесам отримувати доступ до даних або облікового запису. Атака контролю доступу є критичною атакою в системах IoT, тому що як тільки доступ скомпрометовано, то вся система IoT стає вразливою до атак.

3. **Атаки на переривання служби:** ці атаки також називаються незаконними атаками на переривання або DDoS-атаками. Були різні випадки таких атак на додатки IoT. Такі атаки позбавляють законних користувачів можливості користуватися послугами додатків IoT, штучно роблячи сервери або мережу занадто зайнятими, щоб відповідати.
4. **Атаки з впровадженням зловмисного коду:** зазвичай зловмисники вибирають найпростіший або найпростіший метод, який вони можуть використати для проникнення в систему чи мережу. Якщо система вразлива до шкідливих фрагментів коду через недостатню перевірку, то це буде перша точка входу, яку вибере зловмисник. Як правило, зловмисники використовують XSS, щоб ввести шкідливий фрагмент коду на надійний веб-сайт. Успішна атака XSS може призвести до викрадення облікового запису IoT і може паралізувати систему IoT.
5. **Перехоплюючі атаки:** зловмисники можуть використовувати програми перехоплення для моніторингу мережевого трафіку в системах IoT. Це може дозволити зловмиснику отримати доступ до конфіденційних даних користувача, якщо реалізовано недостатньо протоколів безпеки, щоб запобігти цьому [20].
6. **Атаки на перепрограмування:** якщо процес програмування не захищено, зловмисники можуть спробувати перепрограмувати об’єкти IoT віддалено. Це може призвести до викрадення мережі IoT [21].

1.2 Охоронні системи

Охоронні системи – це група фізичних електронних компонентів, які працюють разом для захисту будинку. Система безпеки будинку складається з наступних елементів:

Камера безпеки: інтелектуальні камери безпеки підключаються до Wi-Fi, що дає нам змогу дистанційно транслювати записи та отримувати сповіщення, коли наші камери виявляють рух. Багато камер включають інфрачервоне або кольорове

нічне бачення , хмарне або локальне сховище та двосторонню аудіосистему, що дозволяє нам говорити з тим, хто перебуває на камері. Деякі камери також мають інтелектуальну інтеграцію з платформами, наприклад Amazon Alexa або Google Assistant. Приклад такої камери представлено на рисунку 1.3.

Рис. 1.3 Камера безпеки

Датчик руху: датчики руху слід розміщувати в головному вході чи коридорі на першому поверсі будинку, щоб вони могли виявляти рух. Приклад датчика руху представлено на рисунку 1.4.

Рис. 1.4 Датчик руху

Датчик розбиття скла: це пристрій, призначений для виявлення звуку або вібрації, що виникають при розбитті скла. Він реагує на специфічний акустичний сигнал, який виникає при ударі та розколі скляної поверхні. Основне призначення таких датчиків — захист приміщень від несанкціонованого проникнення через вікна або скляні двері. Приклад датчика розбиття представлено на рисунку 1.5.

Рис. 1.5 Датчик розбиття скла

Сирена: Сирени існують у системах домашньої безпеки як окремо, так і як частина інших пристроїв, таких як базова станція. Приклад сирени представлено на рисунку 1.6.

Рис. 1.6 Сирена

Клавіатура: щоб поставити або зняти з охорони, системам безпеки зазвичай потрібен код, який потрібно ввести на клавіатурі або контрольній панелі, яка кріпиться до стіни або розміщується на плоскій поверхні. Приклад контрольної панелі представлено на рисунку 1.7.

Рис. 1.7 Клавіатура

Детектор диму: За допомогою цього пристрою можна отримувати сповіщення, якщо повітря в нашому домі стає небезпечним для дихання. Приклад детектора диму представлено на рисунку 1.8.

Рис. 1.8 Детектор диму

2 МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ IoT-ТЕХНОЛОГІЙ В ОХОРОНИХ СИСТЕМАХ

Через велику різноманітність протоколів, технологій і пристроїв у системі IoT значні компроміси полягають між економічною ефективністю, безпекою, надійністю, конфіденційністю, покриттям, затримкою тощо. Якщо оптимізувати один показник для покращення, це може призвести до у погіршенні інших показників. Наприклад, застосування занадто великої кількості перевірок безпеки та протоколів у всіх транзакціях даних у системах Інтернету речей може призвести до збільшення вартості та затримки програми, що робить її непридатною для користувачів.

Типова система IoT складається з великого ланцюга підключених пристроїв, технологій, доменів і географічних регіонів. Навіть якщо один із пристроїв, технологій або їх комбінація залишаються вразливими для атак, це може бути причиною загрози безпеці для всієї системи. Останнім часом спостерігається значне збільшення кількості слабких ланок у системах IoT. Наприклад, розумні камери та розумні дверні замки, можна використовувати як слабку ланку в системі розумного дому для отримання пароля користувача Wi-Fi [22].

Як наслідок, потрібні значні вдосконалення та покращення поточної структури та інфраструктури системи IoT, щоб зробити її надійною, безпечною та надійною [23]. Нижче наведені деякі кроки для покращення захисту:

1. Проводити тестування на вразливість для пристроїв IoT це необхідно для кількісної оцінки рівня ризику, пов’язаного з розгортанням цих пристроїв у різних системах. Виходячи з пов’язаного ризику, можна скласти список пріоритетів для більш якісного налаштування пристроїв.
2. Запровадити методи шифрування в системі IoT на різних рівнях і протоколах. Однак існують різні рівні циклів шифрування, дешифрування та повторного шифрування у всій системі. Ці цикли роблять систему вразливою до атак. Наскрізне шифрування було б перспективним рішенням для запобігання різним атакам.

3. Реалізувати протоколи автентифікації. Кожного разу, коли пристрій хоче взаємодіяти з іншим пристроєм, слід запровадити процес автентифікації. Цифрові сертифікати можуть бути якісним рішенням для безперебійної автентифікації з прив'язаними ідентифікаторами, прив'язаними до криптографічних протоколів.
4. Будь-яку реалізовану структуру безпеки IoT слід протестувати та підтвердити на масштабованість. Протоколи безпеки не повинні працювати лише для обмеженого кола користувачів. Справжні загрози починають надходити лише тоді, коли додаток стає публічним і починає широко використовуватися у відкритому доступі. Тому потрібна правильна стратегія та планування.
5. Для захисту даних користувача та середовища від перехоплення потрібен механізм, заснований на методах шифрування, таких як RSA, SHA256 або хешланцюжки. Пристрої Інтернету речей мають бути розроблені таким чином, щоб вони могли передавати отримані дані безпечним і зашифрованим способом. Це допоможе завоювати довіру окремих осіб, державних установ і галузей до додатків IoT.
6. Розробити підхід, щоб впоратися з обмеженнями вартості та потужності, які очікуються найближчим часом. Може знадобитися зміна парадигми від централізованого підходу до деякого децентралізованого підходу, коли пристрої можуть автоматично та безпечно спілкуватися один з одним. Це може допомогти зменшити витрати на керування системами та зменшити проблеми обмеження ємності [24].
7. Оскільки більшість систем Інтернету речей використовують хмарні служби для зберігання та пошуку даних, слід також враховувати ризики. Хмара — це загальнодоступна платформа, яка використовується декількома користувачами, і в хмарі можуть бути зловмисники, які можуть бути причиною загрози для даних, пов'язаних з Інтернетом речей. Дані повинні зберігатися як зашифрований текст у хмарі, і хмарі не можна дозволяти розшифровувати будь-який зашифрований текст. Це може додатково підвищити безпеку даних і позбавити нас від загальних ризиків використання хмарних служб [25].

8. Окрім викликів із боку зовнішніх організацій, існують різні сценарії, коли датчики в системі IoT починають збирати або надсилати помилкові дані. Ці помилки можуть бути легкими для обробки у випадку централізованої архітектури, але можуть стати слабким місцем у випадку автономної децентралізованої архітектури. Неправильне читання або передача даних може призвести до небажаних результатів. Таким чином, необхідно визначити механізм перевірки потоку даних, особливо у випадку розподіленої архітектури [26].
9. Оскільки кінцевою метою всіх систем IoT є створення автономної системи, яка потребує мінімального втручання людини, використання деяких методів або алгоритмів на основі штучного інтелекту (ШІ) для захисту пристроїв IoT може бути корисним. Це може допомогти зменшити аналіз і комунікаційне навантаження на середовище IoT.

2.1 Безпека Інтернету речей за допомогою шифрування даних

Найбільша загроза безпеці систем IoT полягає в тому, що навіть використання пристроїв для збору даних із реального фізичного світу може стати об’єктом кіберзлочинців.

Наприклад, розгортання технології IoT на заводі може значно підвищити продуктивність і ремонтопридатність завдяки збору даних від багатьох датчиків і модулів, встановлених у виробничому обладнанні.

Фальсифікація даних датчиків під час процесу може призвести до неправильного аналізу та помилкового контролю. Навіть якщо проблем немає, важливо враховувати ризики та загрози, які можуть стати очевидними або яскраво вираженими в майбутньому

Шифрування даних — це метод перетворення простих текстових даних у нечитабельний формат за допомогою математичного алгоритму. Цей процес гарантує, що конфіденційна інформація залишається в безпеці під час спілкування між пристроями IoT, хмарою та кінцевими користувачами. Шифрування допомагає за-

хистити дані від крадіжки, кібератак та інших загроз безпеці. Також воно є критично важливим заходом безпеки, який використовується для захисту конфіденційної інформації в IoT. Це допомагає захистити зв’язок між пристроями IoT, хмарою та кінцевими користувачами від потенційних загроз безпеці. Шифрування гарантує, що навіть якщо дані потраплять до чужих рук, до них неможливо отримати доступ або прочитати їх.

Зі швидким зростанням кількості підключених пристроїв захист даних став серйозною проблемою. В IoT конфіденційна інформація, така як особисті дані, місцезнаходження та фінансова інформація, передається через загальнодоступні мережі, що робить її вразливою для кібератак. Зашифровані дані неможливо прочитати без спеціального ключа шифрування, що робить їх найефективнішим способом захисту даних від несанкціонованого доступу. Шифрування даних має важливе значення для захисту від ряду загроз безпеці, таких як атаки типу "людина посередині", витоки даних і прослуховування.

Шифрування даних є критично важливим заходом безпеки, який використовується для захисту конфіденційної інформації в IoT. Це допомагає захистити зв’язок між пристроями IoT, хмарою та кінцевими користувачами від потенційних загроз безпеці. Шифрування гарантує, що навіть якщо дані потраплять до чужих рук, до них неможливо отримати доступ або прочитати їх.

Шифри використовують змінні, відомі як ключі або криптографічні ключі, для блокування та розблокування функцій шифрування або дешифрування. Користувачі створюють секретний код безпеки, відомий як пароль для генерації ключів.

2.1.1 Симетричне - шифрування з секретним ключем

Як видно з назви, він використовує той самий єдиний ключ для функціонування шифрування та дешифрування. У цьому випадку перед встановленням захищеного зв’язку відправник і одержувач повинні узгодити спільний секретний ключ. Залежно від вимог обміну даними, симетричне шифрування працює з потоковими (1 байт або 1 біт) і блочними шифрами (дані фіксованого розміру - зазвичай 64

біти). Він швидший, потребує мало енергії та включає простий і зрозумілий наскрізний процес. Прикладами є DES, AES, IDEA та Blowfish. Схема даного шифрування представлена на рисунку 2.1.

Рис. 2.1 Симетричне шифрування

Стандарт шифрування даних (DES) і Triple-DES. Обидва є симетричними алгоритмами шифрування, де DES є найстарішим і ключовим в криптографії, який зараз поступово припинено (через низький ключ шифрування). Його наступником є Triple-DES, який, як вважають, діятиме до 2030 року. Triple-DES долає всі виклики DES, такі як вразливі атаки зустрічі посередині, застосовує три 56-бітні ключі до кожного блоку даних і додає загальну довжину ключа до 168-біт. Однак існує випадок уразливості середнього рівня, яка знижує рівень безпеки до 112-бітного ключа. У зв'язку з цим він поступово припиняє роботу (замінений AES). Але деякі продукти Інтернету речей і фінансові послуги все ще використовують його через його надійність, сумісність і гнучкість.

Нижче наведено код що реалізує шифрування і дешифрування тексту за допомогою алгоритму DES, використовуючи бібліотеку CryptoJS:

1. Оголошення ключа та вихідного тексту:

```
const key = "0123456789abcdef";
const plaintext = "Student Pavlenko Kyryl";
```

Ключ (key) і текст (plaintext) ініціалізуються. Ключ має вигляд шістнадцяткового числа (16 символів, що відповідає 64-бітному ключу DES).

2. Ініціалізація класу DES:

```
  const des = new DES(key);
```

Створюється новий об'єкт класу DES, що виконує шифрування та дешифрування з використанням зазначеного ключа.

3. Шифрування та дешифрування:

```
const ciphertext = des.encrypt(plaintext);
const decrypted = des.decrypt(ciphertext);
```

Вихідний текст шифрується методом encrypt. Результат шифрування зберігається у змінній ciphertext як шістнадцятковий рядок. За допомогою методу decrypt зашифрований текст ciphertext перетворюється назад у початковий текст decrypted.

4. Виведення результатів:

```
console.log("Plaintext: ", plaintext);
console.log("Ciphertext: ", ciphertext);
console.log("Decrypted: ", decrypted);
```

Код виводить початковий текст, зашифрований текст і розшифрований текст, щоб продемонструвати коректність операцій.

Клас DES реалізує шифрування та дешифрування за алгоритмом DES у режимі ECB (Electronic Codebook).

5. Конструктор класу DES:

```
constructor(key) {
    this.key = CryptoJS.enc.Hex.parse(key);
}
```

Ключ конвертується у формат, сумісний з CryptoJS, використовуючи CryptoJS.enc.Hex.parse.

6. Метод encrypt:

```
encrypt(plaintext) {
    const encrypted = CryptoJS.DES.encrypt(
    plaintext,
    this.key,
    { mode: CryptoJS.mode.ECB }
    );
    return encrypted.ciphertext.toString();
}
```

Метод encrypt шифрує текст за допомогою DES у режимі ECB і повертає зашифрований текст у вигляді шістнадцяткового рядка.

7. Метод decrypt:

```
decrypt(ciphertext) {
        const ciphertextHex = CryptoJS.enc.Hex.parse(ci-
        phertext);
        const decrypted = CryptoJS.DES.decrypt(
    { ciphertext: ciphertextHex },
    this.key,
    { mode: CryptoJS.mode.ECB }
    );
        return decrypted.toString(CryptoJS.enc.Utf8);
    }
}
```

Метод decrypt перетворює шістнадцятковий рядок ciphertext у вихідний текст. Повністю код буде виглядати так:

```
const key = "0123456789abcdef";
const plaintext = "Student Pavlenko Kyryl";

const des = new DES(key);
const ciphertext = des.encrypt(plaintext);
const decrypted = des.decrypt(ciphertext);

console.log("Plaintext: ", plaintext);
console.log("Ciphertext: ", ciphertext);
console.log("Decrypted: ", decrypted);
```

```
class DES {
constructor(key) {
          this.key = CryptoJS.enc.Hex.parse(key);
}

encrypt(plaintext) {
     const encrypted = CryptoJS.DES.encrypt(
     plaintext,
     this.key,
     { mode: CryptoJS.mode.ECB }
     );
     return encrypted.ciphertext.toString();
}

decrypt(ciphertext) {
          const  ciphertextHex  =  CryptoJS.enc.Hex.parse(ci-
          phertext);
          const decrypted = CryptoJS.DES.decrypt(
     { ciphertext: ciphertextHex },
     this.key,
     { mode: CryptoJS.mode.ECB }
     );
          return decrypted.toString(CryptoJS.enc.Utf8);
     }
}
```

Результат роботи коду буде виглядати наступним чином:

```
Encryption:
After initial permutation: 14A7D67818CA18AD
After splitting: L0=14A7D678 R0=18CA18AD
```

```
Round 1 18CA18AD 5A78E394 194CD072DE8C
Round 2 5A78E394 4A1210F6 4568581ABCCE
Round 3 4A1210F6 B8089591 06EDA4ACF5B5
Round 4 B8089591 236779C2 DA2D032B6EE3
Round 5 236779C2 A15A4B87 69A629FEC913
Round 6 A15A4B87 2E8F9C65 C1948E87475E
Round 7 2E8F9C65 A9FC20A3 708AD2DDB3C0
Round 8 A9FC20A3 308BEE97 34F822F0C66D
Round 9 308BEE97 10AF9D37 84BB4473DCCC
Round 10 10AF9D37 6CA6CB20 02765708B5BF
Round 11 6CA6CB20 FF3C485F 6D5560AF7CA5
Round 12 FF3C485F 22A5963B C2C1E96A4BF3
Round 13 22A5963B 387CCDAA 99C31397C91F
Round 14 387CCDAA BD2DD2AB 251B8BC717D0
Round 15 BD2DD2AB CF26B472 3330C5D9A36D
Round 16 19BA9212 CF26B472 181C5D75C66D
Cipher Text: C0B7A8D05F3A829C
Decryption
After initial permutation: 19BA9212CF26B472
After splitting: L0=19BA9212 R0=CF26B472
Round 1 CF26B472 BD2DD2AB 181C5D75C66D
Round 2 BD2DD2AB 387CCDAA 3330C5D9A36D
Round 3 387CCDAA 22A5963B 251B8BC717D0
Round 4 22A5963B FF3C485F 99C31397C91F
Round 5 FF3C485F 6CA6CB20 C2C1E96A4BF3
Round 6 6CA6CB20 10AF9D37 6D5560AF7CA5
Round 7 10AF9D37 308BEE97 02765708B5BF
Round 8 308BEE97 A9FC20A3 84BB4473DCCC
Round 9 A9FC20A3 2E8F9C65 34F822F0C66D
Round 10 2E8F9C65 A15A4B87 708AD2DDB3C0
Round 11 A15A4B87 236779C2 C1948E87475E
Round 12 236779C2 B8089591 69A629FEC913
Round 13 B8089591 4A1210F6 DA2D032B6EE3
Round 14 4A1210F6 5A78E394 06EDA4ACF5B5
Round 15 5A78E394 18CA18AD 4568581ABCCE
Round 16 14A7D678 18CA18AD 194CD072DE8C
Plain Text: 123456ABCD132536
```

Нижче наведені основні випадки використання DES та Triple-DES:

- **Банківська справа та фінансові транзакції:** DES і Triple-DES активно використовувалися у фінансових системах, зокрема для захисту банківських

транзакцій. Triple-DES зокрема використовувався в системах обробки платежів і банкоматах, оскільки забезпечував кращий захист від атак, ніж звичайний DES.

- **Карткові платіжні системи:** Triple-DES став основним шифром у платіжних системах і використовується для забезпечення безпеки транзакцій з використанням кредитних і дебетових карток. Багато банківських систем і систем обробки карток ще деякий час продовжували використовувати Triple-DES через його відповідність фінансовим стандартам безпеки.
- **VPN та захищений зв'язок:** DES використовувався в протоколах VPN на ранніх етапах їх розвитку, а Triple-DES продовжив застосовуватись у цих протоколах, перш ніж VPN-протоколи перейшли на AES через його більшу ефективність і надійність.
- **Захищене зберігання файлів:** DES також використовувався для шифрування файлів на комп'ютерах та у корпоративних мережах. Triple-DES допомагав зберігати конфіденційні документи, хоча зараз він замінений сучаснішими алгоритмами, такими як AES, оскільки вони забезпечують вищий рівень безпеки.
- **Шифрування даних у телекомунікаціях:** DES застосовувався для шифрування голосових даних у телефонії та телекомунікаціях, забезпечуючи базовий рівень захисту від прослуховування. Хоча сьогодні для таких цілей використовуються інші, більш безпечні протоколи, DES і Triple-DES відігравали важливу роль на ранніх етапах розвитку технології захищених телекомунікацій.
- **Захист паролів у корпоративних системах:** У певних системах безпеки DES застосовувався для хешування та зберігання паролів користувачів, хоча він швидко був замінений на більш захищені хеш-алгоритми через вразливість до атак.

Сьогодні DES вважається небезпечним для використання через його недостатню довжину ключа (56 біт), що робить його вразливим до атак з повним перебо-

ром. Triple-DES залишається більш безпечним, але його повільніша робота і недостатня криптографічна стійкість (112-бітна довжина ключа) роблять його менш бажаним, ніж AES. Відповідно, багато систем оновили свої стандарти безпеки до AES, який є більш ефективним та безпечним для сучасних потреб.

Розширений стандарт шифрування (AES). Це найпопулярніший і надійний алгоритм симетричного шифрування, який працює з блочними шифрами від базових 128 до важких 192 і 256-бітних ключів. Він незламний (через більшу довжину ключа) і захищений від кібератак, за винятком грубої сили. Крім того, це футуристична «стандартна програма, яка найкраще підходить» для приватного сектору.

AES широко використовується в багатьох програмах, які потребують безпечного зберігання та передачі даних. Серед поширених випадків використання:

- **Безпека бездротового зв'язку:** AES використовується для захисту бездротових мереж, наприклад мереж Wi-Fi , для забезпечення конфіденційності даних і запобігання несанкціонованому доступу.
- **Шифрування бази даних:** AES можна застосовувати для шифрування конфіденційних даних, що зберігаються в базах даних. Це допомагає захистити особисту інформацію, фінансові записи та інші конфіденційні дані від несанкціонованого доступу в разі порушення даних.
- **Захищений зв'язок:** AES широко використовується в таких протоколах, як Інтернет-зв'язок, електронна пошта, обмін миттєвими повідомленнями та голосові та відеодзвінки. Це гарантує, що дані залишаються конфіденційними.
- **Зберігання даних:** AES використовується для шифрування конфіденційних даних, що зберігаються на жорстких дисках, USB-накопичувачах та інших носіях інформації, захищаючи їх від несанкціонованого доступу в разі втрати або крадіжки.
- **Віртуальні приватні мережі (VPN):** AES зазвичай використовується в протоколах VPN для захисту зв'язку між пристроєм користувача та віддаленим сервером. Це гарантує, що дані, надіслані та отримані через VPN, залишаються приватними та не можуть бути розшифровані перехоплювачами.

- **Безпечне зберігання паролів:** для безпечного зберігання паролів зазвичай використовується шифрування AES. Замість зберігання відкритих паролів зберігається зашифрована версія. Це додає додатковий рівень безпеки та захищає облікові дані користувача у разі несанкціонованого доступу до сховища.
- **Шифрування файлів і дисків:** AES використовується для шифрування файлів і папок на комп'ютерах, зовнішніх накопичувачах і хмарних сховищах. Він захищає конфіденційні дані, що зберігаються на пристроях або під час передачі даних, щоб запобігти несанкціонованому доступу.

Алгоритм шифрування IDEA також є симетричним блочним шифром, що розроблений як вдосконалення DES. IDEA застосовується для шифрування даних з метою забезпечення конфіденційності, хоча сьогодні його використовують рідше через популярність AES.

Серед поширених способів використання IDEA є:

- **Безпечний зв'язок:** IDEA можна використовувати для шифрування даних, що передаються через мережі зв'язку, такі як Інтернет, забезпечуючи конфіденційність і захищаючи від несанкціонованого доступу.
- **Фінансові транзакції:** IDEA можна використовувати для захисту фінансових транзакцій, таких як онлайн-банкінг і операції з кредитними картками, допомагаючи запобігти крадіжці особистих даних і шахрайству.
- **Електронні системи голосування:** IDEA можна використовувати для шифрування голосів в електронних системах голосування, забезпечуючи безпечне та конфіденційне голосування.
- **Шифрування файлів:** IDEA можна використовувати для шифрування файлів і папок на комп'ютері чи іншому запам'ятовуючому пристрої, захищаючи їх від несанкціонованого доступу.
- **Захист паролем:** IDEA можна використовувати для шифрування паролів та іншої конфіденційної інформації, що зберігається на комп'ютері чи в мережі, допомагаючи запобігти несанкціонованому доступу та витоку даних.

Blowfish — це техніка шифрування, розроблена як альтернатива техніці шифрування DES . Він значно швидший, ніж DES, і забезпечує хорошу швидкість шифрування, оскільки на сьогоднішній день не знайдено ефективних методів криптоаналізу . Це один із перших захищених блокових шифрів, які не підлягають жодним патентам і, отже, вільно доступні для будь-кого. Ось ключові особливості та застосування Blowfish:

- **Захист паролів у базах даних:** Blowfish часто використовувався для хешування паролів завдяки своїй стійкості до атак. Він став основою для створення bcrypt, алгоритму, який активно застосовується для захисту паролів у сучасних системах.
- **Захищене зберігання даних:** Blowfish використовується для шифрування файлів, папок і жорстких дисків. Завдяки швидкій швидкодії та гнучкості налаштувань, він забезпечує високу продуктивність при обробці великих обсягів даних.
- **VPN і захищений зв’язок**: Blowfish застосовується в деяких протоколах VPN (наприклад, OpenVPN), забезпечуючи захист даних під час передавання по мережі. Він є одним із варіантів шифру для забезпечення приватності зв'язку між клієнтом і сервером.
- **Інтернет-додатки та безпека даних:** Blowfish інтегрували в різні програми для забезпечення конфіденційності даних користувачів. Його використовували для шифрування конфіденційних даних в Інтернет-додатках, зокрема, у платіжних системах і в захищених каналах передавання даних.
- **Вбудовані системи:** Завдяки ефективності Blowfish підходить для вбудованих систем і пристроїв з обмеженими обчислювальними ресурсами. Це робить його практичним вибором для захисту інформації в пристроях IoT, маршрутизаторах, і навіть банкоматах.
- **Криптографічні бібліотеки:** Blowfish доступний у багатьох криптографічних бібліотеках, таких як OpenSSL, що забезпечило його застосування в різних системах, включаючи корпоративні рішення з обмеженим бюджетом.

Blowfish залишається прикладом простого, надійного алгоритму, який добре зарекомендував себе. Але для довгострокової безпеки, особливо з великими даними, більш придатними є алгоритми з більшими блоками даних, такі як AES.

2.1.2 Асиметричне - шифрування з відкритим ключем

На відміну від симетричного шифрування, він використовує пару ключів - відкритий ключ для шифрування та закритий ключ для дешифрування, пов'язані математично та логічно один з одним.

Будь-який відправник може зашифрувати дані за допомогою відкритого ключа. Однак розшифровка можлива лише призначеним одержувачем за допомогою закритого ключа. Таким чином, асиметричне шифрування передбачає автентифікацію з посиленою безпекою. Найпопулярнішими прикладами є RSA, DSA, ECC. Схема даного шифрування представлена на рисунку 2.2.

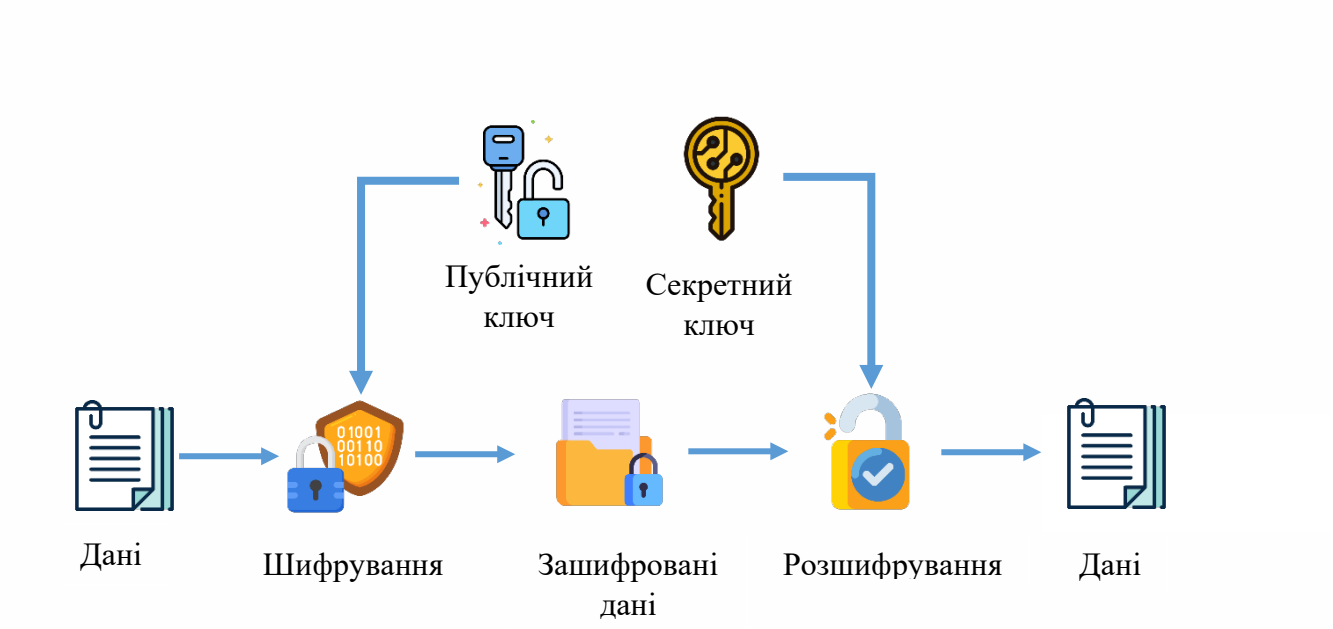


Рис. 2.2 Асиметричне шифрування

Алгоритм RSA. Це масштабований асиметричний алгоритм шифрування, якому найбільше довіряють дані, що передаються через Інтернет, наприклад

SSL/TLS, S/MIME, SSH, криптовалюти тощо. Він ефективно захищає від криптографічних зломів грубою силою, використовуючи більшу довжину ключа (768, 1024, 2048, 4096 біт тощо), що ускладнює та займає багато часу розшифровку даних. Отже, підходить для додатків IoT. Основні випадки його використання такі:

- **Цифрові підписи:** RSA широко використовується для створення цифрових підписів, що гарантує автентичність і цілісність документів та повідомлень. За допомогою RSA можна підтвердити, що повідомлення дійсно надійшло від певного відправника та що воно не було змінене під час передачі.
- **SSL/TLS-сертифікати:** RSA є одним з основних алгоритмів у SSL/TLS-протоколах для захисту інтернет-трафіку. Ці сертифікати використовуються на вебсайтах для шифрування даних, що передаються між браузером користувача та сервером, забезпечуючи захист від прослуховування та атак.
- **VPN та захищений доступ:** RSA застосовується в системах VPN для обміну ключами шифрування між клієнтом і сервером. Це дозволяє обом сторонам безпечно генерувати симетричні ключі, які використовуються для захисту сеансу зв’язку.
- **Шифрування електронної пошти:** RSA використовується в системах захищеної електронної пошти, таких як PGP (Pretty Good Privacy), щоб гарантувати конфіденційність та автентичність електронної кореспонденції. За допомогою RSA можна зашифрувати повідомлення, яке може розшифрувати лише власник відповідного закритого ключа.
- **Захист конфіденційних даних у мобільних і веб-додатках:** RSA часто інтегрується в мобільні та веб-додатки для захисту чутливих даних. Наприклад, RSA застосовується для безпечної передачі фінансових даних та особистої інформації під час користування банківськими додатками або системами електронної комерції.
- **Інфраструктура відкритих ключів (PKI):** RSA є ключовою технологією в інфраструктурі відкритих ключів, де він використовується для генерації сертифікатів, автентифікації користувачів і пристроїв, а також для захисту електронних документів.

- **Шифрування файлів:** RSA інколи використовується для захисту окремих файлів, зокрема для безпечного зберігання конфіденційної інформації, яка передається між пристроями або користувачами. Однак для великих обсягів даних зазвичай застосовують симетричні алгоритми шифрування, оскільки вони швидші.
- **Аутентифікація та захист доступу:** RSA широко використовується для двофакторної автентифікації та захищеного доступу до облікових записів. RSA-криптографія дозволяє створювати цифрові ключі для підтвердження особи користувача.

Завдяки надійності та стійкості до зломів RSA залишається одним із найпопулярніших асиметричних алгоритмів. Проте через високі обчислювальні ресурси він застосовується здебільшого для коротших повідомлень або передачі симетричних ключів.

Алгоритм цифрового підпису (DSA). Як і RSA, це також асиметричний алгоритм шифрування з невеликою, але значною різницею в процесі. DSA використовує електронний/цифровий підпис для передачі даних, що робить шифрування повільнішим (оскільки передбачає автентифікацію). Однак дешифрування відбувається швидше після успішної перевірки (через хеш-функцію). Полегшені алгоритми безпеки на основі цифрового підпису досліджуються для встановлення безпечного зв’язку в екосистемі IoT. Основні випадки використання DSA такі:

- **Цифрові сертифікати та інфраструктура відкритих ключів (PKI):** DSA застосовується для підписування цифрових сертифікатів у PKI, що дозволяє перевіряти достовірність та цілісність інформації. Це критично для систем, де необхідно підтвердити справжність веб-сайтів, електронних документів і користувачів.
- **Захищена електронна пошта:** DSA використовується в протоколах для підпису електронних листів і вмісту, щоб забезпечити цілісність і автентичність повідомлень. Підписані таким чином листи дозволяють одержувачам переконатися, що вміст не було змінено і що він надходить від надійного джерела.

- **Документообіг та юридичні документи:** Завдяки DSA можна підписувати юридичні документи, договори та інші важливі папери, які зберігаються в цифровій формі. Це забезпечує юридичну силу електронного підпису та його автентичність, що важливо для безпечного документообігу в компаніях і державних органах.
- **Захист програмного забезпечення та оновлень:** Цифрові підписи на базі DSA використовуються для підписування програмного забезпечення, оновлень і драйверів, що гарантує користувачам безпечне отримання перевірених версій. Це захищає від шкідливого ПЗ, оскільки користувачі можуть переконатися, що файл був підписаний законним розробником і не змінений.
- **Підписування транзакцій у криптовалютних мережах:** У блокчейн-технологіях DSA може застосовуватися для підпису транзакцій, забезпечуючи захист і перевірку автентичності при передачі криптовалюти. Цей підхід важливий для зменшення ризиків несанкціонованих транзакцій і шахрайства.
- **Безпека мереж та інтернет-з'єднань:** DSA є частиною захищених протоколів, таких як SSH і TLS, де його використовують для автентифікації сторін і підтвердження безпеки з’єднань. Це важливо для забезпечення конфіденційності та цілісності даних, що передаються по мережі.
- **Банківська справа та фінансові транзакції:** DSA може застосовуватись для підпису електронних транзакцій, що гарантує захист від підробки і зміни даних. Він допомагає захистити фінансову інформацію під час обміну між банками і клієнтами, що є особливо актуальним для мобільних і онлайн-банкінгу.

DSA є важливою складовою криптографічних протоколів, що сприяє безпеці в багатьох сферах, хоча для деяких випадків його поступово замінюють на більш сучасні алгоритми, такі як ECDSA (на еліптичних кривих), через підвищену ефективність та надійність.

Криптографія еліптичної кривої (ECC). Це альтернатива RSA і використовує алгебраїчні функції для створення конкретної безпеки між «парами ключів» (публічним і секретним ключами). Використовуючи теорію еліптичної кривої, ECC

генерує коротші, швидші та ефективніші ключі для шифрування та дешифрування. Це робить його найкращим для пристроїв IoT, мобільних додатків і тих, хто має обмежені обчислювальні (ЦП) ресурси. Ось основні випадки застосування ECC:

- **Мобільні та вбудовані пристрої (IoT):** ECC є оптимальним вибором для пристроїв з обмеженими обчислювальними потужностями та пам'яттю, таких як мобільні телефони, розумні годинники, датчики, а також IoT-пристрої. Він дозволяє забезпечувати високий рівень безпеки без значного навантаження на пристрій.
- **Протоколи безпечного зв'язку (TLS/SSL):** ECC широко використовується в сучасних протоколах безпечного зв'язку для забезпечення надійного шифрування в Інтернеті, особливо при передачі даних через HTTPS. Багато вебсайтів та вебсервісів переходять на ECC для підвищення продуктивності та безпеки.
- **Цифрові підписи:** Алгоритм цифрового підпису на основі еліптичних кривих (ECDSA) використовується для захисту документів, електронних транзакцій та електронної пошти. ECDSA забезпечує підвищений рівень надійності при меншій довжині ключа, що значно пришвидшує операції підпису та перевірки підпису.
- **Криптовалюти та блокчейн:** Більшість криптовалют (зокрема Bitcoin та Ethereum) використовують ECC для створення та перевірки цифрових підписів транзакцій. Завдяки цьому ECC забезпечує конфіденційність і автентифікацію транзакцій, захищаючи користувачів від шахрайства.
- **VPN та захищений віддалений доступ:** ECC застосовується в протоколах VPN для захисту даних, переданих між віддаленими пристроями. Це особливо важливо для організацій, що забезпечують безпечний доступ співробітників до корпоративних мереж і ресурсів.
- **Аутентифікація та керування доступом:** ECC використовується для аутентифікації користувачів і пристроїв у корпоративних мережах та вебсистемах. Він дозволяє створювати надійні цифрові сертифікати для підтвердження особистості та захисту від несанкціонованого доступу.

- **Електронні паспорти та ID-картки:** ECC знайшов застосування у сфері захисту персональних даних, зокрема у системах електронних паспортів і ID-карток. Він дозволяє захистити біометричну та особисту інформацію користувачів від підробок та зломів.
- **Двохфакторна аутентифікація (2FA):** ECC також використовується для забезпечення двофакторної аутентифікації, що додає додатковий рівень безпеки при доступі до облікових записів і корпоративних ресурсів.

Завдяки своїй ефективності, ECC і надалі залишається перспективним стандартом криптографії в різних галузях, де потрібен високий рівень безпеки з низьким обчислювальним навантаженням.

2.1.3 Вибір правильного алгоритму шифрування

Вибір правильного алгоритму шифрування є ключовим для впровадження безпечної та ефективної системи шифрування. Алгоритм повинен забезпечувати надійне шифрування без шкоди для загальної продуктивності пристрою. Також важливо переконатися, що алгоритм широко поширений і пройшов перевірку на вразливості безпеки.

Безпечне керування ключами має важливе значення для захисту від несанкціонованого доступу або крадіжки конфіденційної інформації. Система управління ключами повинна бути розроблена для роботи з великою кількістю пристроїв і ключів. Система повинна надавати пріоритет безпечному зберіганню ключів, щоб забезпечити максимальний захист.

Наскрізне шифрування гарантує, що дані шифруються в кожній точці передачі, включаючи IoT-пристрій, хмару та кінцевих користувачів. Щоб досягти максимальної безпеки та конфіденційності, шифрування має бути реалізовано якнайшвидше.

Кілька інструментів і рішень на ринку забезпечують шифрування для охоронних пристроїв IoT. Нижче наведено кілька популярних інструментів шифрування:

OpenSSL - це набір інструментів із відкритим кодом, який забезпечує шифрування для широкого діапазону пристроїв і платформ. Він широко використовується завдяки чудовій продуктивності та функціям безпеки.

Бібліотека Crypto++ - це бібліотека C++, яка надає низку методів шифрування та підтримує кілька платформ, як-от Windows, Linux і macOS. Він відомий своєю високою швидкістю шифрування та дешифрування, також ця бібліотека є для JavaScript.

Bouncy Castle - це бібліотека, яка забезпечує шифрування для різних мов програмування, таких як Java і C#. Він використовується для протоколів SSL/TLS, процедур шифрування та дешифрування.

Шифрування даних має важливе значення для охоронних пристроїв IoT для захисту конфіденційної інформації від кіберзагроз. Хоча впровадження шифрування може бути складним, дотримання найкращих практик і вибір правильних інструментів може допомогти забезпечити безпечну та ефективну систему шифрування. Оскільки кількість підключених пристроїв продовжує зростати, шифрування даних відіграватиме все більш важливу роль у захисті конфіденційності та безпеки даних.

2.2 Безпека Інтернету речей за допомогою блокчейну

Блокчейн та IoT є важливими технологіями, які матимуть великий вплив на індустрію IT та комунікацій. Ці дві технології спрямовані на підвищення загальної прозорості, видимості, рівня комфорту та рівня довіри для користувачів. Пристрої IoT надають дані в реальному часі з датчиків, а блокчейн забезпечує ключ до безпеки даних за допомогою розподіленої, децентралізованої та спільної книги [27].

Інтеграція блокчейну в IoT дозволяє створювати захищені канали обміну даними між пристроями, що знижує ризик зловмисних атак, таких як підміна даних чи несанкціонований доступ.

Смарт-контракти, як частина блокчейн-технології, забезпечують автоматизацію процесів у мережах IoT. Вони можуть виконувати попередньо визначені умови,

наприклад, обмін даними між пристроями або реагування на виявлення аномальної активності. Це робить систему більш ефективною та надійною, оскільки зменшується залежність від людського втручання.

На рисунку 2.3 наведено процес обробки транзакції в блокчейні, у якій користувач 1 хоче відправити повідомлення користувачу 2.

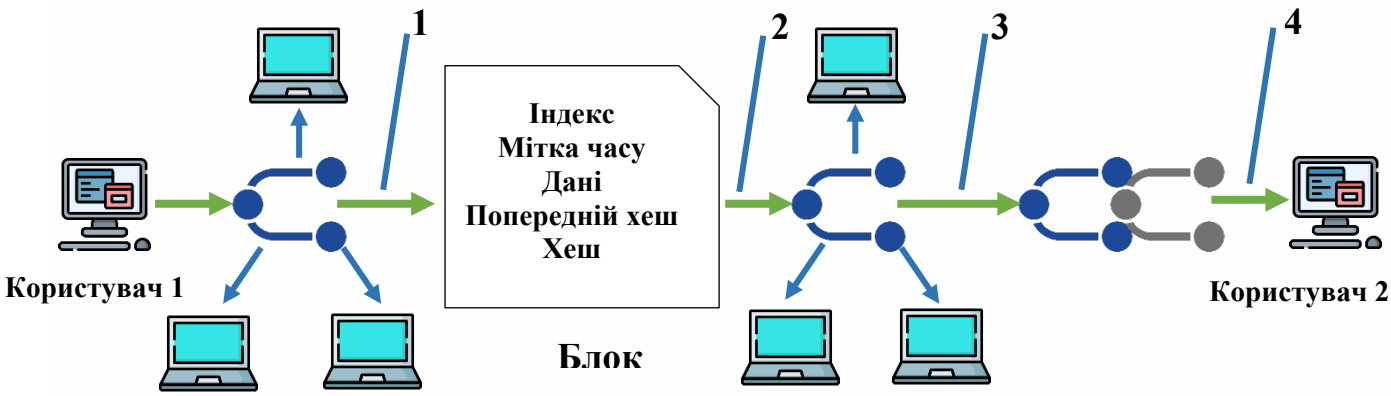


Рис. 2.3 Процес обробки транзакції в блокчейні

1. Передача повідомлення в мережу. Інші вузли можуть перевірити, чи повідомлення авторизований чи ні. Після перевірки повідомлення додається до блоку. Блок містить повідомлення, хеш, попередній хеш, індекс і час його створення;
2. Починається процес видобутку (майнінгу). Майнери починають вирішувати математичну задачу, щоб знайти випадкове значення, щоб хеш нового блоку мав певну заздалегідь визначену складність;
3. Новий блок додається до блокчейну. Кожен вузол оновлює свою локальну копію блокчейна;
4. Користувач 2 отримує повідомлення від користувача 1;

Існує два типи архітектури блокчейну залежно від типу доданих даних і характеру програми, що використовує блокчейн. У блокчейні без дозволів користувачеві не потрібен спеціальний дозвіл, щоб стати частиною мережі блокчейну або

стати майнером. Будь-хто може приєднатися або залишити цю мережу блокчейну без дозволу. Найкращим прикладом блокчейнів без дозволу є біткойн. Хоча пропускна здатність транзакцій не дуже висока, блокчейни без дозволів можуть підтримувати велику кількість вузлів у мережі.

З іншого боку, блокчейни з дозволом мають визначений набір правил для участі в мережі блокчейнів. Майнери також є уповноваженими особами, і блоки можна додавати в ланцюжок лише після їх перевірки. Блокчейн Ripple і Hyperledger є двома яскравими прикладами дозволеного блокчейну. Концепція блокчейну з дозволами покращує загальну пропускну здатність транзакцій у порівнянні з блокчейнами без дозволів.

2.2.1 Переваги Blockchain в IoT

Використання блокчейну має багато переваг у додатках IoT. У таблиці 2.1 наведено короткий перелік деяких конкретних проблем у безпеці IoT та їх можливі рішення за допомогою блокчейну. Різні проблеми безпеки, з якими стикаються системи IoT, були наведені в першому розділі.

Таблиця 2.1

Проблеми в IoT і можливе рішення блокчейну

Виклик для IoT	Специфікація	Можливе рішення блокчейну
Вартість та трафік	Щоб впоратися зі швидким розширенням IoT	Перехід до децентралізації за допомогою блокчейну. Пристрої можуть підключатися та спілкуватися з однорангові вузлами, а не через центральні сервери.
Конфіденційність в пристроях IoT	Пристрої IoT вразливі до розголошення приватних даних користувачів	Щоб вирішити таку проблему, запропоноване рішення полягає у використанні блокчейну з дозволом, який може захистити пристрої IoT.

Продовження таблиці 2.1

Виклик для IoT	Специфікація	Можливе рішення блокчейну
Велике навантаження на хмарний сервіс і недостатня кількість сервісів	Хмарні служби недоступні через атаки, помилки в програмному забезпеченні, живлення або інші проблеми	Записи оновлюються на різних вузлах мережі, які зберігають однакові дані, тому немає єдиної точки відмови.
Дефектна архітектура	Усі частини пристроїв IoT мають точку збою, яка впливає на мережу та весь пристрій	Дійсність пристроїв перевіряється завдяки блокчейну. Дані також перевіряються криптографічно, щоб переконатися, що їх може надіслати лише головний автор.
Маніпулювання даними	Дані витягуються з пристроїв Інтернету речей і після маніпулювання даними використовуються в неналежний спосіб	Завдяки блокчейну пристрої блокують одне одного. Якщо будь-який пристрій оновлює дані, система відхиляє його.

Блокчейн також можна використовувати у поєднанні з іншими технологіями, такими як штучний інтелект. Приклад такої комбінації наведений на рисунку 2.4

Основні переваги використання блокчейну в системах IoT:

- **Дані, які надходять з пристроїв IoT, можуть зберігатися в блокчейні:** системи IoT включають велику різноманітність пристроїв, підключених один до одного. Ці пристрої далі підключаються та контролюються іншими пристроями. Це налаштування додатково підключено до хмари, щоб дозволити використовувати програми IoT з будь-якого місця. Завдяки такому великому простору для переміщення даних, блокчейн є перспективним рішенням для зберігання даних і запобігання їх зловживанню. Незалежно від рівня в системі IoT, блокчейн може діяти як відповідне рішення для зберігання та передачі даних.

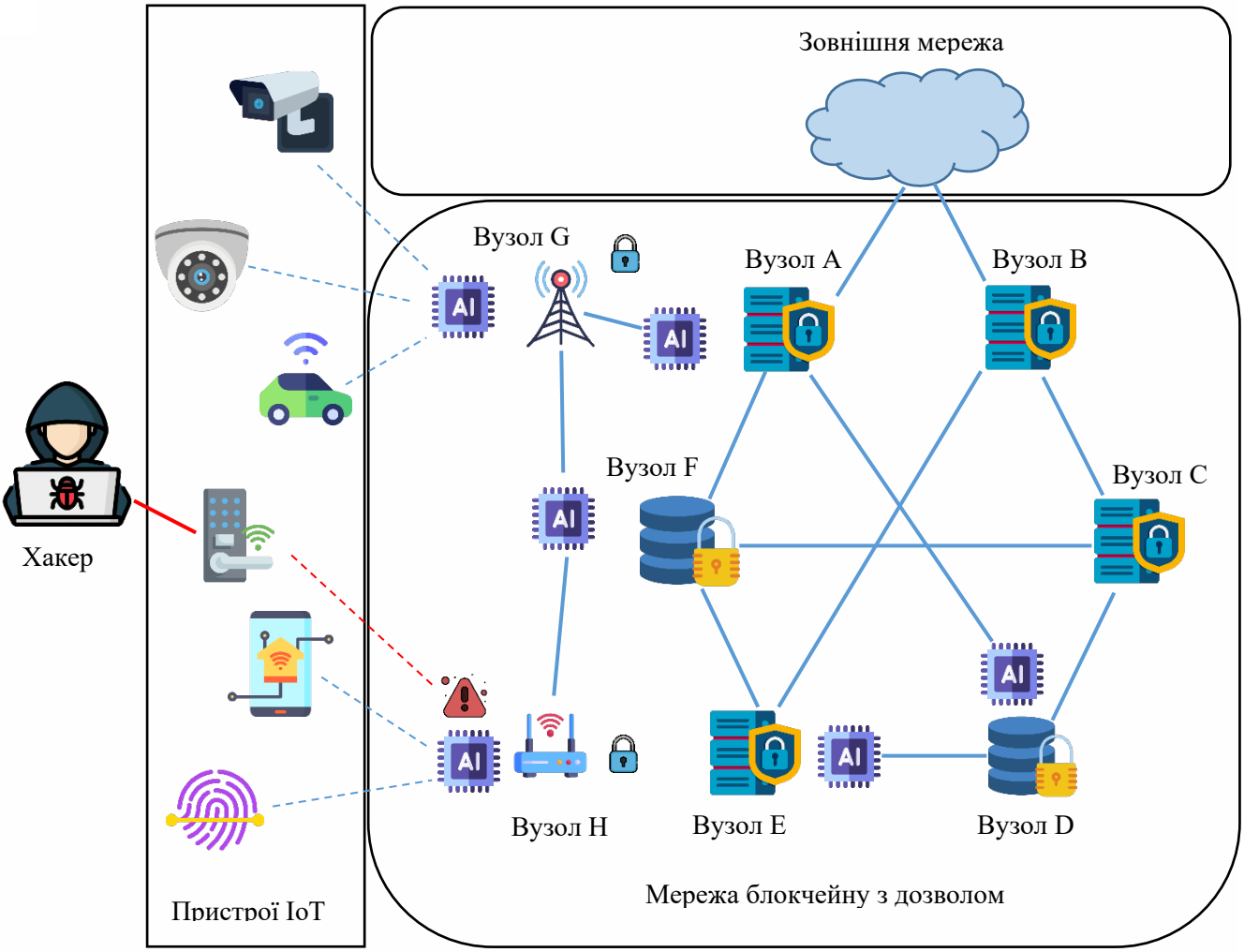


Рис. 2.4 Архітектура на основі штучного інтелекту та блокчейну для систем IoT

- **Розподілена природа блокчейну, що забезпечує безпечне зберігання даних:** оскільки архітектура блокчейну є розподіленою за своєю природою, вона може уникнути ризику бути єдиною точкою збою, як це трапляється в різних системах IoT на основі хмари. Незалежно від відстані між пристроями, створені ними дані можна легко зберігати в блокчейні безпечним способом [28].
- **Шифрування даних за допомогою хеш-ключа та перевірки майнерів:** у блокчейні можна зберігати лише 256-бітний хеш-ключ для даних, а не збері-

гати фактичні дані. Фактичні дані можна зберігати в хмарі, а хеш-ключ можна зіставляти з вихідними даними. У разі будь-яких змін у даних зміниться хеш даних, що робить їх безпечними та конфіденційними. На розмір блокчейна також не впливає розмір даних, оскільки в ланцюжку зберігаються лише хеш-значення. Лише призначені сторони, які мають право використовувати ці дані, можуть отримати доступ до даних із хмари за допомогою хешу даних. Кожен набір даних, що зберігається в блокчейні, належним чином перевіряється різними майнерами в мережі, тому ймовірність зберігання пошкоджених даних із пристроїв зменшується завдяки використанню блокчейну як рішення.

- **Запобігання втраті даних і spoofing-атаки:** під час spoofing-атак на додатки IoT новий вузол-супротивник входить у мережу IoT і починає імітувати, що є частиною вихідної мережі. За допомогою таких атак зловмисник може легко захоплювати, спостерігати або вводити дані в мережу. Блокчейн є перспективним рішенням для запобігання таким атакам. Кожен законний користувач або пристрій зареєстровано в блокчейні, і пристрої можуть легко ідентифікувати та автентифікувати один одного без необхідності центральних брокерів або центрів сертифікації. Будучи малопотужними за своєю природою, пристрої IoT успадковують ризик втрати даних. Можуть бути випадки, коли через зовнішні проблеми середовища дані втрачаються як відправником, так і отримувачем. Використання блокчейну може запобігти таким втратам, оскільки після додавання блоку в ланцюг його неможливо видалити.
- **Використання блокчейну для запобігання несанкціонованому доступу:** багато систем IoT включають багато частих комунікацій між різними вузлами. Комунікація в блокчейні відбувається за допомогою відкритих і закритих ключів, і тому тільки призначена сторона або вузол може отримати доступ до даних. Навіть якщо ненавмисна сторона зможе отримати доступ до даних, вміст даних буде незрозумілим, оскільки дані зашифровано за допомогою ключів. Таким чином, структура даних блокчейну намагається вирішити різні проблеми безпеки, з якими стикаються системи IoT.

- **Архітектура на основі проксі-сервера в блокчейні для пристроїв з обмеженими ресурсами:** хоча блокчейн надає різні функції безпеки для розподіленого середовища, IoT має особливу проблему обмеження ресурсів. Оскільки пристрої IoT дуже обмежені в ресурсах, вони не можуть зберігати великі бухгалтерські книги. Були різні роботи в цьому напрямку, щоб полегшити використання блокчейну в IoT. Архітектура на основі проксі є одним із перспективних рішень, які можуть допомогти пристроям IoT використовувати блокчейн. Проксі-сервери можуть бути розгорнуті в мережі, щоб зберігати ресурси в зашифрованому вигляді. Зашифровані ресурси можуть бути завантажені клієнтом з проксі-серверів.
- **Усунення централізованих хмарних серверів:** блокчейн може підвищити безпеку систем Інтернету речей, оскільки він остаточно усуває централізовані хмарні сервери та робить мережу одноранговою. Централізовані хмарні сервери є головною мішенню для злодіїв даних. За допомогою блокчейну дані розподілятимуться між усіма вузлами мережі та шифруватимуться за допомогою криптографічної хеш-функції.

2.3 Безпека IoT за допомогою туманних обчислень

Інтернет речей та хмарні обчислення — це дві самостійні технології, які знайшли широке застосування у різних сферах. IoT надає користувачам доступ до великої кількості розумних пристроїв та додатків, тоді як хмара забезпечує ефективні рішення для зберігання та обробки даних із можливістю доступу з будь-якої точки світу. Ці технології є незамінними для багатьох організацій. Однак стрімке зростання кількості пристроїв IoT породжує величезний обсяг даних, що створює значне навантаження на інфраструктуру Інтернету. Інтеграція IoT з хмарними обчисленнями дала змогу відкрити нові можливості, а також вирішити низку проблем, пов’язаних із зберіганням, обробкою, управлінням і захистом даних. Водночас цих переваг виявилося недостатньо для подолання всіх викликів, пов’язаних з IoT.

2.3.1 Архітектура туманних обчислень

Архітектура Fog-Cloud-Device показана на рисунку 2.5. Туманні обчислення зменшують трафік даних між хмарою та периферією мережі на 90%, а середній час відповіді для користувача – на 20% у порівнянні з моделлю лише з хмарою.

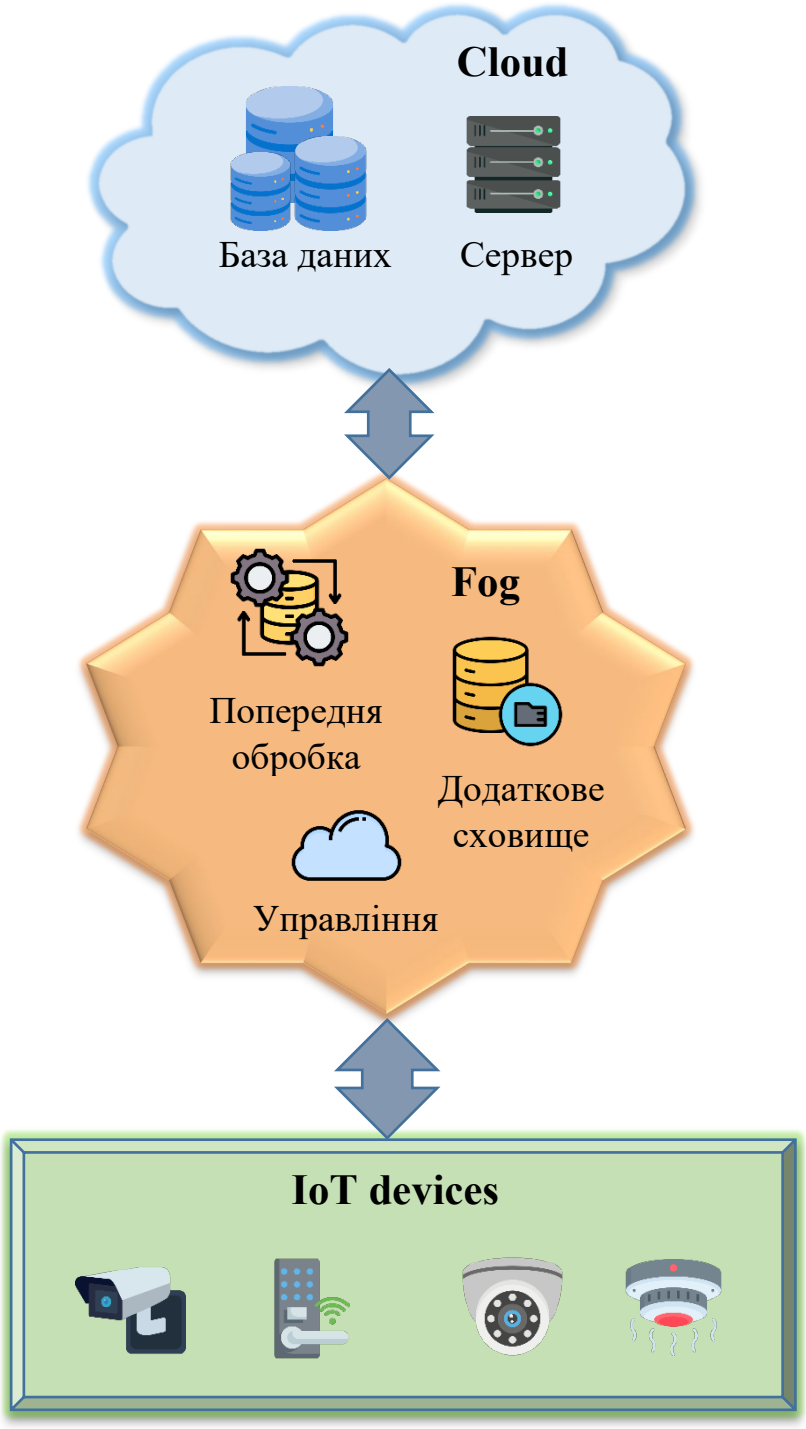


Рис 2.5. Архітектура Fog-Cloud-Device

Основним завданням туманних обчислень є локальна обробка даних, згенерованих пристроями IoT, для кращого управління, і, таким чином, потрібна архітектура, що складається з різних рівнів. Він має два архітектури: Fog-Device і Fog-Cloud-Device. Перша архітектура складається з пристрою та шару туману, а остання структура складається з пристрою, туману та шару хмар.

Розташування шарів здійснюється на основі їх пам'яті та обчислювальної потужності. Зв'язок між різними рівнями здійснюється за допомогою дротового або бездротового зв'язку. У архітектурі Fog-Device вузли туману надають різні послуги користувачеві без залучення хмарних серверів.

Однак у Fog-Cloud-Device прості рішення приймаються в шарі туману, тоді як складні рішення приймаються в хмарі.

2.3.2 Перевага туманних обчислень над хмарними

Пристрої IoT щодня генерують великі обсяги даних. Переміщення цих даних у хмару в реальному часі для аналізу неможливо. Тому була розроблена концепція туманного обчислення. На рисунку 2.5. показано розміщення та функціональність шару туману в дсистемі IoT. Туманні обчислення стосуються розширення хмарних обчислень і надання їхніх послуг на рівень периферії мережі. Це децентралізована інфраструктура для аналізу даних і обчислень, яку можна використовувати для ефективного й швидкого зберігання й обробки чутливих до часу даних. Головна мета — підвищити безпеку, запобігти крадіжкам даних, мінімізувати дані, що зберігаються в хмарі, і підвищити загальну ефективність додатків IoT. Затримка при обчисленні туману менша, ніж при обчисленні хмари, оскільки шар туману розташований набагато ближче до пристроїв, ніж хмара. Лише вибрані та важливі дані надсилаються в хмару для тривалого зберігання. Програми обчислення туману включають розумні транспортні засоби, розумні будинки, розумне сільське господарство, охорону здоров'я, розумні світлофори, розумну роздрібну торгівлю, програмно визначені мережі тощо. Надсилання величезної кількості даних, створених пристроями IoT, у хмару для обробки та аналізу дорогий і трудомісткий. Разом із

мінімізацією вимог до пропускної здатності мережі, туманні обчислення також зменшують частоту двостороннього зв’язку між пристроями IoT і хмарою.

В архітектурі туману дані збираються на пристроях, які називаються вузлами туману, які можуть аналізувати 40 відсотків даних. Він розвантажує трафік з базової мережі, мінімізуючи затримку пристроїв IoT. Туманним вузлом може бути будь-який пристрій, як-от маршрутизатор, комутатор або камера відеоспостереження, який має обчислювальну систему, сховище та підключення до мережі. Ці туманні вузли можна встановити де завгодно, як на заводі, так і в транспортному засобі за умови підключення до мережі. Дані спрямовуються до вузла туману, вузла агрегації або хмари на основі їх чутливості до часу. Туманні вузли забезпечують безпеку зв’язку в додатку IoT, надаючи криптографічні обчислення. Прості датчики та пристрої IoT не завжди мають необхідні вбудовані ресурси для цієї мети.

Стосовно атак, розглянутих у першому розділі, рішення, яке надає або може надати туманне обчислення для подолання цих загроз безпеці, наведені нижче.

- **Атака Man-in-the-middle:** Fog діє як рівень безпеки між кінцевим користувачем і хмарою або системою IoT. Усі загрози чи атаки на системи IoT повинні проходити через проміжний шар туману, і цей шар може ідентифікувати та пом’якшувати незвичайні дії, перш ніж вони будуть передані системі.
- **Атаки на передачу даних:** зберігання та керування даними набагато краще, якщо вони виконуються на захищених туманних вузлах, порівняно з пристроями IoT. Дані будуть краще захищені порівняно зі збереженням даних на пристроях кінцевих користувачів. Туманні вузли також допомагають зробити дані більш доступними для користувачів.
- **Прослуховування:** за допомогою туманних вузлів зв’язок відбувається лише між кінцевим користувачем і туманним вузлом, а не направляє інформацію через всю мережу. Шанси того, що зловмисник намагається підслухати, значно зменшуються, оскільки трафік у мережі зменшується.
- **Проблеми з обмеженням ресурсів:** більшість пристроїв IoT мають обмежені ресурси, і зловмисники користуються цим фактом. Вони намагаються пошкодити периферійні пристрої та використовувати їх як слабкі ланки для входу

в систему. Туманні вузли можуть підтримувати периферійні пристрої та можуть запобігти впливу таких атак на них. Сусідній туманний вузол може виконувати більш складні функції безпеки, необхідні для захисту.

- **Служби реагування на інциденти:** вузли туману можна запрограмувати для надання послуг реагування на інциденти в реальному часі. Вузли туману можуть генерувати позначку для системи IoT або кінцевих користувачів, щойно вони стикаються з підозрілими даними або запитом. Туманні обчислення дозволяють виявляти зловмисне програмне забезпечення та вирішувати проблеми під час транспортування. У багатьох критично важливих програмах може бути неможливо зупинити всю систему для усунення зловмисних програм. Вузли туману можуть допомогти в таких рішеннях, поки система запущена та працює.

2.3.3 Проблеми безпеки та їх рішення в туманному шарі

Хоча туманний шар надає різні функції та аспекти безпеки для програм IoT, переміщення даних і обчислень до туманного шару створює нові вразливості. Таким чином, перед впровадженням додатків IoT з підтримкою туману необхідно вивчити ці цілі безпеки та конфіденційності обчислень у тумані. У нижче наведені різні функції, які надає шар туману, проблеми конфіденційності та безпеки, а також запропоновані рішення для їх подолання.

1. Послуги в режимі реального часу: туманні обчислення прагнуть надавати послуги майже в реальному часі в системах IoT, виконуючи обчислення поблизу точок генерації даних.

- Виявлення вторгнень: порушення політики та шкідливі дії на вузлах туману та пристроях Інтернету речей не будуть виявлені, якщо не реалізовано належний механізм їх виявлення. Атаки можуть не вплинути на всю архітектуру туманних обчислень, але зловмисник може контролювати локальні служби. Атаки, спрямовані на локальні служби, можуть бути виявлені вузлами туману шляхом взаємодії

з їхніми сусідніми вузлами. Спостерігаючи за поведінкою програми та файловими системами хоста, можна виявити атаку на систему.

- Автентифікація: існують різні суб'єкти, залучені в процес пропозиції та доступу до послуг у реальному часі, як-от туманні вузли, постачальники послуг і користувачі. Довіряти всім залученим об'єктам — важке завдання, яке створює проблеми з безпекою для послуг IoT і даних користувачів.

Доступність послуг має надаватися лише справжнім та надійним користувачам; інакше зловмисники можуть скомпрометувати сервер і використовувати служби та конфіденційність користувачів. Тому, щоб запобігти незаконному доступу зловмисників до послуг, необхідний механізми автентифікації.

2. Тимчасове зберігання: користувачі можуть тимчасово зберігати та підтримувати свої дані на туманних вузлах за допомогою тимчасового зберігання.

З одного боку, це допомагає легко керувати даними в локальному сховищі, але з іншого боку, це створює нові проблеми та проблеми безпеки, особливо для підтримки конфіденційності даних.

- Ідентифікація та захист конфіденційних даних: дані, що зберігаються в пристроях IoT, можуть включати соціальні події, стан дорожнього руху, особисту діяльність, температуру тощо. Деякі дані можуть бути особистими або конфіденційними, а деякі дані можуть бути загальнодоступними. Крім того, для різних користувачів ті самі дані мають різні рівні безпеки. Тому важливо ідентифікувати та захистити конфіденційні дані від великого обсягу інформації.

-Безпечний обмін даними: для забезпечення безпеки дані, завантажені на туманні вузли, спочатку шифруються. Ніхто, крім власника, не може прочитати ці дані після того, як вони зашифровані. Це створює проблему для обміну даними. Щоб подолати цю проблему можна використовувати деякі криптографічні методи, такі як шифрування на основі сукупності ключів, повторне шифрування проксі та спільне використання атрибутів.

3. Розповсюдження даних: через проблеми безпеки дані не можуть бути передані на туманний вузол без шифрування.

Завдяки цьому передаванню зашифрованих даних до туманного вузла багатьма необхідними функціями доводиться жертвувати, наприклад обмін, пошук і агрегація.

- Безпечний пошук даних: як обговорювалося у пункті про тимчасове зберігання, дані шифруються перед завантаженням. Однак після того, як він зашифрований, пошук або отримання зашифрованого тексту стає складним для власників, а також для інших організацій.

Щоб отримати інформацію із зашифрованого тексту, шифрування з можливістю пошуку та його рівні конфіденційності необхідно використовувати індексовані запити, шифровані токени та методи, які забезпечують конфіденційність даних, запитів і доступу. Динамічна симетрична схема з можливістю пошуку представлена на рисунку 2.6.

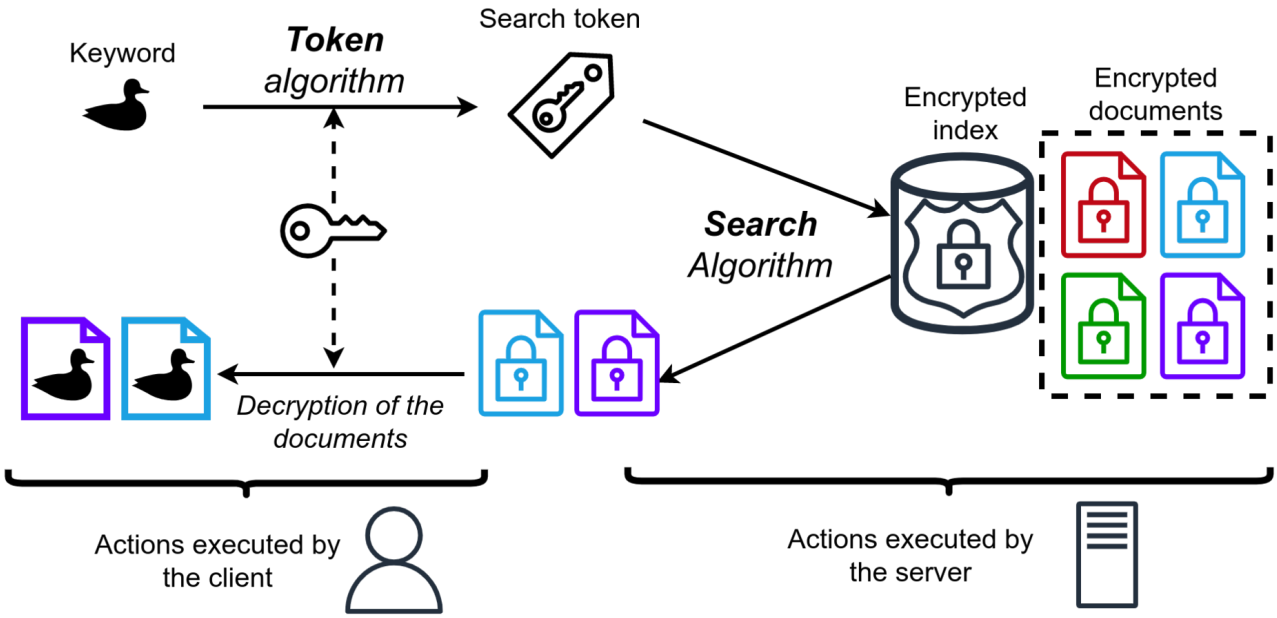


Рис 2.6 Динамічна симетрична схема з можливістю пошуку

- Агрегація даних: у певних випадках вузлам туману може знадобитися агрегувати дані, щоб запобігти витоку даних і зменшити накладні витрати на зв’язок. Важливо розробити безпечні алгоритми агрегації, щоб запобігти крадіжці даних.

Різні гомоморфні схеми шифрування (криптографічні методи, які дозволяють виконувати обчислення над зашифрованими даними без необхідності їхнього розшифрування), такі як шифрування RSA.

4. Децентралізоване обчислення: дані, що зберігаються на вузлах туману, можна обробляти та аналізувати для кращих результатів. Однак такі обчислення пов'язані з кількома загрозами та ризиками. Наприклад, зловмисники можуть не тільки контролювати проаналізовані результати, але також можуть викрити оброблені дані.

- Обчислення за допомогою сервера: завдання, які не можуть бути виконані самими пристроями IoT, обчислюються за допомогою туманних вузлів. Однак це може призвести до розкриття даних зловмисникам, якщо туманні вузли, які отримували дані з IoT, уже скомпрометовані. Обчислення за допомогою сервера є одним із таких методів, метою якого є забезпечення безпечних обчислень.

- Перевірені обчислення: користувачі покладаються на туманні вузли для обчислення своїх даних. Повинен існувати безпечний механізм для перевірки результатів обчислень, що надходять від вузла туману.

2.4 Безпека Інтернету речей за допомогою машинного навчання

Сфера машинного навчання привернула значний інтерес протягом останніх років. Багато доменів використовують ML для своєї розробки, і він також використовується для безпеки IoT. ML є перспективним рішенням для захисту пристроїв IoT від кібератак, забезпечуючи інший підхід до захисту від атак порівняно з іншими традиційними методами.

Стосовно атак, розглянутих у першому розділі , рішення, надані ML для подолання цих загроз безпеці, представлені нижче.

- **DoS-атака**: DoS-атаки на пристрої IoT або з пристроїв IoT викликають серйозне занепокоєння. Одним із підходів до запобігання таким атакам є використання протоколу на основі багаторівневого перцептрона (MLP), який за-

хищає мережі від атак DoS. Можу також запропонувати оптимізацію роїв частинок і алгоритм зворотного поширення для навчання MLP, який допомагає підвищити безпеку бездротових мереж. Технології ML допомагають підвищити точність дедукції та захистити пристрої IoT, вразливі до атак DoS.

- **Підслуховування**: зловмисники можуть підслуховувати повідомлення під час передачі даних. Щоб забезпечити захист від таких атак, можна використовувати такі методи ML, як криптоаналіз. Він використовуються для створення оптимальних ключів шифрування на основі передбачення атак. Прогнозування ризиків у каналах зв'язку. Машинне навчання може динамічно змінювати ключі або маршрути передачі даних для уникнення підслуховування.
- **Цифровий відбиток пальця**: цифровий відбиток пальця є одним із майбутніх і перспективних рішень для захисту систем IoT і допомоги кінцевим користувачам отримати достатню довіру до програм. Відбитки пальців широко використовуються для розблокування смартфонів, схвалення платежів, розблокування дверей автомобіля та будинку тощо. Завдяки низькій вартості, надійності, прийнятності та високому рівню безпеки цифрові відбитки пальців стають домінуючим методом біометричної ідентифікації. Окрім переваг цифрового зняття відбитків пальців, існують різні проблеми для ефективного використання цієї техніки в Інтернеті речей, такі як класифікація відбитків пальців, покращення зображення, зіставлення функцій тощо. Було розроблено різні алгоритми на основі машинного навчання, щоб забезпечити деякі нетрадиційні рішення для подолання ці проблеми, деякі з яких представлені нижче.
- **Витік конфіденційності:** такої як дані про здоров'я, місцезнаходження або фотографії, створює загрозу для приватності користувачів. Для запобігання цьому слід впроваджувати наукові обчислення із захистом конфіденційності (PPSC), які забезпечують безпеку під час обробки чутливих даних. Додатково, алгоритм виявлення цілісності товару (CIDA), розроблений на основі

китайської теореми про залишки (CRT), може бути використаний для підвищення довіри до систем IoT через забезпечення перевірки автентичності та цілісності даних.

- **Support Vector Machine**: SVM — це навчальний алгоритм для нелінійних і лінійних класифікацій, аналізу головних компонентів, категоризації тексту, ідентифікації мовця та регресії. Це максимізує розрив між межею прийняття рішення та шаблонами навчання. Вектор ознак будується на основі значень пікселів відбитка пальця та використовується для навчання SVM. Аналізуються різні візерунки за відбитком пальця, а потім на основі ідентифікованих шаблонів виконується зіставлення відбитка.
- **Штучні нейронні мережі**: ШНМ є одним із найбільш часто використовуваних алгоритмів у машинному навчанні. Він пропонує багато переваг, таких як стійкість до відмов, адаптивне навчання та узагальнення. Цифрові значення різних характеристик у відбитку пальця, таких як дрібниці, закінчення гребня та біфуркації, застосовуються як вхідні дані для нейронної мережі з метою навчання за допомогою алгоритму зворотного розповсюдження ШНМ. Перевірка відбитка пальця виконується на основі попередніх експериментальних значень, що зберігаються в базі даних.

2.5 Безпека Інтернету речей за допомогою периферійних обчислень

Периферійні та туманні обчислення є розширеннями хмарних обчислень, які широко використовуються різними організаціями. Основна відмінність між хмарними, туманними та периферійними обчисленнями полягає в розташуванні інтелектуальних і потужних обчислень. Хмара розгортається в набагато більшому масштабі, потребує обробки величезної кількості даних і розташована на порівняно більшій відстані від своїх користувачів. Щоб подолати проблеми, з якими стикаються хмарні обчислення, периферійні обчислення використовуються як рішення, де між користувачем і хмарою/туманом розміщується невеликий крайовий сервер. Деякі

дії з обробки виконуються на периферійному сервері, а не в хмарі. Архітектура периферійних обчислень складається з периферійних пристроїв, хмарного сервера та туманних вузлів, як показано на рисунку 2.7.

У фреймворку периферійних обчислень потужність обчислень і аналізу надається на самій межі.Пристрої в програмі можуть створювати мережу між собою та співпрацювати один з одним для обчислення даних. Отже, багато даних можна зберегти від виходу за межі пристрою, або до хмари, або до туманних вузлів, і це може підвищити безпеку програми IoT. Граничні обчислення також допомагають забезпечити низькі витрати на зв'язок, запобігаючи необхідності переміщення всіх даних у хмару.

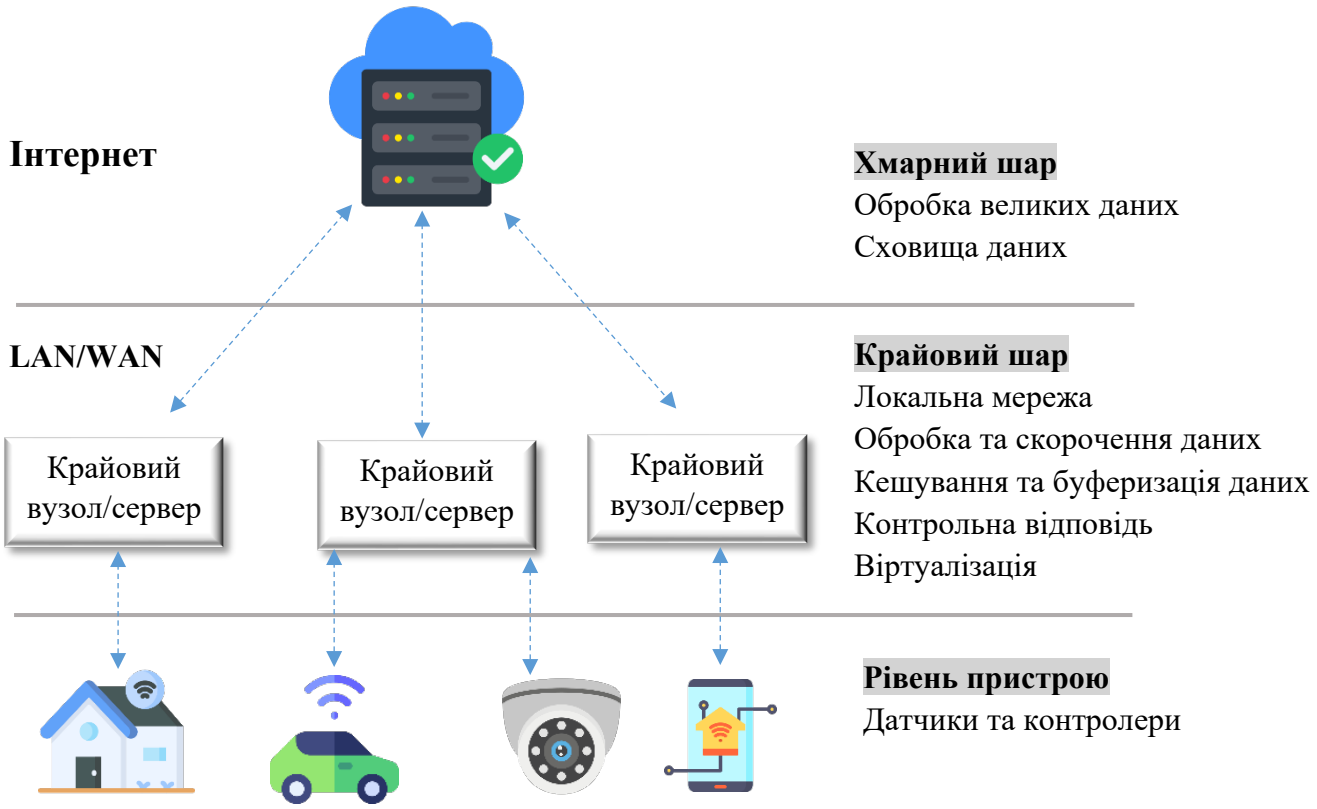


Рис 2.7 Архітектура периферійних обчислень

2.5.1 Використання периферійних обчислень для захисту IoT

Стосовно атак, розглянутих у першому розділі рішення, які периферійні обчислення надають або можуть надати для подолання цих загроз безпеці, наведені нижче:

- **Витоки даних:** у периферійних обчисленнях усі дані зберігаються та обробляються на пристрої або в локальній мережі. Дані не переміщуються від джерела даних до процесора. Це запобігає передачі даних і таким чином запобігає ризику крадіжки та витоку даних. У туманних обчисленнях відбувається переміщення даних від пристрою до шару туману, і зловмисники можуть скористатися цим переміщенням.
- **Питання безпеки:** із збільшенням розгортання кіберфізичних систем безпека та безпека розглядаються як невід'ємні питання. Якщо є навіть невелика затримка відповідей, це може призвести до проблем з фізичною безпекою. Наприклад, якщо датчики в автомобілі передбачають, що ось-ось станеться аварія, подушки безпеки повинні бути негайно розкриті. Якщо датчики повністю покладаються на надсилання всіх даних у хмару та чекають відповіді з хмари для виконання будь-яких дій, тоді це може бути занадто пізно, щоб запобігти травмам. Камери відеоспостереження також можуть бути розширені за допомогою периферійних обчислень, і вони можуть самі аналізувати аномалії та можуть надсилати зведені та підозрювані дані в центри обробки даних для досягнення швидшого часу реакції.
- **Проблеми з пропускною здатністю:** системи IoT генерують багато даних із дуже високою швидкістю. Більшість цих даних необроблені та мають відносно низьку цінність. Надсилання всіх даних у хмару також передбачає значну вартість пропускної здатності, а також виклики безпеки переміщення даних. Якщо використовуються периферійні обчислення, то багато очищення та агрегації даних можна виконати на граничних вузлах, і лише зведені дані, якщо потрібно, потрібно надсилати до хмари.

2.5.2 Проблеми в крайовому шарі

Незважаючи на те, що периферійні обчислення надають різні функції для підвищення безпеки та продуктивності систем Інтернету речей, існують різні проблеми, пов’язані з повною опорою на крайовий рівень для всіх обчислень. Периферійні пристрої включають датчики, пристрої RFID, приводи, мітки та вбудовані пристрої. Крайовий рівень дуже сприйнятливий до атак у системі IoT.

Якщо цей рівень скомпрометований, то може бути скомпрометована вся система. MQTT і COAP є найпопулярнішими протоколами для крайового рівня. Обидва ці протоколи за замовчуванням не використовують жодного рівня безпеки. Хоча опція додавання додаткового рівня безпеки у формі TLS для MQTT і DTLS для COAP присутня, це створює додаткові витрати з точки зору обробки та пропускної здатності.

Проблеми, характерні для периферійних пристроїв, включають атаки з порушенням сну, атаки з розрядженням акумулятора та атаки збоїв. Периферійні пристрої зазвичай мають обмежені ресурси, і найважливішим ресурсом, на який вони покладаються, є резервна батарея.

Найголовніший і найпростіший спосіб атакувати периферійні пристрої — якимось чином розрядити батарею периферійного пристрою. Наприклад, зловмисник може змусити периферійний пристрій виконати деякі енергоємні або нескінченні обчислення.

Процес досягнення балансу між зберіганням і обробкою даних на краю або в хмарі дуже важливий. Зберігання занадто великої кількості даних на периферії також може призвести до перевантаження периферійних пристроїв і може вплинути на всю програму.

2.6 Порівняння методів захисту

У системах охорони на базі IoT кожен із розглянутих методів має свої сильні сторони та обмеження. Ефективний захист систем потребує комбінованого підходу, враховуючи специфіку кожного сценарію:

✓ Шифрування даних — базова технологія, що забезпечує захист конфіденційності під час передачі даних. Її варто використовувати у всіх системах як стандарт.

✓ Блокчейн підходить для систем, де потрібна прозорість дій та надійна історія подій, наприклад, у реєстрах доступу або обліку обладнання.

✓ Туманні обчислення оптимальні для великих IoT-систем з розподіленою архітектурою, де важливий швидкий доступ до попередньої обробки даних.

✓ Машинне навчання є незамінним для прогнозування загроз, аналізу аномалій та підвищення проактивного захисту.

✓ Периферійні обчислення зменшують залежність від хмарних серверів і дають змогу обробляти дані на місці, що корисно для пристроїв із високим ризиком втручання

Таблиця 2.2

Порівняння методів захисту

Метод	Переваги	Недоліки	Типові сценарії
Шифрування даних	Конфіденційність, простота інтеграції	Управління ключами	Захист передачі та зберігання даних
Блокчейн	Децентралізація, незмінність	Високі витрати, затримки	Контроль доступу, реєстрація подій
Туманні обчислення	Зниження затримок, локальна обробка	Складність інфраструктури	Обробка даних у реальному часі
Машинне навчання	Виявлення аномалій, адаптивність	Високі ресурси, помилки класифікації	Аналіз трафіку, виявлення атак
Периферійні обчислення	Мінімальна затримка, автономність	Обмежені ресурси пристроїв	Локальна обробка на IoT-пристроях

3 ПРАКТИЧНІ АСПЕКТИ ВПРОВАДЖЕННЯ СИСТЕМ ІОТ В ОХОРОНІ СИСТЕМИ

У цьому розділі мною були розглянуті реальні кейси використання IoT в охоронних технологіях, аналізуються їх вразливості та ефективність запропонованих методів захисту. Також проводиться порівняння теоретичних підходів до безпеки з їх реалізацією у практичних умовах, що дозволяє оцінити, наскільки сучасні охоронні системи готові протистояти реальним загрозам.

3.1 Приклади реалізованих проектів з використанням IoT в охоронних системах

Нижче наведено конкретні приклади успішної інтеграції IoT у сферу безпеки, які демонструють його потенціал для вирішення складних завдань.

3.1.1 Проект "Smart Home Security System" компанії Ring

Рис 3.1 "Smart Home Security System"

Призначення: Забезпечення безпеки житлових приміщень за допомогою комплексної системи спостереження та контролю.

Реалізація:

- ✓ Камери відеоспостереження Ring Doorbell із функцією розпізнавання обличчя та виявлення руху.
- ✓ Інтеграція з хмарними сервісами для зберігання відео.
- ✓ Дистанційне керування через мобільний додаток і голосові помічники (Alexa).

Особливості:

- ➢ Сповіщення в реальному часі про спроби вторгнення.
- ➢ Створення «віртуального району», де сусіди можуть ділитися відео.

3.1.2 Система безпеки «ShotSpotter» для міського середовища

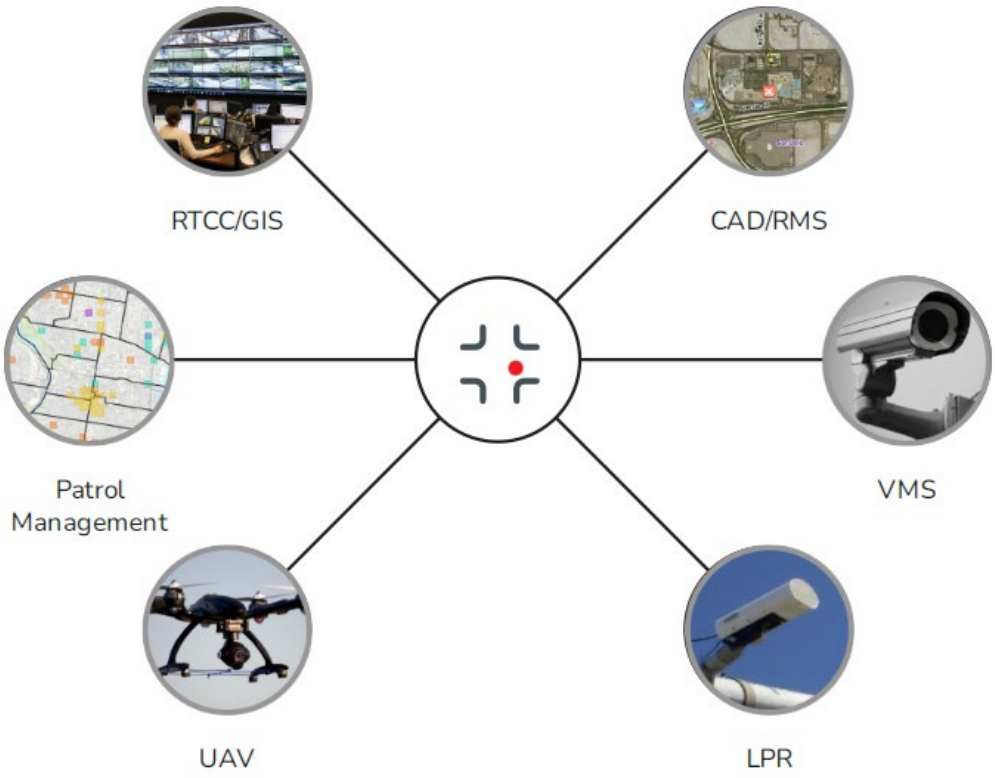


Рис 3.2 Система «ShotSpotter»

Призначення: Виявлення та локалізація пострілів у громадських місцях.

Реалізація:

- ✓ Використання мережі датчиків IoT для аудіозапису пострілів.
- ✓ Технологія аналізу даних у реальному часі для швидкого реагування.
- ✓ Інтеграція з відділами поліції для автоматичного звітування про події.

Особливості:

- ➢ Скорочення часу реагування поліції.
- ➢ Ефективний інструмент зниження рівня злочинності в зонах підвищеного ризику.

3.1.3 Система відеоспостереження на базі Hikvision

Рис 3.3 Комплект відеоспостереження «**Hikvision**»

Призначення: Забезпечення безпеки великих об'єктів (торгові центри, склади, офіси).

Реалізація:

- ✓ Камери з функціями IoT: розпізнавання номерних знаків, поведінковий аналіз, тепловізійний моніторинг.
- ✓ Інтеграція з мобільними додатками для дистанційного керування.
- ✓ Використання штучного інтелекту для аналізу великих обсягів відеоданих.

Особливості:

- ➢ Оптимізація процесів безпеки.
- ➢ Автоматизація виявлення нештатних ситуацій.

3.1.4 Розумні замки August Smart Lock

Рис 3.4 «August Smart Lock»

Призначення: Посилення контролю доступу до приміщень.

Реалізація:

- ✓ Використання блокувань IoT з доступом через мобільні додатки.
- ✓ Інтеграція з технологією Bluetooth і Wi-Fi.
- ✓ Функція автоматичного відкриття/закриття дверей в залежності від підходу власника.

Особливості:

- ➢ Гнучке налаштування доступу для тимчасових гостей.
- ➢ Журнали доступу, щоб відстежувати, хто і коли здійснював доступ.

3.2 Огляд конкретного кейсу: Встановлення та використання камери Swizoo G9 Pro за допомогою додатка Tuya Smart

Одним із прикладів використання IoT у системах безпеки є впровадження інтелектуальних камер відеоспостереження, таких як Swizoo G9 Pro, інтегрованих із додатком Tuya Smart. Ця камера є доступним і ефективним рішенням для домашнього та офісного використання, забезпечуючи можливість віддаленого моніторингу та управління в режимі реального часу.

3.2.1 Про компанію Tuya

Tuya Inc. є провідним глобальним постачальником послуг хмарної платформи, місія якого полягає в тому, щоб побудувати екосистему розробників розумних рішень. Її логотип наведено на рисунку 3.5. Tuya стала однією з перших компаній, які створили хмарну платформу для розробників із хмарними можливостями та генеративними можливостями штучного інтелекту, яка надає повний набір пропозицій, включаючи платформу як послугу або PaaS, програмне забезпечення як послугу або SaaS, а також інтелектуальні рішення для розробників інтелектуальних пристроїв, комерційних програм і галузей. Через свою хмарну платформу розробників Tuya активізувала динамічну глобальну спільноту розробників брендів,

OEM-агентів, агентів штучного інтелекту, системних інтеграторів і незалежних постачальників програмного забезпечення, щоб колективно прагнути до екосистеми розумних рішень, що втілює принципи екологічності та низького рівня викидів, безпеки, високої ефективності, спритність, відкритість.

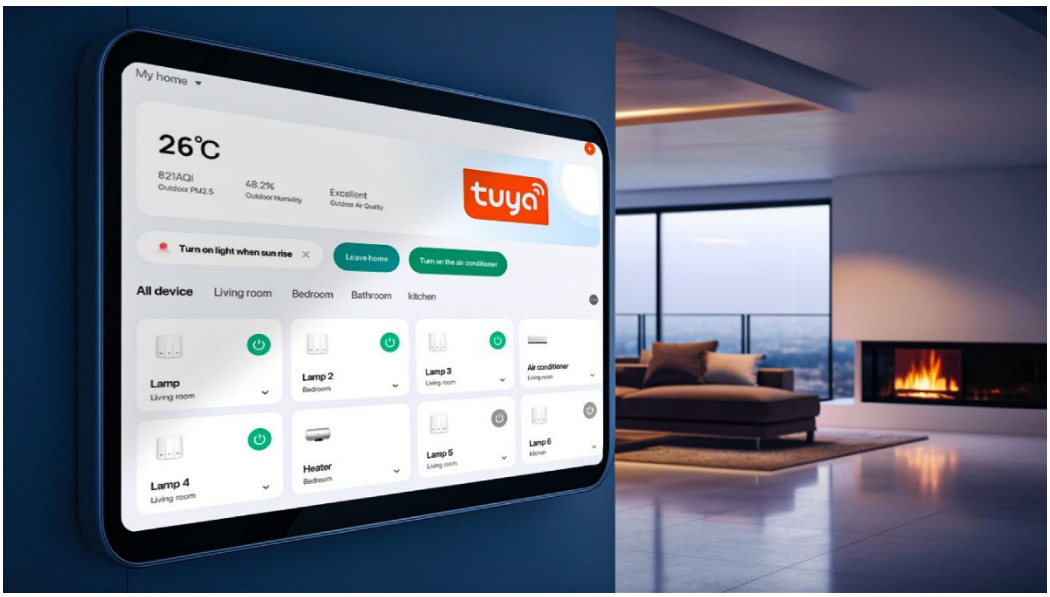


Рис 3.5 Логотип компанії Tuya

Станом на 31 березня 2024 року на платформі розробників Tuya Cloud зареєстровано понад 1 074 000 розробників із понад 200 країн і регіонів.

3.2.2 Огляд камери відеоспостереження Swizoo G9 Pro

Камера Swizoo G9 Pro – це багатофункціональний пристрій для відеоспостереження, який підходить для дому, офісу або догляду за дітьми та домашніми улюбленцями. Вона підтримує роздільну здатність 1920x1080 пікселів (FullHd), забезпечує якісну кольорову зйомку вдень і чітке нічне бачення завдяки інфрачервоному підсвічуванню. Камера здатна обертатися на 355 градусів по горизонталі та 90 градусів по вертикалі, що дозволяє контролювати великий простір.

Однією з ключових функцій є двосторонній аудіозв'язок, який дозволяє не лише чути, що відбувається, а й говорити через камеру. Крім цього, пристрій оснащений датчиком руху, який надсилає сповіщення на смартфон та автоматично записує відео. Дані можна зберігати на карті пам'яті або у хмарі. Камера також має функцію автостеження за рухомими об'єктами.

Керувати пристроєм можна через безкоштовний додаток для Android і iOS, що дає змогу переглядати відео з будь-якої точки світу. Завдяки інтелектуальному фільтру IR-Cut нічна зйомка залишається деталізованою на відстані до 15 метрів. Камера, та те що уходить до неї у комплект, наведено на рисунку 3.6.

Рис 3.6 Комплект камери Swizoo G9 Pro

Більш детальні характеристики наведені в таблиці 3.1

Таблиця 3.1

Характеристики Swizoo G9 Pro

Характеристика	Деталі
Назва бренду	Swizoo
Модель	G9 Pro
Гарантія	6 місяців
Розширення	1920x1080 пікселів
Сертифікація	CE, FCC, RoHS
Функції	Нічне бачення, двостороннє аудіо, PAN-TILT, відстеження руху людини, виявлення руху, RESET
Мережа	Wi-Fi
Формат стиснення відео	H.264
Варіанти зберігання даних	Карта пам'яті, хмарне сховище
Додаток	Tuya Smart
Датчик зображення	1/3 "CMOS
Нічне бачення	Інфрачервона підсвітка до 15 м
Мова	Автоматичне налаштування відповідно до мови мобільного телефону
Потужність	DC 5V2A USB
Кут огляду	По горизонталі: 355° і по вертикалі: 90°
Канали	4
Розмір камери	70x70x110 мм
Вага камери	190 г

3.2.3 Підключення камери Swizoo G9 Pro та огляд функціоналу

Щоб повноцінно скористатися можливостями пристрою, важливо правильно виконати підключення та ознайомитися з його функціоналом. Нижче будуть розглянуті основні етапи налаштування камери, підключення до мережі Wi-Fi та використання фірмового додатка Tuya Smart для керування функціями камери.

1. Реєстрація у додатку Tuya Smart

Якщо у вас ще немає облікового запису програми, ви можете зареєструвати обліковий запис або увійти за допомогою коду підтвердження через SMS. Перегляньте поточну та наступну сторінки, щоб отримати пояснення щодо процесу реєстрації. Натисніть «Зареєструватися», щоб перейти на сторінку політики конфіденційності Tuya Smart.

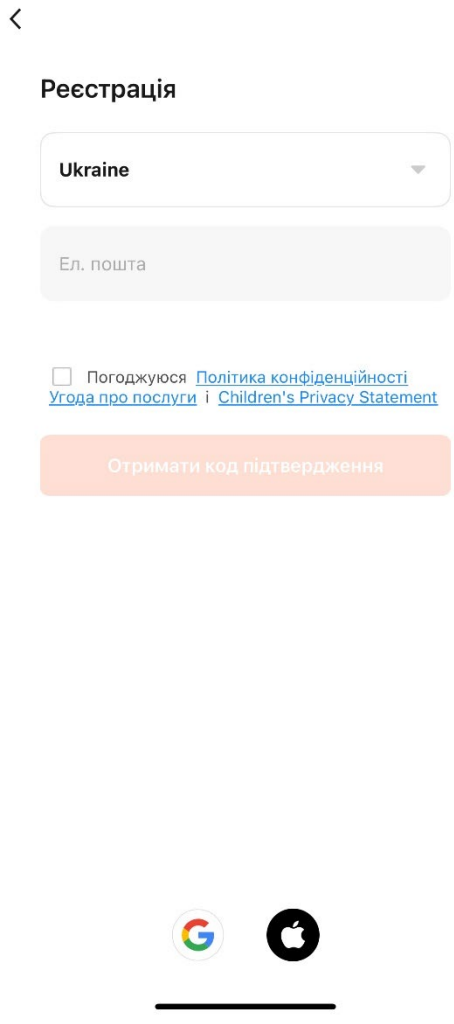


Рис 3.7 Створення облікового запису

2. Підключення камери

У додатку оберіть функцію "Додати пристрій", як показано на рисунку 3.8, та виберіть категорію камери. Слідуйте інструкціям для підключення до Wi-Fi, а саме потрібно вказати Wi-Fi мережу (2.4 ГГц) і пароль. Додаток згенерує QR-код, який

потрібно відсканувати камерою. Наведіть об'єктив камери на екран вашого смартфона. Після успішного зчитування ви почуєте підтвердження звуком.

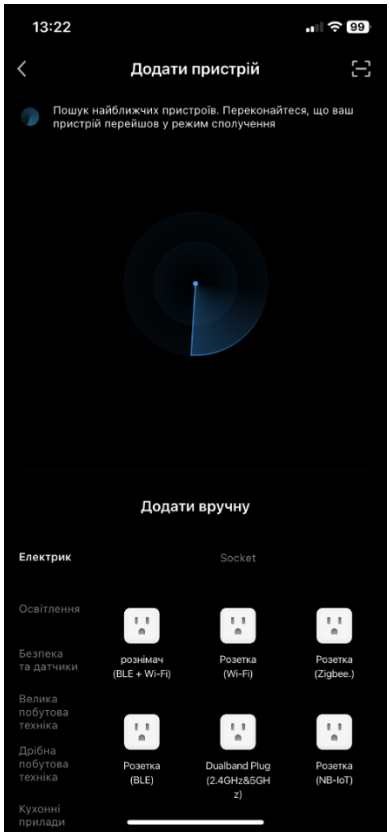


Рис 3.8 Додання пристрою

Якщо всі дії були виконані правильно то пристрій буде додано до вашого списку в додатку, як показано на рисунку 3.8. Після цього потрібно натиснути на іконку камери та почати нею користуватися.

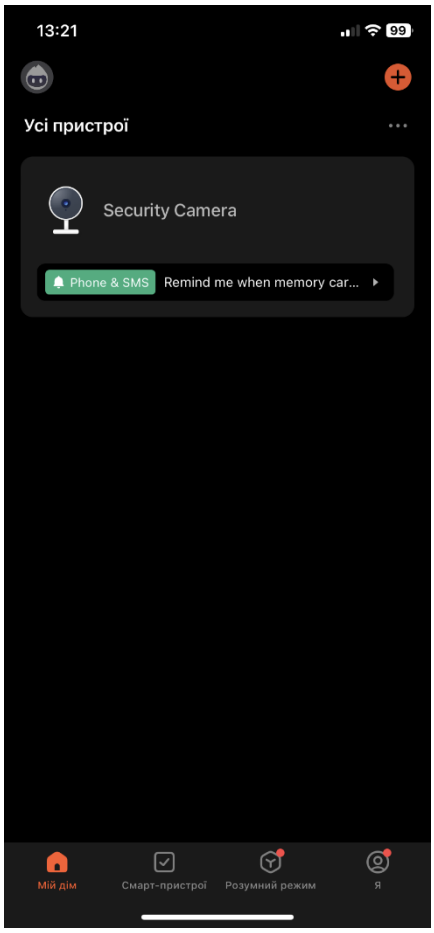


Рис 3.9 Камера підключена

3.2.4 Аналіз вразливостей і захисту системи Swizoo G9 Pro з Tuya Smart

Камера Swizoo G9 Pro використовує сучасні протоколи шифрування для забезпечення безпеки даних. Зазвичай пристрої такого типу, що інтегруються з додатком Tuya Smart, використовують такі методи захисту:

- **Протоколи шифрування:**

- Розширений стандарт шифрування AES-128/256.

Цей алгоритм використовується для захисту даних під час передачі між камерою, маршрутизатором і додатком. Він забезпечує надійне шифрування відео і запобігає несанкціонованому доступу.

- Безпека транспортного рівня TLS.

Застосовується для захисту зв'язку між мобільним додатком Tuya Smart і хмарними серверами. Це забезпечує надійність передачі даних, запобігаючи перехопленню під час з'єднання.

- RSA.

Використовується для аутентифікації пристроїв і ключового обміну під час початкового налаштування.

- **Захист облікового запису Tuya Smart:**

- Двофакторна автентифікація.

Додаток підтримує двофакторну автентифікацію (2FA), що додає додатковий рівень безпеки для доступу до ваших камер.

- Захист хмарного зберігання

Якщо ви використовуєте хмарне сховище Tuya Smart, дані зберігаються із застосуванням рівня захисту, який відповідає стандартам ISO/IEC 27001.

3.2.5 Оцінка ефективності запропонованих методів безпеки Swizoo G9 Pro на практиці

У цьому аналізі я зосередився на практичній реалізації рішень безпеки в системах Swizoo G9 Pro і Tuya Smart. Мною було розглянуто, як ці рішення працюють у реальних умовах, беручи до уваги досвід користувача та типові ситуації.

1. Шифрування даних

Відео та дані передаються через зашифровані канали (AES-256 для даних і TLS для зв'язку). У більшості реальних сценаріїв це ефективно запобігає перехопленню трафіку зловмисниками. Зламати такі шифри в реальному часі практично неможливо, тому витік відеоданих через перехоплення малоймовірний. Але у деяких випадках дешеві пристрої IoT використовують застарілі версії протоколів або допускають помилки в обробці ключів, що створює ризик беспеці.

Висновок: Практично безпечний для користувачів, які користуються приладами відповідно до інструкції.

2. Автентифікація

Користувачі можуть увійти до свого облікового запису Tuya Smart за допомогою імені користувача та пароля. Якщо ввімкнено двофакторну автентифікацію (2FA), безпека значно підвищується. У реальних умовах багато користувачів ігнорують 2FA, роблячи облікові записи більш уразливими для злому.

У разі слабкого пароля або повторного використання одного пароля для кількох облікових записів зловмисники можуть отримати доступ за допомогою фішингу або грубої сили.

Висновок: Ефективно, якщо налаштовано правильно. Але це залежить від обізнаності користувачів.

3. Оновлення мікропрограми

Виробник регулярно випускає оновлення, які можна встановити через додаток. Це допомагає усунути виявлені вразливості та покращити функціональність. У багатьох випадках користувачі не оновлюють мікропрограму через відсутність повідомлень або нехтування безпекою.

Якщо оновлення не виконано, пристрої залишаються вразливими до відомих атак.

Висновок: ефективний лише за умови регулярного оновлення.

4. Сегментація мережі

Користувачі, які налаштовують окрему мережу для пристроїв IoT, отримують високий рівень захисту завдяки ізоляції камери від решти пристроїв у мережі. Для більшості користувачів це залишається недосяжним через складність налаштувань.

Без спеціальних знань користувачі залишають камери в стандартній домашній мережі, що може призвести до ризику скомпрометувати інші пристрої.

Висновок: дуже ефективний, але рідко застосовується.

5. Хмарне сховище

Tuya Smart надає сервіси хмарного сховища з високим рівнем захисту, сертифіковані за міжнародними стандартами. У реальних умовах дані, що зберігаються

в хмарі, менш вразливі до локальних атак (наприклад, фізичне видалення SD-карти). Ризик компрометації хмари існує, хоча й малоймовірний. Хмарне сховище коштує додаткових грошей, тому деякі користувачі відмовляються ним користуватися.

Висновок: надійне рішення для більшості користувачів, але не універсальне через додаткові витрати.

3.3.6 Висновок та рекомендації щодо методів безпеки Swizoo G9 Pro

Swizoo G9 Pro із додатком Tuya Smart добре відповідає основним принципам безпеки, але його ефективність сильно залежить від поведінки користувача та правильної конфігурації. Виробник забезпечує високу базову безпеку (AES-256, TLS, 2FA), але кінцеві користувачі часто не дають рекомендацій, що збільшує ризики.

Для забезпечення максимальної безпеки необхідний комплексний підхід: дотримання рекомендацій виробника, використання додаткових методів захисту (VPN, сегментація мережі) і регулярне оновлення програмного забезпечення.

Swizoo G9 Pro залишається надійним вибором для відеоспостереження, якщо врахувати ці аспекти.

Рекомендації користувачам:

- ✓ Увімкнути двофакторну автентифікацію. Це значно знижує ризик злому облікового запису навіть у разі втрати пароля.
- ✓ Оновіть прошивку і додаток Tuya Smart. Регулярні оновлення усувають відомі вразливості та підвищують стабільність.
- ✓ Використовуйте хмарне сховище. Це захистить ваші дані в разі фізичної крадіжки камери або пошкодження локальної пам’яті.
- ✓ Налаштуйте окрему мережу Wi-Fi для пристроїв IoT. Виділення окремої VLAN для камери зменшить ризик впливу на інші пристрої в разі зламу.
- ✓ Використовуйте складні паролі для Wi-Fi та облікових записів.Це базовий, але ефективний захист від більшості атак.

ВИСНОВКИ

У процесі виконання роботи було здійснено аналіз сучасного стану досліджень у сфері Інтернету речей з акцентом на охоронних системах, а також запропоновано практичні методи підвищення безпеки IoT-технологій. Проведений аналіз підтвердив, що стрімкий розвиток IoT, попри численні переваги, супроводжується значними ризиками, особливо в контексті кіберзахисту.

Розглянуті в роботі загрози безпеці IoT-технологій охоплюють усі рівні інфраструктури – від сенсорного до прикладного. Основними джерелами вразливостей є недоліки протоколів зв'язку, обмежені ресурси пристроїв, недостатньо захищене проміжне програмне забезпечення та шлюзи. Це підкреслює необхідність комплексного підходу до забезпечення безпеки.

У роботі запропоновано та детально проаналізовано низку ефективних методів захисту IoT:

- ✓ Шифрування даних (як симетричне, так і асиметричне), що дозволяє зменшити ризик витоку інформації.
- ✓ Блокчейн-технології, які забезпечують децентралізоване управління даними та підвищують стійкість до атак.
- ✓ Туманні обчислення, які надають переваги в обробці даних на крайових пристроях, зменшуючи затримки і покращуючи захист інформації.
- ✓ Машинне навчання для виявлення аномалій і прогнозування можливих атак.
- ✓ Периферійні обчислення, що оптимізують розподіл обчислювальних ресурсів та посилюють захист крайових пристроїв.

Практична частина роботи включала аналіз функціонування камери відеоспостереження Swizoo G9 Pro, підключеної через платформу Tuya Smart. Проведені експерименти підтвердили, що впровадження розроблених методів дозволяє значно підвищити рівень захищеності пристроїв IoT.

Практична значущість роботи полягає в можливості адаптації запропонованих підходів для використання в охоронних системах України, зокрема для захисту критичних об'єктів інфраструктури.

ПЕРЕЛІК ПОСИЛАНЬ

1. A. Gharaibeh, M. A. Salahuddin, S. J. Hussini, A. Khreishah, I. Khalil, M. Guizani, et al. Smart cities: A survey on data management security and enabling technologies. IEEE Communications Surveys & Tutorials, vol. 19, no. 4, 4th Quart. 2017, pages 2456–2501.
2. D. Eckhoff and I. Wagner. Privacy in the smart city—Applications technologies challenges and solutions. IEEE Communications Surveys & Tutorials, vol. 20, no. 1, 1st Quart. 2018, pages 489–516.
3. X. Xia, Y. Xiao, and W. Liang. ABSI: An adaptive binary splitting algorithm for malicious meter inspection in smart grid. IEEE Transactions on Information Forensics and Security, vol. 14, no. 2, 2019, pages 445–458.
4. V. Namboodiri, V. Aravinthan, S. N. Mohapatra, B. Karimi, and W. Jewell. Toward a secure wireless-based home area network for metering in smart grids. IEEE Systems Journal, vol. 8, no. 2, Jun. 2014, pages 509–520.
5. N. N. Dlamini and K. Johnston. The use benefits and challenges of using the Internet of Things (IoT) in retail businesses: A literature review. In Proceedings of the International Conference on Advanced Computing and Communication Engineering (ICACCE), Nov. 2016, pages 430–436.
6. A. C. Jose and R. Malekian. Improving smart home security: Integrating logical sensing into smart home. IEEE Sensors Journal, vol. 17, no. 13, Jul. 2017, pages 4269–4286.
7. Bridgera.com. IoT System | Sensors and Actuators [Електронний ресурс]. – Режим доступу: https://bridgera.com/IoT-system-sensors-actuators/.
8. S. Kumar, S. Sahoo, A. Mahapatra, A. K. Swain, and K. K. Mahapatra. Security enhancements to system on chip devices for IoT perception layer. In Proceedings of IEEE International Symposium on Nanoelectronic and Information Systems (iNIS), Dec. 2017, pages 151–156.
9. C.-H. Liao, H.-H. Shuai, and L.-C. Wang. Eavesdropping prevention for heterogeneous Internet of Things systems. In Proceedings of the 15th IEEE Annual

Consumer Communications & Networking Conference (CCNC), Jan. 2018, pages 1–2.

10. APWG. Phishing Activity Trends Report [Електронний ресурс]. – Режим доступу: https://docs.apwg.org/reports/apwg_trends_report_q4_2017.pdf.
11. C. Li and C. Chen. A multi-stage control method application in the fight against phishing attacks. In Proceedings of the 26th Computer Security Academy Communication Across Country, 2011, page 145.
12. C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas. DDoS in the IoT: Mirai and other botnets. Computer, vol. 50, no. 7, 2017, pages 80–84.
13. S. Bandyopadhyay, M. Sengupta, S. Maiti, and S. Dutta. A survey of middleware for Internet of Things. In Recent Trends in Wireless and Mobile Networks, Springer, 2011, pages 288–296.
14. M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke. Middleware for Internet of Things: A survey. IEEE Internet of Things Journal, vol. 3, no. 1, Feb. 2016, pages 70–95.
15. J. Kumar, B. Rajendran, B. S. Bindhumadhava, and N. S. C. Babu. XML wrapping attack mitigation using positional token. In Proceedings of the International Conference on Public Key Infrastructure and Applications (PKIA), Nov. 2017, pages 36–42.
16. WS Attacks. Attack Subtypes [Електронний ресурс]. – Режим доступу: https://www.ws-attacks.org/XML_Signature_Wrapping.
17. C. Fife. Securing the IoT Gateway [Електронний ресурс]. – Режим доступу: https://www.citrix.com/blogs/2015/07/24/securing-the-IoT-gateway/.
18. A. Stanciu, T.-C. Balan, C. Gerigan, and S. Zamfir. Securing the IoT gateway based on the hardware implementation of a multi-pattern search algorithm. In Proceedings of the International Conference on Optimization of Electrical and Electronic Equipment (OPTIM) and the International Aegean Conference on Electrical Machines and Power Electronics (ACEMP), May 2017, pages 1001–1006.

19. S.-C. Cha, J.-F. Chen, C. Su, and K.-H. Yeh. A blockchain connected gateway for BLE-based devices in the Internet of Things. IEEE Access, vol. 6, 2018, pages 24639–24649.
20. S. N. Swamy, D. Jadhav, and N. Kulkarni. Security threats in the application layer in IoT applications. In Proceedings of the International Conference on IoT in Social, Mobile, Analytics, and Cloud (I-SMAC), Feb. 2017, pages 477–480.
21. H. A. Abdul-Ghani, D. Konstantas, and M. Mahyoub. A comprehensive IoT attacks survey based on a building-blocked reference model. International Journal of Advanced Computer Science and Applications, vol. 9, no. 3, 2018, pages 355–373.
22. M. Kumar. How to Hack WiFi Password from Smart Doorbells [Електронний ресурс]. – Режим доступу: http://thehackernews.com/2016/01/doorbell-hacking-wifi-pasword.html.
23. A. Mosenia and N. K. Jha. A comprehensive study of security of Internet-of-Things. IEEE Transactions on Emerging Topics in Computing, vol. 5, no. 4, Dec. 2017, pages 586–602.
24. N. Kshetri. Can blockchain strengthen the Internet of Things? IT Professional, vol. 19, no. 4, 2017, pages 68–72.
25. W. Wang, P. Xu, and L. T. Yang. Secure data collection storage and access in cloud-assisted IoT. IEEE Cloud Computing, vol. 5, no. 4, Jul. 2018, pages 77–88.
26. S. Suhail, C. S. Hong, Z. U. Ahmad, F. Zafar, and A. Khan. Introducing secure provenance in IoT: Requirements and challenges. In Proceedings of the International Workshop on Secure Internet of Things (SIoT), Sep. 2016, pages 39–46.
27. D. Miller. Blockchain and the Internet of Things in the industrial sector. IT Professional, vol. 20, no. 3, 2018, pages 15–18.
28. T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang. Untangling blockchain: A data processing view of blockchain systems. IEEE Transactions on Knowledge and Data Engineering, vol. 30, no. 7, Jul. 2018, pages 1366–1385.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ

МАГІСТЕРСЬКА РОБОТА
на тему:
«БЕЗПЕКОВІ АСПЕКТИ ВПРОВАДЖЕННЯ ТЕХГОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ В ОХОРОННІ СИСТЕМИ»

Виконав: студент групи ІСДМ-61
Павленко Кирил Юрійович

Керівник: д.т.н., доцент кафедри
Інформаційних систем та технологій
Срібна Ірина Миколаївна

Київ – 2024

Метою дослідження аналіз вразливостей та використання інноваційних підходів, таких як блокчейн, шифрування даних, туманні й периферійні обчислення.

Об'єктом дослідження є технології Інтернету речей, що використовуються в охоронних системах.

Предметом дослідження є методи забезпечення безпеки IoT-технологій на різних рівнях інфраструктури та в рамках їх практичного застосування.

Для досягнення цієї мети поставлені наступні завдання:

- ✓ Провести аналіз вразливостей на різних рівнях IoT-інфраструктури.
- ✓ Вивчити сучасні методи захисту IoT, включаючи шифрування, блокчейн та інші технології.
- ✓ Провести практичний аналіз функціонування камери Swizoo G9 Pro та оцінити ефективність існуючих засобів захисту.
- ✓ Розробити рекомендації щодо інтеграції IoT у сферу охоронних систем із підвищенням їх безпеки.

Інтернет речей (IoT) відіграє ключову роль у сучасних охоронних системах, забезпечуючи підвищення ефективності, гнучкості та надійності. Його використання дозволяє:

- **Моніторинг у реальному часі**.
- **Швидке реагування**.
- **Централізоване управління**.
- **Аналітика і прогнозування**.

Рівень сприйняття:
- Фізичні атаки;
- Перехоплення даних;
- Підробка даних;

Мережевий рівень:
- Атаки типу Man-in-the-Middle;
- DDoS-атаки;
- Мережеві вторгнення;

Рівень проміжного ПЗ:
- Уразливості в ПЗ;
- Неавторизований доступ;
- Впровадження шкідливого коду;

Прикладний рівень:
- Соціальна інженерія;
- Атаки на кінцеві додатки;
- Недостатня автентифікація;

Методи захисту IoT-систем

Метод	Переваги	Недоліки	Типові сценарії
Шифрування даних	Конфіденційність, простота інтеграції	Управління ключами	Захист передачі та зберігання даних
Блокчейн	Децентралізація, незмінність	Високі витрати, затримки	Контроль доступу, реєстрація подій
Туманні обчислення	Зниження затримок, локальна обробка	Складність інфраструктури	Обробка даних у реальному часі
Машинне навчання	Виявлення аномалій, адаптивність	Високі ресурси, помилки класифікації	Аналіз трафіку, виявлення атак
Периферійні обчислення	Мінімальна затримка, автономність	Обмежені ресурси пристроїв	Локальна обробка на IoT-пристроях

Практичний кейс: камера Swizoo G9 Pro з додатком Tuya Smart

```
const key = "0123456789abcdef";
const plaintext = "Student Pavlenko Kyryl";
const des = new DES(key);
const ciphertext = des.encrypt(plaintext);
const decrypted = des.decrypt(ciphertext);
console.log("Plaintext: ", plaintext);
console.log("Ciphertext: ", ciphertext);
console.log("Decrypted: ", decrypted);
class DES {
constructor(key) {
        this.key = CryptoJS.enc.Hex.parse(key);
}
encrypt(plaintext) {
    const encrypted = CryptoJS.DES.encrypt(
    plaintext,
    this.key,
    { mode: CryptoJS.mode.ECB }
    );
    return encrypted.ciphertext.toString();
}
decrypt(ciphertext) {
const ciphertextHex =
CryptoJS.enc.Hex.parse(ciphertext);
const decrypted = CryptoJS.DES.decrypt(
    { ciphertext: ciphertextHex },
    this.key,
    { mode: CryptoJS.mode.ECB }
    );
        return
decrypted.toString(CryptoJS.enc.Utf8);
}
}
```

Запропоновані заходи безпеки

AES 256

Шифрування даних

AES-256 для даних, TLS для зв'язку.

Автентифікація

Вхід через ім'я користувача та пароль, 2FA підвищує безпеку.

Оновлення мікропрограми

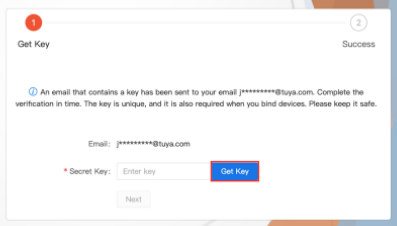
Регулярні оновлення зменшують ризики.

Сегментація мережі

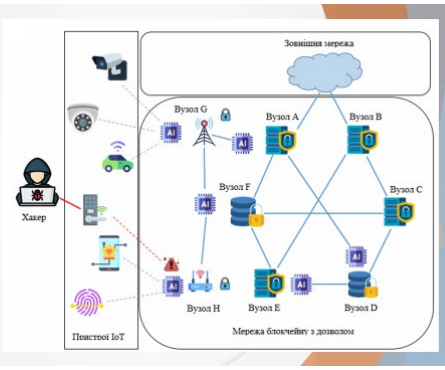
Ізоляція камери підвищує захист.

Хмарне сховище

Захищено за міжнародними стандартами.



Архітектура на основі штучного інтелекту та блокчейну



Висновки

У процесі виконання роботи було здійснено аналіз сучасного стану досліджень у сфері Інтернету речей з акцентом на охоронних системах, а також запропоновано практичні методи підвищення безпеки IoT-технологій. Проведений аналіз підтвердив, що стрімкий розвиток IoT, попри численні переваги, супроводжується значними ризиками, особливо в контексті кіберзахисту.

Розглянуті в роботі загрози безпеці IoT-технологій охоплюють усі рівні інфраструктури – від сенсорного до прикладного. Основними джерелами вразливостей є недоліки протоколів зв'язку, обмежені ресурси пристроїв, недостатньо захищене проміжне програмне забезпечення та шлюзи. Це підкреслює необхідність комплексного підходу до забезпечення безпеки.

Практична частина роботи включала аналіз функціонування камери відеоспостереження Swizoo G9 Pro, підключеної через платформу Tuya Smart. Проведені аналізи підтвердили, що впровадження розроблених методів дозволяє значно підвищити рівень захищеності пристроїв IoT.

Практична значущість роботи полягає в можливості адаптації запропонованих підходів для використання в охоронних системах України, зокрема для захисту критичних об'єктів інфраструктури.

Павленко К.Ю. «Безпекові аспекти застосування технологій інтернету речей в охоронних системах для інтелектуальних житлових та міських рішень». Тези доповіді на II Всеукраїнську науково-технічну конференцію «Технологічні горизонти: дослідження та застосування інформаційних технологій для технологічного прогресу України і світу». – Київ, 18 листопада 2024 р.

Павленко К.Ю. «Моделювання загроз безпеці в IoT-системах охорони: підходи до мінімізації ризиків». Тези доповіді на VII Всеукраїнська науково-технічна конференція «Комп'ютерні технології: інновації, проблеми, рішення». – Житомир, 2 грудня 2024 р.

Дякую за увагу!