НАЦІОНАЛЬНИЙ УНІВЕРСТИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Факультет/(ННІ) Інформаційних Технологій

ПОГОДЖЕНО

Декан факультету (Директор ННІ)
Інформаційних Технологій кібербезпеки
(назва факультету (ННІ))

_____ Ігор БОЛБОТ
(підпис) (ім'я ПРІЗВИЩЕ)

"___" _____ 2025 р.

ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ

Завідувач кафедри
Кафедра комп'ютерних систем, мереж та
(назва кафедри)

_____ Дмитро КАСАТКІН
(підпис) (ім'я ПРІЗВИЩЕ)

"___" _____ 2025 р.

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему: Дослідження безпеки систем «Smart City» на базі контролю доступу

Спеціальність 123 Комп'ютерна інженерія
(код і найменування)

Освітня програма Комп'ютерні системи захисту інформації
(назва)

Орієнтація освітньої програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Гарант освітньої програми
д.п.н, професор _____ Сергій МАМЧЕНКО
(науковий ступінь та вчене звання) (підпис) (ім'я ПРІЗВИЩЕ)

Керівник магістерської кваліфікаційної роботи
к.пед.н., доцент _____ Дмитро КАСАТКІН
(науковий ступінь та вчене звання) (підпис) (ім'я ПРІЗВИЩЕ)

Виконав _____ Сергій ФЕСУН
(підпис) ((ім'я ПРІЗВИЩЕ здобувача)

КИЇВ – 2025

НАЦІОНАЛЬНИЙ УНІВЕРСТИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Факультет (ННІ) Інформаційних Технологій

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____
К.п.н., доцент _____ **Дмитро КАСАТКІН**
(науковий ступінь, вчене звання) (підпис) (ім'я ПРІЗВИЩЕ)
"____" _____2025року

З А В Д А Н Н Я

ДО ВИКОНАННЯ МАГІСТЕРСЬКОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ ЗДОБУВАЧУ

Фесуну Сергію Юрійовичу
(прізвище, ім'я, по батькові)

Спеціальність 123 Комп'ютерна інженерія
(код і найменування)

Освітня програма _ Комп'ютерні системи захисту інформації
(назва)

Орієнтація освітньої програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Тема магістерської кваліфікаційної роботи Дослідження безпеки систем «Smart City» на базі контролю доступу
затверджена наказом ректора НУБіП України від «26» жовтня 2024 р. №1941 «С»

Термін подання завершеної роботи на кафедру 15.11.2025
(рік, місяць, число)

Вихідні дані до магістерської кваліфікаційної роботи Об'єктом дослідження є комплексні системи Smart City, що включають апаратні та програмні засоби керування доступом до інфраструктурних об'єктів міста. Основною особливістю є інтеграція великої кількості різнорідних вузлів, що працюють у реальному часі та забезпечують безперервну взаємодію на рівні міської екосистеми.

Перелік питань, що підлягають дослідженню:

1. Які уразливості виникають у системах контролю доступу Smart City під час обміну даними між пристроями?
2. Рішення кібербезпеки для аналізу вразливостей
3. Які методи уніфікації та стандартизації можуть підвищити безпечність інтегрованих рішень?

Дата видачі завдання "15" листопада 2024 р.

Керівник магістерської кваліфікаційної роботи

к.пед.н., доцент _____ Дмитро КАСАТКІН
(науковий ступінь та вчене звання) (підпис) (ім'я ПРІЗВИЩЕ)

Виконав _____ Сергій ФЕСУН
(ім'я ПРІЗВИЩЕ)

РЕФЕРАТ

Дипломна робота «Потенційні загрози інтернету речей і способи їх подолання» складається з переліку умовних скорочень, вступу, основної частини, що містить 3 розділи, висновків і списку використаних джерел. Загальний обсяг роботи – 59 сторінок. Робота містить 6 рисунків та 1 таблицю. Список використаних джерел включає 27 одиниць.

Відповідно до мети дослідження, у дипломній роботі проводиться аналіз найпоширеніших способів захисту від загроз приладів та сервісів IoT в середовищі Smart City. Проведено дослідження технологій, що гарантують безпеку і вплив використання цих технологій на затримку передачі даних та роботу технологій з точки зору енергоспоживання.

Ключові слова: Smart City, IoT, безпека, FOG, Blockchaine, захист даних

ABSTRACT

Thesis "Potential threats of the Internet of Things and ways to overcome them" consists of a list of abbreviations, introduction, main part, containing 3 sections, conclusions and a list of sources used. The total volume of the work is 59 pages.

The work contains 6 figures and 1 table. The list of used sources includes 27 units.

For research purposes, the thesis analyses the most common methods of protection against threats of Iot devices and services in the Smart City environment. A study has been carried out on technologies to guarantee safety and the impact of the use of these technologies on the delay of data transmission and the operation of technologies in terms of energy consumption.

Keywords: IoT, security, FOG, Blockchaine, data protection, Smart City.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

IoT	(Internet of Things) - Інтернет речей
ІКТ	Інформаційно-комунікаційні технології
GPS	(Global Positioning System) – глобальна система позиціонування;
ПЗ	програмне забезпечення;
LPWAN	(Low-power Wide-area Network) - енергоефективна мережа далекого радіусу дії;
Li-Fi	Li-Fi (Light Fidelity) — Плазмовий інтернет;
IM	(Instant messaging) – миттєві повідомлення;
WSNS	(Wireless Sensor Networks) - бездротові сенсорні мережі;
VSNS	(Virtual Sensor Networks) - віртуальні сенсорні мережі;
VANETS	(Vehicle Ad hoc NETworks) – мережі зв'язку транспортних засобів;
PAN	(Personal Area Network)- персональні обчислювальні мережі;
PKI	(Public Key Infrastructure) – інфраструктура відкритих ключів;
DoS	(Denial of Service) - відмова в обслуговуванні;
IIoT	(Industrial Internet of Things) – промисловий інтернет речей;
BFAN	(Blockchain та Fog Based Architecture) -блокчейн та туманна архітектура
SLA	(Service-level agreement) - угода між постачальником послуг і користувачем про рівень послуг
QOS	(Quality of Service) – якість обслуговування
Pow	(Proof-of-work) – докази роботи
FN	(Fog node) – туманний вузол
P2P	(peer-to-peer) – вузол до вузла
AI	(Artificial intelligence) – штучний інтелект;

ВСТУП

Стрімкий розвиток Internet of things в сучасному своєму становищі несе в собі не тільки переваги, але і значні ризики та загрози безпеці людини та і іншим системам.

Ці розумні пристрої реалізуються з різними, часто сильно різними технологіями, що дозволяє з користю використовувати різноманітність технологій, які можуть бути краще використані для кожного девайсу .Оскільки ці системи ростуть в розмірі та доступності, через них також проходить більше даних.

У міру збільшення кількості таких пристроїв ми повинні бути переконані , що пристрої IoT не пропонують зловмисникам нових векторів, завдяки яким безпека та конфіденційність користувачів можуть бути порушені.

Щоб бути в змозі захистити систему IoT, нам потрібно знати, що вона собою представляє - яку архітектуру використовує, як вона працює, які компоненти і частини вона має, які протоколи використовуються, основні галузі застосування, і так далі. Знаючи всі залежності, сильні і слабкі сторони, ми можемо отримати повне і точне уявлення про типи векторів атаки, до яких уразливі системи IoT. У дипломній роботі представлені уразливості, які типові для різних типів систем IoT, результати, до яких прагнуть нападники, потенційні вигоди, які могли б отримати нападники, і наслідки, які могли б виникнути в разі успіху нападу. Особлива увага приділяється можливостям захисту системи IoT від таких атак і шляхи, які можуть бути значно покращені. При розгляді питання про захист інформації в середовищі IoT, головні питання, які потребують втручання це забезпечення безпеки, захист засобів комунікацій всередині мережі, а також від різних видів загроз безпеки ззовні. В своїй дипломній роботі я розглядаю та

порівнюю два теоретично можливих варіантів забезпечення безпеки пристроїв та сервісів IoT в середовищі Smart City .

Таким чином, ***об'єктом досліджень*** є Blockchain та Fog Based Architecture для IoT в середовищі Smart City

Предмет досліджень – є методи запобігання взлому та атак на системи IoT в середовищі Smart City

Мета досліджень – є підвищення рівня безпеки в Smart city

Наукова новизна дослідження – аналіз застосування різних комбінацій технологій і їх вплив на якість та захищеність передачі даних середовищі IoT.

РОЗДІЛ 1. АНАЛІЗ ІСНУЮЧИХ ЗАГРОЗ, СУТНІСТЬ ТА ПОНЯТТЯ ТЕХНОЛОГІЇ

1.1 Розуміння концепції розумного міста

Сучасна цивілізація характеризується високими темпами розвитку, що забезпечує умови для швидкого впровадження та адаптації новітніх технологій. Така динаміка є природним елементом еволюційних процесів, які породжують як позитивні зміни, так і низку потенційних ризиків.

Одними з головних викликів теперішнього етапу розвитку суспільства виступають економічні дисбаланси, соціальні проблеми, інтенсивне зростання чисельності населення, надмірне споживання природних ресурсів, збільшення енергетичних потреб, забруднення довкілля та глобальні кліматичні трансформації [24, 25].

Сучасний світ не лише швидко змінюється, а й демонструє високу відкритість до технологічних інновацій. Він функціонує як інтегрована багатовимірна система, у якій взаємодіють фізичні, цифрові та соціальні елементи. Крім того, інформаційний прорив, посилення інноваційної активності та розвиток підприємництва істотно трансформували міські процеси та інші сфери суспільного життя [26].

Одним із найперспективніших напрямів вирішення проблем, пов’язаних із зростанням міського населення, є концепція інтелектуального міста. Протягом тривалого часу вона зазнавала різних інтерпретацій і модифікацій, що формувалися як науковою спільнотою, так і фахівцями-практиками. Перші концептуальні підходи з’явилися у 1990-х роках, а вже на початку 2000-х років

ідея набула широкого поширення та практичного інтересу [27].

Інтелектуальні міста покликані реагувати на інтенсивні процеси урбанізації та поєднують комплекс взаємопов'язаних технологічних, соціальних та інфраструктурних компонентів. Їхнє формування та розвиток активно підтримують міжнародні організації, наукові інституції й технологічні компанії. У результаті таких досліджень було створено низку економічних програм та ініціатив, спрямованих на підтримку і впровадження концепції Smart City [28, 29].

У сучасних підходах розумне місто трактують як територію, що використовує цифрові, інформаційно-комунікаційні та телекомунікаційні технології для оптимізації інфраструктури, підвищення ефективності наданих послуг і створення комфортних умов для життя населення та діяльності підприємств [30]. Водночас Smart City – це не тільки технологічний комплекс, а й стратегічне бачення розвитку міського середовища, у якому цифровізація та інновації виступають фундаментом сталого розвитку. Технології нового покоління виконують функцію аналогічну до нервової системи організму, забезпечуючи адаптивність і здатність міста оперативно реагувати на внутрішні й зовнішні зміни [31].

Застосування інструментів збору, оброблення та аналізу інформації, включно з даними, що надходять у режимі реального часу, є базовим чинником розвитку інтелектуальних міст [32]. Аналітика отриманих даних надає можливість міським адміністраціям ефективніше управляти інфраструктурою та підвищувати якість послуг – від систем поводження з відходами до оптимізації громадського транспорту. Такі перетворення сприяють покращенню умов життя мешканців [33].

Підвищення ефективності міських сервісів одночасно веде до скорочення обсягів парникових викидів, що відповідає глобальним кліматичним ініціативам,

та сприяє покращенню стану атмосферного повітря в містах [34]. Крім того, технологічні рішення Smart City здатні стимулювати економічне зростання завдяки модернізованій інфраструктурі, створенню нових робочих місць і розширенню інноваційних можливостей для бізнес-структур [35].

Одним з основних елементів концепції інтелектуального міста є високотехнологічна інфраструктура. Її ключове завдання полягає у впровадженні сучасних технологічних рішень у фізичний простір міста з метою раціонального використання ресурсів та підвищення ефективності функціонування міських сервісів [36]..

Основні елементи міської інфраструктури нового

покоління:

1) розумні енергетичні мережі (Smart Grids),

2) системи, що застосовують цифрові технології для контролю процесів генерації, розподілу та споживання електроенергії,

3) зменшують втрати енергетичних ресурсів, скорочують витрати та забезпечують стабільність електропостачання завдяки адаптації до змін попиту,

4) інтелектуальна транспортна система (Smart Transportation),

5) використання датчиків, супутникового позиціонування та алгоритмів аналізу даних для оптимізації руху транспорту, мінімізації заторів і підвищення ефективності громадського транспорту,

6) включає адаптивні світлофори, автономні транспортні засоби та цифрові рішення для організації паркування,

7) сталий розвиток будівель (Sustainable Buildings).

Використання технологій Інтернету речей (IoT) забезпечує можливість автоматизованого керування мікрокліматичними параметрами будівель, включно з системами опалення, кондиціонування, вентиляції, освітлення та засобами безпеки. Застосування таких рішень сприяє підвищенню енергоефективності, оптимізації витрат та формуванню більш безпечного середовища для користувачів.

Проєктування будівель із акцентом на енергоощадність та екологічну стійкість є важливим напрямом розвитку сучасних міст, оскільки воно сприяє зменшенню рівня забруднення та раціональному використанню ресурсів [40].

Концепція інтелектуального міста становить одну з ключових стратегій розвитку сучасних мегаполісів [41]. Вона передбачає не лише оптимізацію процесів управління міськими ресурсами, а й значне підвищення рівня комфорту та добробуту мешканців шляхом інтеграції інноваційних технологій у всі сфери функціонування міської інфраструктури [42]. Використання технологій Інтернету речей (IoT), штучного інтелекту (AI), великих даних (Big Data) та автоматизованих систем адміністрування створює передумови для формування безпечного, ефективного і екологічно збалансованого міського середовища.

Реалізація концепції Smart City потребує активної координації між державним і приватним секторами. Залучення іноземних інвестицій, впровадження інноваційних технологій та формування сприятливого нормативно-правового середовища є необхідними умовами для успішної адаптації міст до сучасних викликів. Не менш важливим чинником є участь громадськості у процесах цифрової трансформації, що забезпечує підвищення рівня довіри до нових рішень та сприяє їх більш ефективному впровадженню.

Подальший розвиток інтелектуальних міст охоплює широке застосування екологічно чистих джерел енергії, автономних транспортних систем, інноваційних рішень у сфері водопостачання, управління відходами та енергоресурсами. Ці зміни сприятимуть зниженню екологічного навантаження, оптимізації споживання ресурсів і загальному підвищенню рівня комфорту життя населення [46]. Таким чином, концепція Smart City є не тимчасовим трендом, а стратегічним напрямом довгострокового розвитку, спрямованим на забезпечення безпечного, зручного та сталого міського середовища [47].

1.2 Впровадження концепції інтелектуального міста

Одним із провідних завдань місцевих органів влади є ефективна імплементація концепції інтелектуального міста. Незважаючи на відносну новизну цієї ідеї, інтерес до неї є стабільно високим, особливо з огляду на

прогнози, відповідно до яких до 2050 року близько 70% населення світу проживатиме в міських агломераціях.

Результати численних досліджень показують, що за умови належного планування та управління урбанізація може стати важливим драйвером сталого розвитку, підвищуючи продуктивність та стимулюючи інноваційні процеси. Це набуває особливого значення, зважаючи на те, що міста формують понад 80% світового валового внутрішнього продукту [50]. Важливу роль у прискоренні впровадження технологій Smart City відіграла цифровізація, що стрімко активізувалася в умовах пандемії. Багато міських сервісів потребували невідкладної модернізації, що спричинило швидке поширення цифрових рішень та їх інтеграцію у процеси міського управління.

На думку експертів, ефективність концепції інтелектуального міста базується на глибокій інтеграції цифрових технологій у міські системи з метою удосконалення інфраструктури, підвищення результативності наданих послуг та створення сприятливих умов для життєдіяльності населення та розвитку бізнесу [52].

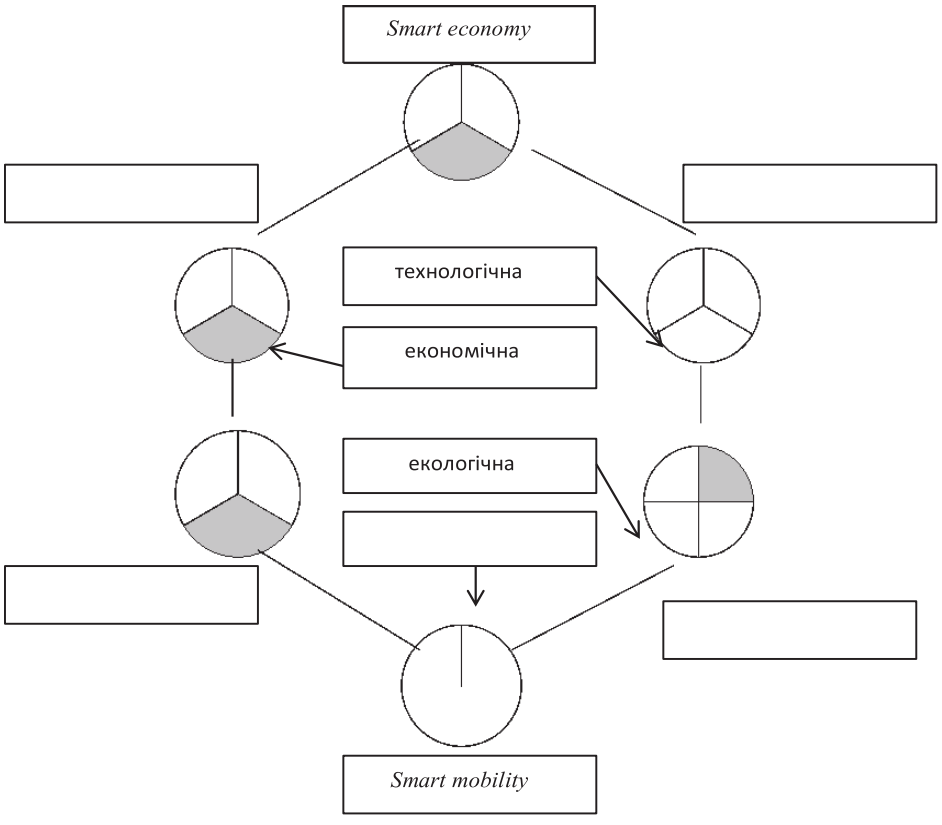

Рис. 1. Складові моделі «розумного міста»

Деякі науковці трактують концепцію розумного міста як форму інтегрованого інтелектуального потенціалу, що поєднує технологічні, соціальні, економічні та інноваційні чинники розвитку урбанізованого середовища [53]. Інші дослідники розглядають інтелектуальне місто як високотехнологічний мегаполіс, спеціально спроєктований для забезпечення потреб населення, органів державної влади та бізнес-структур.

Подібні підходи спрямовані на вирішення широкого кола завдань, що стосуються сталого розвитку та вдосконалення систем управління міським простором [55]. Незважаючи на масштабність та високі вимоги до ресурсів, ці стратегії є критично важливими для ефективної урбанізації та потребують значних інвестицій. Оскільки їх реалізація має довгостроковий вплив, упровадження таких рішень вимагає ретельного аналізу як під час розроблення політики, так і на всіх етапах її практичного застосування.

Проєктування розумних міст повинно здійснюватися на основі стратегічного планування з орієнтацією на досягнення конкретних економічних, соціальних та урбаністичних цілей. Це підтверджує актуальність подальших наукових досліджень у сфері Smart City, спрямованих на вдосконалення існуючих концептуальних моделей та формування ефективних механізмів їх реалізації.

1.2 Ключові елементи інтелектуального міста.

Численні дослідники розділили концепцію інтелектуального міста на кілька ключових аспектів і вимірів, оскільки його управління є багаторівневим та складним процесом. На основі аналізу наукових праць було визначено основні складові, що формують розумне місто[60].

Таблиця 1.1. Переваги та недоліки міст по впровадженню інноваційних технологій «SMART міста»

Міста	Переваги	Недоліки
Барселона	– інтелектуальні парковочні системи; – системи моніторингу трафіку заторів; – сонячні панелі; – гібридний автотранспорт	– не досить зручне використання системи прокату транспорту для гостей міста; – каскадні збої в електромережі
Лондон	– використання альтернативних джерел енергії; – модернізація застарілої системи метрополітену; – зменшення затрат населення	– технологічна проблема модернізації; – фінансові затрати містян на модернізацію помешкань щодо нових стандартів житла
Сінгапур	– повна автоматизація міста; – контроль всіх сфер життя; – прогресивна сфера медицини	– велика вірогідність крадіжки персональних даних; – акумулювання всіх даних в одних «руках»

Було визначено шість ключових напрямів, що забезпечують повноцінне функціонування інтелектуального міста [61]. Для досягнення високого рівня ефективності урбаністичного середовища необхідно приділяти належну увагу кожній із цих сфер, підтримувати їхній розвиток і використовувати як фундамент для формування міської взаємодії та комунікації.

Окремі компоненти виявляються більш важливими для населення, ніж інші. Наприклад, мешканці сучасних мегаполісів найчастіше акцентують увагу на питаннях мобільності та розвитку інфраструктури, адже саме вони безпосередньо впливають на якість повсякденного життя. Водночас екологічна стійкість і якісне міське управління розглядаються громадянами як проміжні, але все ж значущі пріоритети.

Цей напрям охоплює розвиток інноваційного підприємництва, цифрової торгівлі та впровадження різноманітних технологічних рішень, які сприяють підвищенню продуктивності та оптимізації використання ресурсів. Основними характеристиками інтелектуальної економіки є розширення можливостей бізнесу, створення сучасних робочих місць та прогрес у високотехнологічних галузях.

Цифровізація виробничих процесів, застосування штучного інтелекту, інноваційні методи виготовлення продукції та інтеграція міст у глобальні економічні системи сприяють активному залученню інвестицій, збільшенню туристичного потоку та приваблению висококваліфікованих кадрів. Такі зміни позитивно впливають на загальний економічний розвиток міста.

Разом із тим інтенсивний економічний ріст може призводити до виснаження природних ресурсів, що потребує впровадження сучасних

механізмів екологічного менеджменту та політики раціонального використання ресурсів.

Інтелектуальне управління міськими процесами передбачає інтеграцію технологічних інструментів, нормотворчих ініціатив та активної громадської участі з метою підвищення ефективності муніципального адміністрування. Використання інформаційно-комунікаційних технологій забезпечує прозорість державних процедур, покращує якість послуг і стимулює залучення громадян до ухвалення управлінських рішень.

Розгортання інтегрованих цифрових платформ дозволяє централізувати надання адміністративних сервісів, що сприяє скороченню бюрократичних бар'єрів. Застосування принципів електронного урядування (e-Government) та електронної демократії (e-Democracy) сприяє підвищенню відкритості влади, розширенню доступу до державних послуг і зміцненню довіри населення.

Ключові елементи інноваційного управління охоплюють:

1. цифрову комунікацію між мешканцями та органами влади;
2. відкритий доступ до державної інформації й адміністративних послуг;
3. використання великих даних (Big Data) і штучного інтелекту для підтримки управлінських рішень;
4. автоматизацію адміністративних процесів для зниження бюрократичного навантаження.

Забезпечення рівного доступу до цифрових сервісів для всіх груп населення є важливим чинником соціальної інклюзії та сприяє більш ефективному використанню міських можливостей.

Інтелектуальна мобільність та транспорт

Розвиток сучасних транспортних систем має критичне значення для зменшення заторів, підвищення якості пасажирських перевезень і скорочення негативного впливу транспорту на довкілля. Інтелектуальні транспортні системи (ITS) та технології Інтернету речей (IoT) забезпечують ефективне управління транспортними потоками, оптимізацію дорожнього руху та покращення функціонування громадського транспорту.

Використання IoT, штучного інтелекту та блокчейн-технологій також сприяє ефективному моніторингу якості повітря, управлінню відходами та забезпеченню раціонального енергоспоживання.

Основні екологічні ініціативи включають:

1. застосування відновлюваних джерел енергії для зменшення парникових викидів;
2. впровадження інтелектуального управління відходами за допомогою сенсорних систем і «розумних» контейнерів;
3. безперервний екологічний моніторинг для зменшення ризиків для здоров'я населення.

Майбутнє сталого міського розвитку значною мірою залежить від ефективної екологічної політики, спрямованої на покращення умов життя мешканців. Досягнення балансу між економічним зростанням і збереженням довкілля дозволяє формувати гармонійне міське середовище, у якому жоден із цих чинників не потребує компромісних втрат [77].

1.3 Система виявлення та запобігання вторгненням

Система виявлення вторгнень (IDS, Intrusion Detection System) – це технологічний інструмент, призначений для фіксації загроз та спроб несанкціонованого доступу шляхом детального аналізу мережевого трафіку [43]. IDS функціонує у безперервному режимі, здійснюючи цілодобовий моніторинг мережевої активності, контролюючи поведінку користувачів та формуючи аналітичні звіти для фахівців із безпеки.

Основним призначенням IDS є виявлення будь-яких підозрілих дій, зокрема:

- атак на мережеві сервіси, що мають відомі вразливості;
- спроб отримання розширених прав доступу в системі;
- несанкціонованих маніпуляцій з конфіденційними файлами;
- активності шкідливого програмного забезпечення (вірусів, троянських програмних модулів, мережевих черв'яків тощо).

Інша система – IPS (Intrusion Prevention System) – працює в режимі реального часу, здійснюючи аналіз трафіку для виявлення небезпечних дій та зіставляючи їх із заздалегідь визначеними профілями загроз. Головне призначення IPS полягає в тому, щоб зупинити атаку ще на стадії її виконання та запобігти можливому збитку.

Для створення комплексної системи захисту компанії поєднують IDS/IPS із брандмауерами (файрволами) та маршрутизаторами. Відмінність між цими системами полягає у функціональному призначенні: брандмауери контролюють мережевий трафік за IP-адресами та портами відповідно до заданих правил, дозволяючи або блокуючи його.

Файрвол аналізує пакети, порівнюючи їх із дозволеними сигнатурами, і працює за таким принципом:

- якщо пакет відповідає дозволеним правилам, він пропускається далі;
- якщо ні — трафік блокується.

Файрвол виступає початковим рубежем оборони, запобігаючи проникненню базових загроз у мережу. Проте його функціонал обмежений, адже він здатний визначати тільки певні категорії атак. Тому IDS/IPS зазвичай розміщують між зовнішнім і внутрішнім брандмауером, що дозволяє здійснювати поглиблений аналіз мережевих потоків.

IDS/IPS часто інтегрують між мережевим інтерфейсом та веб-сервером, що забезпечує можливість аналізувати всі вхідні пакети та співставляти їх із базою відомих загроз. Такий підхід створює додатковий рівень безпеки для веб-ресурсів і мінімізує ризики несанкціонованих втручань.

Інтернет речей (IoT) у міській інфраструктурі. Запровадження технологій Інтернету речей у міське середовище формує новий етап еволюції урбаністики, трансформуючи принципи проєктування, управління та експлуатації міських систем. У процесі розширення міських територій міста стикаються з численними викликами: транспортними перевантаженнями, екологічними проблемами, значним енергоспоживанням та питаннями громадської безпеки. IoT стає ефективним інструментом для вирішення цих проблем, надаючи технологічні

підходи, які оптимізують міські процеси та адаптують їх до потреб XXI століття [24, 26].

Застосування IoT у міському господарстві. Інтернет речей знаходить широке застосування в різних компонентах міської інфраструктури, зокрема:

- транспорті – інтелектуальні системи керування дорожнім рухом дозволяють мінімізувати затори, скоротити викиди CO_2 та підвищити комфорт мобільності;
- енергетиці – розумні електромережі (smart grids) забезпечують оптимальне енергоспоживання, інтеграцію відновлюваних джерел енергії та підвищення стійкості енергосистем;
- комунальному господарстві – IoT-рішення в галузі управління відходами, водопостачанням та екологічного моніторингу істотно підвищують результативність міських сервісів і якість життя населення;
- міській екосистемі та управлінні ресурсами – аналіз даних з розгалуженої мережі підключених пристроїв дає можливість органам влади ухвалювати зважені рішення, що враховують економічні, соціальні та екологічні чинники.

Сучасні цифрові технології формують основу інтелектуальних міст, роблячи їх ефективнішими, екологічно відповідальнішими та більш комфортними для проживання. Інтернет речей відіграє ключову роль у цій трансформації, забезпечуючи взаємодію між фізичними пристроями та інформаційними системами для збору даних, їх аналізу та оптимізації міських процесів [31].

Впровадження IoT у системи управління міськими ресурсами підвищує адаптивність міста до зовнішніх впливів, покращує його стійкість та сприяє сталому розвитку — критично важливому аспекту в умовах інтенсивної урбанізації.

Безпека Smart City. Ефективне функціонування концепції Smart City передбачає впровадження надійних механізмів кібербезпеки, здатних забезпечити безпечну взаємодію між міськими службами, громадянами та інфраструктурою. У сучасних системах міської безпеки простежуються такі

проблеми підвищена вразливість до кібератак, орієнтованих на централізовані системи управління.

Складнощі з ідентифікацією та контролем доступу до критично важливих міських об’єктів.

1) відсутність прозорих механізмів аудиту дій службових осіб та користувачів,

2) високі корупційні ризики, пов’язані з розподілом прав доступу,

3) недостатній рівень автоматизації у системах реагування на потенційні загрози.

1.4 Проблеми безпеки в середовищі Smart city

Світ вступає в етап масштабної еволюції концепції Розумних Міст. Вони формуються як результат стрімкого розвитку інформаційних та комп'ютерних технологій, які водночас відкривають нові економічні й соціальні можливості та породжують нові виклики у сфері кібербезпеки й захисту приватності.

Переваги використання ІКТ та технологій Інтернету речей (IoT) у середовищі Smart City є значними. Інтелектуальні енергетичні лічильники, сучасні охоронні системи, смарт-пристрої медичного призначення та сенсорні системи для дому істотно підвищують якість життя населення. Міські сервіси та інфраструктура трансформуються під впливом появи нових взаємопов'язаних систем контролю, моніторингу та автоматизації, що забезпечують більш ефективне управління міським середовищем.

Однак ці переваги необхідно оцінювати з урахуванням потенційних ризиків, притаманних високозв'язному цифровому простору. Під час аналізу впровадження таких систем слід брати до уваги технічні, організаційні та фінансові аспекти, а також правові, соціальні та політичні умови функціонування міста.

Попри те, що традиційні кібератаки можуть завдавати шкоди конфіденційності, цілісності та доступності інформації, атаки на інфраструктуру IoT здатні створювати значно серйозніші наслідки, включно з ризиком для життя та здоров'я людей. Уже сьогодні зафіксовано численні інциденти злому бортових комп'ютерів автомобілів і літаків, а також втручання в роботу медичного обладнання, зокрема імплантованих інсулінових помп та інших критично важливих пристроїв.

Рис. 1.2. Структура центрального міського диспетчерського центра

З огляду на те, що перелік критично вразливих компонентів у Smart City охоплює системи опалення, мережі постачання продовольства, медичні установи, світлофорні об’єкти та транспортні мережі, які функціонують у тісній взаємодії, потенційні сценарії атак, що можуть виникати у такому середовищі, виглядають надзвичайно загрозливо. У результаті цього значення заходів кібербезпеки для IoT-інфраструктур різко зростає. Складність забезпечення безпеки IoT зумовлюється низкою чинників:

• Автономність та взаємодія пристроїв. Окрім ризиків, пов’язаних зі зловмисниками, важливо враховувати, що автономні IoT-пристрої можуть невидимо взаємодіяти між собою, впливаючи на життя людей у способи, які важко передбачити. Тому прогнозування загроз через регулярне та глибоке сканування вразливостей є необхідним, хоча залишається складним і потребує постійних досліджень та практичних напрацювань.

• Фрагментованість IoT-ландшафту. Інтернет речей характеризується високою неоднорідністю, оскільки його рішення базуються на різних архітектурах, протоколах, стандартах і програмних платформах. Кожне розумне місто розробляє власні технологічні підходи, реагуючи на місцеві виклики та можливості. До того ж, пристрої та їхні прошивки часто перебувають під захистом комерційної таємниці, а правове регулювання залишається недостатньо

сформованим. Бракує стандартизації, що створює так звані технологічні «ізольованості», до яких залучені численні виробники та оператори. Цей перелік загроз не є вичерпним, однак уже демонструє, наскільки важливим є захист мешканців Smart City за допомогою технічних, економічних, правових і соціальних інструментів.

У подальшому ці питання розглядаються в контексті того, що інтелектуальне місто є синергійною системою взаємодіючих пристроїв, які генерують великі обсяги даних і працюють в інтересах міської спільноти.

Конфіденційність та захист даних

Дані, що збираються IoT-пристроями, є ядром функціонування розумних міст. Проблема полягає в тому, що значна частина цієї інформації має конфіденційний характер і нерідко збирається без усвідомленої згоди громадян. Серед таких даних можуть бути:

– повідомлення,

– медичні й освітні записи,

– особисті фотографії,

– календарні події та місця зустрічей,

– банківська інформація,

– контакти та інші приватні дані.

Необхідність безпечної інтеграції IoT-даних з різних джерел є однією з ключових проблем, адже відсутні гарантовані довірчі відносини між учасниками взаємодії. Додаткову складність становлять питання ідентифікації власника та прав на інформацію: визначення того, кому належать дані, зібрані сенсорами, може бути вкрай складним. Особливо це критично, коли йдеться про фінансову або персональну інформацію.

Через повсюдність IoT-пристроїв межа між приватним та публічним простором поступово стирається, а користувачі можуть не усвідомлювати, де закінчується їхня інформаційна безпека. Сучасні сенсорні системи здатні «бачити», «чути» та «відчувати», передаючи величезні обсяги даних, що може створювати ризики для приватності. Наприклад, звичайні мобільні пристрої збирають інформацію про

місцезнаходження, фізичні показники організму (пульс, тиск), рухову активність, а додатки можуть передавати її без прямої згоди користувача.

Технології IoT також дозволяють отримувати детально ідентифіковані дані про домогосподарства: місцеперебування, переміщення, дії, соціальні зв'язки. Такі дані можуть бути об'єднані, що створює нові профілі користувачів та середовищ. Наприклад, «розумні» будівлі реагують на показники температури, вологості, диму, CO_2, освітленості чи зовнішньої присутності та можуть формувати детальний профіль поведінки мешканців.

Транспортні засоби як елементи Smart City оснащені бортовими комп'ютерами, GPS-модулями і бездротовими інтерфейсами, що дозволяє місту відстежувати маршрути, швидкість, час перебування у певному місці. Такий моніторинг може фактично відтворювати повний поведінковий портрет водія.

Розширення площини атак

У Smart City площина потенційних атак значно більша, ніж у традиційних IT-системах. Окрім класичних загроз (шкідливе ПЗ, фішинг, підроблені мережі, саботаж пристроїв), виникає ціла низка нових ризиків, зумовлених широким використанням сенсорів.

Сучасний смартфон містить десятки таких сенсорів:

GPS, мікрофони, камери, акселерометри, гіроскопи, датчики наближення, магнітометри, барометри, термометри, датчики освітленості, пульсометри тощо. Ці сенсори можуть фіксувати місце розташування, переміщення, звуки, розмови, фізичні параметри тіла, час і координати дій користувача. У результаті смартфон стає потенційним інструментом прихованого спостереження, особливо з огляду на можливість встановлення сторонніх програм.

Не менш небезпечними є атаки на протоколи ближнього радіусу дії. Наприклад:

– Zigbee піддається атакам типу перехоплення трафіку, декодування пакетів, маніпуляцій даними;

– Bluetooth – блуджекінг (спам сусіднім пристроям), блуснарфінг (крадіжка контактів), блютрубінг (неавторизований доступ до функцій пристрою).

1.5 Висновки

Здійснено огляд сучасного стану досліджень у сфері управління безпекою смарт-сервісів в умовах розумного міста. Проаналізовано існуючі підходи до забезпечення безпеки в IoT-інфраструктурах, досліджено архітектури та принципи функціонування програмно-визначених мереж (SDN), особливості використання смарт-контрактів, у контексті захисту даних і контролю доступу. Розглянуто переваги й обмеження централізованих та децентралізованих систем безпеки, що дозволило виявити основні недоліки сучасних рішень - обмежена гнучкість, відсутність механізмів адаптації до контексту середовища та ускладнене масштабування.

У результаті аналізу сформульовано базові вимоги до майбутнього методу управління безпекою, який має поєднувати переваги SDIoT та блокчейн-технологій, забезпечуючи динамічне прийняття рішень щодо автентифікації, авторизації та контролю доступу в умовах взаємодії великої кількості гетерогенних смарт-сервісів. Отримані висновки стали основою для побудови концептуальної моделі управління безпекою, що представлена в наступному розділі.

РОЗДІЛ 2. ВИКОРИСТАННЯ FOG COMPUTING, ЯК ГАРАНТ БЕЗПЕКИ В СЕРЕДОВИЩІ SMART CITY

2.1 Архітектрура Fog Computing

Останні досягнення в галузі апаратного забезпечення, програмного забезпечення та комунікаційних технологій — зокрема поява мереж 5G, Li-Fi та малопотужних глобальних мереж LPWAN — стали ключовим стимулом розвитку Інтернету речей (IoT). Хоча IoT традиційно асоціюється з мережею підключених пристроїв та об’єктів, його значення виходить далеко за межі простого мережевого з’єднання. Сьогодні технології IoT активно проникають у різні сфери життя, включаючи розумні будинки, інтелектуальні міста, моніторинг довкілля, промислове виробництво, сільське господарство, енергетику, медицину та охорону здоров’я.

Базова архітектура систем IoT для широкого спектра потенційних застосувань досі перебуває на етапі розроблення й вдосконалення. Паралельно ведеться масштабна робота зі стандартизації технологій та створення рішень для забезпечення сумісності, масштабованості, зручності використання, конфіденційності й безпеки.

Хмарні обчислення виступають основою для доступу до розподілених обчислювальних ресурсів з практично необмеженими можливостями зберігання й опрацювання даних. Хмарні сервіси доступні користувачам у моделях «інфраструктура як послуга» (IaaS), «платформа як послуга» (PaaS) та «програмне забезпечення як послуга» (SaaS). Сьогодні близько 90% користувачів інтернету у світі покладаються на хмарні технології [3]. На основі поточних тенденцій очевидно, що хмарні технології та IoT у майбутньому утворять єдину інтегровану екосистему — «хмару речей».

IoT отримує значні переваги від доступу до масштабованих ресурсів хмарної інфраструктури. Водночас хмара розширює власні можливості через

інтеграцію з IoT, забезпечуючи керування реальними послугами у динамічних і територіально розподілених середовищах.

Зростання ролі мобільних технологій та формування мобільно-хмарної екосистеми

За останнє десятиліття мобільний зв'язок демонструє стрімке зростання. Сучасні смартфони містять у середньому понад десять різних сенсорів, а поява розумних пристроїв суттєво збільшує кількість мобільних послуг, що доступні користувачам. Хмарні технології забезпечують низьку собівартість обчислень, масштабованість, гнучкі можливості зберігання та управління даними. Це робить інтеграцію хмарних обчислень і мобільних пристроїв фактично неминучою.

Однак створення такої інтегрованої системи супроводжується низкою викликів. Мобільні користувачі потребують значно ширшого спектра послуг, ніж користувачі традиційних комп'ютерів:

— хмарне зберігання;

— системи медичного моніторингу;

— IoT-сервіси;

— миттєві повідомлення (IM);

— рішення доповненої реальності;

— мультимедійні служби;

— навігаційні сервіси;

— кіберфізичні системи тощо.

Керування величезною кількістю запитів від мільярдів мобільних користувачів стає надзвичайно складним завданням для централізованої хмари [8]. Додатково мобільні пристрої обмежені ресурсами — потужністю процесора, обсягом пам'яті, енергоспоживанням — що робить часткове відвантаження завдань у хмару необхідним.

З огляду на зростаюче навантаження та значну відстань між користувачем і хмарним центром обробки даних, критично важливим стає забезпечення стабільного зв'язку в реальному часі. Щоб зменшити затримки під час обміну даними між IoT-пристроями або мобільними клієнтами та хмарою, формується

нова перспективна парадигма — Fog Computing (туманні обчислення). Вона дозволяє розміщувати обчислювальні ресурси ближче до периферії мережі, забезпечуючи менші затримки, підвищену швидкодію та більшу автономність локальних систем..

Рис.2.1 Схема поєднання технологій

Як показано на рис. 2, з концептуальної точки зору fog computing буде служити проміжним рівнем сервісу для узгодженої роботи протоколів cloud computing та IoT. Це принесе багато переваг:

1) cloud computing сервери дуже швидкі на відміну від пристроїв IoT. Пристрої fog computing забезпечать інтерфейс між двома далекими наборами пристроїв.

2) Цей проміжний шар fog computing дозволить робити виправлення (наприклад, частинні оновлення тощо) . Замість внесення змін на пристроях IoT, оновлення програмного забезпечення можна зробити на fog приладах.

3) Fog computing мають усі переваги крайових обчислень, таких як швидкість, масштабованість, децентралізація і інші.

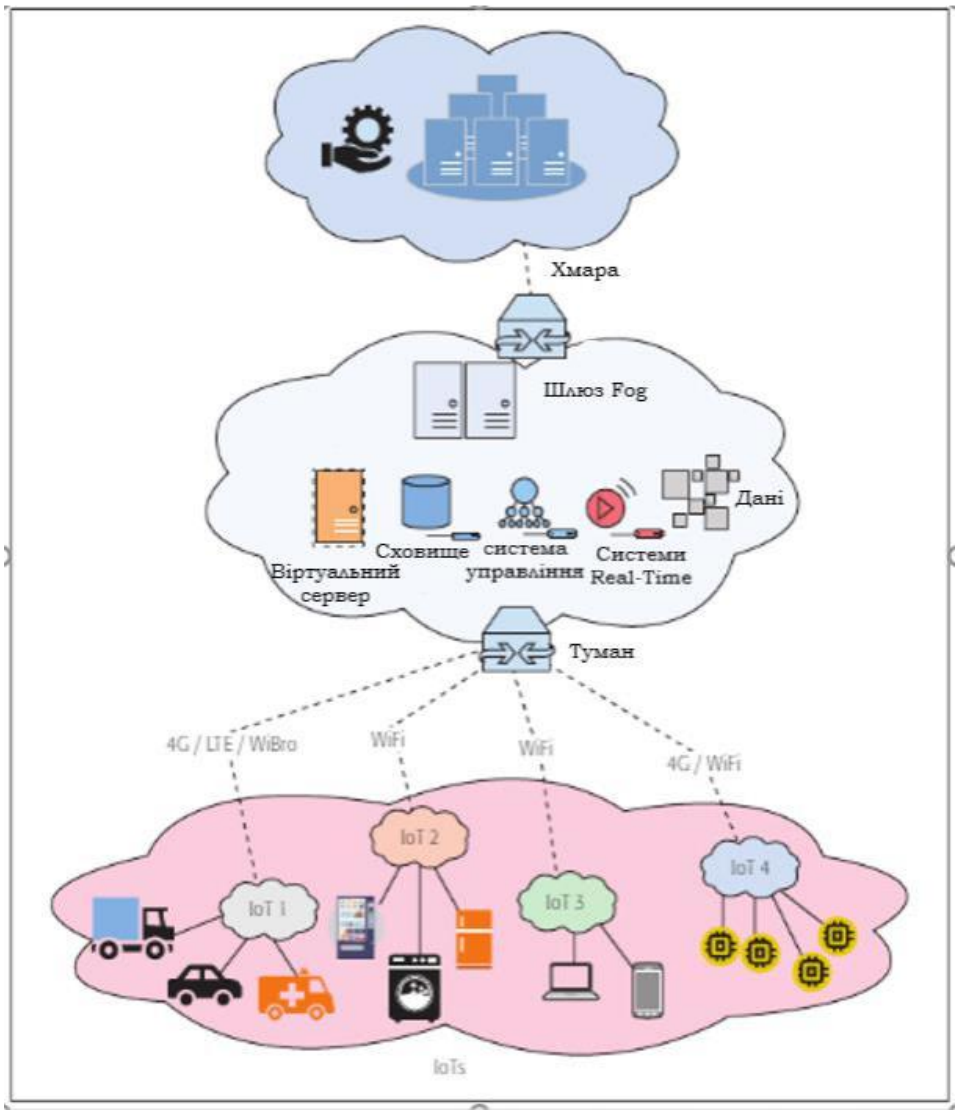

Рис.2.2 Загальна архітектура туманних обчислень

Концепція туманних обчислень полягає в перенесенні мережевих та обчислювальних ресурсів максимально близько до вузлів, що генерують дані, тобто до найнижчого рівня архітектури сприйняття. Fog-інфраструктура являє собою високовіртуалізовану платформу, яка забезпечує обчислювальні потужності, зберігання даних та мережеві сервіси на проміжному рівні між кінцевими IoT-пристроями та традиційними хмарними центрами обробки інформації [9]. Таким чином, туманні обчислення формують спеціалізовану архітектуру як для організації зв’язку, так і для ефективного управління мережею [10].

На рисунку 2.2 подано узагальнену структуру туманних обчислень, у

межах якої різні інстанції Fog-вузлів надають необхідні ресурси елементам, що функціонують у Smart City та IoT-середовищах. Туманні вузли можуть взаємодіяти з широким спектром мережевих технологій, зокрема з бездротовими сенсорними мережами (WSN), віртуальними сенсорними мережами (VSN), мережами транспортних засобів типу VANET, а також персональними обчислювальними мережами (PAN).

Рис.2.3 Рівні туманної архітектури

На рисунку 2.3 показані основні рівні типової туманної архітектури. Фізичний рівень та рівень віртуалізації становлять найнижчий шар архітектури, який оперує кожним окремим «об’єктом» — пристроєм або вузлом, здатним під’єднуватися до мережі чи Інтернету та генерувати дані. До цього рівня належать фізичні й віртуальні сенсори, вузли IoT, віртуалізовані сенсорні мережі, транспортні засоби та інші елементи периферії. Усі такі компоненти

функціонують відповідно до вимог сервісу та характеристик конкретного вузла.

На рівні моніторингу здійснюється контроль активності вузлів і мереж з урахуванням їх обчислювальної потужності, призначення та поточного стану. Цей шар визначає, яку саме задачу має бути виконано далі і коли саме. Додатково відбувається моніторинг енергоспоживання, що дає змогу оптимізувати роботу сенсорів, зокрема забезпечувати своєчасне оновлення або застосування коригуючих дій.

Рівень попередньої обробки відповідає за локальне управління даними. На цьому етапі проводиться детальний аналіз отриманої інформації, її очищення, фільтрація та відсів зайвих даних, що дозволяє мінімізувати обсяг непотрібної або дубльованої інформації, спрямованої до наступних рівнів.

Шар зберігання забезпечує тимчасове збереження даних у межах туманної інфраструктури. Основний обсяг інформації утримується саме локально — у Fog-вузлах, тоді як для довготривалого зберігання більш придатною є хмарна інфраструктура через більші ресурси й можливості масштабування. Після передавання даних до хмари їх подальше зберігання в тумані часто втрачає актуальність.

Окремі типи сервісів вимагають застосування механізмів безпеки та захисту конфіденційності. Наприклад, у повсюдних медичних системах обробляються дані про спосіб життя, харчування й інші персональні параметри, що можуть містити чутливу інформацію. У деяких випадках навіть дані про місцеперебування потребують додаткового захисту. Рівень безпеки туману відповідає за забезпечення належного захисту даних перед їх передаванням через потенційно вразливі канали.

Після завершення підготовки даних активується транспортний шар, який відповідає за передавання інформації у хмару. Це зменшує навантаження на основну мережу та дозволяє хмарним сервісам формувати вдосконалені цифрові послуги значно швидше. Ресурси Fog-інфраструктури розташовані між IoT-вузлами та хмарним рівнем [11], забезпечуючи створення гнучких, персоналізованих і контекстно орієнтованих сервісів.

Близькість Fog-вузлів до кінцевих пристроїв забезпечує низьку латентність і високу якість передавання даних навіть у мобільних сценаріях — наприклад, для транспортних засобів, що рухаються автошляхами та залізницями, через використання локальних проксі-серверів та точок доступу [12].

На основі зворотного зв'язку, отриманого від додатків або хмарної інфраструктури, а також з урахуванням обмежень окремих вузлів, туман здатен динамічно планувати взаємодію між пристроями, мережами та хмарою. Це дозволяє значно ефективніше використовувати як мережеві ресурси, так і ресурси обробки даних.

У галузі медичних сервісів Fog Computing може адаптувати обробку даних до потреб конкретних медичних додатків: виконувати попередню обробку сирих даних, відправляти вже агреговану інформацію у хмару, де вона трансформується у корисні сервіси, наприклад, повідомлення про критичний рівень глюкози чи порушення серцевого ритму.

З огляду на різноманітність типів даних і гетерогенність вузлів, часто виникають проблеми сумісності. Fog-інфраструктура частково розв'язує це питання, забезпечуючи локальне виконання операцій транскодування та перетворення даних. Аналогічно працюють федерації IoT та WSN, де декілька сенсорних або IoT-мереж можуть бути інтегровані для розширення спектра доступних послуг.

Попри схожість із хмарними обчисленнями, Fog Computing має низку ключових відмінностей. Основні з них стосуються доступності й близькості: туманна інфраструктура розташована безпосередньо поруч з кінцевими пристроями у межах локальної мережі, тоді як хмара працює через мережу Інтернет і може бути географічно віддаленою. Fog виконує роль проміжної ланки між периферійними IoT-вузлами, сенсорними мережами та централізованою хмарою, фактично продовжуючи функціональність хмарних обчислень і наближаючи її до краю мережі.

Fog Computing додає додатковий рівень обробки між базовими вузлами та хмарою, що значно покращує процеси аналізу, фільтрації та захисту чутливих

даних (наприклад, інформацію про місцеперебування користувача чи медичні параметри). У випадку мультимедійних сервісів якість обслуговування значною мірою залежить від пропускної здатності основної мережі, тоді як локальний доступ до туманних ресурсів може забезпечити значно менші затримки.

У ситуаціях, коли пристрої потребують передачі обчислювально інтенсивних завдань, Fog Computing є більш оптимальним рішенням порівняно з хмарою. Оскільки хмарні архітектури є централізованими, а туман — розподіленою інфраструктурою, останній краще підходить для обробки задач, чутливих до часу та ресурсних обмежень..

2.2 Fog Computing з точки зору безпеки

Використання хмарних інфраструктур для передавання та аналізу даних супроводжується низкою обмежень, серед яких — значне споживання пропускної здатності мережі та додаткові витрати на комунікаційні ресурси. Дані мають критичне значення для аудиту, контролю активів, оптимізації ефективності та запобігання надзвичайним ситуаціям. Якщо ж інформація, що передається, є конфіденційною, то питання гарантування її безпеки набуває ще більшої актуальності.

У багатьох випадках аналіз даних може виконуватися локально — за допомогою програмного забезпечення, розміщеного на периферійних станціях. Результати такого аналізу можуть передаватися до хмари виключно з метою архівування, аудиту або подальшого аналітичного опрацювання. Агрегація даних на проміжному рівні дозволяє суттєво зменшити навантаження на мережу, знизити витрати, пов’язані з передаванням, та мінімізувати споживання пропускної здатності.

Туманні обчислення (Fog Computing) розглядаються як ефективне рішення для подолання цих проблем завдяки унікальним характеристикам, серед яких — територіальна близькість до джерел даних. Fog-платформи особливо актуальні в таких IoT-застосуваннях, як транспортні мережі, кіберфізичні системи автомобілів та сервіси медичного моніторингу [14], [15].

Fog Computing є логічним продовженням хмарної парадигми, тому частина ризиків безпеки та конфіденційності зберігається. Хоча багато хмарних рішень можуть частково вирішувати ці проблеми, специфіка туману (наприклад, підтримка мобільності та різнорідність підключених вузлів) призводить до появи нових загроз. Це, у свою чергу, може ускладнювати ефективну інтеграцію туманних систем із IoT.

З іншого боку, Fog Computing може стати потужним інструментом для забезпечення безпеки й конфіденційності у середовищі IoT. Завдяки збалансованому поєднанню обчислювальної потужності, можливостей зв'язності та локального контролю туманні ресурси здатні підтримувати широкий спектр задач безпеки. Fog-вузли можуть виступати проксі-серверами, що виконують криптографічні операції, компенсуючи обмежені ресурси сенсорних вузлів. Завдяки цьому туманні обчислення забезпечують додатковий рівень захисту й зменшують ризики атак у середовищі IoT.

Основні проблеми безпеки та конфіденційності в IoT.

Аутентифікація є однією з фундаментальних вимог до захисту IoT-систем. Проте багато пристроїв мають обмежені ресурси (пам'ять, продуктивність процесора), що ускладнює виконання криптографічних операцій. Проблеми масштабованості та продуктивності роблять традиційні механізми аутентифікації неефективними для IoT-середовищ.

Fog Computing здатне частково вирішити цю проблему шляхом застосування легковагових алгоритмів шифрування між туманними вузлами та IoT-пристроями, що суттєво підвищує ефективність процесу аутентифікації. Крім того, Fog-інфраструктура може забезпечувати автономну аутентифікацію мобільних IoT-пристроїв.

У науковій літературі вже пропонується низка моделей управління ключами для захисту великих інтелектуальних середовищ, зокрема смарт-мереж [16]. Такі моделі базуються на інфраструктурі відкритих ключів (PKI) з використанням багатоадресних механізмів аутентифікації. Проте класичні PKI-рішення часто не забезпечують необхідної масштабованості для IoT-мереж.

Природа IoT передбачає взаємодію великої кількості різнорідних пристроїв та сенсорів, що належать різним системам та організаціям. У таких умовах постає важливе питання: наскільки ми можемо довіряти кожному пристрою?

На даний момент не існує універсального механізму, який би визначав рівень довіри до IoT-пристроїв у складних, неоднорідних системах. За відсутності такої оцінки користувачам доводиться приймати рішення щодо доцільності використання певних сервісів, що може знижувати ефективність IoT-екосистем.

Підвищення довіри між пристроями є ключовим для формування безпечного середовища. Моделі довіри, засновані на репутації, успішно функціонують у багатьох цифрових системах, наприклад у соціальних мережах. Сучасні підходи пропонують комбінувати методи репутаційного оцінювання, посилені центри обробки даних, контроль доступу та віртуальні кластери для підвищення довіри в хмарних екосистемах [17].

Для впровадження репутаційної моделі довіри в IoT необхідно забезпечити:

– стабільність та надійність сервісів;

– виявлення випадкових та навмисних збоїв;

– ідентифікацію та блокування шкідливої поведінки;

– точне оцінювання рівня довіри у масштабних мережах..

2.3. Виявлення уражених вузлів IoT

Уражений вузол IoT може маскуватися під легітимний елемент мережі та запитувати або збирати дані інших пристроїв у злочинних цілях. У наукових джерелах пропонуються різні підходи для виявлення таких загроз, зокрема гібридний фреймворк для виявлення незаконних точок доступу в Wi-Fi-інфраструктурі мереж доступу [18]. Компрометований вузол IoT може не лише зловживати користувацькими даними, а й розповсюджувати шкідливу інформацію до сусідніх пристроїв, провокуючи помилки та порушення їхньої поведінки.

Розв’язання цієї проблеми є складним з огляду на різноманітність архітектур і механізмів управління довірою в IoT. Одним із дієвих підходів є побудова моделей довіри, здатних виявляти вузли з аномальною або шкідливою поведінкою. Такі моделі забезпечують підвищення безпеки шляхом ідентифікації й блокування компрометованих пристроїв.

Проблеми конфіденційності та шляхи їх вирішення у Fog Computing

Fog Computing може відігравати ключову роль у збереженні конфіденційності даних IoT, оскільки мінімізує потребу передавання чутливої інформації у хмару для її обробки. Перенесення аналізу даних на край мережі — ближче до пристроїв, які їх генерують — скорочує ризики перехоплення та спрощує контроль над обробкою.

Разом із тим використання туманних обчислень породжує низку викликів, пов’язаних із конфіденційністю, місцеперебуванням та чутливістю користувацьких даних. Техніки забезпечення конфіденційності можна ефективно реалізувати між туманом і хмарою, оскільки ці рівні мають достатню обчислювальну потужність. Проте застосування повноцінних криптографічних рішень між Fog-вузлами та малопотужними IoT-пристроями залишається проблематичним через обмежені ресурси останніх.

Одним із перспективних підходів є використання гомоморфічного шифрування, яке дозволяє виконувати обчислення над зашифрованими даними без їх розшифровування. Ще одним підходом є застосування диференційної конфіденційності, що сприяє зниженню ризику розкриття чутливої інформації під час обробки даних.

Для забезпечення конфіденційності місцеперебування одним із початкових рішень розглядається розподіл даних між кількома Fog-вузлами, хоча це може збільшувати затримки та навантаження на систему. Також застосовується маскування ідентифікаторів, яке приховує джерело даних — у цьому випадку Fog-вузли не можуть визначити, який IoT-пристрій виконує розвантаження.

Перспективним напрямом є методи конфіденційності на основі поділу даних між Fog-вузлами, що дозволяє зменшити ризики витоку за умови

обмежених ресурсів IoT-пристроїв.

Контроль доступу в IoT

Контроль доступу забезпечує можливість керувати тим, які суб'єкти можуть отримувати дані або взаємодіяти з IoT-пристроями. Це критично важливо, оскільки дозволяє гарантувати, що лише авторизовані об'єкти можуть:

– читати конфіденційні дані;

– віддавати команди пристроям IoT;

– виконувати оновлення їхнього програмного забезпечення.

У середовищі IoT контроль доступу ускладнюється масштабом та ресурсними обмеженнями вузлів. Додаткові проблеми виникають через високий рівень розподіленості даних, що ускладнює їх надійний захист.

Виявлення вторгнень в IoT

Методи виявлення вторгнень покликані ідентифікувати шкідливі пристрої або аномальну поведінку й сповіщати інші системи про необхідність захисних дій. Існуючі методи часто не враховують масштабність та мобільність IoT-екосистем, що знижує їхню ефективність.

Однією з головних проблем є проєктування IDS, здатних функціонувати в умовах обмежених ресурсів, високої динамічності та великого масштабу мережі.

Fog Computing надає нові можливості для розробки ефективних систем виявлення вторгнень, оскільки дозволяє переносити частину обчислень із хмари на край мережі. Fog-вузли можуть аналізувати поведінку пристроїв, зіставляти її з відомими шаблонами атак або виявляти аномалії. У наукових роботах пропонуються архітектури, де Fog- та Cloud-вузли спільно діють для спостереження за середовищем IoT і виявлення шкідливої активності.

Fog Computing додає додатковий рівень оборони, здатний оперативно реагувати на аномалії та локально блокувати загрози.

Захист даних та забезпечення цілісності

Обсяг даних, що генеруються IoT-пристроями, експоненційно зростає разом зі збільшенням кількості елементів системи. Через обмежені ресурси пристрої не можуть самостійно забезпечувати повноцінне шифрування та

перевірку цілісності даних. Тому більшість інформації передається до хмари для опрацювання та зберігання.

У цих умовах забезпечення цілісності даних на всіх етапах — під час передавання, обробки та після збереження — є критично важливим. Відсутність локальних засобів криптографії робить IoT-пристрої вразливими до підміни або маніпуляцій даними.

Оновлення IoT-пристроїв

Багато сучасних IoT-пристроїв не підтримують віддалені оновлення мікропрограмного забезпечення. Це створює ризик експлуатації вразливостей, які не можна усунути традиційними засобами безпеки, такими як брандмауери.

Fog-вузли можуть стати ключовим елементом системи масового оновлення IoT-пристроїв. Завдяки георозподіленості туманних обчислень можна забезпечити швидке та ефективне доставлення оновлень до великої кількості пристроїв, що значно підвищує загальний рівень безпеки.

Безпечні та ефективні протоколи зв’язку

Багато протоколів бездротової синхронізації та передавання даних не підходять для IoT через високе енергоспоживання або складність обчислень. Основна проблема полягає у створенні легковагових та енергоефективних криптографічних рішень, що не знижують продуктивність системи.

Виявлення атак у Fog/IoT-середовищах

Fog Computing створює нові можливості для виявлення локальних атак, зокрема інсайдерських, точкових та аномальних. Розроблені для хмар системи IDS можуть бути адаптовані для Fog-рівня, що забезпечує локальну фільтрацію та швидке реагування.

Fog-вузли можуть взаємодіяти між собою, обмінюватися даними про аномалії та узгоджено формувати механізми виявлення та реагування.

Наведені проблеми безпеки та конфіденційності в IoT не є вичерпними, але вони демонструють масштабність викликів, що супроводжують розвиток інтелектуальних мереж. Однак туманні обчислення мають низку властивостей, які дозволяють зменшити кількість атак, підвищити стійкість IoT-сервісів до

загроз та посилити загальний рівень безпеки.

Fog Computing може стати ключовою складовою захисної архітектури для IoT, забезпечуючи протидію атакам типу DoS, шкідливому ПЗ, порушенням цілісності даних та іншим поширеним загрозам. У великих масштабах туманні системи здатні підтримувати надійний та безпечний обмін інформацією між мільярдами пристроїв..

2.4 Переваги та недоліки технології FOG

Масштабні розгортання систем Інтернету речей призвели до появи ситуацій, у яких традиційні хмарні обчислення виявилися недостатньо ефективними. Це насамперед стосується застосувань, що потребують мінімальних затримок під час обробки даних на периферії мережі. У реальних умовах йдеться про значні обсяги інформації, що збираються з множини сенсорів IoT, розміщених у різних середовищах: на виробничих підприємствах (зокрема, заводах мережевого обладнання), у транспортних засобах, промислових машинах, ліфтах, а також у побуті — у складі смарт-систем, домашніх сенсорів тощо.

Такі пристрої є чутливими до затримок, мають різні характеристики, режими роботи та вимоги. Вони можуть бути з’єднані між собою як дротовими каналами, так і за допомогою бездротових технологій, зокрема Wi-Fi. Масове розгортання пристроїв у неоднорідних середовищах ускладнює процес управління, що зумовлює необхідність застосування інтелектуальних підходів до організації комунікацій, де пріоритет надається ефективності та надійності.

Використання виключно хмарної інфраструктури для передавання та аналізу даних має низку обмежень, серед яких — значне споживання пропускної здатності й зростання витрат на зв’язок. Якщо дані мають чутливий характер, додатково постає проблема забезпечення їхньої безпеки. Інформація, що збирається, є важливою для цілей аудиту, контролю активів, підвищення ефективності функціонування систем і запобігання аваріям та катастрофам.

У багатьох випадках аналіз даних доцільно виконувати локально — шляхом запуску спеціалізованого програмного забезпечення на периферійних вузлах. Хмарні ресурси при цьому можуть використовуватися переважно для зберігання вже оброблених результатів з метою подальшого аудиту або довгострокової аналітики. Попередня агрегація даних на краю мережі дозволяє зменшити навантаження на канали зв'язку та скоротити витрати, пов'язані з використанням пропускної здатності.

Показовими прикладами взаємодії IoT та Fog Computing є концепції Smart Office, Smart Factory, Smart Home та системи «розумного» дорожнього руху. У розумному офісі взаємодіють численні пристрої IoT, сенсори та служби, які можуть використовувати Fog-вузли для локальної обробки даних. У розумній фабриці (Smart Factory), що є прикладом промислового IoT (IIoT), можуть бути розгорнуті численні датчики (температури, тиску тощо), електричні приводи та інші керувальні елементи, які формують великий потік технологічних даних.

Концепція Smart Home пов'язана з використанням інтелектуальних побутових пристроїв — телевізорів, пральних машин, сушарок, холодильників тощо, які стають більш «розумними» та ергономічними завдяки підключенню до мережі. У сценарії «розумного» трафіку (smart traffic) збирання даних на місці, їхній оперативний аналіз та обробка на fog-серверах дають змогу приймати критично важливі рішення локально, без потреби постійного звернення до центрального хмарного сервера.

Наприклад, у разі надзвичайної ситуації (дорожньо-транспортна пригода, пожежа тощо) система управління рухом може змінити режими роботи світлофорів для забезпечення пріоритетного проїзду автомобілів екстрених служб (швидкої допомоги, пожежної охорони), спираючись на дані місцевих IoT-пристроїв.

У всіх цих сценаріях спільною є ідея про те, що пристрої IoT генерують величезну кількість даних, які мають бути опрацьовані, узгоджені та використані для ухвалення критичних рішень із мінімальними затримками. Висока швидкість реакції стає ключовою вимогою, і концепція Fog Computing якраз спрямована на

подолання обмежень, пов’язаних із пропускною здатністю та затримками.

Завдяки реалізації механізмів оперативної реакції безпосередньо поблизу крайових вузлів стає можливим швидке масштабування та розвиток бізнес-моделей на основі fog-сервісів для майбутніх IoT-застосувань, зокрема смарт-трафіку та розумних фабрик. При цьому інтеграція торкається не лише побутового IoT, а й промислового IoT (IIoT) та інших галузей, що супроводжується як новими викликами [19], так і суттєвими перевагами.

IoT і Fog Computing відкривають перспективи для створення «розумних» об’єктів та інфраструктур — розумних будинків, інтелектуальних світлофорів, систем Smart City тощо. Наприклад, сенсори в інтелектуальній транспортній системі можуть виявляти аварійні ситуації, фіксувати стан дорожнього покриття, погодні умови та інші фактори, інформуючи водіїв і керуючи потоками транспорту для зменшення заторів.

Стрімке зростання кількості IoT-пристроїв призвело до масового збільшення обсягів даних, що генеруються на периферії мережі. Виникає питання: де, коли і яким чином слід здійснювати їх аналіз?

У хмаро-орієнтованій архітектурі пристрої IoT передають усі дані до хмари, яка виконує роль центрального сервера для зберігання та обробки. Натомість у моделі Fog Computing значна частина аналітики виконується на крайових станціях, а до хмари надсилаються лише результати або агреговані дані.

У цьому сенсі Fog розширює концепцію хмарних обчислень, доповнюючи її рівнем «розумних» пристроїв на краю мережі. Fog переносить обчислювальні потужності ближче до джерел даних, що особливо важливо для застосувань, чутливих до затримок.

FOG надає такі ключові переваги:

• забезпечує швидку реакцію для додатків, чутливих до затримки (зокрема мультимедійні сервіси та системи оповіщення у надзвичайних ситуаціях);

• підтримує агрегування даних від гетерогенних пристроїв, наприклад, об’єднання медичних показників із різних сенсорів здоров’я;

• підвищує рівень захисту конфіденційної інформації (медичні дані,

геолокація користувача та інші персональні дані), зменшуючи потребу у передаванні «сирих» даних у магістральну мережу;

• забезпечує надання контекстно-орієнтованих і локаційно-залежних сервісів завдяки фізичній близькості до користувача та можливості враховувати більше інформації про його стан і оточення.

Консорціум OpenFog розробляє стандарти Fog Computing, формуючи різні комітети та робочі групи [20]. До засновників належать Arm, Cisco, Dell, Intel, Microsoft та Princeton University. Основна увага приділяється створенню та популяризації відкритої референсної архітектури туманних обчислень для вирішення завдань, пов'язаних із пропускною здатністю, затримками, а також для застосувань у сферах штучного інтелекту (AI), IoT, промислової автоматизації, робототехніки тощо.

За даними OpenFog, ключовими стовпами архітектури Fog Computing є: безпека, масштабованість, відкритість, автономність, надійність, доступність, відмовостійкість, гнучкість (спритність), ієрархічність та програмованість.

Fog Computing підтримує екосистеми IoT, 5G та AI, що потребують таких властивостей, як:

– надійні та захищені транзакції;

– обізнаність про контекст (situation awareness);

– масштабованість та гнучкість;

– обробка у режимі реального часу (низька затримка);

– ефективне використання наявних ресурсів.

На думку OpenFog, основні переваги впровадження туманних обчислень включають:

– низьку затримку;

– підвищення бізнес-спритності (оперативність та гнучкість рішень);

– посилення безпеки;

– аналітику в режимі реального часу;

– зменшення вартості;

– скорочення використання пропускної здатності мережі..

Висновки:

З швидким зростанням додатків Internet of Things класична парадигма централізованого хмарного обчислення стикається з декількома проблемами, такими як висока затримка, низька пропускна здатність і збій в мережі.

В даному розділі було розглянуто технологію FOG Computing якості технології, що наближає хмару ближче до пристроїв IoT.

Для вирішення цих проблем, туман обчислень забезпечує локальну обробку і зберігання IoT data на пристроях IoT замість відправки їх в хмару. На відміну від хмари, туман надає послуги з більш швидкою реакцією і більш високою якістю. Таким чином, Fog Computing може вважатися кращим вибором, який дозволить IoT надавати ефективні та безпечні послуги користувачам manyIoT. У цьому розділі представлена інформація про сучасні методи обробки даних за допомогою туману і їх інтеграції з цією технологією, а також про переваги та труднощі, пов'язані з впровадженням.

РОЗДІЛ 3. BLOKCHAIN ТА FOG BASED ARCHITECTURE ДЛЯ IOT В СЕРЕДОВИЩІ SMART CITY

3.1 Blockchain та Fog Based Architecture

Витоки концепції розумних міст пов'язані з потребою підвищення якості життя населення та оптимізації використання міських ресурсів, що стало актуальним у зв'язку зі стрімким зростанням урбанізованих територій. Покращення інфраструктури та міських сервісів стало реальним завдяки розвитку мережі Інтернет, сучасних телекомунікаційних технологій та інформаційних систем. Сутність Smart City полягає у створенні ефективних державних послуг та інфраструктури нового покоління, що є доступною, інтерактивною й орієнтованою на потреби громадян. Реалізація цієї концепції стала можливою завдяки інтеграції технологій Інтернету речей, які перетворили інтелектуальне місто на ключовий напрям розвитку IoT-застосувань. Простір міста поступово насичується фізичними об'єктами, здатними взаємодіяти через мережеві протоколи IoT. Основними складовими такої взаємодії є дані, пристрої, люди та процеси, що формують фундамент для впровадження перспективних цифрових сервісів.

Середовище, яке генерує значні обсяги великих даних, ставить перед містами виклики їх ефективного зберігання та обробки. Хмарні обчислення певною мірою здатні компенсувати ці труднощі, пропонуючи гнучку модель інфраструктури, що розгортається за потребою та оплачується за принципом ресурсоорієнтованої тарифікації. Проте низка внутрішніх обмежень зумовлює недостатню ефективність хмарних рішень для частини міських застосунків [21]. Наприклад, система моніторингу дорожнього руху не може дозволити значну затримку між моментом формування даних, їх передаванням у хмару та отриманням результатів аналізу кінцевими користувачами. Саме тому виникла

необхідність у концепції туманних обчислень, яка передбачає зменшення мережевого трафіку та скорочення часу обробки завдяки наближенню сервісів до крайових пристроїв.

Компанія Cisco визначила Fog Computing як парадигму, що розширює хмарні сервіси, розміщуючи їх на периферії мережі [22]. Туманний вузол (Fog Node) виступає проміжною ланкою між хмарною інфраструктурою та кінцевими користувачами або пристроями IoT. Оскільки IoT-застосування вимагають мінімальних затримок, широкого географічного охоплення та підтримки мобільності, була сформована архітектура BFAN, орієнтована на покращення цих характеристик шляхом локальної обробки більшої частини даних поблизу крайових пристроїв. Додаткове підвищення безпеки досягається завдяки використанню технології блокчейн — розподіленого ланцюга блоків, що забезпечує криптографічний захист транзакцій, часові мітки та децентралізоване управління.

Блокчейн-орієнтований підхід створює умови повної децентралізації та надмірності зберігання, де зашифрованими ключами та фрагментами даних керує виключно користувач, без участі третіх сторін. У разі втрати приватного ключа його відновлення неможливе, що додатково підсилює безпекові властивості системи. Алгоритм раціонального розподілу ресурсів у BFAN дає змогу оптимізувати їх споживання, співвідносити витрати з реальним використанням та корелювати результати з показниками SLA у режимі реального часу.

Туманні вузли виконують роль найближчих вузлів обробки та зберігання даних, що зменшує затримку передачі, оптимізує енергоспоживання та забезпечує оперативність прийняття рішень у віддалених локаціях. Запропонована архітектура BFAN спрямована на вирішення низки ключових проблем:

– Безпека. У смарт-містах важливими є як кібербезпека, так і фізична безпека. Технологія блокчейн забезпечує захист даних, мережевої інфраструктури та обчислювальних ресурсів від атак.

– Кешування. Зниження затримки є критично важливим фактором для Smart City. Збереження найбільш запитуваних даних у різних частинах мережі зменшує перевантаженість інфраструктури та скорочує дублювання трафіку. Завдяки кешуванню туманні обчислення можуть ефективно підтримувати роботу різноманітних міських сервісів.

– Масштабованість. Fog-інфраструктура надає можливість гнучко масштабувати сервіси для забезпечення необхідного рівня QoS шляхом децентралізованого створення «міні-хмар» поблизу пристроїв IoT.

– Стійкість та енергоефективність. Для розумних міст важливо скорочувати енергоспоживання та викиди CO_2, зокрема завдяки використанню відновлюваних джерел енергії. Нині понад 80% енергії у дата-центрах виробляють вугільні джерела [23], що стимулює перехід до більш сталих рішень.

– Контекстуальна обізнаність. Визначення місцезнаходження вузла та його взаємодія з навколишнім середовищем є ключовими параметрами для коректної роботи Smart City. Архітектура BFAN враховує контекстну інформацію для вибору оптимального режиму зв’язку, підвищуючи загальну енергоефективність та якість міських послуг.

3.2 Варіант архітектури Blockchain

Блокчейн - це розподілена база даних, метою якої є створення надійного, децентралізованого способу перевірки дій. Наприклад, в разі економічних угод замість створення єдиного центрального органу - банку -для перевірки операцій блокчейн дозволяє всім учасникам мережі перевіряти кожну операцію. З точки зору безпеки, його найбільша перевага - невідновлення: як тільки щось записується в блокчейн, воно не може бути змінено або видалено. Блокчейн працює в контексті мережі вузлів, всі з яких містять копію поточного стану блокчейна.

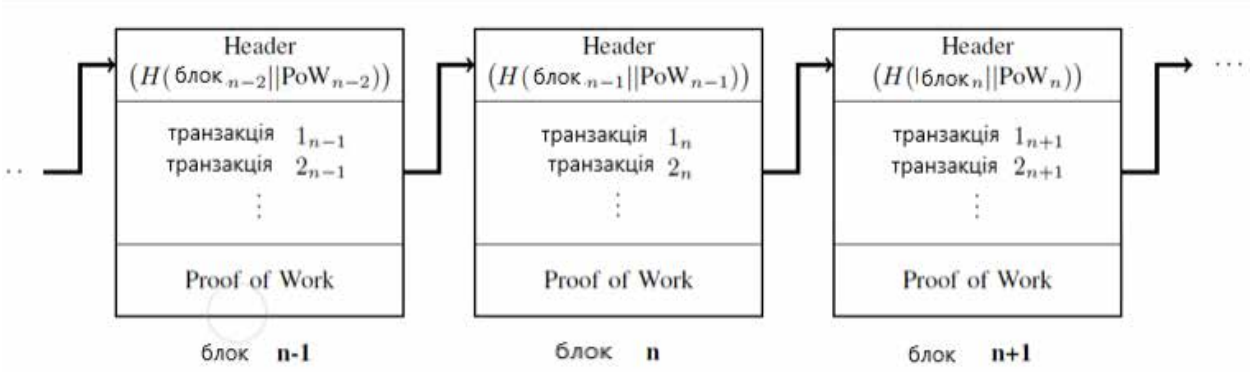

Рис. 3.1 Варіант схеми технології Blockchain

Блокчейн сам по собі є простою послідовністю блоків, кожен блок яких містить кілька транзакцій (див. рис. 3.1). Як тільки вузли в мережі вирішують записати нову транзакцію, ця транзакція додається до наступного доступного блоку, і цей блок в кінцевому підсумку переноситься в інші вузли, таким чином оновлюючи блокчейн для кожного вузла.

Для того щоб забезпечити незмінність послідовності блоків у ланцюгу, застосовується хеш-функція: для кожного нового блока обчислюється хеш попереднього, який записується до заголовка нового блока. Це забезпечує унікальний, однозначно відтворюваний порядок блоків. Водночас теоретично зловмисник усе ще може спробувати перерахувати хеші окремих блоків, щоб змінити послідовність у ланцюгу. Запобігти цьому дозволяє механізм Proof-of-Work (PoW). По суті, PoW встановлює умову до хеш-значення блока, яка змушує вузол витрачати певний час і обчислювальні ресурси на пошук прийнятного хешу. Це унеможливлює масове «проштовхування» підроблених або змінених блоків зловмисними вузлами в мережу.

Зазвичай така умова формулюється як проста обчислювальна задача, яку можна розв’язати лише перебором, наприклад: знайти таке значення додаткових даних у блоці (nonce), за якого хеш блока починається з певної кількості нулів (наприклад, з 50 нулів або одиниць). У цьому разі вузол змушений багаторазово змінювати блок даних та перераховувати хеш, доки не буде виконано цільову умову. Кожен вузол у мережі може працювати або пасивно (лише ініціюючи транзакції), або активно (ініціюючи та перевіряючи транзакції). Останні вузли називають майнерами; саме вони перевіряють коректність транзакцій,

обчислюють хеш блока відповідно до заданої умови та розповсюджують новий блок до інших вузлів, оновлюючи таким чином блокчейн.

Кожен блок містить заголовок, у якому зберігаються хеш попереднього блока та певні додаткові дані, що забезпечує однозначність послідовності блоків і, відповідно, історії транзакцій (див. рис. 3.1).

Якщо зловмисник намагатиметься змінити порядок блоків або вміст транзакцій, йому доведеться не лише повторно обчислити всі хеші блоків, які він хоче змінити, а й перерахувати хеші всіх наступних блоків, щоб переконати інші вузли мережі, що його варіант ланцюга є «правильним».

Однак лишається ще одна потенційна загроза: що буде, якщо зловмиснику випадково пощастить і він першим знайде коректний хеш блока? У такому разі він міг би нав'язати мережі власну версію історії транзакцій. Для протидії цьому блоки не вважаються остаточно підтвердженими одразу. Якщо кілька вузлів одночасно знаходять різні коректні блоки, у блокчейні утворюється вилка (fork). Згодом мережею визнається дійсною та гілка, яка стає найдовшою (тобто містить найбільше підтверджених блоків).

Таким чином, якщо зловмисник хоче додати фальшиві транзакції в блокчейн, йому недостатньо просто «пощастити» і першим знайти допустимий блок. Він також має безперервно будувати власну гілку блокчейна швидше, ніж усі інші майнери, щоб саме вона стала найдовшою та була прийнята мережею як легітимна. Це можливо лише тоді, коли зловмисник контролює понад 50% обчислювальної потужності мережі, тобто більшість майнерів. Така загроза відома як атака 51%. Як стверджують дослідники, у великих і популярних мережах, таких як Bitcoin або Ethereum, реалізація подібної атаки є практично нереалістичною [24].

Отже, блокчейн задовольняє дві ключові вимоги безпеки:

– Цілісність даних – інформація не може бути змінена після фіксації в блокчейні.

– Невідмовність (non-repudiation) – кожна транзакція підписується сторонами, що беруть у ній участь, а оскільки дані не можуть бути змінені, жоден

вузол не може правдоподібно заперечити свою участь у вже записаній транзакції.

Крім того, блокчейн забезпечує високий рівень доступності, оскільки децентралізована архітектура передбачає безперервне функціонування системи навіть у разі відмови окремих вузлів. Це особливо важливо для IoT-систем, де у випадку централізованих хмарних рішень збій центрального сервера фактично блокує доступ до даних [25].

Переваги використання блокчейну в IoT-додатках

1) Зберігання даних з IoT-пристроїв у блокчейні. Додатки IoT передбачають функціонування великої кількості взаємопов'язаних пристроїв, які можуть керувати один одним і бути підключеними до хмарної інфраструктури, що забезпечує віддалений доступ. За таких умов блокчейн розглядається як перспективне рішення для надійного зберігання даних і запобігання їх несанкціонованому використанню. Незалежно від рівня архітектури IoT-додатку (пристрої, шлюзи, сервіси), блокчейн може виступати універсальним механізмом для захищеного зберігання та передавання інформації.

2) Розподілений характер блокчейну та відсутність єдиної точки відмови.

Децентралізована природа блокчейну дозволяє уникнути проблеми «single point of failure», характерної для класичних хмарних рішень. Незалежно від фізичної відстані між пристроями, дані, які вони генерують, можуть бути розподілено збережені в блокчейні, гарантуючи їх доступність і стійкість до збоїв окремих вузлів.

3) Шифрування й перевірка даних за допомогою хеш-значень та майнерів.

У блокчейні зазвичай зберігається не сам масив даних, а його 256-бітний хеш-ключ, тоді як первинна інформація може розміщуватися у хмарному сховищі. Хеш-значення однозначно відповідає вихідним даним: будь-яка зміна вмісту призводить до зміни хешу. Це забезпечує конфіденційність та контроль цілісності: розмір блокчейну не залежить від обсягу даних, оскільки в ланцюгу зберігаються лише хеші, а не самі файли. Доступ до вихідних даних можуть отримати лише уповноважені сторони, які мають хеш-ідентифікатор та відповідні права доступу до хмарного сховища. Кожен запис у блокчейні

проходить верифікацію майнерами, що зменшує ймовірність збереження спотворених або шкідливих даних [26].

4) Запобігання втраті даних та атакам підміни (spoofing). В умовах IoT можливі атаки, за яких у мережу додається зловмисний вузол, що видає себе за легітимний елемент системи. Такий вузол може перехоплювати, спостерігати або підміняти дані. Блокчейн дозволяє протидіяти цьому, оскільки кожен легальний пристрій та користувач проходить реєстрацію в мережі блокчейну, а їх взаємна ідентифікація та автентифікація відбувається без централізованих посередників і сертифікаційних центрів. Через обмежені ресурси IoT-пристрої також мають високий ризик втрати даних (збої живлення, вплив зовнішнього середовища тощо). Оскільки інформація в блокчейні не може бути видалена після додавання блока, використання цієї технології суттєво знижує ймовірність незворотної втрати критичних даних [26].

5) Запобігання несанкціонованому доступу. Багато IoT-додатків передбачають інтенсивний взаємообмін даними між вузлами. У блокчейні взаємодія ґрунтується на використанні пар відкритих і приватних ключів. Доступ до зашифрованих даних має тільки вузол, який володіє відповідним приватним ключем. Навіть якщо третя сторона перехопить зашифровану інформацію, її зміст залишиться незрозумілим без ключа розшифрування. Такий підхід дозволяє блокчейну суттєво зменшити ризики, пов’язані з несанкціонованим доступом та крадіжкою даних у IoT-додатках.

6) Проксі-архітектури для пристроїв з обмеженими ресурсами. Повноцінна участь пристроїв IoT у блокчейн-мережі ускладнюється через їхні обмежені обчислювальні та пам’яттєві ресурси (вони не можуть зберігати повну копію розподіленого реєстру). У відповідь на це досліджуються різні архітектури, орієнтовані на зниження навантаження, серед яких перспективною є проксі-архітектура. У такій моделі проміжні вузли (проксі-сервери) зберігають зашифровані дані та виконують основні операції з блокчейном, тоді як IoT-пристрої взаємодіють із ними як «тонкі клієнти», завантажуючи зашифровані ресурси за потребою [27].

7) Усунення залежності від централізованих хмарних серверів.

Блокчейн сприяє підвищенню безпеки IoT-систем завдяки переходу від централізованої моделі до однорангової (peer-to-peer) архітектури. Централізовані хмарні сервери є привабливою ціллю для атак та крадіжки даних; у блокчейн-мережі інформація розподіляється між численними вузлами та захищається криптографічними хеш-функціями. Це значно знижує ризик компрометації всієї системи внаслідок атаки на один центр обробки..

3.3 Варіант поєднання Blockchain та Fog Based Architecture

Архітектурна мережа, заснована на блокчейн і тумані (BFAN) пропонується для підключення до Інтернету пристроїв IoT в середовищі розумного міста. Для отримання високої продуктивності і низької затримки, розподілена технологія допомагає надавати послуги за запитом. Це поліпшить якість життя громадян і виправдає очікування жителів. Туманні обчислення прискорять обробку даних, що допоже компонентам IoT, зменшуючи затримку передачі даних. Архітектура BFAN показана намалюнку 2, зможе запропонувати краще рішення для майбутнього розумного міста.

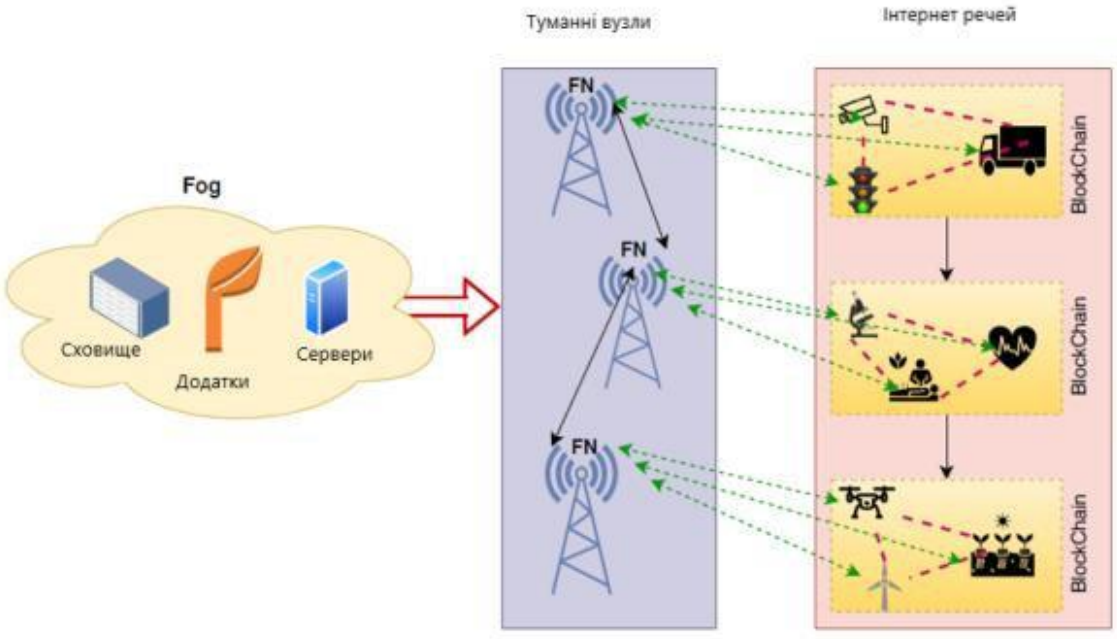

Рис.3.2 Схема архітектури BFAN

Архітектура BFAN складається з двох рівнів. Перший рівень - це вузли Fog, які зменшують затримку, спричинену обробкою даних натуманних вузлах, отриманих від вхідного трафіку IoT. Це також допомагаже задовольнити очікування користувачів, пов'язаних з швидким обслуговуванням. Пропонується багаторівнева архітектура, як показано на рис. 2 для додатків, пов'язаних з великими даними в майбутніх розумних містах. Перший шар в цій архітектурі є підключення пристрою один з одним і з FN. Важлива комунікація між підключеними пристроями та безпека, гарантована технологією Блокчейн. Другий рівень використовується для зменшення часу очікування, обробляючи трафік від пристроїв IoT. Це допоможе задовольнити потреби користувачів у послугах.

Функціонування рівнів архітектури BFAN у середовищі Smart City

Питання функціонування кожного рівня розглядається в наступних підрозділах.

1. Рівень протитуманних вузлів (Fog Nodes Layer)

Попит користувачів на сервіси розумного міста задовольняється за рахунок взаємодії пристроїв IoT із середовищем туманних обчислень (Fog Computing). Блокчейн-технологія інтегрується як додатковий компонент підвищення надійності, забезпечуючи контроль доступу та захист даних за умови отримання відповідних прав доступу від допоміжних систем.

Декілька фізичних серверів об'єднуються у Fog Node (FN), який охоплює визначену географічну зону та забезпечує обробку, зберігання й маршрутизацію даних. Вузли туману можуть бути під’єднані як дротовими каналами, так і бездротовими інтерфейсами. FN функціонує як невеликий віртуалізований центр обробки даних, який включає процесори, конфігуровані апаратні ресурси та мережеві сервіси.

Інтелектуальні датчики збирають інформацію з навколишнього середовища, після чого Fog Node виконує її попередній аналіз у режимі реального часу, формуючи релевантні відомості для прийняття оперативних рішень. Окрім цього, FN забезпечує функціонування радіомереж доступу, підтримуючи одноадресний

та багатоадресний типи передавання даних.

У локальну інфраструктуру FN може бути інтегрована база даних для тимчасового зберігання частини IoT-додатків, що суттєво зменшує затримки при обробці інформації та скорочує час завантаження «важких» сервісів. Важливим компонентом є концепція Social IoT (SIoT), що забезпечує підвищення пропускної здатності, зниження затримок, оптимізацію взаємодії пристроїв та зміцнення безпеки мережі. У цьому контексті передача даних може здійснюватися між різними Fog-вузлами, що створює розподілену та відмовостійку структуру.

2. Рівень Інтернету речей (IoT Layer)

Другий рівень формує фізичне середовище для розгортання IoT-додатків, у якому користувачі можуть експлуатувати сервіси без обмежень щодо масштабування. Пристрої IoT групуються за їх просторовим розміщенням та функціональним призначенням. Це дозволяє зменшити енергоспоживання, покращити продуктивність, оптимізувати витрати та скоротити час реакції системи.

Зростання кількості сенсорів і виконавчих пристроїв призводить до збільшення навантаження на центри обробки та зберігання даних, адже необхідно забезпечити сумісність апаратних засобів, інтеграцію та узгодженість програмних компонентів. Комунікація між IoT-пристроями може здійснюватися за моделями peer-to-peer (P2P) або TCP/IP на невеликих дистанціях. Якщо ж пристрої розташовані на значній відстані, вони використовують Fog Nodes як проміжні точки доступу через Wi-Fi, Zigbee або Bluetooth.

3. Блокчейн для IoT (Blockchain Layer for IoT)

Більшість сучасних IoT-систем у Smart City ґрунтуються на централізованій моделі, де хмарні сервери виконують роль контролера для верифікації пристроїв та обробки даних. Такий підхід призводить до підвищення вартості інфраструктури, технічного обслуговування та створює залежність від однієї точки відмови. Крім того, зростання кількості пристроїв у великих міських системах ускладнює масштабування та підтримку централізованих платформ.

З огляду на ці обмеження, децентралізована модель блокчейну є значно

ефективнішою. Вона забезпечує:

- стійкість до втручань та підробки даних;
- можливість відслідковувати мільярди IoT-пристроїв;
- виключення атаки типу «людина посередині» завдяки відсутності єдиного контролюючого сервера;
- зниження витрат на підтримку серверної інфраструктури;
- безпечне збереження даних сенсорів у розподіленому реєстрі.

У додатках SIoT обсяг передаваних даних збільшується експоненційно, що підвищує потреби у пропускній здатності мережі, обчислювальних ресурсах та швидкості обробки. Дані надходять від IoT-пристроїв, веб-ресурсів, локальних сховищ, проходять очищення, фільтрацію, нормалізацію та інтеграцію.

Fog Nodes виконують попередню обробку даних та формують метадані, а хмара використовується лише для їх довготривалого зберігання. Такий підхід значно знижує затримки та розвантажує центральні сервери. Архітектура BFAN підвищує мобільність і масштабованість IoT-додатків, а також захищає від несанкціонованих доступів завдяки блокчейн-аутентифікації.

Комунікація між компонентами здійснюється у такому порядку:

1. Первинний (локальний) зв’язок.

Пристрої IoT – датчики, ноутбуки, комп’ютери, сенсорні панелі – взаємодіють між собою за принципом P2P. Зв’язок забезпечується Wi-Fi у межах середньої відстані та використовується для обміну чутливими даними з мінімальною затримкою.

2. Зв’язок із Fog Nodes.

Здійснюється як через бездротові канали, так і через дротові інтерфейси (CAT-5/6, оптичне волокно, TCP/IP). Локальний бездротовий канал використовується для комунікації з кінцевими пристроями.

Прямий і непрямий зв’язок:

- Прямий – між FN, що забезпечує низькі затримки та формує відмовостійку інфраструктуру.
- Непрямий – багатоадресна передача між пристроями у первинних і

вторинних сегментах мережі.

3. Масштабованість FN може змінюватися відповідно до потреб інфраструктури. Первинний рівень відповідає за локальний зв'язок, тоді як вторинний працює через зовнішні канали.

Блокчейн виконує функції аутентифікації, авторизації та контролю доступу до IoT-додатків, забезпечуючи цілісність і захищеність усієї системи.

Висновки.

В даному розділі були розглянені варіанти використання туманних обчислень для економії енергоспоживання в поєднанні з технологією Blokchain для надійного забезпечення безпеки. Туманні обчислення (ПК) використовуються для скорочення енергоспоживання і затримок для різнорідних комунікаційних підходів в додатках розумних міст Інтернету речей. Мета технології для інтелектуальних міст полягає в розвитку додатків на основі транзакційних відносин в режимі реального часу. На данний час можна зробити висновок , що існують різні системи підтримки IoT в інтелектуальних містах, але вони стикаються з такими проблемами, як безпека, незалежність платформ, і ресурсами управління. Новий підхід на основі на технологій блокчейн і FOG computing представляє собою захищену архітектуру Blockchain and Fog-based Architecture Network (BFAN) для додатків IoT в розумних містах. Дана архітектура забезпечує захист чутливих даних за допомогою шифрування, аутентифікація і блокчейн. Вона допоможе системним розробникам і архітекторам в розгортанні додатків в парадигмі розумних міст. Мета пропонованої архітектури - зменшити затримку і енергії, а також забезпечити поліпшені елементи безпеки за допомогою технології блокчейн.

ЗАГАЛЬНІ ВИСНОВКИ

Сучасний стан розвитку пристроїв та сервісів IoT має велику кількість питань, які потребують уваги. Найважливішими з них є питання забезпечення захисту даних. Загострення цього питання викликає велику кількість спроб втручань, як з зовнішнього так і внутрішнього боку, порушення цілісності, доступності і конфіденційності даних. Для майбутніх стандартів важливо усунути недоліки існуючих механізмів безпеки IoT. Керівництву міст слід приділяти пильну увагу захисту безпеки і недоторканності приватного життя, мережевим протоколам, управління ідентифікаційними даними та стандартизації, а також визначити ймовірність і наслідки загроз для IoT.

В даній роботі був проведений детальний аналіз загроз безпеці пристроям та сервісам IoT в середовищі розумного міста та розглянуто способи протистояння цим загрозам. Визначено, що найкраще використовувати комплексні методи – в нашому випадку це поєднання технологій Blockchain та Fog Computing. Дана технологія буде значно ефективнішою з точки зору безпеки порівняно з Fog computing та Cloud computing, але якщо порівняти її з технологією Fog computing, то затримки тут будуть більшими, адже ще буде йти час на обробку даних технологією Blockchain.

Даний метод заснований на технологіях блокчейн і туману представляє собою захищену архітектуру. Використання туманних обчислень сприяє скороченню споживання енергії і затримок для різних комунікаційних підходів в додатках розумних міст. Для вирішення цих проблем, туман обчислень забезпечує локальну обробку і зберігання IoT data на пристроях IoT замість відправки їх в хмару. На відміну від хмари, туман надає послуги з більш швидкою реакцією і більш високою якістю. Блокчейн допомагає забезпечити справжню надмірність і повну децентралізацію. Децентралізація об’єктів об’єднань в середовищі розумного міста є необхідною, адже якщо й

відбудеться атака, то постраждає не вся мережа об’єднаних елементів, а лише один вузол, який буде простіше відновити.

Мета додатків для інтелектуальних міст полягає в розвитку транзакційних відносин в режимі реального часу, тому використання цієї технології є доречним, тому що затримки в порівнянні з іншими технологіями менші. У реальному світі існують різні системи підтримки таких систем в інтелектуальних містах, але вони стикаються з такими проблемами, як безпека, незалежність платформ, багатофункціональність допомоги і ресурсами управління. Пропонована архітектура забезпечує захист чутливих даних за допомогою шифрування, аутентифікації і блокчейн. Вона допоможе системним розробникам і архітекторам в розгортанні додатків в парадигмі розумних міст.

Мета пропонованої архітектури - зменшити затримку і енергоспоживання, а також забезпечити поліпшені елементи безпеки за допомогою технології блокчейн. BFAN має здатність отримувати розташування вузла і інформацію про навколишнє середовище. Це надає великої ваги сучасному рівню енергоефективності та енергопослуг розумних міст. Також це допомагає забезпечувати швидке і масштабоване середовище обробки даних поблизу пристроїв IoT.

Поширення пристроїв IoT в навколишньому оточенні є необхідним, і це буде можливо, якщо в якості домінуючої опорної архітектури використовувати туман. Згідно з висновками, використання туманних обчислень в поєднанні з Blockchaine, IoT може мати кілька переваг: з точки зору витрат, Qos і, що більш важливо, безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Newman, Peter. “There Will Be More Than 55 billion IoT Devices by 2025—These Are the Biggest Drivers For Adoption.” [Електронний ресурс] – Режим доступу до ресурсу: https://www.businessinsider.com/internet-of-things-report?op=1

2. Рішення Київської Міської Ради [Електронний ресурс] – Режим доступу до ресурсу: https://kmr.gov.ua/sites/default/files/461-6512.pdf

3. Ініціатива Kyiv Smart City [Електронний ресурс] – Режим доступу до ресурсу: https://www.kyivsmartcity.com/initiative/

4. Як “розумні” технології дозволяють керувати Києвом з планшета [Електронний ресурс] – Режим доступу до ресурсу: https://www.ukrinform.ua/rubric-kyiv/2790966-klicko-pokazav-ak-rozumni-tehnologii-dozvolaut-keruvati-kievom-z-plansetu.html

5. Приклади 5 населених пунктів в Україні, які реалізовують Smart City [Електронний ресурс] – Режим доступу до ресурсу: https://sites.google.com/site/666smartcity/prikladi-5-naselenih-punktiv-v-ukraieni-aki-realizovuut-smart-city.

6. Smart-інновації українських міст [Електронний ресурс] – Режим доступу до ресурсу: http://www.urbanua.org/dosvid/ukrayinski-pryklady/340

7. T. H. Luan et al., “Fog Computing: Focusing on Mobile Users at the Edge,” arXiv preprint arXiv:1502.01815 (2015).

8. K. Habak et al., “7 Elastic Mobile Device Clouds: Leveraging Mobile Devices to Provide Cloud Computing Services at the Edge,” Fog for 5G and IoT, 2017.

9. M. Chiang et al., “Clarifying Fog Computing and Network ing: 10 Questions and Answers,” IEEE Commun. Mag., vol. 55, no. 4, Apr. 2017, pp. 18–20.

10. A. Manzalini and N. Crespi, “An Edge Operating System Enabling AnythingasaService,” IEEE Commun. Mag., vol. 54, no. 3, Mar. 2016, pp. 62–67.

11. K. Hong et al., “Mobile Fog: A Programming Model for LargeScale Applications on the Internet of Things,” Proc. 2nd ACM SIGCOMM Wksp. Mobile Cloud Computing, Aug. 2013, pp. 15–s20.

12. L. M. Vaquero and L. RoderoMerino, “Finding Your Way in the Fog: Towards a Comprehensive Definition of Fog Com puting,” ACM SIGCOMM Computer Commun. Review, vol. 44, no. 5, 2014, pp. 27–32

13. S. Yi, Z. Qin, and Q. Li, “Security and Privacy Issues of Fog Computing: A Survey,” Proc. Int’l Conf. Wireless Algorithms, Systems, and Applications, 2015, pp. 685–695.

14. M. Al Faruque and K. Vatanparvar, “Energy Management- as-a-Service Over Fog Computing Platform,” IEEE Internet of Things J., vol. 3, no. 2, 2012, pp. 161–169.

15. Y.W. Law et al., “Wake: Key Management Scheme for Wide-Area Measurement Systems in Smart Grid,” IEEE Communications Mag., vol. 51, no. 1, 2014, pp. 34–41.

16. K. Hwang, S. Kulkareni, and Y. Hu, “Cloud Security with Virtualized Defense and Reputation-Based Trust Management,” Proc. 8th IEEE Int’l Conf. Dependable, Autonomic, and Secure Computing (DASC), 2009, pp. 717–722.

17. L. Ma, A.Y. Teymorian, and X. Cheng, “A Hybrid Rogue Access Point Protection Framework for Commodity Wi-Fi Networks,” Proc. 27th IEEE Conf. Computer Comm., 2008; doi:10.1109/infocom.2008.178.

18. W. Wei, F. Xu, and Q. Li, “MobiShare: Flexible Privacy- Preserving Location Sharing in Mobile Online Social Networks,” Proc. IEEE Conf. Computer Comm., 2012, pp. 2616–2620.

19. S. Forsstr¨om, I. Butun, M. Eldefrawy, U. Jennehag, and M. Gidlund, “Challenges of securing the industrial internet of things value chain,” in 2018 Workshop on Metrology for Industry 4.0 and IoT. IEEE, 2018, pp. 218–223.

20. O. What we do [Електронний ресурс] – Режим доступу до ресурсу: https://www.openfogconsortium.org/what-we-do/.

21. Gupta, H.; Vahid Dastjerdi, A.; Ghosh, S.K.; Buyya, R. iFogSim: A

toolkit for modeling and simulation of resource management techniques in the Internet of Things, Edge and Fog computing environments. Softw. Pract. Exp. **2017**, 47, 1275–1296.

22. Solutions, C.F.C. Unleash the Power of the Internet of Things; Cisco Systems Inc.: San Jose, CA, USA, 2015.

23. Li,W.; Yang, T.; Delicato, F.C.; Pires, P.F.; Tari, Z.; Khan, S.U.; Zomaya, A.Y. On enabling sustainable edge computing with renewable energy resources. IEEE Commun. Mag. **2018**, 56, 94–101.

24. M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, “Bubbles of trust: A decentralized blockchain-based authentication system for IoT,” Computers & Security, vol. 78, pp. 126–142, 2018.

25. “On the features and challenges of security and privacy in distributed internet of things,” [Електронний ресурс] – Режим доступу до ресурсу: http://dx.doi.org/10.1016/j.comnet.2012.12.018.

26. “Juno: Smart contracts running on a bft hardened raf t[Електронний ресурс] – Режим доступу до ресурсу: https://github.com/kadena-io/juno.

27. “Blockchain app development simplified tendermint.” [Електронний ресурс] – Режим доступу до ресурсу: https://tendermint.com/.