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

Інститут телекомунікаційних систем

Кафедра Інформаційно-телекомунікаційних мереж

До захисту допущено:

Завідувач кафедри

_____ Лариса ГЛОБА

«___»_____2020 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Інформаційно-комунікаційні технології»

спеціальності 172 «Телекомунікації та радіотехніка»

на тему: «Потенційні загрози інтернету речей і способи їх подолання»

Виконала:
студентка IV курсу, групи ТІ-61
Піхота Катерина Володимирівна _____

Керівник:
Доцент кафедри ІТМ ІТС, доцент, к.т.н.
Кононова Ірина Віталіївна _____

Рецензент:
Професор кафедри ТК ІТС, професор, д.т.н.
Романов Олександр Іванович _____

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

Київ – 2020 року

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

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 «Телекомунікації та радіотехніка»

Освітньо-професійна програма «Інформаційно-комунікаційні технології»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Лариса ГЛОБА
«___»_____2020 р.

ЗАВДАННЯ

на дипломну роботу студенту
Піхоти Катерини Володимирівни

1. Тема роботи «Потенційні загрози інтернету речей та способи їх подолання», керівник роботи доцент кафедри інформаційно-телекомунікаційних мереж ІТС Кононова Ірина Віталіївна, доцент, к.т.н., затверджені наказом по університету від «30» березня 2020 р. № 924-с
2. Термін подання студентом роботи 8 червня 2020 р.
3. Вихідні дані до роботи
    1. Середовище Smart city
    2. Blockchain
4. Зміст роботи
    2. Аналіз існуючих загроз, сутність та поняття технології .
    3. Використання computing, як гарант безпеки в середовищі Smart city
    4. Blockchain та Fog based architecture для IoT в середовищі Smart city
5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо)

    Плакат №1 (слайд) Тема роботи, мета, об’єкт та предмет дослідження, завдання дослідження;
    Плакат №2 (слайд);
    Плакат №3 (слайд);
    Плакат №4 (слайд);
    Плакат №5 (слайд) Висновки по роботі, напрями подальших досліджень.

6. Дата видачі завдання 25.01.2020

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1.	Отримання завдання	25.01.2020	виконано
2.	Збір інформації	01.04.2020	виконано
3.	Аналіз загроз приладам та сервісам IoT	15.04.2020	виконано
4.	Ознайомлення зі способами захисту приладів та сервісів IoT в середовищі Smart City	01.05.2020	виконано
5.	Визначення найоптимальнішого способу захисту IoT в середовищі Smart City	15.05.2020	виконано
6.	Оформлення дипломної роботи	01.06.2020	виконано
7.	Отримання допуску до захисту	08.06.2020	виконано

Студент Катерина ПІХОТА

Керівник Ірина КОНОНОВА

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: IoT, безпека, FOG, Blockchaine, захист даних, Smart City.

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. Сучасна ситуація в області інтернету речей

Впровадження послуг Інтернету речей значно прискорилось, так як багато галузей визнали, що послуги IoT можуть надати значні переваги споживачам, підприємствам і державним установам. З огляду на широкий спектр послуг та продуктів, заснованих на IoT, їх швидке впровадження в повсякденне життя та все більш чутливу і критично важливу роль, яку вони можуть грати, забезпечення безпеки повинно бути головним пріоритетом.

Поява послуг на основі IoT вже створює вибуховий попит на нові пристрої і додатки. Так дослідження Business Insider прогнозує, що «до 2025 року буде більш ніж 55 мільярдів IoT-пристроїв в порівнянні з 9 мільярдами в 2017 році» [1]. Далі прогнозується, що «сукупні інвестиції в IoT в період між 2017 і 2025 рр. складуть близько 15 трлн. доларів, показуючи, що плани компаній інвестувати в IoT-рішення прискорюються ».

Ця величезна мережа фізичних пристроїв стала можливою завдяки вбудованій електроніці, програмному забезпеченню, датчикам і виконавчим механізмам, які допомагають пристроям IoT з'єднуватися один з одним і обмінюватися даними. Підключення цих розрізнених пристроїв привело до широкого спектру споживчих додатків.

В даний час існує п'ять типів додатків IoT:

- Побутовий IoT - такі як світильники, побутова техніка та голосова допомога для літніх людей.
- Комерційний IoT - застосування IoT в сфері охорони здоров'я і транспорту, таких як інтелектуальні кардіостимулятори, системи моніторингу та зв'язок між транспортними засобами .

- Промисловий Інтернет речей - включає в себе цифрові системи управління, статистичну оцінку, інтелектуальне сільське господарство і великі промислові дані.
- Інфраструктура IoT - забезпечує можливість підключення «розумних» міст за рахунок використання датчиків інфраструктури, систем управління і зручних для користувача додатків.
- Військові речі - застосування технологій IoT у військовій області, наприклад роботи для спостереження.

І хоча про побутовий IoT-простір говорять найбільше, важливо також відзначити, що великий сегмент IoT потрапляє в промисловий простір. Він включає в себе ряд унікальних додатків, таких як автоматизація виробництва, управління інфраструктурою, управління запасами і активами, інтелектуальні мережі, електролічильники і управління енергоспоживанням. Це допомагає знизити виробничі витрати, пильно стежачи за продуктивністю співробітників, надаючи покупцям великий досвід і забезпечуючи безпеку магазинів від крадіжки.

Але багато організацій все ще ігнорують технологію IoT через недостатню обізнаність і нездатності протистояти загрозам. Все змінюється з використанням Інтернету речей.

Як на споживчому, так і на промисловому ринках можливості IoT безмежні, і більш широке впровадження обіцяє зробити наші повсякденні завдання простішими, ефективними і приємними як на роботі, так і вдома.

На сьогоднішній день є актуальним питання розвитку інфраструктури міст. Протягом історії людства міста намагалися забезпечити своїм жителям більш високу якість життя, безпечне і комфортне середовище і економічне процвітання. В даний час громадяни розраховують на те, що зі своїх міст вони будуть користуватися ергономічним транспортом, чистим повітрям, відповідальним споживанням комунальних послуг, постійною взаємодією з міськими адміністраціями, прозорим управлінням, належними системами

охорони здоров'я та освіти і значними культурними об'єктами. Щоб забезпечити ці запити, місто має стати «розумним». Ідея Smart City визначається як майбутнє, кращий стан існуючого міста, де використання і експлуатація як матеріальних (тобто транспортної інфраструктури, енергетичних мереж та природних ресурсів), так і нематеріальних активів (тобто людський капітал, інтелектуальний капітал компаній і організаційний капітал органів державного управління) оптимізуються.

На сьогоднішній день виділяють розвиток декількох цілей, необхідних для досягнення успішного функціонування розумних міст:

• інтелектуальну мобільність (управління рухом, спільне використання велосипедів / автомобілів / мікроавтобусів, контроль за кондиціонуванням доріг, систему стоянки, планування маршрутів, електромобілі);

• енергію (виробництво / розподіл / зберігання електроенергії, управління енергією, розумний вимірювальний прилад, оптимізація вуличного освітлення);

• Громадську безпеку (відео / радіолокаційне / супутникове спостереження, екологічний і територіальний моніторинг, захист дітей, тобто більш безпечний домашній моніторинг, екстрені рішення, раціональне видалення відходів, якість повітря, метеорологічні дані для очищення снігу);

• розумне управління (транспарентний процес прийняття рішень, більш широку участь громадян в законодавчих ініціативах, державно-приватні партнерства; онлайнові системи оподаткування);

• розумну економіку (робочі місця високого рівня, конкурентоспроможність, підприємницький дух, інновації та дослідження в цій області);

• розумне життя (культурні і освітні об'єкти, заходи, розваги та екскурсії, доступ до культурних пам'яток і історичних пам'ятників);

Відносини між містом і розумним громадянином повинні характеризуватися відкритістю міст, яка визначається як здатність систем забезпечувати інноваційну діяльність з урахуванням інтересів користувачів в

рамках існуючих і нових послуг, розробка послуг на основі широкої участі і наявність відкритої платформи даних. Крім того, обов'язковими є інновації в сфері послуг, налагодження партнерських відносин і підвищення активності в містах (ступінь, в якій інтелектуальні міські служби просуваються в напрямку сталого використання енергії, а також послуг з використанням ІКТ).

В останні роки досягнення цих цілей все більше і більше залежить від технології, особливо ІКТ. Отже, один з основних нюансів терміна "розумне місто" обумовлений впровадженням ІКТ в міську інфраструктуру з такими рішеннями, як міські операційні системи, централізовані кімнати управління, міські приладові панелі, інтелектуальні транспортні системи, інтегровані проїзні квитки, схеми спільного використання велосипедів, дисплеї інформації про пасажирах в режимі реального часу, системи управління логістикою, смарт-енергосистеми, кероване освітлення, смарт-метро, сенсорні мережі, системи управління будівлями, різні додатки для смартфонів і економні платформи і т.д. .

Інтернет речей займає центральне місце серед цих технологій. У IoT фізичні речі підключаються до інших фізичних і віртуальним речей, використовуючи бездротовий зв'язок і пропонуючи контекстні послуги. IoT базується на глобальній інфраструктурної мережі, яка з'єднує унікально ідентифіковані об'єкти, використовуючи дані, зібрані датчиками і приводами, і обладнання, що використовується для зв'язку і локалізації. Радіочастотна ідентифікація (RFID) лежить в основі цієї розробки, але IoT розробила шляхом включення таких технологій, як датчики, друковані електронні або коди, PLC, Enocean, GPS, мобільні (2G / GSM, 3G, 4G / LTE, GPRS) та ближнього радіусу дії (NFC, Bluetooth, Zigbee, Wi-Fi, ANT, Z-Wave, IEEE 802.15.4) зв'язку. Співпраця між кібер-реальними артефактами змінює міську інфраструктуру, і їх автономні і кочові характеристики можуть привести до серйозних проблем безпеки, які повинні бути зрозумілі і вирішені своєчасно. Однією з ключових завдань IoT в області створення інтелектуальних міських

програм є забезпечення їх надійності, включаючи питання етики, безпеки (конфіденційності / цілісності / доступності), надійності і гнучкості з урахуванням швидко мінливих екологічних умов. Без гарантій того, що пов'язані між собою об'єкти точно сприймають навколишнє середовище і обмінюються даними та інформацією безпечним чином, користувачі неохоче йдуть на впровадження цієї нової технології. Довіра населення до компонентів IoT в розумному місті тісно пов'язане з поняттями ризику, безпеки та забезпечення приватного життя, які повинні бути належним чином враховані міським керівництвом.

1.2 Досягнення та проблеми Smart City в містах України

Україна має позитивну тенденцію за групою рейтингів економічного розвитку. Відбулося суттєве покращення позицій за глобальним інноваційним індексом 2018: Україна посіла найвищу позицію за останні 12 років – 43 місце із 126 країн, що потрапили до рейтингу[2].

На жаль, впровадження технологій Smart City в міста України відбувається не такими швидкими темпами, як того б хотілося. Але на сьогоднішній день цілий ряд українських міст може похвалитися своїми «розумними» впровадженнями в інфраструктуру міста.

Лідером цього списку безсумнівно є Київ. У 2017 році Київська міська рада затвердила Концепцію «Київ Смарт Сіті 20202»[3]. Ця концепція була затверджена з метою формування планів розвитку головних напрямків столиці з метою залучення у прийнятті рішень громадськості. Періодично тут затверджується Комплексна цільова міська програма «Електронна столиця», в якій затверджуються цілі, які необхідно втілити, за визначений термін.

Робота цієї ініціативи базується на принципах відкритих даних, розумного використання цифрових послуг та прозорого управління[4]. Абсолютно будь-яка людина може долучитися до цієї ініціативи або запропонувати своє рішення в даній області.

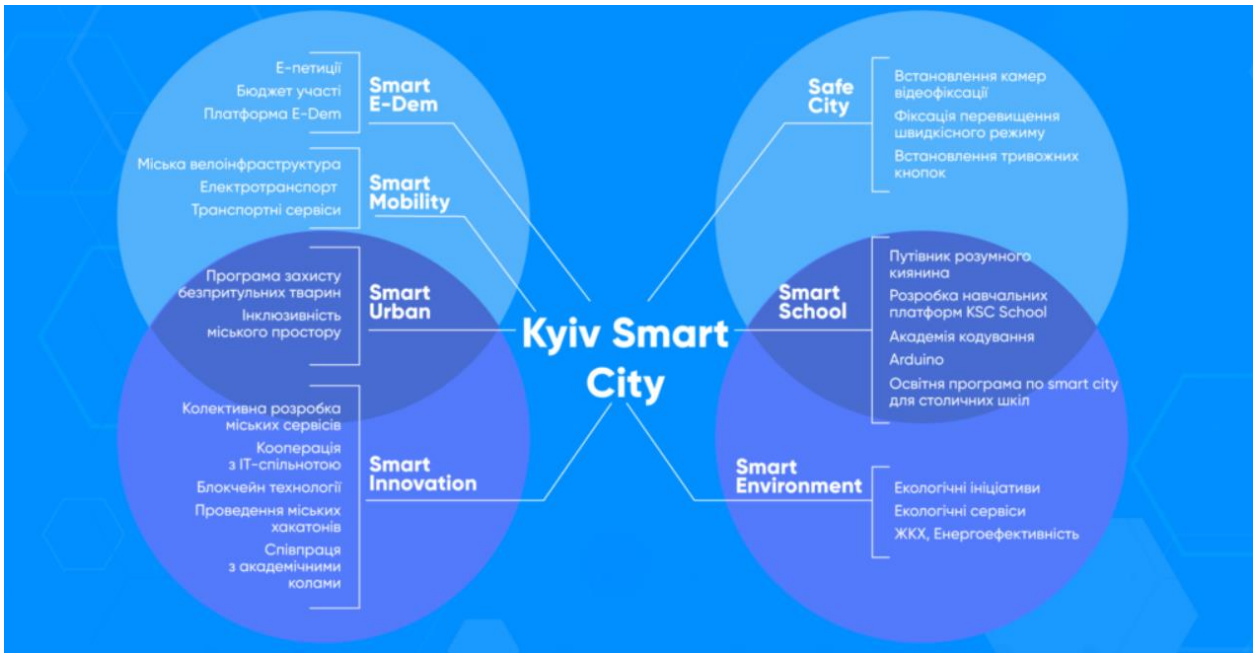

Рис. 1.1 Схема галузей проекту Smart City

Нині в Києві в повному обсязі функціонують реалізується ідея публічності прийняття рішень, влада в повному обсязі зробила відкритий доступ громадськості до документообігу Київ міськдержадміністрації, створила систему електронних торгів та відкритих тендерів, і реалізувала систему електронного бюджету. Так наприклад, в столиці кожного року проходить проект ГБ – громадський бюджет, до якого громадяни вносять власні ідеї покращення інфраструктури міста, або стартапи, які підуть на користь його жителям. Громадяни міста голосують за ці проекти в онлайн форматі та обирають найкращий проект. За підсумком, в наступному прийнятті бюджету міста бронюються кошти на реалізацію даного проекту чи стартапу. Дана ініціатива є прикладом прозорого обороту бюджету та суспільного прийняття рішення містян. Успішним також є проект «Безпечне місто», головною функцією якого є посилення безпеки киян, управління транспортним трафіком в місті та контролем комунальних служб. Уже сьогодні в столиці встановлено більше 5 тисяч камер відеоспостереження, як можуть розпізнавати номерні автомобільні знаки та обличчя людей. За допомогою GPS-трекерів та бортових комп'ютерів, встановлених у авто комунальної техніки, можна контролювати її роботу. Під онлайн-контролем

сьогодні 1 211 одиниць громадського транспорту та 729 технологічних машин[5].

У місті Львів за останній рік було прокладено 80 кілометрів велодоріжок, побудовано 6 муніципальних пунктів велопрокату, почались впровадження пунктів заряду електромобілів та електронних паркоматів. Також у місті був представлений перший в Україні електробус «Електрон» [6].

Своїми темпами розвитку вражає місто Дніпро. В місті дуже швидко впроваджується система e-gov і збільшується кількість електронних адміністративних послуг. У Дніпрі існує ряд сервісів та додатків, що робить життя людей комфортнішим та безпечнішим. Наприклад, сервіс електронної інвентаризації доріг Navizor, дозволяє оцінювати їх стан доріг і стежити за якістю виконання робіт підрядниками. Створений дніпровськими IT-волонтерами додаток "Моя поліція" для екстреного виклику поліції вже впроваджено в Києві і Дніпрі, а функція "Активний свідок" дозволяє громадянам відправляти в поліцію зафіксовані факти правопорушень[7].

У Харкові діє найбільша географічна інформаційна система муніципального управління. На інтерактивних картах ви можете знайти всі дані про спільну власність, генплан, правила будівництва і правила розвитку територій,

інформація про розподіл земель, комунікаційних планах та вартості землі.

Дані про звернення громадян, розкопках, ремонти та нещасні випадки є в Інтернеті на єдиній мапі онлайн звернень громадян. За допомогою мобільного додатка "Активний житель Харкова" проводиться онлайн-голосування з різних питань міського життя: розвиток інфраструктури, озеленення, паркування і т.д.

Розумне місто – це не наше майбутнє, а наша реалія. Воно потребує інвестицій в свій розвиток, а наші міста не можуть цього забезпечити в повній мірі. Українські міста в порівнянні з європейськими є біднішими,

тому пріоритетом є забезпечення життєдіяльності міста, інновації відходять на другий план.

1.3 Проблеми безпеки в середовищі Smart city

Світ переживає еволюцію Розумних Міст. Вони є наслідком інновацій в області інформаційних і комп'ютерних технологій, які, створюючи нові економічні та соціальні можливості, створюють проблеми для нашої безпеки і очікування щодо недоторканності приватного життя.

Переваги ІКТ в Smart City і IoT величезні. Лічильники розумної енергії, охоронні прилади, смарт-пристрої в області охорони здоров'я і сімейного життя: ці та інші зручності та підвищення якості життя міської інфраструктури і послуг змінюються в міру появи нових взаємопов'язаних систем моніторингу, контролю та автоматизації.

Ці переваги слід розглядати з урахуванням потенційної шкоди, яку може бути завдано в цьому взаємопов'язаному світі. Технічні, адміністративні та фінансові чинники повинні бути з урахуванням правових, політичних і соціальних умов міста.

В той час як сучасні "класичні" інтернет-атаки можуть завдати шкоди конфіденційності, цілісності та доступності інформації, аналогічні дії в IoT можуть привести навіть до загибелі людей. На сьогоднішній день зафіксовано безліч випадків втручання хакерів в роботу бортових комп'ютерів автомобілів / літаків і нападу в хірургічних відділеннях або на пацієнтів з імплантованими інсуліновими насосами або іншими медичними пристроями.

Оскільки перелік вразливих систем включає системи опалення, мережі розподілу продовольства, лікарні, системи світлофорів, транспортні мережі, які тісно пов'язані між собою в розумному місті, сценарії нападу, які можна

було б передбачити починаючи з цього моменту, дійсно лякають. В результаті в IoT значно зростає значення заходів безпеки.

Труднощі, пов'язані із забезпеченням безпеки IoT, обумовлені наступними факторами:

• Крім нападників, автономна поведінка речей, які невидимо спілкуються один з одним, може впливати на наше життя, і це все ще важко передбачити. Прогнозування небезпек в IoT через серйозне сканування уразливості стає необхідністю, але процес є важким і може бути виконаний тільки за допомогою постійних досліджень і практичних зусиль.

• Ландшафт IoT фрагментований, тому що його застосування засновані на різних архітектурах, стандартах і програмних платформах різної складності. Кожне розумне місто розробляє власні технологічні рішення, реагуючи на свої власні проблеми і можливості. У багатьох ситуаціях прилади, технології та їх прошивки захищені комерційною таємницею. Правові рамки поки не є адекватними, а юридичні обов'язки недостатньо ясні. Існуючі рішення не пов'язані між собою і не стандартизовані, створюючи так звані технологічні відокремленості; крім того, в них бере участь велика кількість суб'єктів, і різні регіони систем контролюються різними організаціями. Навіть це невичерпний виклад питань безпеки, пов'язаних з IoT, є тривожною ознакою того, що в розумному місті кожен житель повинен бути впевнений в тому, що він захищений ефективними технічними, економічними, правовими та соціальними заходами. Далі, вищезгадані проблеми будуть розглядатися в рамках, в яких розумні міста розглядаються як синергетична сума інтелектуальних пристроїв, що генерують величезну кількість даних, працюючи на благо розумних громадян.

Дані, що збираються розумними речами, перебувають в центрі розумних міст. Проблема полягає в тому, що мова йде про конфіденційних даних, які часто збираються без прямої згоди громадян. Наприклад, повідомлення, медичні та академічні записи, особисті фотографії, зустрічі,

інформація про банківський рахунок, контактів та іншої інформації можуть використовуватися інфраструктурою розумних міст при прийнятті більш-менш заходів безпеки. Безпечне об'єднання даних IoT з різних джерел є серйозною проблемою в розумному місті, оскільки немає гарантованих довірчих відносин між залученими сторонами. Що стосується майнових прав на дані та інформацію, то труднощі виникають у зв'язку з правильною ідентифікацією авторів: наприклад, відповідь на питання: "Хто є власником даних, що витягають за допомогою датчиків, підключених до IoT важко уявити. Коли інформація особиста або фінансова, все стає серйозніше. Всюдисущність зробить кордон між громадським та приватним простором невидимими, і люди не знатимуть, де закінчується їх інформаційна безпека. На конфіденційність користувачів сильно впливає той факт, що об'єкти оснащені датчиками, які дозволять їм "бачити", "чути" або навіть "відчувати". Дані, що реєструються датчиками, передаються в великих кількостях і різними способами через мережі, що може завдавати шкоди приватному життю людини. Наприклад, сучасні середні інтелектуальні мобільні пристрої і прикладні програми здатні реєструвати пробіг користувача, кров'яний тиск, імпульси і інші інтимні медичні дані, які можуть зберігатися або направлятися та можуть представляти інтерес до них без прямої згоди користувача.

Різні технології дозволяють отримувати ідентифіковану інформацію особистого характеру і дані на рівні домашніх господарств про громадян (їх характеристиках, їх місцезнаходження, переміщення і діяльності), об'єднувати ці дані для отримання нових похідних даних, і використовувати їх для створення профілів людей і місць і прийняття рішень про них. Наприклад, розумна будівля чутлива з точки зору стану навколишнього середовища (температура, вологість, дим, CO2, екстремальний світло, забруднення повітря, зовнішнє присутність), а також здатна визначити дуже точний профіль користувача на основі його звичок. Транспортні засоби є активними членами міст; вони взаємодіють один з одним, з водіями /

пасажирами і з пішоходами. Вони мають вбудовані комп'ютери, GPS-приймачі, бездротові мережеві інтерфейси ближнього радіусу дії і потенційно мають доступ до бортових датчиків і Інтернету. Інфраструктура розумного міста може зчитувати дані про транспортні засоби, які використовують радари, детектори Bluetooth і камери номерних знаків. Швидкість, потік і час руху відомі таким чином і можуть бути пов'язані з особистістю водія. Згідно з цим пунктом відстеження може виявити чутливі місця, такі, як вдома або на роботі, а також час і тривалість кожного відвідування, що фактично дозволяє скласти докладний опис поведінки водіїв, інформацію про найважливіші з точки зору безпеки події, швидкість, адреси місця призначення, будинки і місця роботи, час, проведений в конкретному місці, і т.д.

У розумному місті зона атаки розширена. Звичайні проблеми пов'язані з умисним пошкодженням / розкраданням пристроїв, нападами на пристрої / компоненти, призначені для рециркуляції, шкідливою програмою і фішинговими атаками, атаками з використанням неправдивих мереж або соціальною інженерією. Але є і численні нові проблеми, які роблять сценарії атаки невичерпними. Перш за все відзначається велике і зростаюче число нападів з використанням датчиків. Починаючи з наших кишень, ми повинні визнати, що інвентаризація сенсорів в смартфоні лякає: чіпи GPS, мікрофони, камери, акселерометри, гіроскопи, сенсори близькості, магнітометри, датчики навколишнього світу, сканери відбитків пальців, барометри, термометри, педометри, монітори частоти серцевих скорочень , датчики, здатні виявляти шкідливе випромінювання, світлові датчики RGB. Такі датчики визначають місце розташування мобільного телефону, таким чином допомагаючи користувачам орієнтуватися в містах за допомогою карт / зображень, вимірювати положення, нахил, удар, вібрацію і прискорення (швидкість зміни швидкості), обертання / скручування, виявляють присутність близьких пунктів без будь-якого фізичного контакту , фіксують яскравість навколишнього світу, вимірюють атмосферний тиск, передають

дані про висоту, виявляють хвилинні пульсації кровоносних судин в пальці і обчислюють пульс. Вони можуть фіксувати місце розташування, рух, тимчасові позначки, навіть особисті розмови і фонові шуми. В результаті, смартфон може використовуватися для спостереження за об'єктом. Це в поєднанні з можливістю установки програмного забезпечення третьої сторони і тим фактом, що смартфон тісно пов'язаний з людиною, робить його корисним інструментом шпигунства. З іншого боку, використання цих датчиків в різних областях застосування, кількість і мета зібраних даних не в повній мірі розуміються і контролюються їх власниками. Наприклад , відео та зображення можуть розкривати соціальне коло і поведінку громадянина абсолютно несподіваним чином; крім того, смартфони все частіше стають мішенню шкідливого ПО, яке отримує доступ до мікрофона, камери і іншим датчикам. Різні нові атаки також допускаються за допомогою технології зв'язку ближнього радіусу дії. Zigbee є глобальним стандартом і протоколом, розробленим в якості легкого бездротового зв'язку для допомоги розумним об'єктам звертатися один до одного загальним і простим способом. При низьких витратах і високої ефективності технології Zigbee використовуються в багатьох областях, таких як автоматизація будинку, промисловий контроль або збір медичних даних. Системи з підтримкою Zigbee уразлива до загроз безпеці, таким як відстеження трафіку (підслуховування), декодування пакетів і маніпулювання даними. Переходячи до Bluetooth, деякі атаки з синім префіксом є Блюджекінг (спам прилеглих користувачів об'єктів з незапрошенной повідомленнями), блюснарфінгом (крадіжка контактної інформації, знайденої на вразливих пристроях) і блютбукінгом (доступ до команд смарт-об'єктів без повідомлення або оповіщення їх користувача).

Висновки:

IoT стикається з низкою загроз, які повинні бути визнані для прийняття захисних заходів. У цьому розділі були представлені проблеми безпеки та

загрози безпеці Інтернету речей. Мета цього розділу полягала в тому, щоб дати детальний огляд потенційних загроз, атак і вразливостей, в контексті інтелектуальних міст.

Було досліджено головні досягнення впроваджень IoT в інфраструктуру міст України та проведено огляд найбільш важливих проблем безпеки IoT з особливим акцентом на проблеми безпеки, пов'язані з пристроями і послугами IoT.

Був зроблений висновок про те, що 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.

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

2.1 Архітектрура Fog Computing

Останні досягнення в області апаратних засобів, програмного забезпечення і комунікаційних технологій, таких як 5G, Li-Fi, і малопотужних глобальних мереж LPWAN привели до появи Інтернету речей. В основному, IoT відноситься до мережевих об'єктів та пристроїв, але його значення набагато більше. IoT вже почав проникати в різні аспекти нашого життя з технологіями в розумних будинках, розумних містах, природи і навколишньому середовищі, промисловості і сільському господарстві, енергетиці, медицині і охороні здоров'я, і так далі. Базова архітектура системи для цих потенційних послуг все ще розробляється і тестується, в той час як проводиться величезна робота по стандартизації IoT, і вивчаються рішення для сумісності, масштабованості, зручності використання, конфіденційності та безпеки. Хмарні обчислення забезпечують платформу для доступу до різних обчислювальних ресурсів з більш широкими можливостями з точки зору зберігання і обробки, що дає доступ до хмарних послуг з будь-якого місця та в будь-який час.

Cloud може надавати послуги у вигляді інфраструктури як послуги (IAA), платформи як послуги (PAA), і програмного забезпечення як послуги (SAAS). Сьогодні майже 90% світових користувачів Інтернету покладаються на хмарні послуги[3]. Аналізуючи поточні тенденції, можна зробити висновок, що хмара і IoT будуть діяти як комплексні ментальні технології майбутнього Інтернету, утворивши хмара речей . IoT отримає перевагу від необмежених ресурсів хмари і капабільних властивостей. Аналогічно, хмара може взяти користь від IoT, розширивши сферу свого охоплення, щоб управляти реальними послугами динамічно і широко розподілено. Крім того,

за останнє десятиліття в геометричній прогресії зросло поширення мобільного зв'язку. Сучасні смартфони містять в середньому більше десятка датчиків. З різними розумними пристроями, повсюдно приносять в руки людей обчислення і комунікації, останнім часом з'явилося безліч мобільних послуг. Хмарні обчислення забезпечують меншу затратність , масштабованість, зберігання даних і управління ними, що робить інтеграцію хмарних і мобільних пристроїв неминучою.

Однак для того, щоб така плавна інтеграція стала реальністю, необхідно вирішити ряд проблем, з тим щоб створити надійний механізм надання послуг. Мобільні користувачі запитують більш різноманітні види послуг в порівнянні з традиційними користувачами комп’ютерів. Спектр послуг варіюється від хмарного зберігання, моніторингу здоров'я, IoT, миттєвих повідомлень (IM)і до доповненої реальності, мультидіа потоку, навігації, кіберфізичних систем і багатьох інших . Управління такими різноманітними запитами на послуги від мільярдів кочових мобільних користувачів стає надзвичайно складним для централізованої хмари [8]. Крім того, мобільні пристрої природним чином обмежені в ресурсах, і з атрибутом мобільності, стає необхідним о завантажувати деякі завдання в хмару. З останніми досягненнями опора на хмару стає все більш необхідним. Проте, оскільки відстань між хмарою і мобільними пристроями, як правило, велика, стає важливим досягнення надійного зв'язку в реальному часі. Для вирішення проблеми великих затримок між IoT або мобільними пристроями і хмарою, FOG Computing став багатообіцяючою парадигмою для доповнення хмарних послуг.

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.

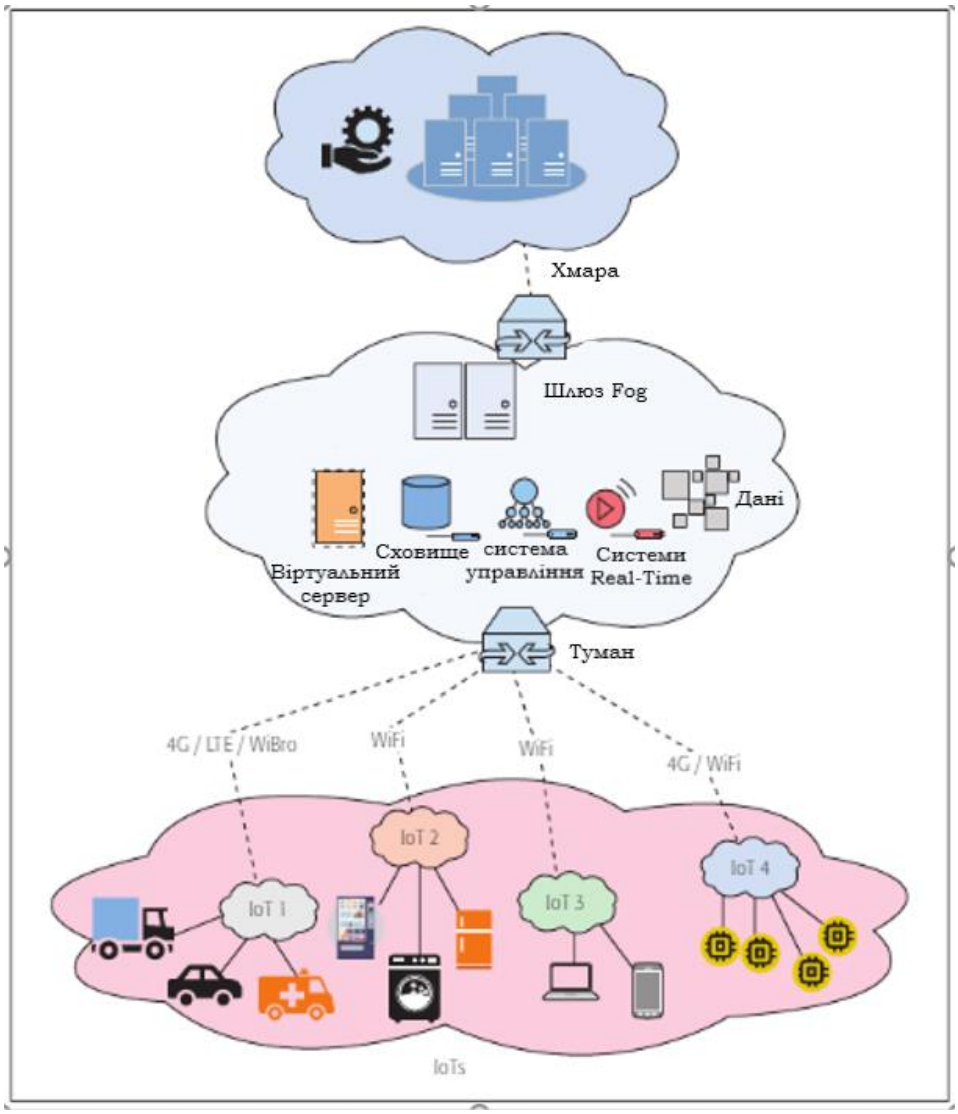

Рис.2.2 Загальна архітектура туманних обчислень

Концепція туманних обчислень полягає в тому, щоб наблизити мережеві ресурси до вузлів, що генерують дані, які знаходяться на найнижчому рівні сприйняття. Fog – високо віртуалізована платформа, відповідальна за забезпечення обчислення, зберігання і мережеві послуги між кінцевими вузлами в середовищі IoT і традиційними хмарами [9]. Туман є архітектурою як для зв'язку, так і для управління мережею [10].

На рисунку 2.2 показана загальна архітектура туманних обчислень, де різні екземпляри виділених туманів забезпечують ресурсами об’єкти, що лежать в основі мереж або середовища IoT з мережами, такими як бездротові сенсорні мережі (WSNS), віртуальні сенсорні мережі (VSNS) Представлені VANETS і персональні обчислювальні мережі (PAN).

Рис.2.3 Рівні туманної архітектрури

На рисунку 2.3 показані основні рівні типові туманної архітектури. Фізичний рівень і рівень віртуалізації - це нижній рівень, який має справу з кожною одиницею "річ", яка здатна підключитися до Інтернет / мережі і генерувати дані. Вона містить вузли, пристрої, фізичні та віртуальні датчики, віртуальні сенсорні мережі, транспортні засоби та т.д. Всі такі вузли працюють відповідно до вимог служби і характеристикам вузла. На рівні моніторингу активації вузлів і мереж контролюються відповідно до потужності і завданнями вузла. Цей шар визначає наступну виконувану задачу і час. Вузли також контролюються на предмет їх енергоспоживання, з тим щоб можна було вживати ефективних заходів (наприклад, завдання оновлення) з урахуванням стану датчика. Рівень попередньої обробки

відповідає за управління даними. Тут проводиться детальний аналіз даних, і на основі отриманих результатів проводиться очищення і фільтрація даних з метою зведення до мінімуму непотрібної інформації. Шар зберігання відповідає за зберігання даних в тумані. Більша частина даних, що зберігаються в тумані, зберігається на тимчасовій основі. Для довгострокового зберігання хмара більш підходить, тому що вона має набагато більше ресурсів. Після того як дані будуть передані хмарі, їх, можливо, більше не потрібно буде зберігати в тумані. Деякі служби вимагають вжиття заходів безпеки і конфіденційності.

Повсюдна медична допомога і розумні медичні послуги дають дані про споживання їжі, які містять особисту інформацію про пацієнтів. У деяких випадках дані, що враховують місце розташування, можуть також бути конфіденційними. Рівень безпеки туману забезпечує належну безпеку та конфіденційність функцій для захисту даних перед їх відправкою по уразливому каналу. Як тільки дані готові для передачі хмарі, викликається транспортний шар, який передає їх в хмару, тим самим зменшуючи навантаження на основну мережу і дозволяючи хмарі створювати поліпшені сервіси набагато швидше. Ресурси туману розташовані між вузлами IoT і хмарним шаром [11]. Туман дозволяє створювати більш витончені, адаптовані і зрозумілі текстові сервіси через свою близькість до основних пристроїв. В результаті він забезпечує низький рівень латентності і високу якість потоків в мобільні вузли, включаючи рухомі транспортні засоби за допомогою проксі-серверів і точок доступу, розташованих поряд (наприклад, автомагістралі та залізничні шляхи) [12]. На основі зворотного зв'язку, отриманої від програми та / або хмари, і в залежності від обмежень вузлів, що генерують дані, туман може планувати зв'язок між машинами, вузлами, датчиками, сенсорними мережами і хмарою. Таким чином, забезпечується більш ефективне використання мережевих і хмарних ресурсів. Для деяких медичних послуг туман може обробляти дані відповідно до вимог кожної медичної служби. Він може виконувати попередню обробку необроблених

даних і передавати оброблені дані в хмару, які згодом перетворює попередньо оброблену інформацію, відправлену туманом, в поліпшені сервіси. Наприклад, служба охорони здоров'я може інформувати пацієнта про підвищення рівня цукру в крові або незвичайному серцебитті. З різними типами даних, що генеруються різнорідними вузлами, виникають питання сумісності. Туман може допомогти у вирішенні цієї проблеми, забезпечуючи швидке виконання завдань, пов'язаних з транскодуванням і перекладом, на місцевому рівні. Схожими є IoT і WSN федерації, в яких численні мережі IoT і WSN можуть бути інтегровані для розширення портфеля послуг, які вони надають. Ресурси однієї IoT можуть бути агреговані з ресурсами інший, створюючи велику IoT.

Незважаючи на те, що хмара і туман забезпечують обчислення, зберігання, застосування, інфраструктуру і ресурси даних, між двома парадигмами є деякі відмінності. Основна відмінність - доступність і близькість. Комп'ютерна інфраструктура туману розташована близько до основних вузлів (туман зазвичай розташовується в локальній мережі), в той час як хмара доступна через Інтернет з центром даних або сервером локації в будь-якій точці світу. Туман в основному пов’язує традиційну віддалену хмару з краєм, ближче до IoT, WSN, і окремими пристроям, які отримують до нього доступ. Таким чином, туман можна розглядати як нащадок хмари. Туман розширює хмару, щоб забезпечити додаткові вигоди для базових вузлів і мереж, використовуючи віртуалізацію для створення віртуальних датчиків і мереж, які необхідні для різних послуг [13]. Таким чином, туман додає додатковий шар між базовими вузлами і хмарою, що допомагає в аналізі даних, обробки, і фільтрації, і підвищує безпеку для чутливих даних (наприклад, місце розташування користувача, інформація про охорону здоров'я). У разі хмарних послуг, і особливо для мультимедіа, якість послуг сильно залежить від базової мережі. На відміну від цього, для додатків з затримкою, так як туман доступний локально, доступ до контенту може бути швидший при використанні ресурсів туманних обчислень. Аналогічним

чином, коли пристрої повинні розвантажити свої обчислення і обробку, туман є найкращим варіантом в порівнянні з хмарою. Хмара є більш централізованою, в той час як туман працює з розподіленими додатками .

У таблиці 1 представлені деякі з основних відмінностей між хмарою і туманними обчислювальними системами.

Таблиця 2.1.

Порівняння хмарної та туманної архітектури

Показник	Хмара	Туман
Географічне покриття	Глобальне	Локальне
Відстань між клієнтом та серверним вузлом	Декілька хопів	Один хоп
Доступність	Тільки Інтернет	Окремі ділянки Інтернету
Затримки	Високі	Низькі
Масштабність	Дата-центри	З відокремлених серверів до мікро дата-центрів
Цільовий користувач	Інтернет користувачі	Мобільно та ресурсно обмежені користувачі
Продовження таблиці 1.1.		
Ресурси	Практично безлімітні	Лімітовані та ресурсами, пам’яттю та обчисленнями
Масштаб послуги	Глобальні дані	Орієнтовані на клієнтів і додатки
Тип послуги	Інфраструктура як сервіс, платформа як сервіс, програмне забезпечення як сервіс	

Продовження таблиці 2.1.

Географічний розподіл розгортання	Централізований	Децентралізований
Зв'язок	Бездротовий та фіксований	Переважно бездротований
Генератор контенту	Людина	Прилади та сенсори
Основний споживач	Прилади(смартфони, комп'ютери, сервери)	Будь-які речі
Зберігання даних	Дні, роки	Тимчасово
Дані та безпека зв'язку	Залежить від сервісу	Додається додатковий рівень безпеки, перед тим як відправити дані до ядра
Пропускна здатність	висока	низька
Підтримка мобільності	обмежена	повна
Ціна за серверний пристрій	1500-3000	50-200
Операційні витрати	високі	низькі

2.2 Fog Computing з точки зору безпеки

Використання хмарної мережі для передачі та аналізу даних має такі обмеження, як споживання пропускної здатності та витрати на зв'язок .

Дані важливі для аудиторської мети або контролю над активами для підвищення ефективності або запобігання катастроф тощо . Якщо дані користувача є чутливими, безпека даних є ще одним важливим питанням.

Аналіз даних може бути зроблений на місці за допомогою запуску програмного забезпечення на місцевих станціях. Хмара буде

використовуватися для зберігання результатів аналізу для подальших цілей аудиту. Агрегація даних зменшить пропускну здатність, а також витрати, пов’язані з пропускною здатністю.

Туманні обчислення можуть служити потенційним рішенням через ряд відмінних характеристик, однією з яких є визначення місця розташування. FOG розглядають як концепцію застосування до додатків IoT, таких як спеціальні мережеві транспортні засоби і системи моніторингу здоров'я[14][15]. Туман вважається нетривіальним продовженням хмари, тому деякі проблеми безпеки і конфіденційності будуть зберігатися. Хоча деякі існуючі рішення в контексті хмарних обчислень можуть вирішувати багато питань безпеки та конфіденційності , але туман може створювати і нові проблеми безпеки і конфіденційності через ряд відмінних характеристик, таких як підтримка мобільності. Ці проблеми можуть вплинути на реалізацію туманних обчислень сумісно з IoT. З іншого боку, туманні обчислення можуть стати ідеальною платформою для вирішення багатьох питань безпеки та конфіденційності в IoT. Баланс обчислювальної потужності, зв'язності і діапазону управління дозволяє туману підтримувати додатки IoT і служити різним цілям безпеки. Протитуманні вузли можуть бути представлені як проксі, які забезпечують криптографічні обчислення, в той час як пристрої і датчики IoT під ними не мають необхідних для цього ресурсів. Таким чином, протитуманні обчислення можуть забезпечити не тільки додаткові обчислювальні ресурси, а й безпрецедентний рівень безпеки, який допоможе мінімізувати атаки в середовищі IoT.

Нижче узагальнено основні проблеми безпеки і конфіденційності в середовищі IoT.

Аутентифікація

Аутентифікація є однією з основних вимог безпеки пристроїв IoT. На жаль, багато пристроїв IoT не мають достатньої пам'яті і потужності процесора для виконання криптографічних операцій, необхідних для протоколу аутентифікації. Аутентифікація в IoT має кілька проблем, таких як

масштабованість і ефективність. Традиційна аутентифікація неефективна, і існує потреба в безпечному, масштабованому, ефективному і зручному для користувача рішення, щоб впоратися з обмеженими ресурсами пристроями IoT. За допомогою туману може бути застосований легкий алгоритм шифрування між протитуманними вузлами і пристроями IoT для підвищення ефективності процесу аутентифікації. Крім того, туман може створити можливість для аутентифікації пристроїв IoT, особливо мобільним пристроям.

Провідні фахівці запропонували модель системи управління ключами, що може охоплювати обширну площудля смарт-сітки[16]. Ця модель заснована на інфраструктурі з відкритим ключем (PKI) з використанням багатоадресної аутентифікації для безпечних комунікацій. У той час як традиційна аутентифікація Pki -based може вирішити проблему, але не буде добре масштабирована для систем IoT.

Довіра

У зв'язку з природою середовища IoT, яка об'єднує різні пристрої і датчики, що належать до різних механізмів, виникає наступне питання: Якою мірою ми можемо довіряти пристроям IoT? Немає ефективного механізму, який може вирішити, коли і як довіряти розумним пристроям. За відсутності оцінки довіри користувачі послуг IoT повинні розглянути питання про те, чи вигідно утримуватися від використання деяких послуг IoT. Таким чином, зміцнення довіри між пристроями IoT грає центральну роль в створенні безпечних умов для збереження безпеки і надійності послуг IoT. Моделі довіри, засновані на репутації, були успішно застосовані в багатьох сценаріях, наприклад онлайн-соціальних мережах. Кай Хван і його колеги запропонували новий підхід до підвищення довіри в хмарах, який поєднує в собі посилені центри даних, доступ до даних і віртуальні кластери, орієнтовані на системи репутації [17]. Для розробки моделі довіри, заснованої на репутації в IoT, необхідно вирішити , як підтримувати надійність сервісу і запобігати випадкових збоїв, обробляти і виявляти

проблеми неправильної поведінки, та коректно ідентифікувати шкідливі дії і побудувати моделі довіри, заснованої на репутації в великомасштабних мережах.

Виявлення уражених вузлів

Уражений вузол IoT може претендувати на законність обміну і збору даних, що генеруються іншими пристроями IoT, в злочинних цілях. Провідні фахівці даної області запропонували гібридний фреймворк, який може виявити наявність пунктів доступу в мережі доступу на базі Wi-Fi[18]. Уражений вузол IoT може зловживати даними користувачів або надавати шкідливі дані сусіднім вузлам, щоб порушити їх поведінку. Вирішення цієї проблеми може бути пов'язане з труднощами в Iot через складність управління довірою в різних схемах. Однак модель, заснована на вимірі довіри, може бути використана для виявлення шкідливих вузлів в середовищі IoT, що може забезпечити захист безпеки.

Конфіденційність

Парадигма туманних обчислень може допомогти зберегти конфіденційність в IoT і захистити користувачів, мінімізуючи необхідність передачі чутливих даних в хмару для аналізу. Використання цієї нової моделі допоможе в аналізі та обробці даних на краю мережі, поблизу пристроїв IoT, які генерують і діють на ці дані. Однак цей підхід породжує ряд проблем, пов'язаних з даними, місцем розташування і конфіденційністю користувачів. У туманних обчисленнях методи збереження конфіденційності можуть застосовуватися між туманом і хмарою для збереження конфіденційності даних, оскільки обидва мають достатнє сховище і потужність. Однак, складно використовувати ці технології між пристроями туману і IoT через обмеження ресурсів останнього. Одним з можливих рішень є метод збереження конфіденційності, заснований на гомоморфічних функціях, які можуть бути застосовані для підтримки конфіденційності даних. Диференціальна конфіденційність є ще одним методом забезпечення нерозголошення конфіденційності в наборі даних. Для збереження

конфіденційності розташування одним з початкових рішень є дозвіл IoT розподіляти дані між кількома туманними вузлами. Таке рішення призвело б до розтрачання ресурсів туману і збільшення часу затримки. Технологія маскування ідентифікатора може бути використана в протитуманних обчисленнях пристроїв IoT так, що туманні вузли не зможуть визначити, який пристрій IoT розвантажує дані. Іншим можливим рішенням для захисту конфіденційності користувачів є розробка ефективного методу збереження конфіденційності на основі поділу даних між туманними пристроями.

Контроль доступу

Контроль доступу - це метод гарантії безпеки, що дозволяє забезпечити доступ до певного ресурсу, наприклад до пристрою IoT, або до зібраних даних тільки уповноваженим суб'єктам. У IoT нам потрібен контроль доступу, щоб переконатися, що тільки довірені об’єкти можуть виконувати певні дії, такі як доступ до даних пристроїв IoT, видача команди на пристрій IoT або оновлення програмного забезпечення пристроїв IoT. Ця програма ставить нові завдання в галузі контролю доступу, оскільки ми маємо справу з величезною кількістю "речей", які мають обмежені ресурси (тобто, потужність і пропускна здатність). Крім того, забезпечення доступу до високорозподілених даних само по собі є серйозною проблемою.

Виявлення вторгнень

Методи виявлення вторгнень знаходять неправильне поводження або шкідливі пристрої IoT і повідомляють інших в мережі про прийняття відповідних заходів. Більшість існуючих методів в IoT націлене на кілька атак з низькою ефективністю. Природа середовища IoT ускладнює виявлення інсайдерських та зовнішніх атак в таких універсальних платформах. Крім того, ще одним питанням є складна конструкція методів виявлення вторгнень, які відповідають за обмеженість ресурсів в Іот. Основна проблема полягає в тому, як спроектувати і побудувати систему виявлення, яка може працювати в великомасштабному і високомобільному середовищі.

Захист даних

Експонентний обсяг даних, що генеруються IoT, зростає зі збільшенням кількості пристроїв. Ці дані повинні зберігатися не тільки на рівні комунікації, а й на рівні обробки. Через обмеженість ресурсів складно обробляти дані на пристроях IoT, тому дані зазвичай відправляються в хмару для подальшої обробки та аналізу. На даному етапі цілісність даних повинна бути збережена на етапі обробки і після нього. Відсутність у пристроїв IoT можливості шифрування або дешифрування робить обчислення автентичності та цілісності даних критичною проблемою.

Оновлення пристроїв IoT

На жаль, багато пристроїв IoT все ще не мають можливості оновлення віддаленого програмного забезпечення, що повинно бути розроблене для роботи з оновленнями безпеки. Fog-обчислення можуть бути важливою частиною рішення, яке визначає уразливості і відстежує оновлення програмного забезпечення в пристроях IoT. Вразлива мікропрограма може залишити пристрої IoT відкритими для атак, проти яких традиційні рішення безпеки (такі як брандмауери) можуть виявитися неефективними. Оновлення мільярдів пристроїв IoT є громіздкою завданням, але геодистрибутивна характеристика туманних обчислень може допомогти постачати пристрої IoT необхідними оновленнями безпеки, щоб забезпечити їх безпеку.

Безпечні та ефективні протоколи

Багато існуючих протоколів, такі як синхронізація в часі, засновані на бездротових пакетних передачах, і вони не підходять для пристроїв IoT з обмеженими ресурсами. Бездротові передачі і обчислення безпеки споживають значну частину енергетичного бюджету. Основна проблема полягає в тому, як розробити ефективні безпечні схеми в IoT без шкоди для продуктивності та споживання енергії.

Виявлення атак

Туманні обчислення надають нові можливості для виявлення незвичайного поведінки і точкових зловмисних атак. Як правило, система

виявлення може бути заснована на підписі або аномалії, в якій шаблон може бути зіставлений або перевірений з існуючими можливими шаблонами. Так як туман є продовженням хмари на краю мережі, можливе повторне використання розроблених систем виявлення в хмарах на платформі туману. Провідні фахівці даної області запропонували архітектуру хмарної сітки, засновану на співробітництві членів хмари для спостереження і виявлення шкідливого ПО, зловмисних атак і інших загроз. Метод виявлення може бути використаний між протитуманними вузлами для моніторингу середовища IoT і його оточення. Протитуманні обчислення надають нову можливість для розробки ефективного вирішення виявлення вторгнення з боку як хмари, так і пристроїв IoT. Використання такого рішення в протитуманних вузлах додасть захисний шар, який буде відстежувати і виявляти будь-яку незвичайну поведінку в середовищі IoT.

Згадані вище питання безпеки і конфіденційності в умовах IoT є показовими і не вичерпними. Існують і інші проблеми в галузі безпеки, такі як управління ключами і агрегування даних, що піддаються перевірці обчислення. Проте, відмінні риси туманних обчислень можуть сприяти вирішенню питань, пов'язаних з безпекою та конфіденційністю в середовищі IoT. Крім того, туманні обчислення можуть бути частиною рішення безпеки для забезпечення того, щоб служби IoT були менш уразливі до найбільш поширеним атак , таким як відмова в обслуговуванні (Dos) та атаки на основі шкідливого ПЗ. Наприклад, при сценаріях атаки Dos широкий розподіл протитуманних вузлів може допомогти зберегти стійкість для служб IoT.

Пристрої IoT повинні надавати надійну інформацію постачальникам, клієнтам і іншим пристроям IoT. Гарантія безпечного зв'язку між пристроями IoT в масовому масштабі, звичайно, є критично важливим завданням. Важко мати безпечні канали у великому масштабі IoT, але незаперечно, що туманні обчислення гратимуть фундаментальну роль у вирішенні питань безпеки та конфіденційності в додатках IoT.

2.3 Переваги та недоліки технології FOG

Масштабні розгортання IoT створювали ситуації, з якими cloud computing не могли працювати доречно та ефективно. Наприклад додатки , що вимагають малого часу затримки при обробці даних на кордоні мережі. У реальному житті, це значна кількість даних, що збираються з безлічі різних датчиків IoT в різних середовищах , таких як завод по виробництву мережевого обладнання, транспортні засоби, машини, ліфти і або індивідуальні пристрої, такі як домашні- смарт системи, датчики і т.д.

Ці пристрої є дуже чутливими та мають різні характеристики та особливості. Вони підключаються один до одного через провідний кабель або WiFi.

Масштабне розгортання пристроїв у неоднорідних середовищах спричиняє проблеми управління. Отже, потрібні інтелектуальні підходи до комунікацій, в яких пріоритет надається ефективності та надійності.

Використання хмарної мережі для передачі даних та аналізу даних має такі обмеження, як споживання пропускної здатності та витрати на зв’язок . Якщо дані користувача є чутливими, безпека даних є ще одним важливим питанням. Дані важливі для аудиторської мети або контролю над активами для підвищення ефективності або запобігання катастроф тощо . Аналіз даних може бути зроблений на місці за допомогою запуску програмного забезпечення на місцевих станціях. Хмара буде використовуватися для зберігання результатів аналізу для подальших цілей аудиту. Агрегація даних зменшить пропускну здатність, а також витрати, пов’язані з пропускною здатністю .

Концепція Smart Office може бути прикладом загального співвідношення пристроїв IoT та fog computing . Smart Factory - приклад промислового застосування IoT (IIoT) та туманних обчислень . Тут може бути багато приладів IoT, датчиків (температура, тиск тощо), електричних приводів чи інших пристроїв управління . Концепція Smart Home

з'являється з пристроями IoT та побутовою технікою, такими як телевізор, пральна машина, сушарка, холодильник тощо, оскільки вони стають ергономічнішими та розумнішими. У прикладі смарт-трафіку збір даних на сайті, негайний аналіз та обробка даних на fog сервісі можуть допомогти у швидкому прийнятті рішень на місцевому рівні, а не надсилати дані до центрального серверу. Наприклад, у разі надзвичайної ситуації, світлофорами можна керувати, щоб відкрити шлях для аварійних транспортних засобів, таких як пожежна машина та швидка допомога на базі місцевих пристроїв IoT. У цих чотирьох різних сценаріях загальна ідея полягає в тому, що пристрої генерують величезну кількість даних і, можливо, знадобиться співпрацювати між собою та приймати критичні рішення, зменшуючи затримку. Отже, спритна реакція є важливою, і філософія fog computing може допомогти подолати пропускну здатність та проблеми, пов'язані із затримкою таким чином.

Завдяки впровадженню швидкої реакції поблизу крайових компонентів, можливе швидке впровадження та зростання бізнесу fog computing для майбутніх додатків IoT, таких як смарт-трафік та смарт-заводи. Тим самим інтеграція не залишиться лише в IoT, а розшириться до промислового IoT (IIoT) та інших інших областей. Це покладе власні виклики на IIoT [19], а також принесе користь. IoT і fog computing можуть бути корисними при розробці «розумних» речей, таких як розумний будинок, розумні світлофори, розумні міста тощо. Наприклад, датчики в інтелектуальній системі руху можуть виявити аварії або відчути дорожні умови через погоду чи деякі інші фактори та інформують водіїв. Пробка може регулюватися розумною системою руху. В останні роки, завдяки використанню IoT та інших датчиків, дані, що генеруються кінцевими пристроями, масово збільшуються. Питання, де / коли / як слід аналізувати ці дані? У дизайні, орієнтованому на хмару, пристрої IoT генерують дані та передають їх у хмару (працює як центральний сервер) для зберігання та аналізу. Однак при туманному обчисленні дані аналізуються на крайових

станціях і просто необхідні результати надсилаються до хмари. Fog розширює cloud computing та доповнює його концепцією розумних пристроїв, які можуть працювати на краю мережі. FOG розширює традиційну хмару до краю мережі, де чутливі до затримки додатки можуть отримувати користь близькості з туман. Fog надає наступні переваги :

• Він забезпечує швидке реагування на чутливі до затримки додатки, такі як мультимедіа або на повідомлення про надзвичайні ситуації;

• Він підтримує агрегування даних гетерогенних пристроїв. Наприклад, він може комбінувати дані від декількох сенсорів, пов'язаних з охороною здоров'я.

• Він забезпечує захист і безпеку чутливих даних, таких, як медична інформація, інформація про місцезнаходження користувача, і інша приватна інформація. Це дозволяє уникнути непотрібної передачі даних перед відправкою в основну мережу.

• Забезпечує надання послуг, які враховують контекст і місце розташування, завдяки близькості до місця розташування користувача і можливості отримати більше інформації про нього.

Консорціум OpenFog визначає стандарти fog computing з різними комітетами та робочими групами[20]. Членами-засновниками - Arm, Cisco, Dell, Intel, Microsoft та University of Princeton основна увага приділяється створенню та просуванню відкритої довідкової архітектури для fog computing для вирішення таких завдань, як пропускна здатність, затримка у різних областях, таких як AI, IoT, промислова техніка, робототехніка тощо. За даними консорціуму OpenFog , ключових стовпів Архітектура Fog computing - це безпека, масштабованість, відкритість, автономність, надійність, доступність, справність, спритність, ієрархія та програмованість. Fog computing допомагають системам IoT, 5G та AI, які потребують особливих унікальних властивостей, таких як безпека (надійні транзакції), пізнання (об'єктивна обізнаність), спритність (масштабованість), затримка (обробка в режимі реального часу) та ефективність (використання невикористані

ресурси). На думку OpenFog , переваги використання туманних обчислень є: низька затримка, спритність бізнесу, безпека, аналітика в режимі реального часу, знижена вартість, менше використання пропускної здатності .

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 TA FOG BASED ARCHITECTURE ДЛЯ IOT В СЕРЕДОВИЩІ SMART CITY

3.1 Blockchain та Fog Based Architecture

Витоки розумних міст є наслідком поліпшення якості життя громадян і оптимального використання ресурсів міста, обумовлене недавнім прискоренням темпів зростання міського життя. Поліпшення в області інфраструктури та послуг підвищилася якість життя. Це стало можливим завдяки Інтернету, досягненням в галузі зв'язку та інформаційних технологій . Ідеї розумних міст включають в себе ефективні державні послуги, а також більш досконалу інфраструктуру, яка буде доступною і більш інтерактивною. Концепція розумних міст стала реальністю завдяки Інтернету речей . Як наслідок, розумне місто стало однією з головних рухаючих сил для додатків IoT. Все місто покрите фізичними об'єктами, які взаємопов'язані з системою IoT. Чотири стовпи, які можуть бути пов'язані з концепціями IoT - це дані, речі, люди і процеси. Тому концепція інтелектуального міста інтегрована з основними напрямками діяльності з надання сприяння перспективним послуг в майбутньому.

Розподілена середовище, що використовується для генерації великих даних (БД), має потенціал піднімати проблеми зберігання і обробки даних. Хмарні обчислення можуть бути рішенням; обробка та зберігання можуть бути придбані на вимогу, на основі розподільної оплати. Однак внутрішні проблеми є причиною неефективної роботи додатків в хмарі [21]. Наприклад, додаток для моніторингу руху міста не може дозволити собі затримку в передачі даних від джерела до центру обробки хмарних даних, і до кінцевої програми. Тому з'явилася концепція туманних обчислень. Скорочення мережевого трафіку і часу обробки даних стає за рахунок наближення кінцевих користувачів до хмарних служб на краю мережі .

Cisco дав FC первинне визначення як "Fog Computing - парадигма, яка розширюється хмарні обчислення і сервіси на краю мережі [22]. "Туманний вузол (Fog Node) допомагає у застосовувати іот, яке є одним з основних елементів FC. Як правило, FC діє в якості проміжного шару між хмарною інфраструктурою і кінцевим пристроєм / кінцевим користувачем. Додатки IoT потребують малих затримок, широкого географічного розподілу та мобільності. Метою запропонованої архітектури BFAN є поліпшення вищезгаданих параметрів шляхом обробки більшої частини даних, ближче до кінцевих користувачів; або кінцевих пристроїв. Безпека підвищується за допомогою технології блокчейн. Блокчейн - це ланцюжок блоків, який зростає з кожною транзакцією і пов'язаний через криптографію. Блок - це комбінація даних транзакцій, міток часу і криптографічних хешів попередніх блоків.

Блокчейн допомагає забезпечити справжню надмірність і повну децентралізацію. Алгоритм раціонального розподілу допомагає забезпечувати ресурсами на вимогу і рахунки генеруються після використання. Ключем і сховищем фрагментів в зашифрованому форматі управляє користувач. Третя сторона не бере участі в контролі і доступі до даних. Тому немає способу відновити втрачені закриті ключі.

Контроль за використанням ресурсів допомагає в зіставленні показників ефективності на рівні управлінні сервісами (SLA)з показниками реального часу.

Туманні вузли можуть бути обрані в якості найближчого засобу обробки і зберігання, який може зменшити затримку передачі даних в віддаленому місці, а також зекономить енергію. Запропонована система BFAN

намагається відповісти на різні питання, зокрема:

• Безпека: Безпека в інтелектуальних містах, пов'язаних з кібербезпекою і фізичної безпекою. У цій системі захист даних від атак,

обчислювальної інфраструктури і мережі виконується з використанням технології Блокчейн.

• Кешування: Низька затримка є одним з найважливіших аспектів смарт-сіті. Для цього використовується кешування, збереження більш частих даних в різних точках мережі. Кешування також допомагає зменшити мережу

перевантаженість за рахунок уникнення потоку повторюваних даних в мережі. Туманні обчислення з кешуванням дозволяють використовувати різні додатки в розумних містах.

• Масштабованість: Це дозволяє використовувати гнучкі сервіси в комп'ютерах Fog для забезпечення QoS. У запропонованій архітектурі

забезпечувати швидке і масштабоване хмарне середовище поблизу пристроїв IoT.

• Стійкість: енергоефективні системи є вимогою для розумних міст за рахунок використання відновлюваних джерел енергії. Мета забезпечення стійкості полягає в скороченні викидів вуглецю. В даний час вугільні джерела виробляють понад 80% енергії, що використовується в центрах даних [23].

Розуміння контексту: здатність отримувати розташування вузла і інформацію про навколишнє середовище називається контекстуальна обізнаність. BFAN враховує контекст оточення парам і місце розташування вузла для вибору відповідного режиму зв'язку. Це надає великої ваги сучасному рівню енергоефективності та енергопослуг розумних міст.

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.

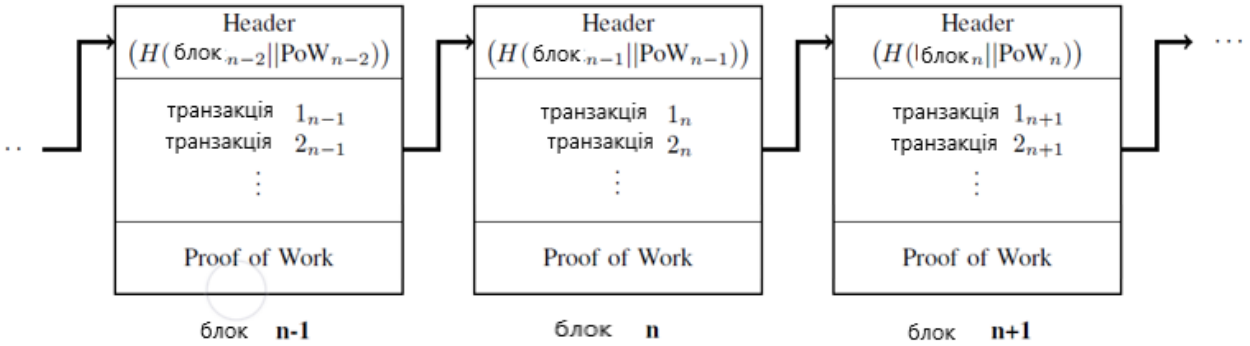

Рис. 3.1 Варіант схеми технології Blockchain

Блокчейн сам по собі є простою послідовністю блоків, кожен блок яких містить кілька транзакцій (див. Рис. 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.

Однак для забезпечення того, щоб блоки не порушували порядок, використовується хеш-функція для обчислення хешу попереднього блоку, щоб його можна було додати в заголовок нового блоку. Ця дія зберігає унікальний порядок блоків; проте, в даний момент для нападника все ще можливо перерахувати деякі блокові хеші, щоб змінити порядок блоків. Те, що зупиняє це, є Proof-of-Work : Pow по суті є умовою на хеш-блок, який змушує вузол, який обчислює хеш, витрачати деякий час на цей розрахунок; це утримує шкідливі вузли від штовхання підроблених або змінених блоків в інші вузли. Ця умова може бути представлено у вигляді простої математичної задачі, яка може бути тільки грубо вирішена, наприклад, запит вузла, що обчислює хеш, для додавання частини даних в новий блок, так що

його хеш-значення починається з 50 нулів або одиниць. За такої умови, вузол, який обчислює хеш, повинен пройти через кілька випадкових блоків даних, поки умова не буде виконана (по суті, грубе рішення задачі).

Кожен вузол бере участь в мережі або пасивно (тільки виконуючи транзакції), або активно (виконуючи транзакції і перевіряючи їх). Останні вузли називаються шахтарями; ці вузли перевіряють достовірність транзакцій, обчислюють їх хеш при заданому умови і потім проштовхують блок до інших вузлів, таким чином оновлюючи блокчейн. Щоб відновити, кожен блок містить заголовок, який включає хеш попереднього блоку плюс випадковий шматок даних, так що порядок блоків, і, таким чином, історія транзакції є однозначним (див. Рис. 3.1).

Якщо зловмисник спробує змінити порядок блоків, їй доведеться перерахувати не тільки все хеши, необхідні для того, щоб перемістити блоки, які вона хоче змінити, але також їй доведеться обчислити хеш-кодування для всіх наступних блоків, в спробі переконати будь-який інший вузол в мережі, що її версія ланцюжка є правильною.

Однак, все ще є вразливість: що якщо зловмисникові вдасться обчислити правильний хеш перед іншими вузлами, просто з чистої удачі? Потім вона могла б переконати всю мережу в тому, що її блок є законною версією історії укладених угод. Цьому перешкоджає той факт, що блоки не затверджуються відразу; замість цього, якщо кілька вузлів перевіряють один і той же блок, в блокчейне створюється вилка. Вилка, яка в кінцевому підсумку стає найдовшою, в кінцевому підсумку приймається мережею в якості справжнього запису транзакцій, які відбулися.

Тепер ми бачимо, що якщо зловмисник хоче додати помилкові транзакції в блокчейн, він повинен не тільки отримати удачу і бути одним з перших вузлів для перевірки нового блоку, але їй також довелося б будувати швидше на своїй вилці блокчейн, щоб вона стала найдовшою і була прийнята. Це можливо тільки в тому випадку, якщо зловмисник контролює понад 50% шахтарів в мережі, тому він зазвичай називають атакою 51%. Як

стверджують багато авторів, така атака практично неможлива в сучасних, популярних дистанціях, таких як Bitcoin або Ethereum [24].

Таким чином, блокчейн задовольняє двом дуже важливим принципам безпеки: цілісності, тому що дані не можуть бути змінені після того, як вони увійшли в блокчейн, і невідновлення, тому що кожна угода підписана всіма сторонами, які беруть участь в ній, і оскільки інформація не може бути змінена, жоден вузол не може відмовити в транзакції, в якій вони брали участь. Крім того, блокчейн пропонує Доступність, оскільки його децентралізований характер має на увазі, що система буде продовжувати працювати, навіть якщо деякі вузли стануть недоступними. Це надзвичайно важливо в контексті IoT, як в простих, централізованих хмарних рішень, якщо центральний сервер стає недоступним, то дані більше не доступні [25].

Використання blockchain має багато переваг в IoT-додатках Основні переваги використання blockchain в додатках IoT обговорюються нижче.

1) Дані, що надходять з пристроїв IoT, можуть зберігатися в Blockchain: До додатків IoT належить велика кількість пристроїв, підключених один до одного. Ці пристрої додатково підключаються та контролюються іншими пристроями. Ця установка додатково підключена до хмари, щоб дозволити використовувати програми IoT з будь-якого місця. Завдяки такому великому простору для руху даних, blockchain є перспективним рішенням для зберігання даних та запобігання їх неправильному використанню. Незалежно від шару в додатку IoT, блокчейн може виступати як підходяще рішення для зберігання та передачі даних.

2) Розподілений характер blockchain, що забезпечує безпечне зберігання даних: Оскільки архітектура blockchain поширюється в природі, це може уникнути ризику стати єдиною точкою відмови, з якою стикаються різні програми IoT на основі хмари. Незалежно від відстані між пристроями, генеровані ними дані можуть легко зберігатися на блокчейні безпечним способом.

3) Шифрування даних за допомогою хеш-ключа та перевірено шахтарями: У блокчейні може зберігатися лише 256-бітний хеш-ключ для даних, а не зберігати фактичні дані. Фактичні дані можна зберігати у хмарі, а хеш-ключ можна зіставити з вихідними даними. Якщо є якісь зміни в даних, хеш даних зміниться. Це робить дані захищеними та приватними. На розмір blockchain також не впливатиме розмір даних, оскільки у ланцюжку зберігаються лише хеш-значення. Тільки призначені сторони, які мають право використовувати ці дані, можуть отримати доступ до даних із хмари, використовуючи хеш даних. Кожен набір даних, що зберігаються на блокчейні, належним чином перевіряється різними шахтарями в мережі, і тому ймовірність зберігання пошкоджених даних з пристроїв зменшується, використовуючи блокчейн як рішення.

4) Запобігання втраті даних та атакам підробляння: У підробці атак на додатки IoT новий противний вузол входить у мережу IoT і починає імітувати як частину вихідної мережі. Підробляючи підробку, противник може легко захоплювати, спостерігати чи вводити дані в мережу. Blockchain виступає як перспективне рішення для запобігання подібних атак. Кожен законний користувач або пристрій зареєстрований у blockchain, і пристрої можуть легко ідентифікувати та автентифікувати один одного без необхідності центральних посередників чи сертифікаційних органів . Будучи малопотужними в природі, пристрої IoT успадковують ризик втрати даних. Можуть бути випадки, коли через деякі зовнішні екологічні проблеми дані втрачаються як відправником, так і одержувачем. Використання blockchain може запобігти такі втрати, оскільки після того, як блок буде доданий у ланцюг, немає можливості його зняти [26].

5) Blockchain для запобігання несанкціонованого доступу: Багато програм IoT передбачають багато частого спілкування між різними вузлами. Комунікація в blockchain відбувається за допомогою відкритого та приватного ключів, і тому лише цільова сторона або вузол можуть отримати доступ до даних. Навіть якщо ненавмисна сторона зможе отримати доступ до

даних, вміст даних буде незрозумілим, оскільки дані шифруються ключами. Тому структура даних blockchain намагається вирішити різні проблеми безпеки, з якими стикаються програми IoT.

6) Архітектура, заснована на проксі, в blockchain для обмежених ресурсів пристроїв: Хоча blockchain надає різні функції безпеки для розподіленого середовища, IoT має певну проблему обмеження ресурсів. Будучи обмеженими ресурсами, пристрої IoT не можуть зберігати великі книги. У цьому напрямку проводилися різні роботи щодо полегшення використання blockchain в IoT. Архітектура на основі проксі - одне з перспективних рішень, яке може допомогти пристроям IoT використовувати блокчейн. Проксі-сервери можуть бути розгорнуті в мережі для зберігання ресурсів у зашифрованому вигляді. Зашифровані ресурси клієнт може завантажувати з проксі-серверів [27].

7) Усунення централізованих хмарних серверів: Blockchain може підвищити безпеку систем IoT, оскільки в кінцевому рахунку виключає централізовані хмарні сервери та робить мережу одноранговою. Централізовані хмарні сервери є головною ціллю злодіїв даних. Використовуючи блокчейн, дані будуть розподілятися між усіма вузлами мережі та шифруватися за допомогою криптографічної хеш-функції.

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 на

малюнку 2, зможе запропонувати краще рішення для майбутнього розумного міста.

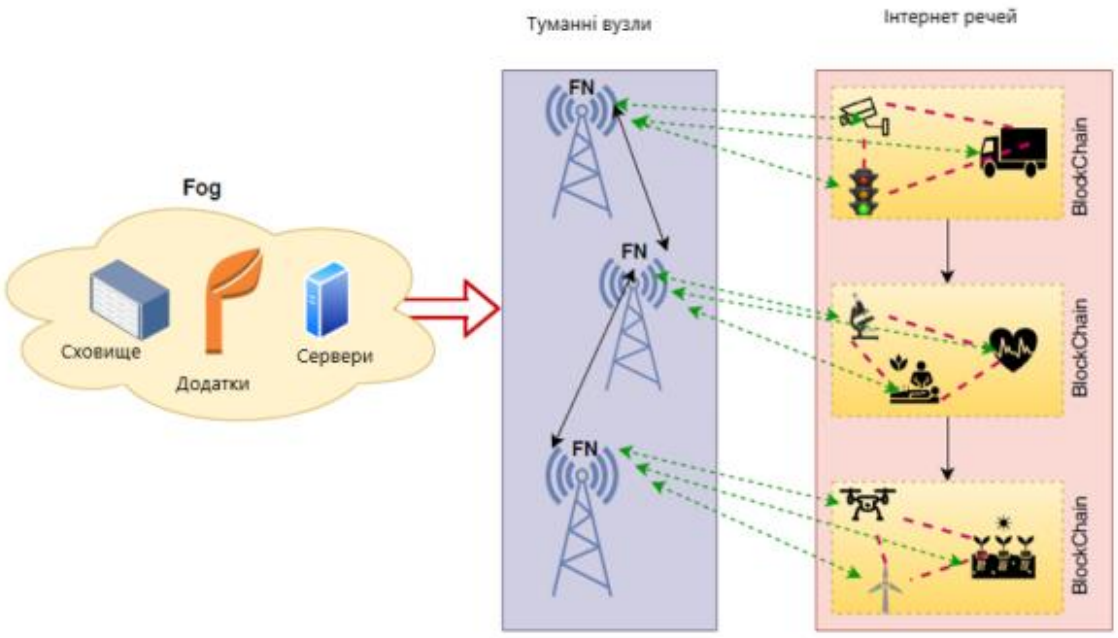

Рис.3.2 Схема архітектури BFAN

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.

Питання про функціонування кожного рівня розглядається в наступних підрозділах.

1 Рівень протитуманних вузлів

Попит користувачів на послуги може бути задоволений за допомогою пристроїв IoT в середовищі розумного міста, які підключені до туманного обчислювального середовища. Блокчейн використовується для підвищення надійності шляхом додавання нового компонента в місто, після отримання належного дозволу від супутніх технологій. Численні фізичні сервери об'єднуються, щоб зробити FN, який охоплює конкретну площу. Туманні вузли можуть бути з'єднані дротовими / бездротовими носіями. FN діє як невеликий віртуальний центр даних для процесора, конфігураційних апаратних ресурсів і мережевих послуг. Вузли Fog складаються з процесорів, що настроюються апаратних ресурсів і мережевих служб. Розумні датчики збирають дані з навколишнього середовища, а FN проводить аналіз цих даних в режимі реального часу і дає внутрішню інформацію, яка допомагає в прийнятті рішень. Крім того, мережа радіодоступу також полегшується FN для забезпечення одноадресної бездротового зв'язку в певному діапазоні. Паралельна передача даних підтримується недавно розробленими протоколами для передачі пакета в усі пункти призначення або в конкретне місце призначення. Локальна база даних може бути вбудована в FN, яка забезпечує зберігання пасивних додатків, які знаходяться в пам'яті. Це дозволяє скоротити час обробки і завантаження важких Іот-додатків. Одним з найважливіших додатків є Social IoT (SIoT), що грає важливу роль в надійності, пропускної спроможності, оптимізації затримок, розгортанні IoT і безпеки мережі IoT. В даному випадку зв'язок здійснюється між різними туманними вузлами для передачі основних даних.

2 Рівень Інтернету речей

Цей рівень є реальним середовищем для користувачів для розгортання програм без будь-яких обмежень. Пристрої IoT згруповані в залежності від їх місця розташування і функціональності. Це допомагає знизити

енергоспоживання, продуктивність, вартість і витрати часу. Робоче навантаження центрів зберігання і обробки даних зросте в зв'язку з необхідністю інтеграції і обробки програмного і апаратного забезпечення. Комунікація на основі peer-to-peer (P2P) чи TCP/IP відбувається між пристроями IoT, на короткій відстані. Якщо вони далекі один від одного, то ці пристрої можуть використовувати FN через технології Wifi, Zigbee і Bluetooth.

3 Блокчейн для IoT

Існуючий IoT працює над централізованої моделлю для зв'язку. Централізовані хмарні сервери перевіряють пристрої IoT. Таким чином, існуючі рішення для IoT в розумних містах використовують хмарні обчислення і мережеві ресурси, що призводить до високих витрат на інфраструктуру і технічне обслуговування. У Smart містах, що мають масштабоване оточення, кількість пристроїв змінюється регулярно. Це означає, що смарт-сенсори частіше додаються в інфраструктуру смарт-міст в якості спеціальної мережі. Поточна система не підтримує великі пристрої IoT через проблеми масштабованості. У міру збільшення обсягу ресурсів зростає і взаємодія між пристроями і серверами. Хмарні сервери також стикаються з проблемою однієї точки збою. У розумному місті централізована система є недоліком, і тому модель рівноправних відносин може бути більш ефективною. У запропонованій моделі застосовується блокчейн для IoT, тому що він децентралізований і захищений від втручання. Легко відстежити мільярд пристроїв, підключених до мережі. Це також знижує вартість управління сервером і його установки. Він також рятує розумні міські пристрої IoT від атаки людини в середині, тому що існує кілька каналів зв'язку. Дані, отримані від смарт-датчиків, зберігаються в блокчейн.

4 Передача даних

Такі додатки як SIoT, мають велику кількість даних для передачі, і цей розмір регулярно зростає швидкими темпами. Це також підвищує вимоги до пропускної здатності мережі, зберігання даних і швидкості обробки. Дані

передаються з локальних пристроїв зберігання, веб і IoT. Обробка даних здійснюється відповідно до протоколу організації, таким як очищення, фільтрація і інтеграція.

Тут хмара використовується в останньому шарі для обробки метаданих. FN аналізує дані і робить метадані. Архітектура BFAN підвищує мобільність користувачів додатків IoT за допомогою FN, додаткова безпека надається через блокчейн, який відключає анонімний користувальницький вхід в пристрої IoT. FN надає сервісне обслуговування додатків і сховище даних для пристроїв IoT. Зв'язок здійснюється в наступному порядку:

- зв'язок між локальними пристроями, з чутливістю та оброблюваною здатністю, що відомий як первинний або міжгалузевий зв'язок. Такими пристроями можуть бути датчики, ноутбуки, сенсорні екрани і комп'ютери, які використовуються для зв'язку P2P. Wi-Fi використовується для зв'язку між пристроями IoT, де відстань є середньою.
- Зв'язок з Fog Nodes відбувається за допомогою бездротових або дротових носіїв. Оптичне волокно CAT-5/6 використовується для TCP/IP для наскрізного з'єднання.

Локальний бездротовий зв'язок використовується для зв'язку між кінцевими компонентами. Існують прямі і непрямі види зв'язку. Система прямих видів застосовується для зв'язку між FN. Це робить архітектуру BFAN стійкішою до затримок. Багатоадресна передача виконується вторинним видом зв’язку. Система передачі даних між первинними і міжгалузевими мережами поліпшується завдяки високошвидкісному зв'язку з низькою затримкою.

Пристрої зберігання, сервери та інші компоненти показані на малюнку 2. Компоненти туману пов'язані з конкретним сервером, як показано на малюнку 3. Первинний і вторинний зв'язок ізольовані один від одного на відстані від компонентів. Масштабованість FN може бути збільшена або зменшена. Первинний зв'язок здійснюється локальним з'єднанням, а

відповідальність за вторинний зв’язок покладається на зовнішні з'єднання. Блокчейн використовується для аутентифікації і авторизації додатків.

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 ПО РОБОТІ

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/.