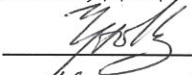


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ У МЕДИЦИНІ ТА ТЕЛЕКОМУНІКАЦІЯХ

УДК 621.37

«Допущено до захисту»

Завідувач кафедри
комп'ютерних технологій у
медицині та телекомунікаціях
к.т.н., доц. Чухов В.В.

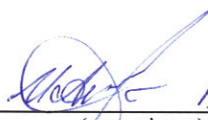

« 19 » 12 2023 р.

КВАЛІФІКАЦІЙНА РОБОТА

на тему ДОСЛІДЖЕННЯ ІОТ ДЛЯ ВИКОРИСТАННЯ В СИСТЕМАХ
ОХОРОНИ ЗДОРОВ'Я

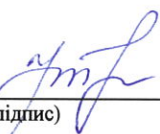
за спеціальністю 163 «Біомедична інженерія»
освітній ступінь «магістр»

Виконавець роботи
студент 2 курсу, гр.БІм-22-1


19.12.2023
(дата, підпис)

Александров І.І.

Керівник роботи
к.т.н., доц.

19.12.2023 
(дата, підпис)

Нікітчук Т.М.

Житомир
2023

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ У МЕДИЦИНІ ТА ТЕЛЕКОМУНІКАЦІЯХ

Пояснювальна записка
до кваліфікаційної магістерської роботи

на тему Дослідження IoT для використання в системах охорони
здоров'я

Виконав: студент 2 курсу,
групи БІМ-22-1 спеціальності
163 «Біомедична інженерія»

Александров І.І.

Керівник Нікітчук Т.М.

Рецензент Чухов В.В.

«Затверджено»

Завідувач кафедри комп'ютерних
технологій у медицині та
телекомунікаціях

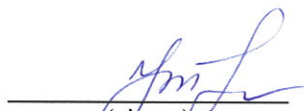
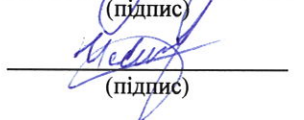
 Владислав ЧУХОВ
« 27 » 10 2022 р.

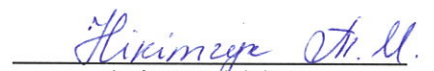
Завдання на кваліфікаційну магістерську роботу

- Александров І.І.
(прізвище, ім'я, по батькові)
1. Тема роботи Дослідження ІОТ для використання в системах охорони здоров'я
 - затверджено наказом по університету від « » 202_ р. №
 2. Мета дослідження дослідження, аналіз технологій ІОТ для використання в системах охорони здоров'я
 3. Вихідні дані (характеристики об'єкта, умов дослідження та ін. технологій ІОТ, медичні дані, передача даних з датчиків на віртуальний сервер, телемоніторинг
 4. Основні задачі дослідження аналіз технологій ІОТ, мережі охорони здоров'я дослідити реалізацію ІОТ систем медичного призначення
 5. Термін подання роботи до захисту липень, 2023
 6. Дата видачі завдання « 27 » 10 2022 р.

Науковий керівник

Завдання прийняв
до виконання


(підпис)

(підпис)


(прізвище, ініціали)
Александров І.І.
(прізвище, ініціали)

АНОТАЦІЯ

Віддалений моніторинг є інтенсивним технологічним розвитком, тоді як телемедицина – це інтенсивний процес для людини та експертів; лікарі ставлять діагноз за допомогою своєї експертизи.

У роботі проведено огляд політик та правил електронного здоров'я та IoT на користь різних зацікавлених сторін, зацікавлених в оцінці медичних технологій на основі IoT.

У роботі запропоновано структуру апаратно-програмного комплексу моніторингу життєдіяльності особи, що дозволяє пацієнтам самостійно відслідковувати життєво важливі показники свого здоров'я, а лікуючим лікарям – контролювати в реальному часі стан здоров'я своїх пацієнтів у режимі віддаленого доступу та проводити аналіз результатів спостереження за допомогою спеціальних мобільних програм-застосунків з метою своєчасного та ефективного корегування лікувальних та профілактичних заходів

ЗМІСТ

ВСТУП	6
РОЗДІЛ 1 ТЕХНОЛОГІЇ ІОТ, ТЕЛЕМЕДИЦИНА ТА ВІДДАЛЕНИЙ МОНІТОРИНГ ЗДОРОВ'Я	8
1.1 Інтернет речей	8
1.2 Застосування Інтернет речей у сфері охорони здоров'я	12
1.3 Віддалений моніторинг здоров'я	22
1.4 Проблеми в дистанційному моніторингу здоров'я	25
1.5 Різниця між телемедициною та дистанційним моніторингом здоров'я	26
РОЗДІЛ 2 МЕРЕЖІ ОХОРОНИ ЗДОРОВ'Я ІОТ	29
2.1 Топологія IoThNet	29
2.2 Архітектура IoThNet	32
2.3 Послуги і застосунки IoT	34
2.4 Архітектура апаратно-програмного комплексу моніторингу в реальному часі стану організму людини	36
РОЗДІЛ 3 ДОСЛІДЖЕННЯ РЕАЛІЗАЦІЇ ІОТ СИСТЕМИ МЕДИЧНОГО ПРИЗНАЧЕННЯ	40
3.1 Проєктні рішення по структурі та архітектурі побудови IoT системи медичного призначення	40
3.2 Передача даних з давачів на телефон Android з використанням Arduino і модуль NRF24L01 через Bluetooth (BLE)	42
3.3 Використання модуля Raspberry PI для передачі медичних даних за технологією Wi-Fi	46
3.4 Архітектура програмного забезпечення віддаленої системи моніторингу медичних даних	47
3.5 Об'єднання сенсорів та модулів в єдину систему	48
3.6 Передача даних на сервер	52
3.7 Захист та конфіденційність при передачі медичних даних	57
3.8 Додаток IoT системи медичного призначення	61
ВИСНОВКИ	64
ЛІТЕРАТУРА	65

ВСТУП

Медичне обслуговування та охорона здоров'я є однією з найпривабливіших областей застосування IoT. Технологія IoT наразі знайшла безліч медичних застосувань: віддалений моніторинг стану здоров'я, програми фітнесу, хронічні захворювання та догляд за літніми людьми тощо. Очікується, що послуги охорони здоров'я на основі IoT зменшать витрати, підвищать якість життя та збагатять досвід користувачів.

З точки зору постачальників медичних послуг, IoT може зменшити час простою пристроїв за допомогою віддаленого забезпечення. IoT забезпечує ефективне планування обмежених ресурсів, забезпечуючи найкраще їх використання та обслуговування більшої кількості пацієнтів.

Важливим трендом є простота економічно вигідних взаємодій завдяки безперебійному та безпечному зв'язку між окремими пацієнтами, клініками та медичними організаціями. За останні кілька років ця сфера привернула широку увагу дослідників для дослідження потенціалу IoT у сфері охорони здоров'я шляхом розгляду різних практичних проблем. Як наслідок, зараз у галузі є численні застосунки, послуги та прототипи. Тенденції досліджень в галузі охорони здоров'я на основі IoT включають архітектури мереж та платформи, нові сервіси та додатки, взаємодію та безпеку, серед іншого. Крім того, були розроблені політики та рекомендації щодо впровадження технології IoT у медичні технології. Однак IoT залишається у зародковому стані у сфері охорони здоров'я. На цьому етапі глибоке розуміння сучасних досліджень IoT у контексті охорони здоров'я буде корисним для різних зацікавлених сторін, зацікавлених у подальших дослідженнях.

У цій кваліфікаційній роботі висвітлюються тенденції досліджень охорони здоров'я на основі IoT та розкриваються різні проблеми, які необхідно вирішити, щоб трансформувати технології охорони здоров'я за допомогою інновацій IoT.

Мета роботи – дослідження IoT для використання в системах охорони здоров'я.

Задачі, які необхідно вирішити для досягнення мети роботи:

- 1) провести огляд та аналіз технологій IoT, засобів телемедицини та віддаленого моніторингу здоров'я;
- 2) розглянути та проаналізувати мережі охорони здоров'я IoT;
- 3) провести аналіз топологій IoThNet та архітектури IoThNet
- 4) дослідити реалізацію IoT системи медичного призначення.

РОЗДІЛ 1 ТЕХНОЛОГІЇ ІОТ, ТЕЛЕМЕДИЦИНА ТА ВІДДАЛЕНИЙ МОНІТОРИНГ ЗДОРОВ'Я

1.1 Інтернет речей

Інтернет речей (англ. Internet of Things, скорочено IoT) – це сукупність пристроїв, які оснащено датчиками, сенсорами, засобами передавання сигналів і підключено до глобальної мережі Інтернет (рис. 1.1).

Ці цифрові пристрої, використовуючи різні датчики, можуть:

- сприймати різноманітні сигнали з навколишнього світу (наприклад, температуру, освітленість, вологість, рух тощо);
- вступати у взаємодію з іншими пристроями (наприклад, вмикати кондиціонер після підвищення температури, відкривати гаражні двері, коли до них наближається автомобіль, фотографувати автомобілі, поливати рослини після зниження вологості ґрунту тощо);
- обмінюватися даними для віддаленого стеження за станом об'єктів, аналізу зібраних даних і прийняття на їх основі рішень.



Рисунок 1.1 – Інтернет речей

Ця концепція дає змогу пристроям виконувати певні дії без втручання людини.

Термін «Інтернет речей» запропонував у 1999 році засновник дослідницького центру Auto-ID Center в Массачусетському технологічному інституті Кевін Ештон (народ. 1968 р.) (рис. 1). Він висловив припущення, що

згодом у кожної з речей реального фізичного світу в IoT буде цифровий двійник, її віртуальне представлення.

Напрямок IoT став активно розвиватися, коли на початку 2000-х років кількість пристроїв, підключених до мережі Ін-тернет, перевищила кількість користувачів Інтернету. Тобто Інтернет речей перевищив Інтернет людей.

Період з 2008 по 2009 рік аналітики корпорації Cisco вважають «справжнім народженням Інтернету речей», тому що саме в цей період кількість пристроїв, підключених до глобальної мережі, перевищила чисельність населення Землі. А за даними компанії Ericsson у 2018 році кількість таких пристроїв перевищила кількість мобільних телефонів у світі, а до 2022 року.

У зв'язку з такими глобальними масштабами набуває поширення новий термін – Всеохопний Інтернет, Інтернет усього (англ. Internet of Everything, IoE), який із часом прийде на зміну IoT.

У такому цифровому середовищі створюються нові умови для бізнесу, для охорони здоров'я, для забезпечення екологічної безпеки, змінюються особисті та соціальні аспекти життя (рис. 1.2).

Так, у Австралії уже зараз лікарі використовують переносні датчики, завдяки яким можуть віддалено відстежувати стан здоров'я пацієнта і реагувати на зміни в режимі реального часу. Автодорожні служби встановлюють спеціальні датчики на автомобільних шляхах для відстеження швидкості автомобілів, автоматичної фіксації порушень і відправлення інформації про цей факт у патрульну службу та водію.

Для відстеження стану оточуючого середовища об'єкти оснащуються датчиками (сенсорами), які реалізують з'єднання фізичного й віртуального світів, забезпечуючи збирання та опрацювання даних у реальному часі. Наприклад, датчики для вимірювання температури, тиску, швидкості руху, місця розташування, вологості та іншого. Мініатюризація, яка привела до зменшення фізичних розмірів датчиків, надала можливість убудовувати їх безпосередньо в об'єкти фізичного світу (годинники, браслети, замки, брелоки, пульти тощо). Найкраще, коли пристрої мають автономне живлення.



Рисунок 1.2 – Інтернет речей в галузях



Рисунок 1.3 – Технології Інтернету речей

Датчик вимірює фізичні параметри контрольованого об'єкта/явища і перетворює їх у цифровий сигнал, який може бути переданий і прийнятий відповідним комп'ютерним пристроєм. Для опрацювання та накопичення даних з датчиків використовують вбудовані комп'ютери (мікрочипи), до яких датчики приєднано через контролери. Контролери – це спеціальні пристрої, які призначені для керування зовнішніми пристроями комп'ютера або датчиками.

Якщо ж опрацювання отриманих даних планується на локальному комп'ютері, смартфоні, сервері, то для обміну даними між пристроями використовують різні канали передавання даних (бездротові або дротові мережі). Важливим на цьому етапі є забезпечення надійності та конфіденційності передавання даних.

Для аналізу даних і прийняття рішення комп'ютерні пристрої використовують відповідне програмне забезпечення, яке за певними алгоритмами опрацьовує отримані дані. Ці програми можуть установлюватися на мобільні пристрої або використовувати хмарні технології.

Загальну схему функціонування мережі Інтернет речей наведено на рисунку 1.4.

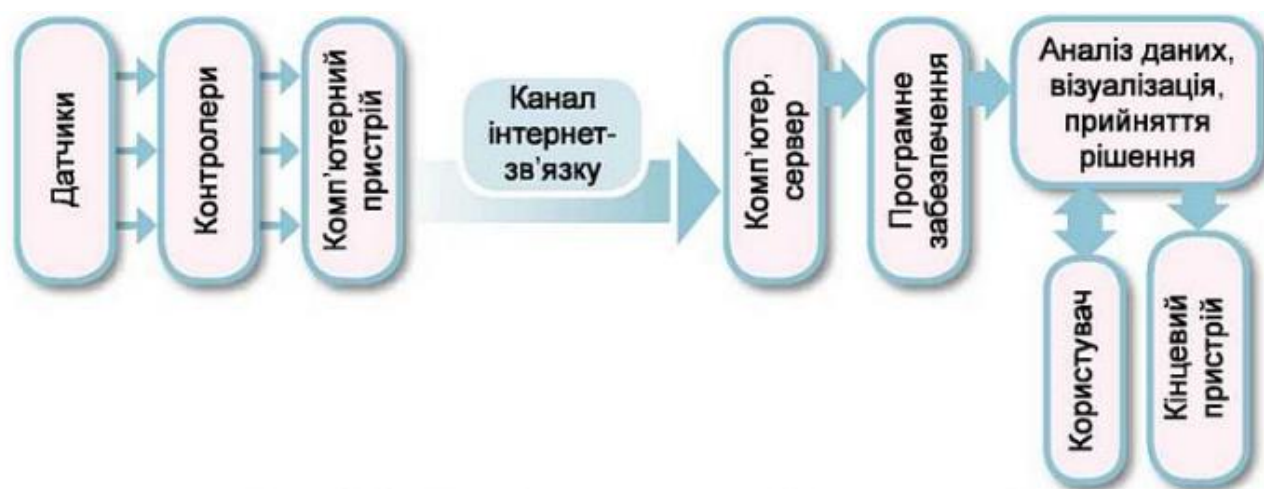


Рисунок 1.4 – Функціонування мережі Інтернет речей

1.2 Застосування Інтернет речей у сфері охорони здоров'я

Багато існуючих проблем можна вирішити спільно з IoT. Рішення IoT може покращити рівень ефективності лікування та моніторингу пацієнтів. Розглянемо приклади додатків Інтернету речей у секторі охорони здоров'я.

1.2.1. Дистанційний моніторинг пацієнтів. Як показує статистика, 30 % медичних пацієнтів повторно госпіталізуються після операції. Однозначною відповіддю є відсутність спостереження за пацієнтом. Вирішення надзвичайної ситуації все ще залишається проблемою.

Віддалений моніторинг пацієнтів можливий за допомогою співпраці IoT. Носимі пристрої з вбудованими датчиками можуть контролювати стан пацієнта протягом усього дня і повідомляти лікаря (рис.1.5). Наприклад, за допомогою технології може повідомляти лікарям, якщо пацієнт не приймає ліки регулярно.



Рисунок 1.5 – Дистанційний моніторинг пацієнтів

1.2.2 Управління операціями лікарні. Навколо лікарні працює багато людей, і, очевидно, це людне, зайняте місце. Крадіжка медичного обладнання – це злочин, який може коштувати життя. Іноді лікарі настільки зайняті, що не мають можливості спостерігати одночасно за пацієнтами. Наприклад, можна проводити моніторинг реакції лікарні на надання допомоги пацієнту. Лікарі зможуть дізнатися про поточне розташування необхідного обладнання, яке може бути ефективним за часом тощо (рис.1.6).

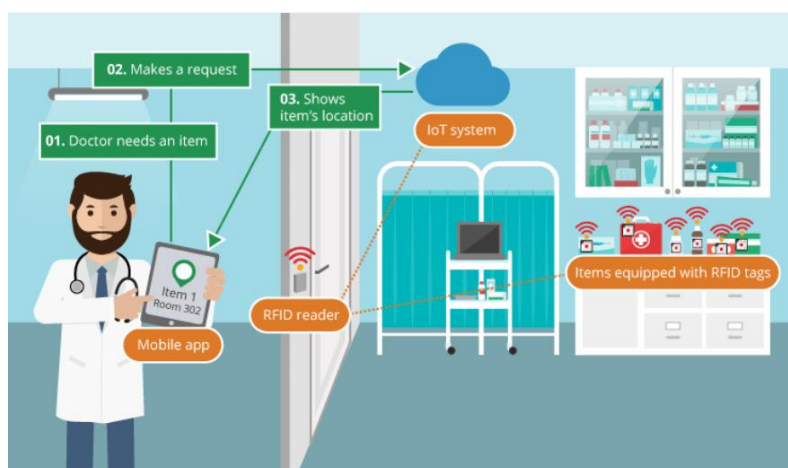


Рисунок 1.6 – Управління операціями лікарні

1.2.3 IoT в охороні здоров'я: моніторинг глюкози. Діабет – хронічне захворювання, яке проявляється при порушенні функцій підшлункової залози. Основне завдання підшлункової залози – виробляти гормон інсулін. Інсулін контролює рівень глюкози в крові. Коли підшлункова залоза виробляє менше або зовсім не виробляє інсулін, рівень цукру в крові може підвищуватися і знижуватися. Це може призвести до життєво важливих пошкоджень внутрішніх органів. Тож додатки Інтернету речей із носіями або вбудованими датчиками тіла, які постійно контролюють та надсилають дані про рівень цукру в крові, можуть мінімізувати ризик смерті від діабету. Передавач або датчики надсилають дані на екран комп'ютера або смартфона, після чого їх може проаналізувати лікар. Оскільки можна виявити рівень цукру, ранні пацієнти зможуть вчасно вжити необхідних заходів (рис.1.7).



Рисунок 1.7 – IoT в охороні здоров'я: моніторинг глюкози

1.2.4. Підключений інгалятор (рис.1.8). Астма – це захворювання, яке не піддається лікуванню, але його можна контролювати за допомогою інгалятора. Симптоми нападу астми пацієнт може усвідомити за півгодини до восьми годин до цього. Інгалятор, підключений до датчика, може попередити пацієнта про спрацьовуючий фактор (пилوک повітря, температуру), щоб запобігти нападу астми. Тобто, використання мобільного додатка дасть можливість тривалий час боротися з респіраторними захворюваннями. Лікарі зможуть відстежувати стан хвороби та повідомляти пацієнта, якщо необхідно використовувати інгалятор. Обчислює дані, отримані з датчика, і пропонує пацієнтам вжити необхідних заходів.



Рисунок 1.8 – Підключений інгалятор

1.2.5 IoT в охороні здоров'я: Взаємодія. Різні організації охорони здоров'я почали збирати величезну кількість даних, зареєстрованих пристроями IoT. Збираючи ці дані, IBM Watson та TEVA розпочали нову Проект IoT, у результаті виконання якого планується створення нових методів лікування та прогнозування хронічних захворювань. Для організації цих даних організації охорони здоров'я використовують штучний інтелект. Пристрій IoT надсилає та отримує дані через хмарне сховище. В результаті одні й ті ж дані можуть бути доступні для кількох пристроїв, що насправді неможливо для поточної системи.



Рисунок 1.9 – IoT в охороні здоров'я: Взаємодія.

1.2.6 Розумні контактні лінзи. Око – надзвичайний орган людини. Завдяки поєднанню датчика та контактної лінзи можна виявити симптоми різних захворювань, які можуть стати надзвичайним прогресом IoT у охороні здоров'я.

Визначення рівня слізної глюкози та раннє виявлення діабету може бути можливим за допомогою контактної лінзи на основі Інтернету речей. Дослідники працюють над вирішенням пресбіопії (захворювання, спричиненого втратою еластичності очної кришталика) за допомогою контактної лінзи на основі датчика. Розумна контактна лінза Triggerfish може виявити зміну розміру очного яблука, що є симптомом глаукоми.

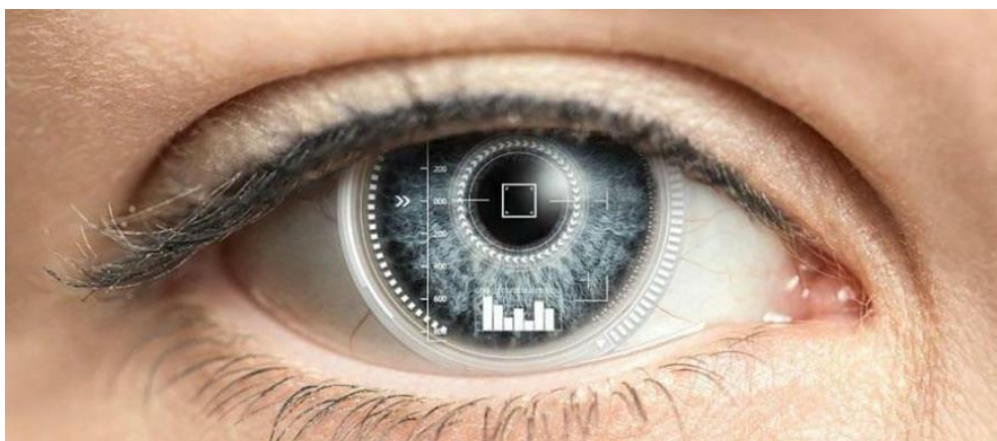


Рисунок 1.10 – IoT в охороні здоров'я: Взаємодія

1.2.7. Інтернет речей у сфері охорони здоров'я: Слуховий апарат.

Інтернет речей у сфері охорони здоров'я відіграє провідну роль, і додаток слухових апаратів на основі Інтернету речей уже знайомий. Майже 500 мільйонів людей мають прогресуючі проблеми зі слухом. Нижче наведено деякі характеристики додатків слухових апаратів на основі Інтернету речей: переваги прослуховування дзвінка у двері з будь-якої точки світу за допомогою слухового апарату, якщо обидва пристрої підключені через Інтернет; можливість увімкнути або вимкнути світло з віддалених місць за голосовою командою; користувачі можуть слухати кілька бесід одночасно тощо.



Рисунок 1.11 – Інтернет речей у сфері охорони здоров'я: Слуховий апарат

1.2.8 Тест на згортання крові. Рівень згустків крові відіграє важливу роль в організмі людини. Для лікування різних захворювань, таких як діабет, інсульт тощо, необхідно знати рівень згустків крові. Ця технологія з підтримкою Bluetooth допомагає пацієнту контролювати, як швидко у них згортається кров. Зменшують ризик інсульту мозку та проблеми з кровотечею у хворих на цукровий діабет. Знижує лікарняні витрати на дослідження тромбів, оскільки лікарі можуть стежити за пацієнтом з віддалених місць.



Рисунок 1.12 – Тест на згортання крові

1.2.9 Розумні годинники для депресії. Нещодавно технологічний гігант Apple почав працювати над своїм розумним годинником для виявлення рівня депресії, адже щороку багато людей проходять курс лікування від депресії. Цей пристрій може відстежувати та пропонувати, що робити у разі депресії. Це інноваційний приклад штучний інтелект або машинне навчання в охороні здоров'я, що допомагає передбачити рівень депресії користувачів, оцінює та контролює рівень депресії пацієнта та зберігає дані у хмарі. Це дозволяє психологу зрозуміти уявлення про проблеми пацієнта шляхом моніторингу з віддалених місць.



Рисунок 1.13 – Розумні годинники для депресії

1.2.10 Виявлення раку пристроями IoT. Рак молочної залози – друге небезпечне явище для жінок після раку легенів. Ідея виявлення раку молочної залози – використання «розумної тканини», більш ефективного, ніж звичайна процедура виявлення раку. Ця тканина може виявляти зміни температури за

допомогою семи вбудованих датчиків на тканині молочної залози. Аналізуючи аномальний малюнок, він використовує а алгоритм машинного навчання для прогнозування раку на ранніх стадіях. Відсутня радіація або побічні ефекти цієї «носимої» технології.

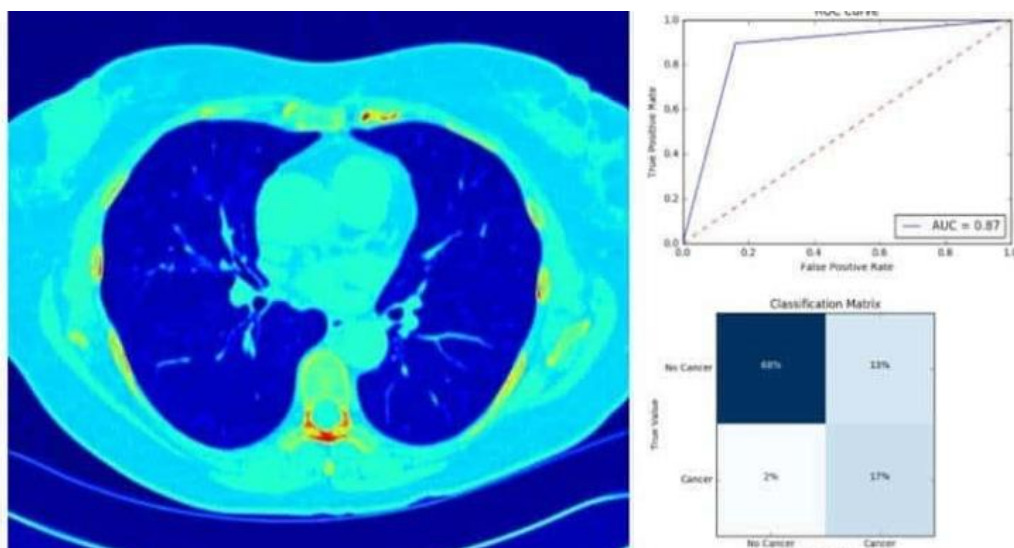


Рисунок 1.14 – Виявлення раку пристроями IoT

1.2.11 Моніторинг пацієнтів з Паркінсоном. Пацієнти хвороби Паркінсона потрібно спостерігати щохвилини. Застосування IoT у охороні здоров'я дають позитивні рішення. Результати таких досліджень, як “API рухових розладів”, можуть виявити ненормальні кроки, нестабільність довжини кроку у пацієнтів, щоб намалювати графік. Лікар аналізує та перевіряє дані з хмари та пропонує родичам цих пацієнтів, що робити.

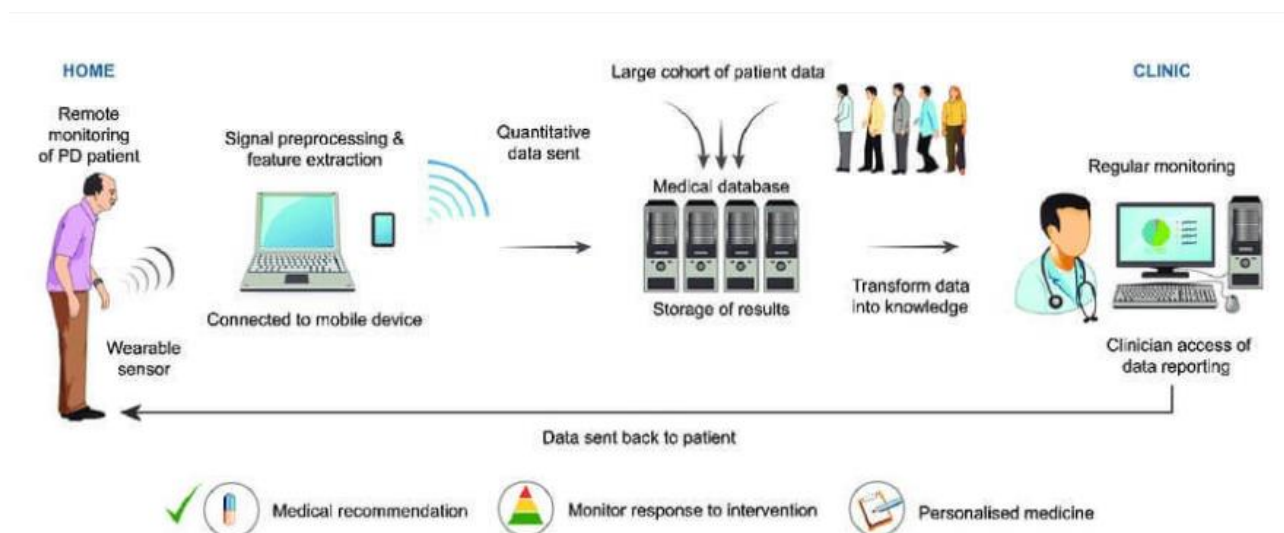


Рисунок 1.15 – Моніторинг пацієнтів з Паркінсоном

1.2.12 Датчики для прийняття ліків. Згідно з дослідженням ВООЗ 50%, люди не приймають ліки за призначенням лікаря. Ця практика призводить до важких станів пацієнта. Датчики для засвоєння з магнієвим та мідним покриттям можуть викликати сигнал, якщо ліки не вживатись у певний час.



Рисунок 1.16 – Датчики для прийняття ліків

1.2.13 Інтернет речей у сфері охорони здоров'я: Роботизована хірургія. Для виконання хірургічної операції лікарі використовують роботизовані пристрої з підтримкою Інтернету речей. Маленький роботизований пристрій може виконувати операції всередині тіла пацієнта. Це дозволяє лікарям проводити операцію з більшим контролем і точністю. Це дає можливість проводити операцію з віддаленого місця, що може врятувати багато життів як у шпиталі, так і в зоні бойових дій.

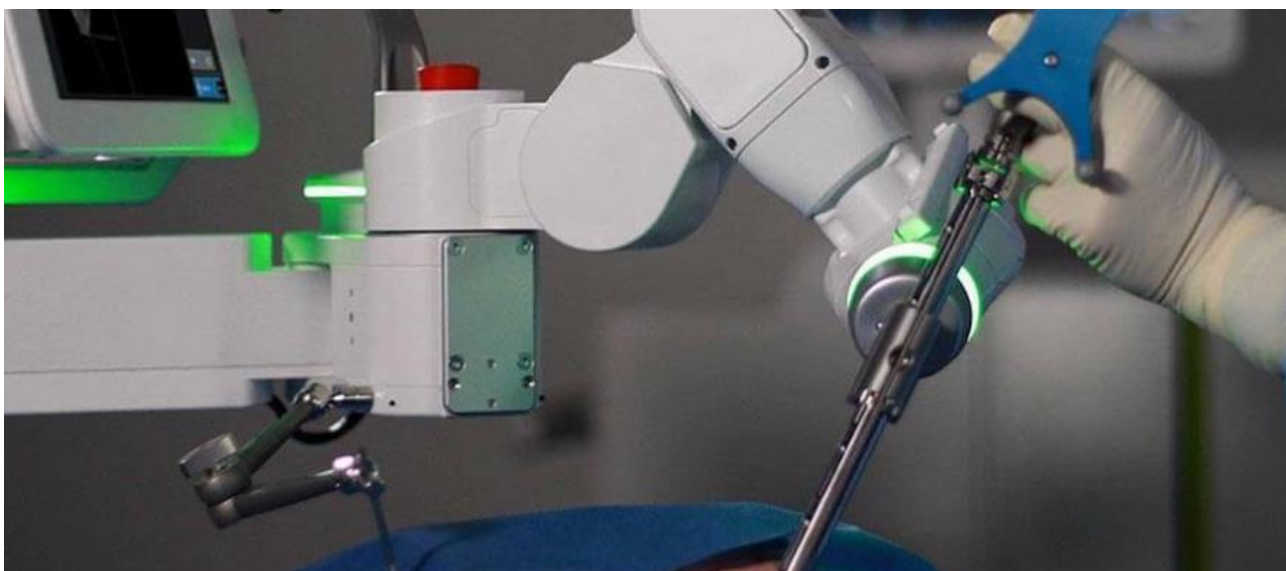


Рисунок 1.17 – Роботизована хірургія

1.2.14 Розумна підощва GPS. Лікування хворого на Альцгеймера - завдання не з легких. Вони забувають щоденні необхідні завдання і речі, і часто виявляються загубленими. Розумна устілка, вбудована з GPS, може стати рішенням для моніторингу її розташування. Можливо використовувати як супутникову, так і стільникову технологію для відстеження GPS.

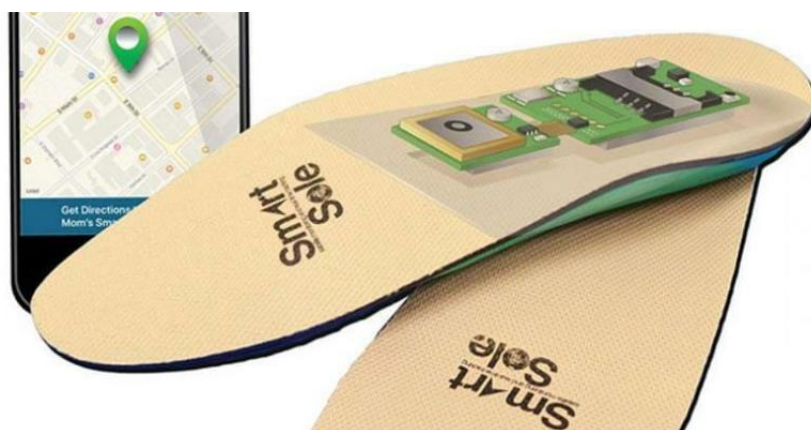


Рисунок 1.18 – Розумна підощва GPS

1.2.15 IoT в охороні здоров'я: сканування тіла. Кожен хоче мати підтягнуте тіло. Але регулярні огляди фітнесу іноді обходяться дорого. Розумний сканер тіла є прикладом IoT у охороні здоров'я, який відстежує зміни вашого тіла, включаючи інші параметри та показує порівняння між попередніми результатами. Ми говоримо про комбінацію виводу серед повнорозмірного дзеркала з 3D камери і вагову вагу та мобільний додаток.

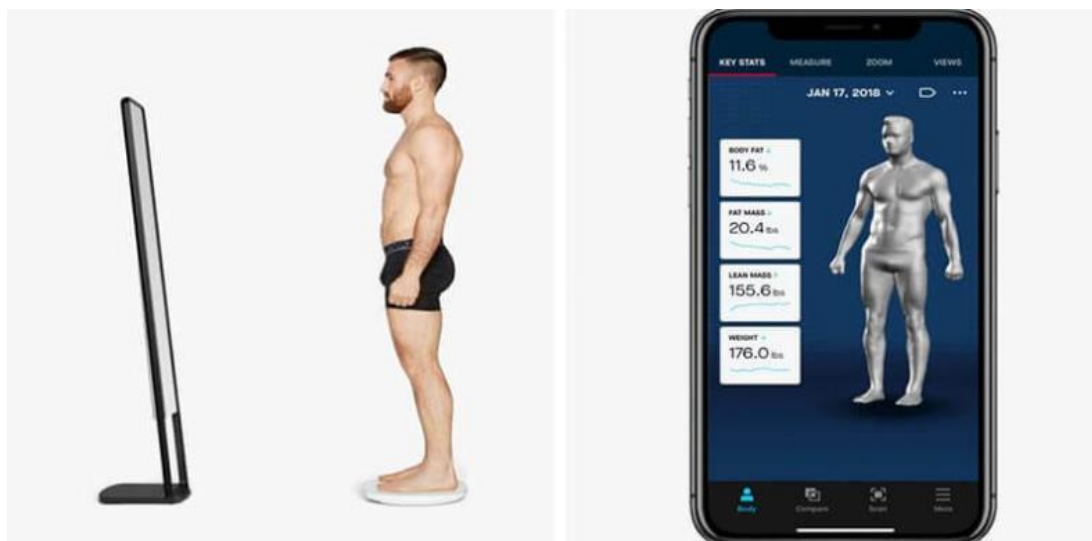


Рисунок 1.19 – Сканування тіла

1.2.16 Моніторинг серцевого ритму. Кількість серцево-судинних хворих у всьому світі зростає з кожним днем. Додатки IoT можуть виявляти серцебиття та пульс, що може зменшити фактор ризику. Пристрій, підключений до датчика, надсилає в хмару частоту пульсу в режимі реального часу, і лікарі можуть перевірити ці дані з будь-якої точки світу

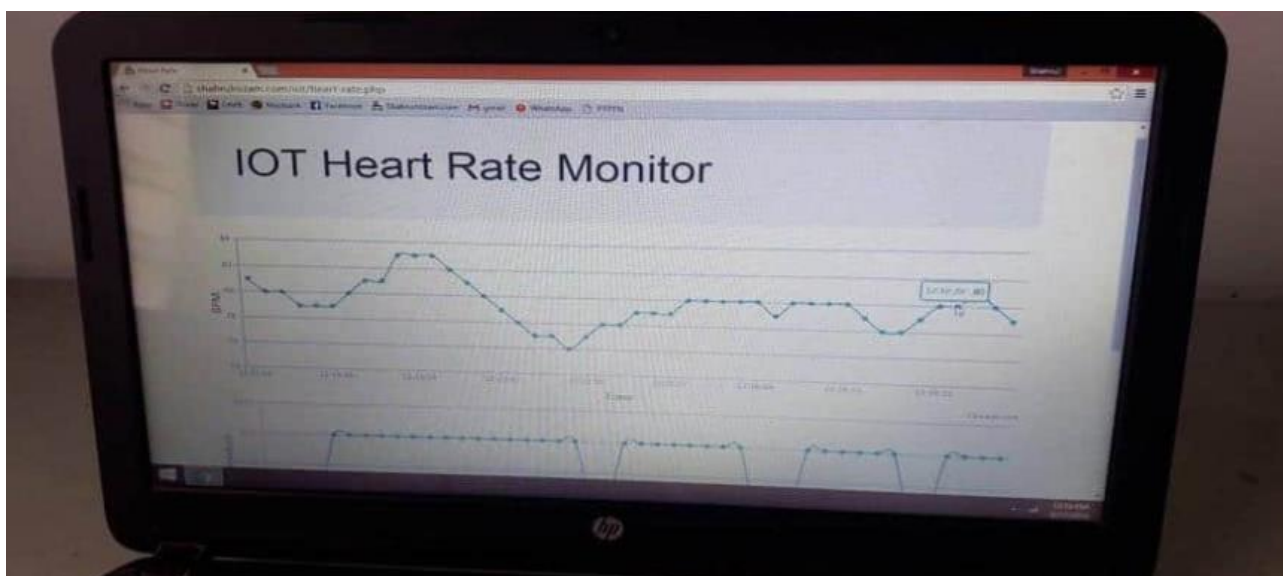


Рисунок 1.19 – Моніторинг серцевого ритму

1.2 Телемедицина

Зростання охорони здоров'я на базі інформаційних та комунікаційних технологій породило інноваційну концепцію практичної медицини та клінічних послуг на відстані, використовуючи телекомунікації, названу телемедициною.

Телемедицина дозволяє лікарям віддалено обслуговувати пацієнтів, отримуючи доступ до медичної інформації за допомогою телекомунікаційного зв'язку. Телемедицина має велике полегшення для людей в сільських та віддалених районах, де є обмежена медична установа, включаючи лікарів та інфраструктуру. Лікарі діагностують та консультують пацієнтів віддалено за допомогою місцевих медичних працівників, які безпосередньо ведуть пацієнтів.

Ключовим фактором телемедицини є телекомунікаційне посилення, що використовується технологіями, такими як мобільний зв'язок, відеоконференції, факс, сканери тощо для комунікації та обміну медичними документами (наприклад, рентгенівське та сонографічне зображення, фотографія інфекції, попередні приписи, патологічний звіт, звіт ЕКГ тощо). Спираючись на ці документи, лікарі оцінюють умову та рекомендації пацієнтів [1,5]. Широке поширення та всюдисутність в Інтернеті розширили сферу телемедицини.

Концепція телемедицини реалізується трьома способами [3,4,6]:

- Зберігати та передавати: Це асинхронний процес, і не потрібно, щоб обидві сторони були одночасно у контакті чи в Інтернеті. Інформація про стан здоров'я та медична документація пацієнта надсилаються лікарям для оцінки. Лікарі вивчають звіти у зручний час та надають відгуки /вказівки місцевим медичним працівникам.

- Віддалений моніторинг: Лікар дистанційно відстежує життєву статистику пацієнта.

- Взаємодія в режимі реального часу: Лікар і пацієнт із віддаленого місця взаємодії в реальному часі. Зручність для лікаря-лікаря вдома або в сусідньому медичному закладі заздалегідь встановлюється інтерактивний графік з лікарем [7].

1.3 Віддалений моніторинг здоров'я

Віддалений моніторинг здоров'я є частиною віддаленої охорони здоров'я чи електронної охорони здоров'я. Це підхід для автоматизованого моніторингу

здоров'я з будь-якого місця. Це стало можливим завдяки просуванню сенсорів та WSN та інших новіших технологій, таких як WBAN [8] та IoT [9]. Різні сенсори здоров'я, вживленні в тіло, відбирають різні фізіологічні дані, такі як температура тіла, показники серця та пульсу, артеріальний тиск, рівень цукру в крові, мозкові хвилі, рівень кисню в крові тощо [2]. Ці дані надсилаються зацікавленим медичним працівникам, які інтерпретують їх для оцінки стану здоров'я пацієнта, діагностики та рекомендацій щодо лікування ліками або лікування.

Аналізуючи дані, може бути вирішено, чи потрібно профілактичне терапевтичне втручання чи потрібно змінити протокол лікування пацієнта. Якщо прилади моніторингу підключені до Інтернету безпосередньо, лікарі можуть стежити за пацієнтами в режимі реального часу. Крім того, інтеграція системи віддаленого моніторингу із складними аналітичними інструментами забезпечує лікарям більшу видимість та розуміння стану здоров'я пацієнта.

Віддалений моніторинг здоров'я виявляє кілька переваг:

- Віддалений моніторинг здоров'я забезпечує надання постійної та якісної допомоги пацієнтам у віддалених місцях
- Охорона здоров'я стає доступнішою. Віддалений моніторинг дозволяє лікарям звертатися до потенційних пацієнтів, особливо до тих людей, які з певних причин не можуть дозволити собі відвідати лікаря або не змогли звернутися до лікарень.
- Забезпечує кращу якість життя, покращену мобільність та зниження рівня смертності для непривілейованого населення з точки зору медичних послуг.
- Скорочення витрат на охорону здоров'я за рахунок зменшення тривалого перебування на лікарняному ліжку, зменшує частоту повторної госпіталізації.
- Попередження погіршення стану здоров'я шляхом постійного моніторингу за допомогою сучасних.

- Поширений доступ до даних про пацієнтів дозволяє міждисциплінарне співробітництво та консультації, що допомагає в точному та загальному кращому процесі лікування, що призводить до якісного лікування пацієнтів.

- Більш швидкий доступ до відповідних даних про пацієнта дозволяє швидко розпочати лікування, а також скоротити тривалість лікування.

- І лікарі, і пацієнти мають кращий доступ до медичної інформації з актуальними значеннями життєвих параметрів. Буде легше лікарів опрацьовувати дані, зібрані з моніторингових пристроїв, у режимі реального часу за допомогою засобів візуалізації, таких як діаграми та діаграми.

- Дані, що контролюються, автоматично надходять у експертні системи та проводиться аналіз даних для кращого розуміння стану здоров'я пацієнта. Можна виявити погіршення невідповідності та клінічного стану пацієнта на ранньому етапі, проаналізувавши тенденцію зміни фізіологічних показників [12].

- Автоматизований моніторинг знижує ймовірність помилкового діагнозу та неправильного лікування.

- Зменшує можливість дублювання послуг (особливо діагностичних) .

- Автоматизований моніторинг може значно спростити деякі складні клінічні завдання, такі як гемодіаліз та лікування діабету [15].

- Повідомлення про надзвичайні ситуації за допомогою портативних та інтелектуальних пристроїв, таких як смартфони.

- Дані в режимі реального часу, що надаються приладами моніторингу, покращують своєчасність догляду та підвищують якість лікування [16].

- Економія часу як для лікарів, так і для пацієнтів. Лікарі та медичні працівники не повинні бути повністю зайняті конкретним пацієнтом. Вони можуть краще збалансувати відвідування інших пацієнтів [15].

- Віддалений моніторинг суттєво покращує спостереження за пацієнтом, дозволяючи коригувати лікування, дієту чи спосіб життя пацієнта.

- Уникає важкого тягаря перевезення пацієнтів.

- Дозволяє лікарням зменшити інфраструктурні та експлуатаційні витрати.

1.4 Проблеми в дистанційному моніторингу здоров'я

Для досягнення обіцяних переваг віддаленого моніторингу стану здоров'я необхідно вирішити деякі перешкоди, як зазначено нижче [17].

Філософія дистанційного моніторингу здоров'я полягає в наданні медичних послуг людям у віддалених місцях, де недостатньо інфраструктури охорони здоров'я. Але навіть для впровадження та використання віддаленого моніторингу необхідна мінімальна технічна інфраструктура. Наприклад, для опрацювання отриманих даних необхідний мінімальний обчислювальний інструмент. Так само для спілкування потрібний хороший широкосмуговий зв'язок. Іноді цих мінімумів також немає в невеликих закладах охорони здоров'я та в сільській місцевості.

Зазначу, що також потрібен час, щоб звикнути до імплантованих пристроїв. Відсутність прямого контакту лікарів робить пацієнтів скептичними та боязкими. Лікування, що базується лише на технології, може порушити поведінку пацієнта. Вони також можуть бути стурбовані тим, що деякі треті сторони можуть отримати власні приватні медичні дані та використовувати неетично.

Аналогічно, медичні працівники можуть побоюватися покладатися лише на системи охорони здоров'я на основі технологій, особливо для пацієнтів з високим рівнем ризику. Сенсори не помиляються. В недавньому дослідженні різних засобів, що відстежують фізичну активність, спостерігається велика різниця в точності в різних пристроях. Похибки реєструються до 25% [18]. Щоб віддалений моніторинг був ефективним та переконливим, неточність слід усунути шляхом підвищення точності пристрою.

Щоб отримати максимальну користь від віддаленого моніторингу здоров'я, його слід доповнити відповідним ефективним програмним забезпеченням. Ці програми повинні бути налаштовані для різних випадків використання та повинні мати сумісність з різними сторонніми програмами. Системи віддаленого моніторингу здоров'я повинні мати доступ до

електронних систем медичного обліку з різних клінік та лікарень, щоб мати загальну візуалізацію історії хвороби пацієнтів.

Незважаючи на ці виклики, віддалений моніторинг здоров'я має великий потенціал у зміні традиційного способу надання медичних послуг. Він ще знаходиться на ранній стадії, але, безумовно, він матиме перспективну роль у майбутньому охорони здоров'я.

Медичні працівники повинні докладати більше зусиль для ефективного використання віддаленого моніторингу, і пацієнтів потрібно мотивувати до більш активного залучення, оскільки користь від цього значною мірою залежить від здатності пацієнтів користуватися залученими технологіями.

Заклади, що забезпечують дистанційний моніторинг стану здоров'я, та зацікавлені сторони повинні застосовувати стандартні практики.

1.5 Різниця між телемедициною та дистанційним моніторингом здоров'я

Розглянемо терміни "телемедицина" та "дистанційний моніторинг здоров'я". Отже, між ними немає узгоджених та конкретних диференціюючих факторів. Обидва терміни стосуються обміну медичною інформацією в електронному вигляді [19]. Обидва мають на меті допомогти пацієнтам віддалено. Ось чому люди часто використовують терміни взаємозаміно.

Але насправді це зовсім інші підходи до електронної охорони здоров'я. Насправді дистанційний моніторинг здоров'я є ключовим фактором, що відрізняє традиційну телемедицину від сьогоденної електронної медичної допомоги, що включає як телемедицину, так і дистанційний моніторинг здоров'я. Основні диференціюючі фактори обговорюються нижче. У таблиці 1.1 наведені різниці між телемедициною та дистанційним моніторингом здоров'я.

Мета телемедицини – дати можливість пацієнтам, особливо з віддалених та сільських районів, безпосередньо взаємодіяти з віддаленими лікарями, які, можливо, сидять у міській лікарні. Лікарі оцінюють стан пацієнта різними способами за допомогою телекомунікацій та направляють його на лікування.

На відміну від цього, дистанційний моніторинг здоров'я – це автоматизований підхід для дистанційного спостереження та оцінки стану здоров'я пацієнтів. Оцінюючи медичні дані, медики та співробітники безпосередньо спрямовують пацієнта на прийняття відповідних заходів.

Таблиця 1.1 – Різниця між телемедициною та дистанційним моніторингом здоров'я

	Телемедицина	Віддалений моніторинг здоров'я
Підхід	Реактивний	Проактивний
Роль лікарів та персоналу	Сильно зайнятий	Менш зайнятий, лише для прийняття рішень.
Період залучення медичного персоналу до лікування	Короткострокова основа	Постійний моніторинг
Охорона здоров'я, надана	В основному лікарі, за допомогою місцевих медичних працівників.	Лікарі та загальноосвітні працівники, включаючи медичних сестер, клініцистів та інших.
Сфера спостереження за пацієнтами в реальному часі	Менше	Більше
Сфера прогнозування здоров'я	Менший розмах	Високо можливий
Точність медицини	-	-
Автоматизована охорона здоров'я	Ні	Так
Технічна витонченість	Низька	Висока
Підходить для більш високої кількості	Не зовсім	Так
Надійність	Залежить від розмовної та комбінованої здатності медичного персоналу з обох кінців.	Залежить від точності приладів моніторингу.
Ризик безпеки	Низький	Високий
Консультація пацієнтів	Часто	Низько
Спілкування лікар-пацієнт	Високий	Низький
Інфраструктура необхідна на кінці приймача	Не багато	Необхідна мінімальна інфраструктура для обробки даних про здоров'я та для їх передачі.
Відповідальність пацієнтів	Не багато. Дотримується вказівок місцевих медичних працівників.	Пацієнти повинні бути знайомі з приладами, якщо їх застосовують зовнішньо.
Свобода пацієнтів	Низька	Висока
Залежність пацієнтів від медичних працівників	Висока	Низька
Служба охорони здоров'я, отримана	В клініці	Вдома

Попереднє планування взаємодії пацієнта з лікарем	Більшість випадків повинні	Не вимагається
Первинне комунікаційне середовище	Телекомунікації, Інтернет	RFID, WBAN, WSN, Інтернет
Перевага для літніх людей	Не особливо	Дуже
Вигідний для реабілітації пацієнтів	Не особливо	Ідеально підходить
Технічні критерії медичних працівників	Не обов'язково	Повинен

У телемедицині лікарі повністю відповідають за оцінку пацієнтів, прийняття рішення та рекомендують лікування та ліки.

При дистанційному моніторингу здоров'я автоматизований моніторинг робить роботу лікаря значно спрощеною. Використовуючи сучасні аналітичні засоби, оцінку здоров'я також можна дещо автоматизувати.

Моніторингові пристрої фіксують дані про стан здоров'я у континуумі, дані, записані за минуле, можуть бути проаналізовані для моніторингу та прогнозування майбутніх проблем зі здоров'ям та прогресу у здоров'ї.

На відміну від цього, телемедицина – це короткий час, коли лікарі на короткому сеансі оцінюють поточну медичну умову пацієнта та рекомендують враховувати наявні симптоми. Як результат, дистанційний моніторинг має багато можливостей у загальній охороні здоров'я.

Віддалений моніторинг є інтенсивним технологічним розвитком, тоді як телемедицина – це інтенсивний процес для людини та експертів; лікарі ставлять діагноз за допомогою своєї експертизи.

РОЗДІЛ 2 МЕРЕЖІ ОХОРОНИ ЗДОРОВ'Я ІОТ

Мережа охорони здоров'я IoT або мережа IoT для охорони здоров'я є одним із життєво важливих елементів IoT в охороні здоров'я. Вона підтримує доступ до магістралі IoT, полегшує передачу та прийом медичних даних та дозволяє використовувати спеціальні для охорони здоров'я комунікації.



Рисунок 2.1 – Мережі охорони здоров'я IoT

У цьому розділі розглянемо топології, архітектуру та платформм IoThNet (рис.2.1). Однак слід зазначити, що запропоновані архітектури є відправною точкою для розвитку уявлень про мережу IoT.

2.1 Топологія IoThNet

Топологія IoThNet стосується розташування різних елементів мережі охорони здоров'я IoT і вказує на репрезентативні сценарії безкоштовних середовищ охорони здоров'я. На рис.2.2 описано, як обчислювальна мережа відбирає величезну кількість життєвоважливих показників та даних давачів, таких як артеріальний тиск (АТ), температура тіла, електрокардіограми (ЕКГ) та насичення киснем крові та утворює типову топологію IoThNet.

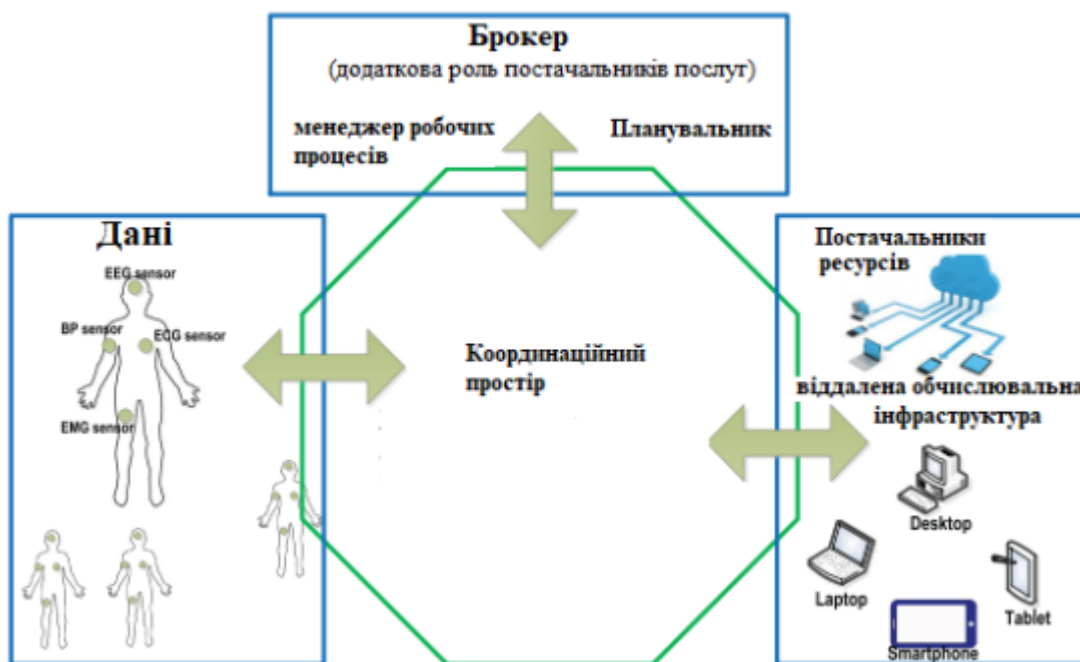


Рисунок 2.2 – Концептуальна схема рішень в галузі охорони здоров'я на основі IoT

Рис. 2.3 візуалізує сценарій, при якому профілактика здоров'я пацієнта та стан життєвоважливих органів фіксуються за допомогою портативних медичних пристроїв та давачів, прикріплених до тіла. Потім віддібрані дані аналізуються та зберігаються.

На основі аналізу лікарі можуть спостерігати за пацієнтами з будь-якого місця і відповідати відповідно. Крім того, топологія включає необхідну структуру мережі для підтримки потокової передачі медичних відео.

Наприклад, топологія на рис.1.3 підтримує потокове передавання ультразвукових відео через взаємопов'язану мережу WiMAX, мережі Інтернет-протоколу (IP) та глобальної системи для мобільної (GSM) мережі, а також звичайних шлюзів та мереж послуг доступу. Подібні концептуальні структури зустрічаються в [1] - [4].

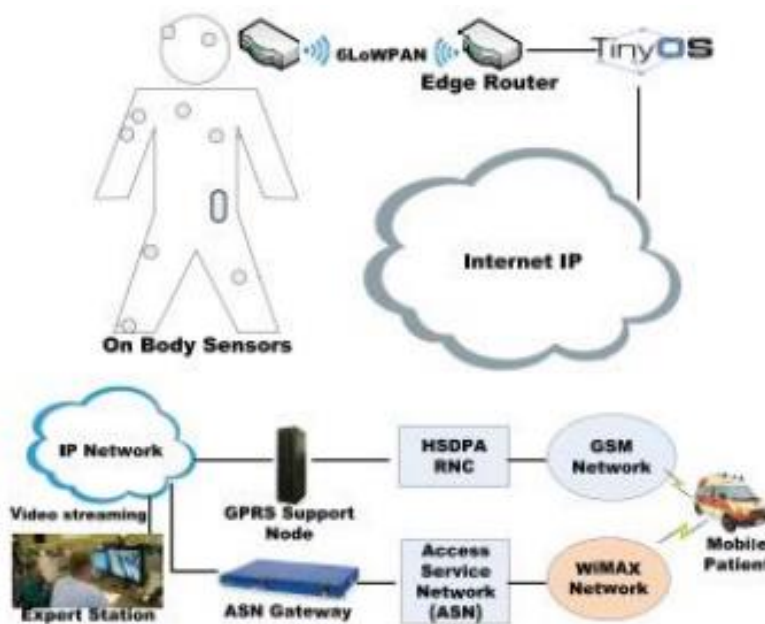


Рисунок 2.3 – Дистанційне спостереження за носими пристроями та індивідуальне медичне обслуговування

На рис. 2.4 представлена топологія IoThNet, що висвітлює роль шлюзу. Тут інтелектуальна фармацевтична упаковка (iMedPack) - це не що інше, як пристрій IoT, який вирішує проблему зловживання лікарськими засобами, забезпечуючи тим самим відповідність лікарським засобам.

Інтелектуальна коробка для ліків (iMedBox) вважається воротами охорони здоров'я з набором різноманітних необхідних датчиків та інтерфейсів безлічі бездротових стандартів. Різні носимі датчі та пристрої IoT бездротово підключені до шлюзів охорони здоров'я, що з'єднують середовище пацієнта із хмарою IoT для здоров'я, гетерогенною мережею (HetNet), що дозволяє проводити клінічну діагностику та інші аналізи. Сам шлюз може досліджувати, зберігати та відображати всі зібрані дані [4]. Подібний IoThNet топологія знаходиться в роботі [5], яка об'єднує клінічні пристрої з інфраструктурою підприємств охорони здоров'я IoT.

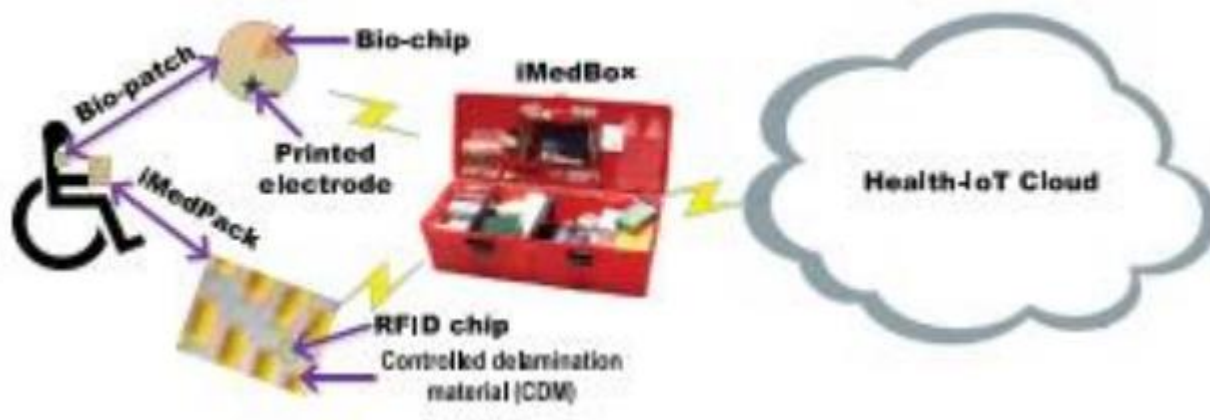


Рисунок 2.4 – Топологія IoThNet з інтелектуальним шлюзом охорони здоров'я

Визначення пов'язаних видів діяльності та ролей у медичних послугах є основним фактором у розробці топології IoThNet. Опрацювання до та під час лікування та після лікування включає медичні послуги переважно з точки зору постачальників медичних послуг. Така діяльність у галузі охорони здоров'я була продемонстрована в контексті надання невідкладної медичної допомоги та топології IoThNet, включаючи хмару запропоновано обчислення для всепроникного медичного обслуговування. Це можна розглядати як звичайну мережеву систему з повною мережею з повсюдною присутністю підключення до Інтернету.

2.2 Архітектура IoThNet

Архітектура IoThNet посилається на схему специфікації фізичних елементів IoThNet, їх функціональної організації та принципів та методів роботи.

Для початку на рис.2.5 представлена архітектура для систем телемедицини та навколишнього середовища, рекомендованих Continua Health Alliance.

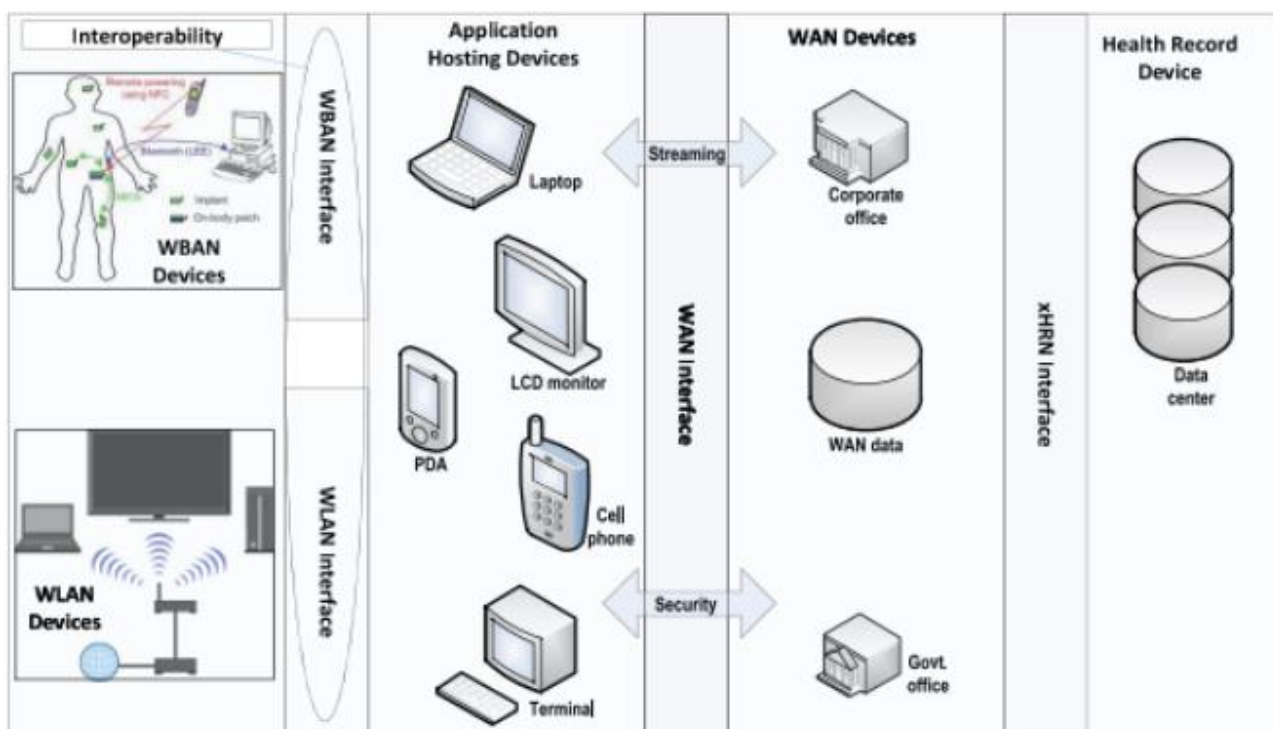


Рисунок 2.5 – Спрощена архітектура, що базується на структурі Health Alliance

Для цієї архітектури було визначено ключові проблеми [8]:

- сумісність шлюзу IoT та бездротової локальної мережі мережа (WLAN) / бездротова персональна мережа (WPAN),
- потокове передавання мультимедіа та безпечний зв'язок між шлюзами IoT та особами, які здійснюють догляд.

Багато досліджень [9-18] обґрунтовували, що 6LoWPAN на основі IPv6 є основою IoThNet.

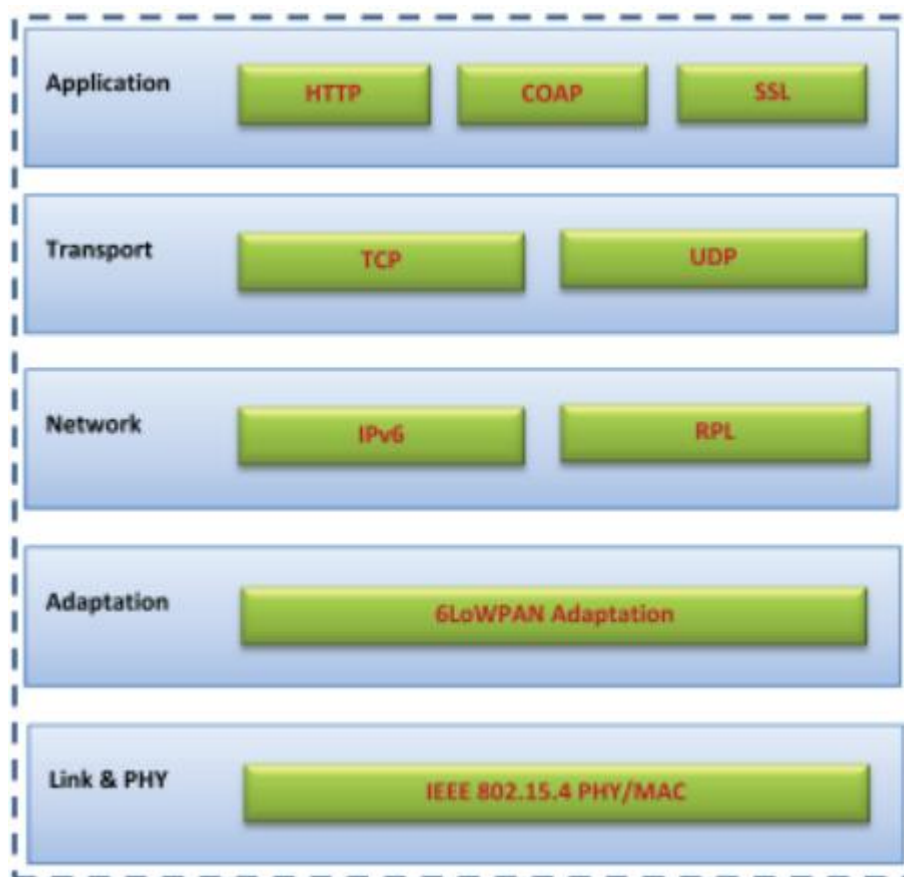


Рисунок 2.6 – Стек протоколів 6LoWPAN

На рис.2.6 показана структура шарів 6LoWLAN. Згідно з концепцією IoThNet, давачі та носимі пристрої використовують системи IPv6 та 6LoWPAN для передачі даних за протоколом 802.15.4. Однак 6LoWPAN обмежений тим, що не підтримує мобільний IPv6 (MIPv6), підмножину протоколу IPv6 з мобільністю.

2.3 Послуги і застосунки IoT

Системи охорони здоров'я на основі IoT можуть застосовуватися в різних сферах, включаючи догляд за педіатричними та літніми пацієнтами, нагляд за хронічними захворюваннями та управління приватним здоров'ям та фізкультурою. Для кращого розуміння цієї обширної теми цей документ широко класифікує дискусію у двох аспектах: сервісах та додатках. Програми додатково поділяються на дві групи: одно- та кластерні програми.

У цьому розділі представлено кожен із служб та застосунків, показаних на рисунку 2.7.

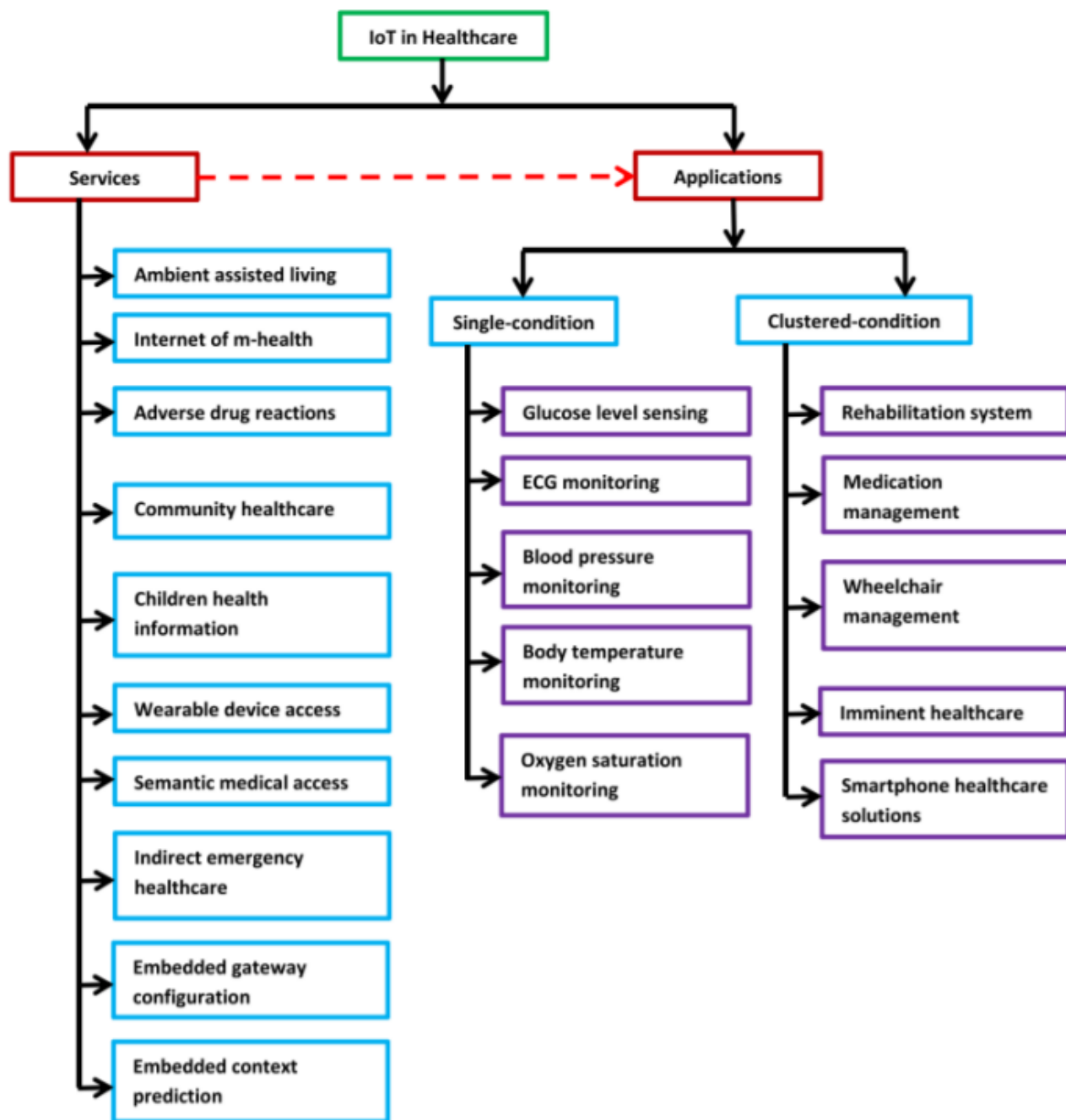


Рисунок 2.7 - Служби та програми охорони здоров'я IoT

2.4 Архітектура апаратно-програмного комплексу моніторингу в реальному часі стану організму людини

Запропоновано концепцію створення багаторівневої мобільної персоналізованої системи з поєднанням архітектур: клієнт-серверної та публікаційно-підписної. Структурно частина публікаційно-підписної для задач

особисто-орієнтованої медицини передбачає виконання процедури ідентифікації користувачів; передавання даних від медичних давачів, або внесення даних вимірювань з клавіатури; модуль локальних обчислень та відображення результатів. Сервером формується глобальна база даних та реалізується інформаційно-технологічна процедура комплексного аналізу, результати якого використовують для вчинення дій щодо запобігання ускладнень та локалізації процесів розвитку можливих захворювань.

На рисунку 2.9 подано загальну схему системи дистанційного моніторингу стану здоров'я з використанням сервісів IoT та технології передачі даних 4G/5G.

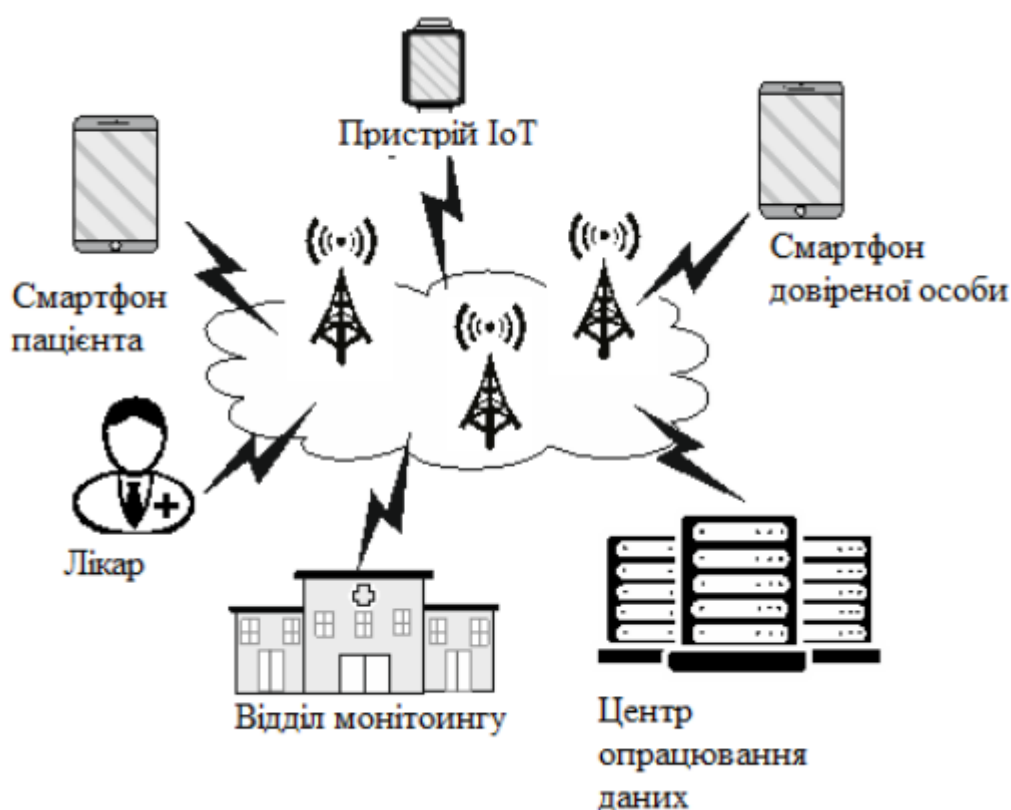


Рисунок 2.9 – Система дистанційного моніторингу показників стану здоров'я

Термінальні пристрої, які використовують IP-протокол, забезпечують збір та передавання даних. Після авторизації клієнт або його довірені особи 33 отримують доступ до зібраних даних шляхом взаємодії з веб-сервером за технологією клієнт-сервер.

Апаратно-програмний комплекс дозволяє реалізовувати:

- автоматизацію системи збору телеметричних даних з використанням технологій IoT, на базі 4G/5G телекомунікаційних мереж з забезпеченням QoS-пріоритетів;
- проведення аналізу зібраних даних для попередження виникнення можливих захворювань та їх ускладнень;
- миттєве реагування на критичні зміни показників стану здоров'я;
- підвищення якості та рівня надання медичних послуг різним групам населення через використання новітніх мобільних технологій;
- забезпечення оперативної діагностики з індивідуальним підходом до пацієнта;
- розширення спектру використання телекомунікаційних технологій шляхом впровадження телемедицини на базі мереж оператора мобільного зв'язку.

Комплекс реалізовується з врахуванням принципів масштабованості архітектурних рішень у галузі телемедицини, що дозволяє його розгортання для однієї лікарні, так і для району так і цілої країни. В ході реалізації проекту, передбачається розміщення моніторингових станцій у лікарнях, які здійснюють безперервне онлайн спостереження за станом здоров'я пацієнта, та при виникненні критичної ситуації оперативно повідомляють про це лікуючого лікаря.

У випадку масштабування проекту з охопленням населення окремого міста або району, пропонується винесення моніторингової станції до окремої установи. Це дозволяє мінімізувати витрати на обслуговування комплексу, за рахунок усунення фактору дублювання моніторингових станцій.

Апаратно-програмний комплекс забезпечує ефективне функціонування структури діагностики стану здоров'я особи. На першому рівні користувачі мають змогу самостійно контролювати свої показники життєдіяльності та рівень своєї фізичної активності. На другому рівні забезпечується реалізація комплексного аналізу отриманих даних, доступ до професійного програмного забезпечення фахових лікарів, більш детальне дослідження результатів вимірювання, експрес-аналіз даних і формування відповідних рекомендацій.

Пристрій, що дозволяє моніторити параметри стану здоров'я особи повинен бути обладнаний модулем 4G/5G, GPS-трекером, вбудованим акумулятором та можливістю бездротового підзарядження. Заряд акумулятора повинен забезпечувати безперебійну роботу пристрою впродовж 72 годин. Для подовження часу безперервного функціонування пристрій можна оснастити засобами що викорситовують енергію активних рухів.

Smart-пристрої моніторингу параметрів стану здоров'я можуть бути виконані у вигляді браслету, пластирів, поясів, сенсорів, які кріпляться на одяг чи безпосередньо на тіло, або імплантуються підшкірно. Зазвичай спосіб виконання пристрою залежить від набору показників, які він повинен вимірювати (температура, кров'яний тиск, частота серцевих скорочень, ЕКГ, рівень SpO2, рівень інсуліну і т.ін.). Водночас такі пристрої можуть забезпечувати вимірювання показників зовнішнього середовища, таких як, рівень токсинів у повітрі, температуру та зовнішній тиск та повідомляти про це свого власника [12]. Передбачається, що давачі забезпечують інформацією в реальному масштабі часу і реалізують її попереднє опрацювання.

Апаратно-програмний комплекс моніторингу параметру життєдіяльності людини повинен забезпечувати взаємодію таких пристроїв, як: пристрій IoT пацієнта, термінали довірених осіб, термінал лікаря та моніторингової станції.

Розглянемо функціональне призначення кожного з перелічених пристроїв:

- пристрій IoT пацієнта містить сенсори, які вимірюють параметри життєдіяльності людини, та передає дані в мобільні мережі, що підтримують стандарти 4G/5G;

- термінали довірених осіб пацієнта можуть реалізовуватися у смартфонах, планшетах, комп'ютерах чи інших пристроях, які мають доступ до мережі інтернет. Довірені особи мають можливість отримувати дані щодо стану здоров'я пацієнта з баз даних розміщених сервері аналітики;

- термінал лікаря має доступ до даних про актуальний стан здоров'я пацієнта, а також до статистичних даних, які містяться у базах даних сервера аналітики;

– моніторингова станція забезпечує цілодобовий нагляд за станом здоров'я пацієнта. У випадку його погіршення генерується повідомлення для лікаря, який приймає фахове експертне рішення.

До кожного з перелічених пристроїв висувається ряд вимог, які залежать від використовуваних функцій та інформаційно-технологічних сервісів. Наприклад, однією з основних функцій призначенням пристрою IoT пацієнта є цілодобове вимірювання показників здоров'я та передавання їх значень до баз даних, що розміщені на сервера. Оскільки зазначений пристрій асоціюється з критичними сервісами IoT, він повинен бути високо надійним та постійно доступним. Окрім цього важливим є забезпечення якомога вищої мобільності користувача, яка досягається за рахунок розширення мобільного покриття, так і зменшення його енергоспоживання. З огляду на це доцільним видається використання протоколу Message Queue Telemetry Transport, який забезпечував би оптимальну взаємодію пристроїв.

РОЗДІЛ 3

ДОСЛІДЖЕННЯ РЕАЛІЗАЦІЇ ІoT СИСТЕМИ МЕДИЧНОГО ПРИЗНАЧЕННЯ

3.1 Проектні рішення по структурі та архітектурі побудови ІoT системи медичного призначення

Проектовану інфраструктуру ІoT системи медичного призначення складають:

- обладнання ІoT, включаючи комп'ютерну та медичну складові;
- активне мережеве обладнання для формування LAN і WAN-сегментів;
- ОКП (сервера підсистеми управління, контролю і архівації даних);
- модулі загального та спеціалізованого програмного забезпечення;
- пасивне обладнання та девайси телекомунікацій, за допомогою яких буде функціонувати основне технологічне обладнання інформаційно-комунікаційної системи передачі медичних даних.

Виходячи з того, що проектувана інформаційно-комунікаційна система в своєму складі містить сукупність телемедичних центрів, пунктів (стаціонарних, віддалених і мобільних) можливі два основні варіанти архітектури побудови системи – централізована і розподілена.

Відповідно до технічних вимог та тенденцій розвитку існуючих систем віддаленого моніторингу, ця робота пропонує своєрідну інформаційно-комунікаційну систему, яка має тришарову архітектуру: «вузли домашнього моніторингу», «центр моніторингу громади», «центр моніторингу лікарень».

Таким чином, система може здійснювати управління здоров'ям, моніторинг стану здоров'я, віддалену медичну допомогу тощо, і ці функції можуть взаємодіяти та взаємозв'язуватись, тому система може гарантувати моніторинг стану здоров'я людей при постійній передачі медичних даних.

Спроектowana архітектура системи дистанційного моніторингу на базі технології Інтернет-речей показана на рисунку 3.1.

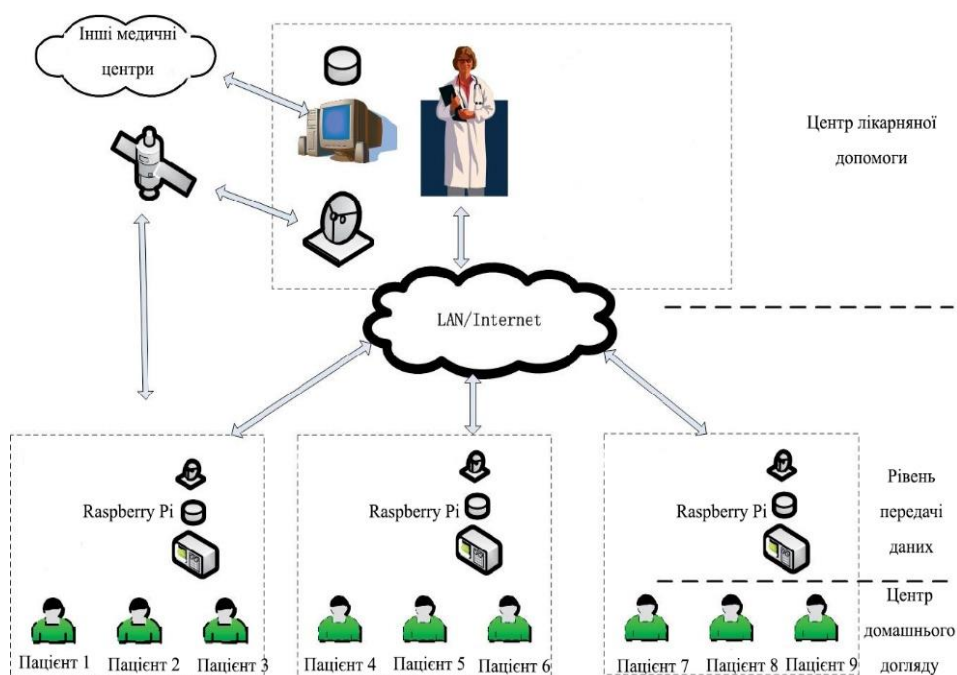


Рисунок 3.1 – Архітектура IoT системи

На рівні сімейних моніторингових вузлів система збирає життєві показники людини, такі як температура, пульс, кисень та рівень цукру крові, кров'яний тиск, тощо, завдяки інтеграції датчиків пацієнтам, а потім ця інформація, яка пройшла через модулі бездротового приймача-передавача вузлів, буде надіслана до моніторингового центру («сервера») за допомогою самоорганізуючої та бездротової мережі.

У центрі медичної допомоги сигнали про стан людського організму, які надсилають пацієнти, що носять бездротові датчики, можуть прийматися релейними вузлами і попередньо оброблятися. Коли центр виявить «ненормальний» сигнал (ознаки стану «перед хвороби»), він видасть пацієнтові вказівки про необхідність негайної перевірки в медичному центрі, де лікарі можуть виявити загальну хворобу. Для складних або критичних захворювань ретрансляційна станція передаватиме параметри життєво важливих ознак пацієнтів у великомасштабний центр моніторингу лікарні через мережу Ethernet.

У центрі медичної допомоги сигнали про стан людського організму, які надсилають пацієнти, що носять бездротові датчики, можуть прийматися релейними вузлами і попередньо оброблятися. Коли центр виявить «ненормальний» сигнал (ознаки стану «перед хвороби»), він видасть пацієнтові вказівки про необхідність негайної перевірки в медичному центрі, де лікарі

можуть виявити загальну хворобу. Для складних або критичних захворювань ретрансляційна станція передаватиме параметри життєво важливих ознак пацієнтів у великомасштабний центр моніторингу лікарні через мережу Ethernet.

Центр віддаленого моніторингу лікарні встановлює центральну базу даних, яка зберігає основні особисті дані медичного закладу, дані про медичну поведінку, дані про прийняття рішень тощо. Центр створює систему зв'язку між пацієнтом і лікарем через мережу Ethernet та мережі 3G/4G/5G, а також автоматично отримує, аналізує, обробляє та діагностує дані про фізіологічні особливості пацієнтів, що надсилаються медичним центром, а потім визначає результат. У той же час вихідні дані, передані інтелектуальним терміналом, також можуть зберігатися для подальшої діагностики та прийняття рішень.

Розподілена архітектура побудови інформаційно-комунікаційної системи характеризується тим, що елементи підсистеми управління контролю та архівації можуть перебувати всередині будь-яких телемедичних центрів і пунктів.

3.2 Передача даних з давачів на телефон Android з використанням Arduino і модуль NRF24L01 через Bluetooth (BLE)



Рисунок 3.1 – Зображення передачі медичних даних

Bluetooth Low Energy (BLE) – це версія Bluetooth, представлена у вигляді зменшеної високооптимізованої версії класичного Bluetooth (як зазначалось у розділі 2). Він також відомий як Smart Bluetooth. BLE був розроблений з урахуванням мінімально можливого енергоспоживання, особливо для обладнання низької вартості, низької пропускну здатності, низької потужності і низької складності. ESP32 має вбудовані можливості BLE, але для інших мікроконтролерів, таких як Arduino, можна використовувати nRF24L01. Цей дешевий радіочастотний модуль також можна використовувати в якості модуля BLE для відправки даних на інший пристрій Bluetooth, такі як смартфони, комп'ютер і т.д.

BLE був прийнятий через його особливості енергоспоживання, оскільки він міг працювати протягом тривалого періоду часу, використовуючи тільки одну батарейку-таблетку. У порівнянні з іншими бездротовими стандартами швидке зростання популярності BLE була також завдяки наявності додатків для смартфонів, планшетів і мобільних комп'ютерів.



Рисунок 3.2 – Приклад – передача даних температури з датчика DHT11 на смартфон за допомогою модуля Arduino и nRF через BLE.

BLE використовує ту ж смугу 2,4 ГГц зі швидкістю передачі від 250 Кбіт/с до 2 Мбіт/с, яка дозволена в багатьох країнах і може застосовуватися в промислових і медичних додатках. Смуга частот починається з 2400 МГц до 2483,5 МГц і розділена на 40 каналів. Три з цих каналів відомі як «Advertising» і використовуються пристроями для відправки мовних пакетів з інформацією про них, щоб інші пристрої BLE могли підключатися. Ці канали були спочатку обрані в нижній верхній частині смуги і в середині смуги, щоб уникнути перешкод, які можуть створювати наводки для ряду каналів.

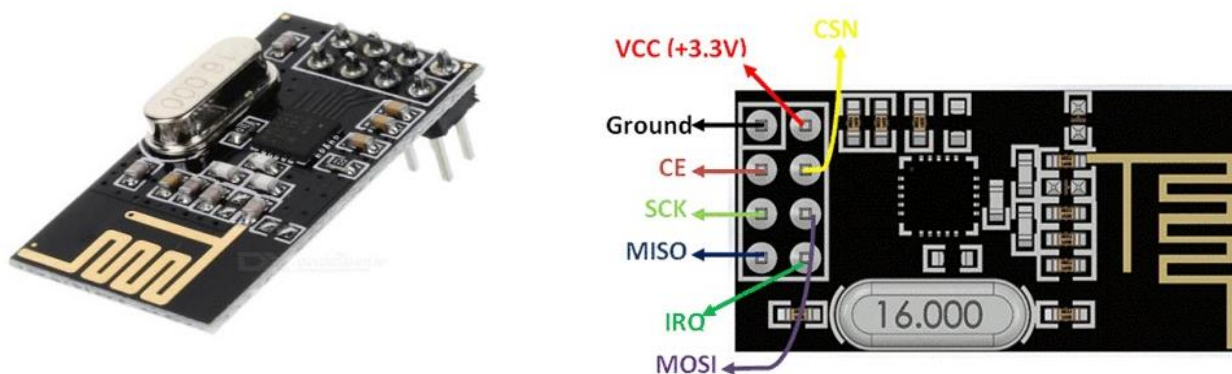


Рисунок 3.3 – Модуль nRF24L01 для передачі даних на смартфон

Для розробки та дослідження інформаційно-комунікаційної системи передачі медичних даних модуль nRF24L01 (рисунок 3.3) буде сполучатися з МК Arduino, а дані про температуру датчика DHT11 будуть відправлятися офіційному додатку Nordic BLE для Android.

Модулі nRF24L01 є приймально-передавальними модулями, тобто кожен модуль може відправляти та отримувати дані, але, оскільки вони напівдуплексні, вони можуть відправляти або отримувати дані одночасно. Мікросхема обмінюється даними з використанням протоколу SPI і, отже, може легко взаємодіяти з будь-якими МК. З Arduino стає набагато простіше, оскільки бібліотеки легкодоступні. Розпіновка стандартного модуля nRF24L01 показана на рисунку 3.3.

Модуль має робочу напругу від 1,9 В до 3,6 В (зазвичай 3,3 В) і споживає всього 12 мА при нормальній роботі, що робить його ефективним для живлення від батареї і, отже, може працювати навіть на елементах типу «таблетка». Незважаючи на те, що робоча напруга становить 3,3 В, більшість виводів допускають 5 В і, отже, можуть безпосередньо підключатися до 5 В МК, таких як Arduino.

Кожен модуль може зв'язуватися з 6 іншими модулями для передачі або отримання даних. Це робить його придатним для створення зіркових в додатках IoT. Крім того, вони мають широкий діапазон адрес 125 унікальних ідентифікаторів, тому в закритому просторі ми можемо використовувати 125 з цих модулів, які не заважатимуть один одному.

Схема підключення Arduino до модуля nRF24L01 і датчику DHT11 зображена на рисунку 3.4.

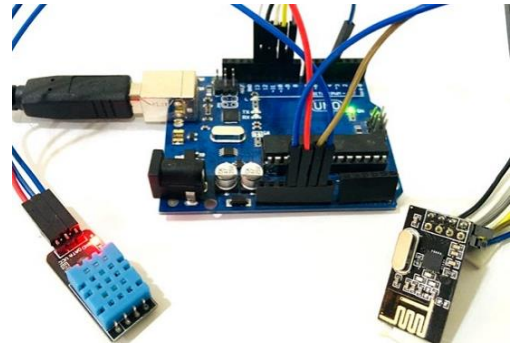
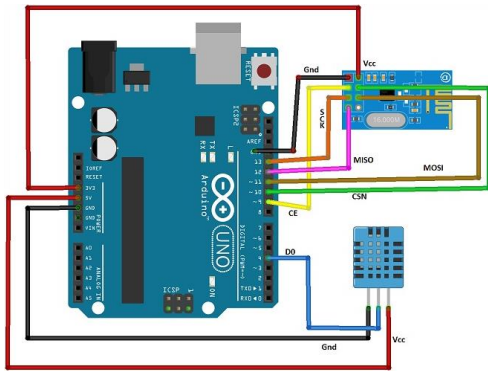


Рисунок 3.4 – Схема підключення Arduino до модуля nRF24L01 і датчика (на прикладі датчика DHT11)

NRF24L01 працює по SPI, тому в якості інтерфейсу будемо використовувати протокол SPI. Приклад коду наведено далі

```
include <SPI.h>
#include <RF24.h>
#include <BTLE.h>
#include <DHT.h> // Библиотека датчика температуры и влажности dht11
#define DHTPIN 4 // к какому цифровому контакту подключаем
#define DHTTYPE DHT11 // выбираем тип DHT как DHT11 или DHT22или другой датчик
DHT dht(DHTPIN, DHTTYPE);
RF24 radio(9, 10); // CE, CSN
BTLE btle(&radio);
void setup() {
  Serial.begin(9600);
  delay(1000);
  Serial.print("BLE and DHT Starting... ");
  Serial.println("Send Temperature Data over BTLE");
  dht.begin(); // инициализировать датчик DHT11
  btle.begin("CD Temp"); // Максимум 8 символов типа char
  Serial.println("Successfully Started");
}
void loop() {
  float temp = dht.readTemperature(); // считать данные о температуре
  if (isnan(h) || isnan(t)) { // Проверить, не удалось ли выполнить какое-либо считывание, и
    // завершить работу досрочно (повторить попытку)
    Serial.println(F("Failed to read from DHT sensor!"));
    return;
  }
  Serial.print(" Temperature: "); Serial.print(t); Serial.println("&#194;°C ");
  nrf_service_data buf;
  buf.service_uuid = NRF_TEMPERATURE_SERVICE_UUID;
  buf.value = BTLE::to_nRF_Float(temp);
  if (!btle.advertise(0x16, &buf, sizeof(buf))) {
    Serial.println("BTLE advertisement failed..!");
  }
  btle.hopChannel();
}
```

```
delay(2000);  
}
```

Після завантаження коду і спряження смартфона з модулем nRF отримуємо значення в додатку nRF Temp 2.0 для BLE для Android.

Єдиний недолік використання даного модуля. В телефонах з версією Android 10 програма nRF Temp 2.0 може працювати некоректно (зазвичай не знаходить при скануванні пристрій). Без проблем програма nRF connect працює на телефонах з версією Android 9 і старіше.

Тому, для вирішення поставлених завдань в передачі даних на сервер, в ланцюгу архітектури системи, по якій передаються дані про стан пацієнта, після Arduino було використано Raspberry PI.

3.3 Використання модуля Raspberry PI для передачі медичних даних за технологією Wi-Fi

Модель Raspberry Pi 4B, з габаритами 85,6 мм × 56,5 мм, побудована на основі системи на кристалі (SoC) BCM2711, в якій використаний чотирьох ядерний процесор 1.5GHz ARM Cortex-A72 з тактовою частотою 1,5 ГГц.

Цей мікропроцесор має підтримку стандартного ARM GIC (Generic Interrupt Controller), що істотно пришвидшує роботу систем віртуалізації.



Рисунок 3.6 – Модуль Raspberry PI для передачі медичних даних

Підтримка Wi-Fi лишилась на рівні стандарту 802.11ac, але на відміну від попередньої серії додана підтримка Bluetooth версії 5.0. Мережевий адаптер Gigabit Ethernet, на відміну від попередньої версії Raspberry Pi3, працює на повну пропускну здатність та не обмежений 300 Мбіт/с шлюзу USB

2.0. Raspberry Pi 4B підтримує технологію живлення через Ethernet (PoE) з встановленням додаткової плати розширення.

Замість одного порту HDMI нова серія має два порти мікро-HDMI. Здатна виводити сигнал в форматі HDMI 2.0 4K@60 Гц на один монітор, або 4K@30 Гц на два монітори, програвати відео в форматі 4K.

Живлення системи забезпечує порт USB Type-C.

3.4 Архітектура програмного забезпечення віддаленої системи моніторингу медичних даних

Інтеграція програмного забезпечення є одним з найважливіших аспектів системи віддаленого моніторингу стану здоров'я. Це мозок, який вчиться функціонувати відповідно до гнучкості користувача. Починаючи від використання мікроконтролера IDE до використання набору інструментів розробки Android, складається архітектура програмного забезпечення віддаленої системи моніторингу стану здоров'я. Зчитування даних здійснюється Arduino IDE відкритим кодом, який можливо написати в модулі. Після цього Raspberry Pi надсилає дані в хмарне сховище.

Використовуване хмарне сховище є Google Firebase, що є платформою для зберігання та передачі даних з мобільних та веб-додатків, розроблене Google. За допомогою Android Studio була розроблена програма проекту, яка може віддалено отримувати доступ до бази даних Google Firebase, але разом із шифруванням від користувача до користувача. Це захищає персональну базу даних пацієнта доступ до несанкціонованого персоналу.



Рисунок 3.7 – Архітектура блоків модулів віддаленої системи моніторингу

3.5 Об'єднання сенсорів та модулів в єдину систему

Після того, як були визначені окремі конструкції схем та здійснено калібрування модулів, необхідно підключити всі датчики до Arduino Uno, щоб забезпечити його функціонування як єдину систему.

Arduino Uno виявляє значення з датчиків і відповідно їх обробляє, тоді як під час передачі, Raspberry Pi, підключений до Arduino, отримує дані від Arduino. Через складну обробку та аналіз дані передаються в хмарне сховище, в подальшому з якого доступні для аналізу.

Розраховані значення кожного з датчиків зберігаються у хмарному сховищі, до якого згодом отримав доступ розроблений додаток Android для віддаленої візуалізації.

Підключення модуля Raspberry Pi до модуля Ардуіно. Підключаємо мікроконтролери Raspberry Pi і Ардуіно таким чином, щоб обидві плати могли спілкуватися один з одним (рисунок 3.8).

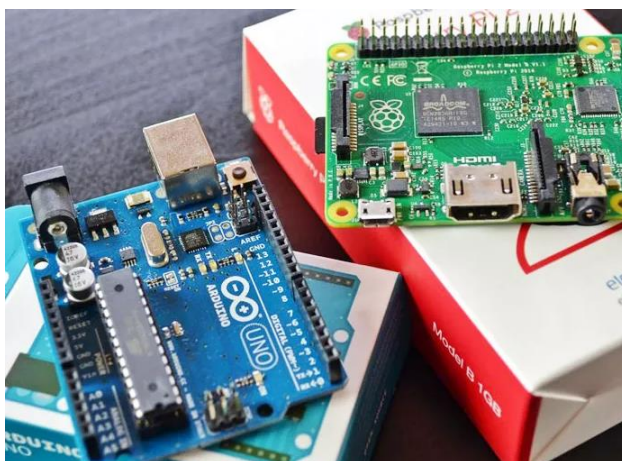


Рисунок 3.8 – Плати контролерів, які використовуються при експерименті

Вмикаємо Raspberry Pi і за допомогою мови Python прописуємо:

```
import serial
import RPi.GPIO as GPIO
import time

ser=serial.Serial("/dev/ttyACM0",9600) #change ACM number as found from ls /dev/tty/ACM*
ser.baudrate=9600
def blink(pin):

    GPIO.output(pin,GPIO.HIGH)
    time.sleep(1)
    GPIO.output(pin,GPIO.LOW)
    time.sleep(1)
    return

GPIO.setmode(GPIO.BOARD)
GPIO.setup(11, GPIO.OUT)
while True:

    read_ser=ser.readline()
    print(read_ser)
    if(read_ser=="Hello From Arduino!"):
        blink(11)
```

Відкриваємо Arduino IDE (це програмне середовище розробки, що використовує C++ і призначене для програмування всіх плат Arduino) і завантажуюмо наступний код в Arduino:

```
String data="обчислення частоти CCC!";

void setup() {
    // put your setup code here, to run once:
    Serial.begin(9600);
```

```

}

void loop() {
  // put your main code here, to run repeatedly:
  Serial.println(data); //data that is being Sent
  delay(200);
}

```

В інтерфейсі Raspberry Pi вмикаємо Serial і I2C в PiConfig.

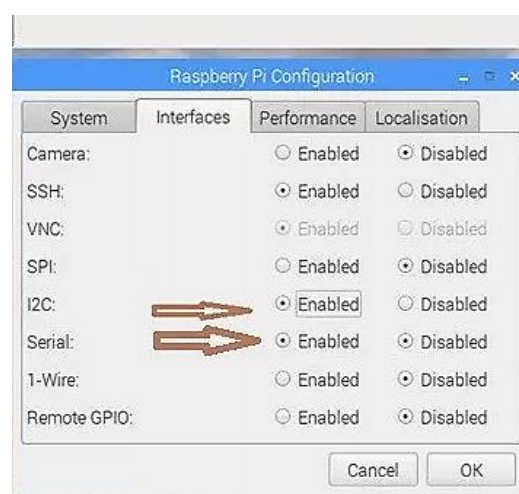


Рисунок 3.9 – Вікна інтерфейсу для налаштування з'єднання модулів Arduino і Raspberry Pi

Перезавантажуємо Raspberry Pi, відкриваємо термінал і виконуємо наступні команди:

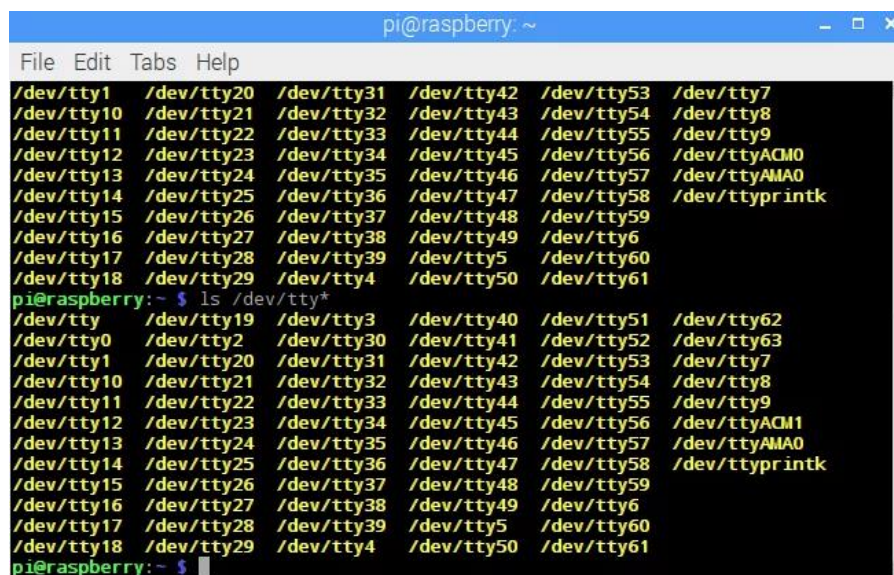
```
sudo apt-get install python-serial
```

```
sudo pip install pyserial
```

Підключаємо Ардуіно до Raspberry Pi. Виконуємо:

```
ls /dev/tty*
```

Знаходимо рядок типу `/dev/ttyACM0`, перевіряємо числом 0,1,2...



```
pi@raspberrypi: ~
File Edit Tabs Help
/dev/tty1 /dev/tty20 /dev/tty31 /dev/tty42 /dev/tty53 /dev/tty7
/dev/tty10 /dev/tty21 /dev/tty32 /dev/tty43 /dev/tty54 /dev/tty8
/dev/tty11 /dev/tty22 /dev/tty33 /dev/tty44 /dev/tty55 /dev/tty9
/dev/tty12 /dev/tty23 /dev/tty34 /dev/tty45 /dev/tty56 /dev/ttyACM0
/dev/tty13 /dev/tty24 /dev/tty35 /dev/tty46 /dev/tty57 /dev/ttyAMA0
/dev/tty14 /dev/tty25 /dev/tty36 /dev/tty47 /dev/tty58 /dev/ttyprintk
/dev/tty15 /dev/tty26 /dev/tty37 /dev/tty48 /dev/tty59
/dev/tty16 /dev/tty27 /dev/tty38 /dev/tty49 /dev/tty6
/dev/tty17 /dev/tty28 /dev/tty39 /dev/tty5 /dev/tty60
/dev/tty18 /dev/tty29 /dev/tty4 /dev/tty50 /dev/tty61
pi@raspberrypi: ~ $ ls /dev/tty*
/dev/tty /dev/tty19 /dev/tty3 /dev/tty40 /dev/tty51 /dev/tty62
/dev/tty0 /dev/tty2 /dev/tty30 /dev/tty41 /dev/tty52 /dev/tty63
/dev/tty1 /dev/tty20 /dev/tty31 /dev/tty42 /dev/tty53 /dev/tty7
/dev/tty10 /dev/tty21 /dev/tty32 /dev/tty43 /dev/tty54 /dev/tty8
/dev/tty11 /dev/tty22 /dev/tty33 /dev/tty44 /dev/tty55 /dev/tty9
/dev/tty12 /dev/tty23 /dev/tty34 /dev/tty45 /dev/tty56 /dev/ttyACM1
/dev/tty13 /dev/tty24 /dev/tty35 /dev/tty46 /dev/tty57 /dev/ttyAMA0
/dev/tty14 /dev/tty25 /dev/tty36 /dev/tty47 /dev/tty58 /dev/ttyprintk
/dev/tty15 /dev/tty26 /dev/tty37 /dev/tty48 /dev/tty59
/dev/tty16 /dev/tty27 /dev/tty38 /dev/tty49 /dev/tty6
/dev/tty17 /dev/tty28 /dev/tty39 /dev/tty5 /dev/tty60
/dev/tty18 /dev/tty29 /dev/tty4 /dev/tty50 /dev/tty61
pi@raspberrypi: ~ $
```

Рисунок 3.10 – Вікно програмного коду для налаштування з'єднання модулів Arduino і Raspberry Pi

Відкриваємо Python і замінюємо `ser = serial.Serial("dev/ttyACM1", 9600)` на знайдений номер ACM.

Raspberry Pi була запрограмована відповідно до наведених алгоритмів. Спочатку порти датчика ініціалізувались, потім вихідні дані були взяті з кожного з датчиків. Для вимірювання стандартних значень частоти серцевих скорочень, температури тіла та сатурації використовувались відповідні бібліотечні функції та математичні формули для розрахунку значень.

Таким чином, датчики підключено до Arduino, а значення передаємо і отримуємо від Raspberry Pi. Тобто, можна відокремити обчислювальні завдання (виконуються Raspberry Pi) і керуючі завдання (виконуються Ардуіно).

3.6 Передача даних на сервер

Коли мікросхема завершує зчитування, вона продовжує надсилати дані на сервер. Зв'язок здійснюється за протоколом Web-Sockets. Цей API забезпечує двонаправлений зв'язок між клієнтом та сервером через TCP-з'єднання (Chopra, 2015), мікросхема здійснює HTTP та TCP-з'єднання спочатку, щоб можна було реалізувати протоколи Web-Socket. Для встановлення з'єднання спочатку запит робиться в HTTP, в ньому клієнт просить сервер оновити з'єднання. Його перевага полягає в безперервному зв'язку з сервером, що дозволяє передавати дані в режимі реального часу, з невеликою затримкою.

SQLite – це дуже проста у використанні база даних. З командного рядка виконуємо наступне:

```
sqlite3 pulseox.db "CREATE TABLE pulseox(stampdate text, stamptime text, spo2 text, bpm text, id integer primary key)"
```

Це створить файл, який називається pulseox.db, у поточному каталозі, який містить єдину таблицю, як визначено вище.

Щоб перевірити базу даних та стовпець id, використано таку команду insert / select:

```
sqlite3 pulseoxdb "INSERT into pulseox(stampdate, stamptime, spo2, bpm) values('12/30/14','08:00:00','SPO2=100%','BPM=100');SELECT *from pulseox"
12/30/14|08:00:00|SPO2=100%|BPM=100|1
```

Тепер, коли база даних налаштована, можна перейти до синтаксичного аналізу даних у режимі реального часу та збереження їх у таблицю.

3.6.1 Розміщення даних у хмарних базах даних. Google Firebase – це хмарна платформа, як зазначалось вище, що дозволяє створювати бази даних у реальному часі. Тобто, наша мета передавати дані з Arduino, що підключений до Raspberry Pi, для надсилання даних до бази даних у реальному часі.

Зазначаємо наступну команду в терміналі, щоб встановити пакет Python для Google Firebase «sudo pip» запити на встановлення «python-firebase».

```
cd ~/Documents/Codebase
nano firebase_dht.py
```

Відредагуємо наступний рядок (рядок 9 у наведеному нижче коді) і додамо URL-адресу Firebase

```
https://OUR_FIREBASE_URL.firebaseio.com/
```

Для запуску коду:

```
python firebase_dht.py
import RPi.GPIO as GPIO
from time import sleep
from firebase import firebase
import Adafruit_DHT

sensor = Adafruit_DHT.DHT11
pin = 4

firebase = firebase.FirebaseApplication('https://YOUR_FIREBASE_URL.firebaseio.com/', None)
firebase.put("/", "/temp", "0.00")
firebase.put("/", "/humidity", "0.00")

while True:
    humidity, temperature = Adafruit_DHT.read_retry(sensor, pin)
    if humidity is not None and temperature is not None:
        str_temp = ' {0:0.2f} *C '.format(temperature)
        str_hum = ' {0:0.2f} %'.format(humidity)
        print('Temp={0:0.1f}*C Humidity={1:0.1f}%'.format(temperature, humidity))
        firebase.put("/", "/temp", str_temp)
        firebase.put("/", "/humidity", str_hum)
    else:
        print('Failed to get reading. Try again!')
        sleep(5)
```

3.6.2 Скрипт для збору та вставки даних. Запуск сценарію оболонки як фоновий процес, який відкриває послідовний пристрій і постійно перевіряє наявність даних. Коли він читає рядок, він «рубляє» його (з необроблених даних один пробіл є роздільником) і вставляє рядок в базу даних. Буде

використовувати PHP як мову сценаріїв та PDO як розширення API для підключення до бази даних.

```
$ser = fopen("/dev/ttyUSB0","r");

$dbh=new PDO('sqlite:/var/www/pulseox.db');
$query=$dbh->prepare("INSERT into pulseox (stampdate, stamptime, spo2, bpm) VALUES (
:param0, :param1, :param2, :param3);");

while (!feof($ser)) {
    $buffer = fgets($ser);
    $din = explode(" ", $buffer);
    $query->bindParam(':param0', $din[0]); # stampdate - 12/30/14
    $query->bindParam(':param1', $din[1]); # stamptime - 08:00:00
    $query->bindParam(':param2', $din[3]); # spo2 - SPO2=100%
    $query->bindParam(':param3', $din[4]); # bpm - BPM=123
    $query->execute();
}
```

Для стислості було видалено виявлення помилок із наведеного вище коду, наприклад, перевірку, чи не вдається відкрити послідовний пристрій, чи перевірку різних помилок бази даних.

Коли кожен рядок зчитується, команда "explode" вірізає рядок у кожен фрагмент даних. Потім кожен фрагмент даних прив'язується до правильного розташування в операторі SQL бази даних перед виконанням SQL [33].

3.6.3 Затримка передачі даних. У реальній передачі відбувається:

- втрата пакетів, а потім повторна передача
- затримка по шляху передачі.

Емпіричне правило для ланцюгів від 1 до 10 Мегабіт в секунду полягає у зменшенні пропускної здатності на

- Від 10 до 15% для внутрішньоконтинентальної передачі
- Від 20 до 25% для основних економік північної півкулі (Великобританія, Європа, США),

3.6.4 Шифрування. Додавання шифрування (IPSec або SSL) ще більше збільшить кількість переданих даних. Фактичний вплив буде сильно залежати від середнього розміру пакета. IPSec зазвичай додає до заголовка 40 байт, що

менше впливає на велику передачу даних з MTU 1350 байт, ніж для інтерактивної сесії, обмін пакетами з MTU 400 байт.

Часто забувають про затримку шифрування та дешифрування, що робить передачу більш прихованою.

3.6.5 Розрахунок експериментальної передачі даних з медичних датчиків. Якщо ми передаємо ці дані (без шифрування) зі швидкістю 10 мегабіт в секунду:

$224\,000\,000\,000 \text{ bits} / 10\,000\,000 \text{ bits per second} = 22400 \text{ seconds} = 373 \text{ minutes.}$

І потім, згідно відомих значень:

Додати 20% для передачі даних з Великобританії в США.

Додати 10% для шифрування в IPsec.

Отримуємо:

$373 \text{ minutes} * 20\% * 10\% = 492 \text{ minutes.}$

Довжина захищених даних. Необхідно оцінити довжину даних, які є предметом захисту, тобто довжину даних, які надходять у алгоритм автентифікації або шифрування. Рисунок 3.11 ілюструє, які частини пакета захищені протоколом AH (a), ESP (b) або тим і іншим (c), та обчислює довжину певних заголовків [31]. У таблиці (c) довжина захищених полів підсумована для всіх можливих комбінацій AH та ESP. Слід зазначити, що автентифікація AH, на відміну від ESP, захищає також новий IP-заголовок, за винятком так званих змінних полів, тобто полів, які шляхом маршрутизації через мережу змінні. Незмінні поля в IP заголовки мають довжину 12 байт.

Таблиця 3.1

Довжина захищених даних

Ауентифікація/Шифрування	Довжина захищених даних (крім корисного навантаження та ESP)
--------------------------	---

AH / -	78 bytes / -
- / ESP	- / 40 bytes
ESP / ESP	56 bytes / 40 bytes
AH / ESP	92 bytes / 40 bytes

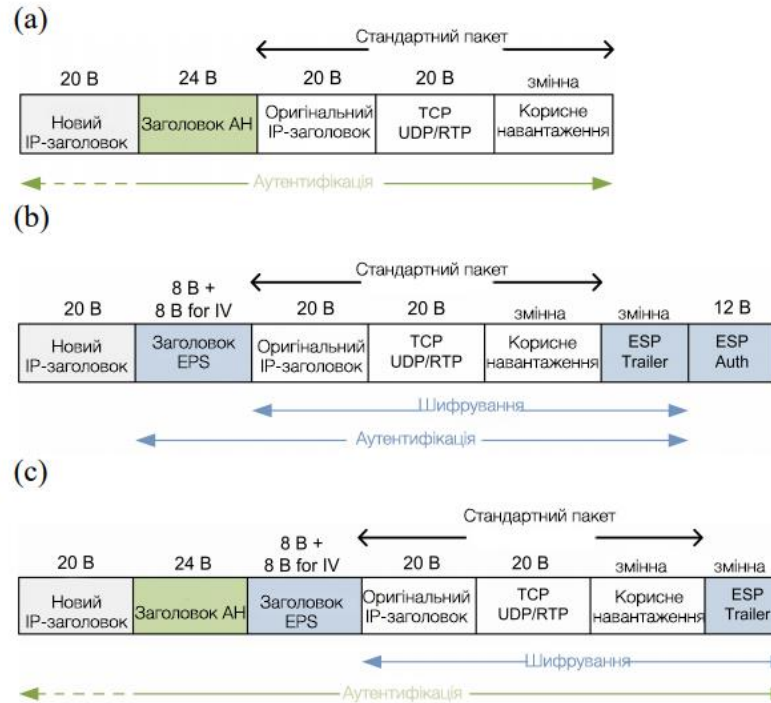


Рисунок 3.11 – Довжина даних, захищених протоколом (a) AH, (b) ESP, (c) обома

Якщо ми виразимо це математично, загальна кількість зашифрованих даних, включаючи заповнення та корисне навантаження, буде (згідно [31]):

$$N_{alg} = \left\lceil \frac{N'_{alg} * b + 2}{4} \right\rceil * 4 \quad (3.1)$$

де N_{alg} – довжина зашифрованих даних без заповнення (тобто корисне навантаження плюс заголовки),

b – розмір блоку.

Значення "+2" у чисельнику обумовлене полем. Хоча AH не мають спеціального поля для заповнення, алгоритми автентифікації HMAC-SHA-1 та HMAC-MD5 працюють також із блоками, в даному випадку 64 байтовими [33], [34]. Таким чином, довжина автентифікованих даних буде

$$N_{alg} = \left\lceil \frac{N'_{alg}}{64} \right\rceil * 64 \quad (3.2)$$

де N_{alg} – довжина автентифікованих даних без заповнення (тобто корисне навантаження плюс заголовки).

Наприклад, у випадку 20-байтового корисного навантаження лише для аутентифікації АН буде

$$N_{alg} = \left\lceil \frac{20=78}{64} \right\rceil \times 64 = 2 \times 64 = 128 \text{ байти}, \quad (3.3)$$

для 1390 байт корисного навантаження

$$N_{alg} = \left\lceil \frac{1390=78}{64} \right\rceil \times 64 = 23 \times 64 = 1472 \text{ байта}. \quad (3.4)$$

3.7 Захист та конфіденційність при передачі медичних даних

Аутентифікація в службах OAuth2. Для безпечного доступу до Інтернет-сервісу користувачам необхідно пройти автентифікацію до служби – вони повинні надати підтвердження своєї особи. Для програми, яка отримує доступ до сторонньої служби, проблема безпеки є ще більш складною. Щоб отримати доступ до послуги, користувач повинен мати не тільки автентифікацію, але й дозвіл діяти від імені користувача.

Стандартним способом роботи з аутентифікацією для сторонніх служб є протокол OAuth2. OAuth2 надає єдине значення, яке називається токеном аутентифікації, яке представляє як ідентичність користувача, так і дозвіл програми діяти від імені користувача. В роботі реалізовуємо підключення до сервера Google, який підтримує OAuth2. Хоча служби Google використовуються як приклад, продемонстровані методи працюють на будь-якій службі, яка правильно підтримує протокол OAuth2.

Використання OAuth2:

- Отримання дозволу користувача на доступ до онлайнової служби за допомогою його облікового запису.
- Автентифікація до Інтернет-сервісу від імені користувача.
- Обробка помилок автентифікації.

Щоб почати використовувати OAuth2, необхідно знати кілька речей про API, до якого необхідно отримати доступ:

- URL-адреса служби, до якої необхідно отримати доступ.
- Сфера автентифікації, яка є рядком, що визначає конкретний тип доступу, про який вимагає ваша програма.

Наприклад, область автентифікації доступу лише для читання до Google Tasks – це «Перегляд завдань», а область автентифікації доступу для читання та запису до Google Tasks – «Керування завданнями».

- Ідентифікатор клієнта та секрет клієнта – це рядки, що ідентифікують додаток до служби. Необхідно отримати ці рядки безпосередньо у власника служби. Google має систему самообслуговування для отримання ідентифікаторів клієнта та паролей. У статті [34] «Авторизація та використання REST API» пояснюється, як використовувати цю систему для отримання цих значень для використання з API Google Tasks

Запит інтернет-дозволу. Для додатків, націлених на Android 6.0 (рівень API 23) і вище, сам метод `getAuthToken` не вимагає жодних дозволів. Однак, щоб виконувати операції з маркером, потрібно додати дозвіл на INTERNET до файлу-маніфесту, як показано в наступному фрагменті коду:

```
<manifest ... >
    <uses-permission android:name="android.permission.INTERNET" />
    ...
</manifest>
```

Запит маркера аутентифікації. Щоб отримати маркер, потрібно викликати `AccountManager.getAuthToken`. Наступний фрагмент показує, як працювати з низкою зворотних викликів, щоб отримати маркер:

```
AccountManager am = AccountManager.get(this);
Bundle options = new Bundle();

am.getAuthToken(
    myAccount_,           // Account retrieved using getAccountsByType()
    "Manage your tasks",   // Auth scope
    options,              // Authenticator-specific options
    this,                 // Your activity
```

```
new OnTokenAcquired(),      // Callback called when a token is successfully acquired
new Handler(new OnError())); // Callback called if an error occurs
```

У цьому прикладі `OnTokenAcquired` – це клас, який реалізує `AccountManagerCallback`. Виклики `AccountManager.run()` на `OnTokenAcquired` з `AccountManagerFuture`. Якщо виклик вдавсь, маркер знаходиться всередині набору.

Отримати маркер із набору можна наступним чином:

```
private class OnTokenAcquired implements AccountManagerCallback<Bundle> {
    @Override
    public void run(AccountManagerFuture<Bundle> result) {
        // Get the result of the operation from the AccountManagerFuture.
        Bundle bundle = result.getResult();

        // The token is a named value in the bundle. The name of the value
        // is stored in the constant AccountManager.KEY_AUTH_TOKEN.
        String token = bundle.getString(AccountManager.KEY_AUTH_TOKEN);
        ...
    }
}
```

Якщо все вірно, `Bundle` містить дійсний маркер у ключі `KEY_AUTH_TOKEN`.

Програми можуть тривіально розглянути перші два випадки, як правило, просто показуючи користувачеві повідомлення про помилку. Якщо мережа не працює або користувач вирішив не надавати доступ, програма з цим мало що може зробити. Останні два випадки є дещо складнішими, оскільки, програми, що працюють належним чином, автоматично обробляють ці збої.

Третій випадок помилки, маючи недостатньо облікових даних, передається через Комплект, який ми отримуємо у своєму `AccountManagerCallback` (`OnTokenAcquired` з попереднього прикладу). Якщо Пакет містить дозвіл у ключі `KEY_INTENT`, тоді аутентифікатор повідомляє нам, що йому потрібно взаємодіяти безпосередньо з користувачем, перш ніж він зможе дати нам дійсний маркер.

Причин для того, щоб аутентифікатор повернув запит може бути багато. Можливо, це перший раз, коли користувач увійшов до цього облікового запису. Можливо, термін дії облікового запису користувача закінчився, і їм потрібно ввійти ще раз, або, можливо, їхні збережені облікові дані неправильні.

Сам модуль аутенфікації буде розроблено у повній мірі в подальшому.

Підключення до онлайн-сервісу. У наведеному нижче прикладі показано, як можливо підключитися до сервера Google. Google використовує галузевий стандартний протокол OAuth2 для аутентифікації запитів.

API Google вимагає, щоб було надавано чотири значення з кожним запитом: ключ API, ідентифікатор клієнта, секрет клієнта та ключ аутентифікації. Перші три надходять із веб-сайту консолі Google API. Останнє – це значення рядка, яке отримане, викликавши `AccountManager.getAuthToken()`. Ми передаємо їх на сервер Google як частину запиту HTTP.

```
URL url = new URL("https://www.googleapis.com/tasks/v1/users/@me/lists?key=" + your_api_key);
URLConnection conn = (URLConnection) url.openConnection();
conn.addRequestProperty("client_id", your_client_id);
conn.addRequestProperty("client_secret", your_client_secret);
conn.setRequestProperty("Authorization", "OAuth " + token);
```

Якщо запит повертає код помилки HTTP 401, маркер відхилено. Як зазначалося, найпоширенішою причиною цього є те, що термін дії маркера закінчився. Виправлення просто: зателефонувати

```
AccountManager.invalidateAuthToken ()
```

Оскільки токени, термін дії яких минув, є настільки поширеним явищем, і виправити їх настільки просто, багато програм просто припускають, що термін дії маркера закінчився, ще до того, як звернутись до нього [35]. Цей модуль також в розробці, але перше підключення з мобільного додатку, що представлений нижче, отримано.

3.8 Додаток IoT системи медичного призначення

Нам потрібно відобразити останній зареєстрований рівень кисню та частоту серцевих скорочень на веб-сторінці. Спочатку необхідно розмістити частину PHP-коду на просту веб-сторінку для отримання даних.

На наступному кроці:

```
$dbh = new PDO('sqlite:/var/www/pulseox.db');
$query=$dbh->prepare("SELECT stampdate, stamptime, spo2, bpm from pulseox order by id desc
limit 1");
$query->execute();
$result=$query->fetch();

echo "$result[0] $result[1] $result[2] $result[3]";
```

Поки що ми отримуємо лише такий результат:

```
01/03/15 07:33:18 SPO2=094% BPM=090
```

Також потрібно показати на веб-сторінці середній рівень кисню та частоту серцевих скорочень за останню годину. Наступний код – це те, як було отримано ці 2 значення:

```
$query=$dbh->prepare("SELECT round(avg(substr(bpm,5,3)),1), round(avg(substr(spo2,6,3)),1)
from pulseox where bpm != 'BPM=---' and spo2 != 'SPO2=---%' and id > ((select max(id) from
pulseox) - 3600)");
$query->execute();
$result=$query->fetch();

$avg_bpm = $result[0];
$avg_spo2 = $result[1];
```

Аналогічно повторюємо код для температури та частоти серцевих скорочень.

Візуалізація додатку. Оглянувши різні бібліотеки, нам для цього потрібно використовувати візуалізацію Google. Нижче наведено код, який перетворює результати php у формат, зрозумілий Google Visualization. Цей код також встановлює текстову мітку для кожного датчика.

```
var bpm_data = google.visualization.arrayToDataTable([[ 'Label', 'Value'],[ 'BPM', <?php echo
$chart_bpm_data; ?>]]);
```

```

var spo2_data = google.visualization.arrayToDataTable([[ 'Label', 'Value'],[ 'SPO2', <?php echo $chart_spo2_data; ?>]]);
var avg_bpm_data = google.visualization.arrayToDataTable([[ 'Label', 'Value'],[ 'AVG BPM', <?php echo $chart_avg_bpm_data; ?>]]);
var avg_spo2_data = google.visualization.arrayToDataTable([[ 'Label', 'Value'],[ 'AVG SPO2', <?php echo $chart_avg_spo2_data; ?>]]);

```

Інтерфейс додатку контролю параметрів з датчиків, які описані та розроблені в роботі представлено на рисунку 3.11.

Однак будь-що в хмарі має ризик втрати конфіденційності. Щоб запобігти цьому, додаток шифрується обліковими даними для входу в цілях безпеки.

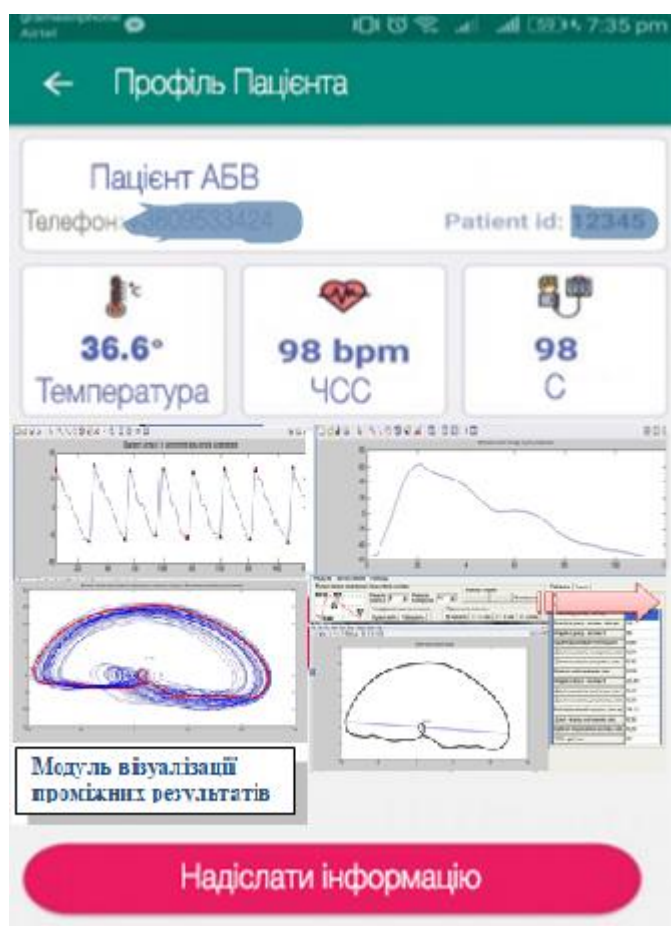


Рисунок 3.11 – Інтерфейс додатку контролю параметрів

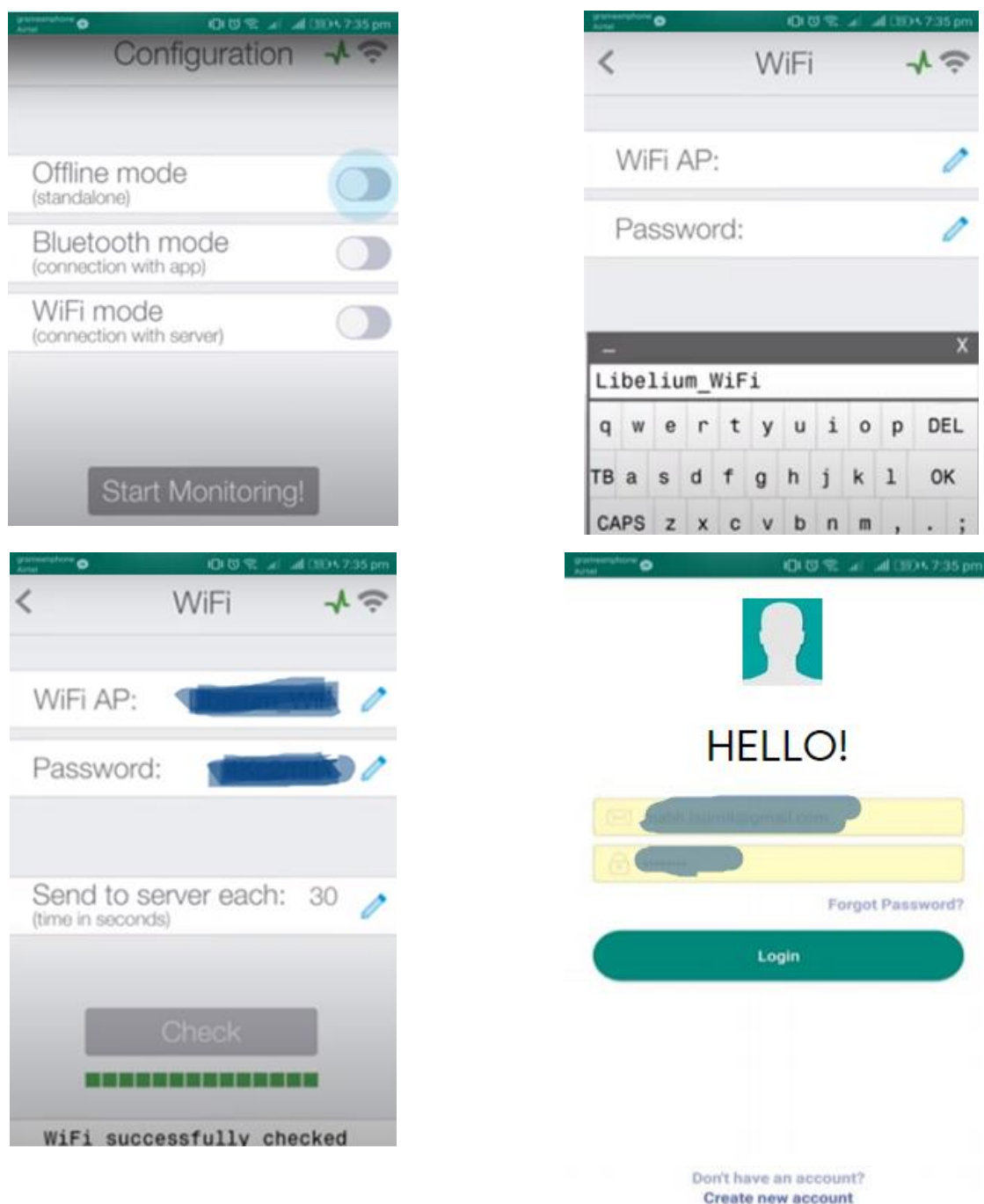


Рисунок 3.12 – Додаток із запитом на реєстраційні дані користувача

Висновки до розділу 3

Проведено дослідження по передачі медичних даних з давачів (сенсорів) на телефон Android з використанням Arduino і модуля NRF24L01 через Bluetooth (BLE). Але з врахуванням недоліків, з'ясованих в ході роботи, запропонована методика передачі даних на віртуальний сервер та на мобільний додаток за допомогою модуля Raspberry PI за технологією Wi-Fi.

ВИСНОВКИ

Дослідники в усьому світі почали досліджувати різні технологічні рішення для покращення надання медичної допомоги таким чином, щоб доповнювати існуючі послуги, мобілізуючи потенціал IoT.

У кваліфікаційній роботі розглядаються різноманітні аспекти технологій охорони здоров'я на основі IoT та представлені різні архітектурні мережі та платформи охорони здоров'я, які підтримують доступ до хребта IoT та полегшують передачу та отримання медичних даних.

Для того, щоб краще зрозуміти безпеку охорони здоров'я в Інтернеті, розглядаються різні вимоги та проблеми безпеки та розкриває різні проблеми дослідження в цій галузі, щоб запропонувати модель, яка може зменшити супутні ризики для безпеки. Обговорення важливих питань, таких як стандартизація, тип мережі, бізнес-моделі, якість обслуговування та захист даних про здоров'я, сприяють створенню основи для подальших досліджень медичних послуг на базі IoT.

Зроблено огляд політики та правил електронного здоров'я та IoT на користь різних зацікавлених сторін, зацікавлених в оцінці медичних технологій на основі IoT.

В роботі запропоновано структуру апаратно-програмного комплексу моніторингу життєдіяльності особи, що дозволяє пацієнтам самостійно відслідковувати життєвоважливі показники свого здоров'я, а лікуючим лікарям – контролювати в реальному часі стан здоров'я своїх пацієнтів у режимі віддаленого доступу та проводити аналіз результатів спостереження за допомогою спеціальних мобільних програм-застосунків з метою своєчасного та ефективного корегування лікувальних та профілактичних заходів.

ВИСНОВКИ

1. W. Zhao, W. Chaowei, and Y. Nakahira, “Medical application on Internet of Things,” in Proc. IET Int. Conf. Commun. Technol. Appl. (ICCTA), Oct. 2011, pp. 660–665.

2. N. Yang, X. Zhao, and H. Zhang, “A non-contact health monitoring model based on the Internet of Things,” in Proc. 8th Int. Conf. Natural Comput. (ICNC), May 2012, pp. 506–510.

3. S. Imadali, A. Karanasiou, A. Petrescu, I. Sifniadis, V. Veque, and P. Angelidis, “eHealth service support in IPv6 vehicular networks,” in Proc. IEEE Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob), Oct. 2012, pp. 579–585.

4. R. S. H. Istepanian, “The potential of Internet of Things (IoT) for assisted living applications,” in Proc. IET Seminar Assist. Living, Apr. 2011, pp. 1–40. 5. G. Yang et al., “A health-IoT platform based on the integration of intel-ligent packaging, unobtrusive bio-sensor, and intelligent medicine box,” IEEE Trans. Ind. Informat., vol. 10, no. 4, pp. 2180–2191, Nov. 2014.

5. A. J. Jara, M. A. Zamora, and A. F. Skarmeta, “Knowledge acquisition and management architecture for mobile and personal health environments based on the Internet of Things,” in Proc. IEEE Int. Conf. Trust, Security Privacy Comput. Commun. (TrustCom), Jun. 2012, pp. 1811–1818.

6. B. Xu, L. D. Xu, H. Cai, C. Xie, J. Hu, and F. Bu, “Ubiquitous data accessing method in IoT-based information system for emergency medical services,” IEEE Trans. Ind. Informat., vol. 10, no. 2, pp. 1578–1586, May 2014.

7. C. Doukas and I. Maglogiannis, “Bringing IoT and cloud computing towards pervasive healthcare,” in Proc. Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput. (IMIS), Jul. 2012, pp. 922–926.

8. S. Imadali, A. Karanasiou, A. Petrescu, I. Sifniadis, V. Veque, and P. Angelidis, “eHealth service support in IPv6 vehicular networks,” in Proc. IEEE Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob), Oct. 2012, pp. 579–585.

9. A. J. Jara, M. A. Zamora, and A. F. Skarmeta, "Knowledge acquisition and management architecture for mobile and personal health environments based on the Internet of Things," in Proc. IEEE Int. Conf. Trust, Security Privacy Comput. Commun. (TrustCom), Jun. 2012, pp. 1811–1818.
10. C. Doukas and I. Maglogiannis, "Bringing IoT and cloud computing towards pervasive healthcare," in Proc. Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput. (IMIS), Jul. 2012, pp. 922–926.
11. M. S. Shahamabadi, B. B. M. Ali, P. Varahram, and A. J. Jara, "A network mobility solution based on 6LoWPAN hospital wireless sensor network (NEMO-HWSN)," in Proc. 7th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput. (IMIS), Jul. 2013, pp. 433–438.
12. A. J. Jara, A. F. Alcolea, M. A. Zamora, A. F. J. Skarmeta, and M. Alsaedy, "Drugs interaction checker based on IoT," in Proc. Internet Things (IOT), Nov./Dec. 2010, pp. 1–8.
13. R. S. H. Istepanian, S. Hu, N. Y. Philip, and A. Sungoor, "The potential of Internet of m-health Things 'm-IoT' for non-invasive glucose level sensing," in Proc. IEEE Annu. Int. Conf. Eng. Med. Biol. Soc. (EMBC), Aug./Sep. 2011, pp. 5264–5266.
14. N. Bui, N. Bressan, and M. Zorzi, "Interconnection of body area networks to a communications infrastructure: An architectural study," in Proc. 18th Eur. Wireless Conf. Eur. Wireless, Apr. 2012, pp. 1–8.
15. P. Lopez, D. Fernandez, A. J. Jara, and A. F. Skarmeta, "Survey of Internet of Things technologies for clinical environments," in Proc. 27th Int. Conf. Adv. Inf. Netw. Appl. Workshops (WAINA), Mar. 2013, pp. 1349–1354.
16. A. J. Jara, M. A. Zamora-Izquierdo, and A. F. Skarmeta, "Interconnection framework for mHealth and remote monitoring based on the Internet of Things," IEEE J. Sel. Areas Commun., vol. 31, no. 9, pp. 47–65, Sep. 2013.
17. R. Tabish et al., "A 3G/WiFi-enabled 6LoWPAN-based U-healthcare system for ubiquitous real-time monitoring and data logging," in Proc. Middle East Conf. Biomed. Eng. (MECBME), Feb. 2014, pp. 277–280. 45

18. M.F.A. Rasid et al., “Embedded gateway services for Internet of Things applications in ubiquitous healthcare,” in Proc. 2nd Int. Conf. Inf. Commun. Technol. (ICoICT), May 2014, pp. 145–148.
19. A. J. Jara, M. A. Zamora, and A. F. Skarmeta, “Knowledge acquisition and management architecture for mobile and personal health environments based on the Internet of Things,” in Proc. IEEE Int.Conf. Trust, Security Privacy Comput. Commun. (TrustCom), Jun. 2012, pp. 1811–1818.
20. B. Xu, L. D. Xu, H. Cai, C. Xie, J. Hu, and F. Bu, “Ubiquitous data accessing method in IoT-based information system for emergency medical services,” IEEE Trans. Ind. Informat., vol. 10, no. 2, pp. 1578–1586, May 2014.
21. C. Doukas and I. Maglogiannis, “Bringing IoT and cloud computing towards pervasive healthcare,” in Proc. Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput. (IMIS), Jul. 2012, pp. 922–926.
22. G. Zhang, C. Li, Y. Zhang, C. Xing, and J. Yang, “SemanMedical: A kind of semantic medical monitoring system model based on the IoT sensors,” in Proc. IEEE Int. Conf. eHealth Netw., Appl. Services (Healthcom), Oct. 2012, pp. 238–243.
23. X. M. Zhang and N. Zhang, “An open, secure and flexible platform based on Internet of Things and cloud computing for ambient aiding living and telemedicine,” in Proc. Int. Conf. Comput. Manage. (CAMAN), May 2011, pp. 1–4.
24. M. S. Shahamabadi, B. B. M. Ali, P. Varahram, and A. J. Jara, “A network mobility solution based on 6LoWPAN hospital wireless sensor network (NEMO-HWSN),” in Proc. 7th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput. (IMIS), Jul. 2013, pp. 433–438.
25. A. J. Jara, A. F. Alcolea, M. A. Zamora, A. F. J. Skarmeta, and M. Alsaedy, “Drugs interaction checker based on IoT,” in Proc. Internet Things (IOT), Nov./Dec. 2010, pp. 1–8.
26. R. S. H. Istepanian, S. Hu, N. Y. Philip, and A. Sungeor, “The potential of Internet of m-health Things ‘m-IoT’ for non-invasive glucose level sensing,” in Proc. IEEE Annu. Int. Conf. Eng. Med. Biol. Soc. (EMBC), Aug./Sep. 2011, pp. 5264–5266.

27. N. Bui, N. Bressan, and M. Zorzi, “Interconnection of body area networks to a communications infrastructure: An architectural study,” in Proc. 18th Eur. Wireless Conf. Eur. Wireless, Apr. 2012, pp. 1–8.
28. P. Lopez, D. Fernandez, A. J. Jara, and A. F. Skarmeta, “Survey of Internet of Things technologies for clinical environments,” in Proc. 27th Int. Conf. Adv. Inf. Netw. Appl. Workshops (WAINA), Mar. 2013, pp. 1349–1354.
29. A. J. Jara, M. A. Zamora-Izquierdo, and A. F. Skarmeta, “Interconnection framework for mHealth and remote monitoring based on the Internet of Things,” IEEE J. Sel. Areas Commun., vol. 31, no. 9, pp. 47–65, Sep. 2013.
30. R. Tabish et al., “A 3G/WiFi-enabled 6LoWPAN-based U-healthcare system for ubiquitous real-time monitoring and data logging,” in Proc. Middle East Conf. Biomed. Eng. (MECBME), Feb. 2014, pp. 277–280.
31. M. F. A. Rasid et al., “Embedded gateway services for Internet of Things applications in ubiquitous healthcare,” in Proc. 2nd Int. Conf. Inf. Commun. Technol. (ICoICT), May 2014, pp. 145–148.
32. Z. Shelby and C. Bormann, 6LoWPAN: The Wireless Embedded Internet, 1st ed. London, U.K.: Wiley, 2009.
33. L. You, C. Liu, and S. Tong, “Community medical network (CMN): Architecture and implementation,” in Proc. Global Mobile Congr. (GMC), Oct. 2011, pp. 1–6.
34. P. Swiatek and A. Rucinski, “IoT as a service system for eHealth,” in Proc. IEEE Int. Conf. eHealth Netw., Appl. Services (Healthcom), Oct. 2013, pp. 81–84.
35. M. Diaz, G. Juan, O. Lucas, and A. Ryuga, “Big data on the Internet of Things: An example for the e-health,” in Proc. Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput. (IMIS), Jul. 2012, pp. 898–900.