Хмельницький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

Галузь знань 12 – Інформаційні технології

Спеціальність 123 –Комп'ютерна інженерія

на тему:
«Метод та підсистема ідентифікації користувача кіберфізичної системи «Розумний будинок»»

КвРКІ. 170154.21.01.26 ПЗ

Виконав: студент 2 курсу, група КІ2м-21-1 С.І. Талапчук
Підпис Ініціали, прізвище

Керівник доктор техн. наук, професор Т.О.Говорущенко
Науковий ступінь, вчене звання Підпис Ініціали, прізвище

До захисту допускаю:
Зав. кафедри КІІС, д.т.н, проф.
Т.О. Говорущенко
10 05 2023 р.

Хмельницький, 2023

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

Освітній рівень МАГІСТР

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 123 КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

Освітня програма ОСВІТНЬО-НАУКОВА ПРОГРАМА «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ ТА ПРОГРАМУВАННЯ»

ЗАТВЕРДЖУЮ

Зав. кафедри Т.О.Говорущенко

"01" 09 2022 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА

Талапчук Сніжані Іванівні

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Метод та підсистема ідентифікації користувача кіберфізичної системи „Розумний будинок"

Керівник проекту (роботи) Говорущенко Т.О, д.т.н, професор

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 09.01.2023 р. № 1

2. Строк подання студентом проекту (роботи) на кафедру 01.05.2023 р.

3. Вихідні дані до проекту (роботи) Завдання на дипломне проектування

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

Аналіз відомих методів та рішень для ідентифікації користувача кіберфізичної системи «Розумний будинок»

Моделювання процесу ідентифікації користувача кіберфізичної системи «Розумний будинок»

Метод ідентифікації користувача кіберфізичної системи «Розумний будинок»

Підсистема ідентифікації користувача кіберфізичної системи «Розумний будинок»

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

6. Консультанти розділів кваліфікаційної роботи магістра

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Лисенко С.М, професор кафедри КІІС		
Антиплагіат	Нічепорук А.О, доцент кафедри КІІС		

7. Дата видачі завдання «_06_»_____09_____2022р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи магістра	Термін виконання етапів проекту (роботи)	Примітка
1	Вибір напряму дослідження та узгодження тематики КвРМ з керівником	05.09.2022	виконано
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	05.10.2022	виконано
3	Робота над розділом 1 – аналіз відомих моделей, методів за темою; постановка задачі	05.11.2022	виконано
4	Робота над розділом 2 – розробка моделей для вирішення поставленої задачі	05.12.2022	виконано
5	Робота над науковою статтею	05.01.2023	виконано
6	Робота над розділом 3 – розробка методів для вирішення поставленої задачі	15.02.2022	виконано
7	Робота над розділом 4 – проектування та розробка ПЗ для вирішення поставленої задачі, експериментальна частина	05.04.2023	виконано
8	Оформлення пояснювальної записки згідно вимог	15.04.2023	виконано
9	Попередній захист ДРМ	18.04.2023	виконано
10	Захист ДРМ на засіданні ЕК	До 10.05.2023	

Студент _____ С.І. Талапчук
Підпис Ініціали, прізвище

Керівник роботи _____ Т.О. Говорущенко
Підпис Ініціали, прізвище

РЕФЕРАТ

Тема дипломної роботи: Метод та підсистема ідентифікації користувача кіберфізичної системи «Розумний будинок»

Автор роботи: С.І. Талапчук

Керівник роботи: Т.О. Говорущенко

Пояснювальна записка: 81 с, 5 рис, 3 дод, 83 джерела.

ПЕРЕЛІК КЛЮЧОВИХ СЛІВ: кіберфізична система, програмне забезпечення, штучний інтелект, розумний будинок.

Об’єктом дослідження є процес ідентифікації користувача кіберфізичної системи «Розумний будинок».

Предметом дослідження підсистема ідентифікації користувача кіберфізичної системи.

Метою дипломної роботи є підвищення ефективності ідентифікації користувача кіберфізичної системи «Розумний будинок».

Для розв’язання поставлених задач використовувалися методи:

1. Аналіз відомих методів та рішень для ідентифікації користувача кіберфізичної системи «Розумний будинок».

2. Моделювання процесу ідентифікації користувача кіберфізичної системи «Розумний будинок».

3. Метод ідентифікації користувача кіберфізичної системи «Розумний будинок».

4. Підсистема ідентифікації користувача кіберфізичної системи «Розумний будинок».

Наукова новизна отриманих результатів:

− метод ідентифікації користувача кіберфізичної системи «Розумний будинок», який забезпечує верифікацію наданих під час автентифікації користувачем даних (відбиток пальця, скан сітківки ока, тощо) та висновок про

можливість доступу до тих чи інших ресурсів та підсистем кіберфізичної системи «Розумний будинок» на основі такої верифікації;

– архітектура підсистеми ідентифікації користувача кіберфізичної системи «Розумний будинок», спрямована на перевірку даних користувача, наданих під час автентифікації, а також на формування висновку про ідентифікацію користувача та його роль і права доступу.

На основі проведених досліджень розроблена архітектура і компоненти програмного забезпечення підсистема ідентифікації користувача кіберфізичної системи «Розумний будинок»

Практична значимість отриманих результатів полягає у створенні підсистеми ідентифікації користувача кіберфізичної системи «Розумний будинок», спрямована на перевірку даних користувача, наданих під час автентифікації, а також на формування висновку про ідентифікацію користувача та про можливість доступу до тих чи інших ресурсів та підсистем кіберфізичної системи «Розумний будинок» на основі такої верифікації.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

КФС - кіберфізична система

РБ – розумний будинок

БД - база даних

БПР - блок прийняття рішень

ММ – математична модель

АУ – алгоритм управління

ЕС - експертна система

ВСТУП

Дуже важливо бути в безпеці в сучасному світі розумних пристроїв і розумних середовищ, де майже всі пристрої підключені до інтернету. Люди, які роблять свої пристрої більш безпечними, також роблять їх ефективнішими. Немає значення, чи працюють дослідники в організації чи над своїми особистими даними,безпека важлива для всіх нас, тому зростає попит на різні типи технологій ідентифікації користувачів як для онлайнових, так і для фізичних систем. Користувачі повинні розуміти, що паролі — не єдиний спосіб ідентифікації. Існує велика різноманітність технологій ідентифікації та ще більший спектр дій, для яких потрібні методи ідентифікації.

Кіберфізична система або інтелектуальна система — це комп'ютерна система, в якій механізм контролюється або перевіряється за допомогою комп'ютерних алгоритмів. У кіберфізичних системах фізичні та програмні компоненти глибоко переплетені, здатні працювати в різних просторових і часових масштабах, проявляти численні та відмінні модальності поведінки та взаємодіяти один з одним способами, які змінюються залежно від контексту. Кіберфізична система передбачає трансдисциплінарні підходи, поєднуючи теорію кібернетики, мехатроніки, проектування та науки про процеси. Управління процесом часто називають вбудованими системами. У вбудованих системах наголос більше робиться на обчислювальних елементах і менше на інтенсивному зв'язку між обчислювальними та фізичними елементами. Кіберфізична система також схожий на Інтернет речей, маючи ту саму базову архітектуру. Незважаючи на це, кіберфізична система представляє вищу комбінацію та координацію між фізичними та обчислювальними елементами[1].

Кіберфізична система побудовані на інтеграції обчислювальних алгоритмів і фізичних компонентів які залежать від неї. Ці системи поєднують цифрові та аналогові пристрої, інтерфейси, датчики, мережі, виконавчі механізми та комп'ютери з природним середовищем, об'єктами та конструкціями створеними людиною. Подібно до того, як інтернет змінив спосіб взаємодії людей з

інформацією, кіберфізичні системи змінюють спосіб взаємодії людей із фізичним світом. У той же час, масштаб і властива неоднорідність цих систем створюють величезні інженерні проблеми. Потрібні нові технологічні підходи, щоб формалізувати їх дизайн, керувати ними та контролювати їх у масштабований, ефективний і безпечний спосіб, а також забезпечити їх зручність у використанні.

Система «Розумний будинок». зазвичай використовується для автоматизації різних процесів у будинку, таких як освітлення, опалення, кондиціонування повітря, безпека та інші. Ідентифікація користувача - це важлива частина розумного будинку, оскільки вона дозволяє відрізняти різних користувачів та налаштовувати систему відповідно до їхніх потреб.

На сьогоднішній день кіберфізичні системи широко використовуються і охоплюють різні сфери життя людини. В побуті все частіше можна зіткнутись з КФС. Для того щоб безпечно та ефективно використовувати ці системи, нам потрібно покращити або розробити більш досконалу методику ідентифікації користувача в системі.

Метою дипломної роботи є підвищення ефективності ідентифікації користувача кіберфізичної системи «Розумний будинок».

Поставлена мета досягається розв’язанням таких основних задач:

1. Здійснити аналіз існуючих методів та рішень для ідентифікації користувача кіберфізичної системи;

2. Моделювання процесу ідентифікації користувача кіберфізичної системи «Розумний будинок».

3. Розробити метод ідентифікації користувача кіберфізичної системи «Розумний будинок».

4. Розробити підсистему ідентифікації користувача кіберфізичної системи «Розумний будинок».

Об’єктом дослідження є процес ідентифікації користувача кіберфізичної системи «Розумний будинок».

Предметом дослідження є метод та підсистема ідентифікації користувача кіберфізичної системи «Розумний будинок».

Наукова новизна отриманих результатів:

1. Метод ідентифікації користувача кіберфізичної системи «Розумний будинок», який забезпечує верифікацію наданих під час автентифікації користувачем даних та висновок про можливість доступу до тих чи інших ресурсів та підсистем кіберфізичної системи «Розумний будинок» на основі такої верифікації.

2. Архітектура підсистеми ідентифікації користувача кіберфізичної системи «Розумний будинок», спрямована на перевірку даних користувача, наданих під час автентифікації, а також на формування висновку про ідентифікацію користувача та його роль і права доступу.

Практична цінність отриманих результатів. В результаті виконаного наукового дослідження розроблена підсистема ідентифікації користувача кіберфізичної системи «Розумний будинок», спрямована на перевірку даних користувача, наданих під час автентифікації, а також на формування висновку про ідентифікацію користувача та про можливість доступу до тих чи інших ресурсів та підсистем кіберфізичної системи «Розумний будинок» на основі такої верифікації.

За темою дипломної роботи опублікована одна стаття у фаховому науковому виданні “Computer Systems & Information Technologies 2022” [2].

1 АНАЛІЗ ВІДОМИХ МЕТОДІВ ТА РІШЕНЬ ДЛЯ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА КІБЕРФІЗИЧНОЇ СИСТЕМИ «РОЗУМНИЙ БУДИНОК»

1.1 Ідентифікації користувача та її види.

Ідентифікація - це процедура розпізнавання користувача за його ідентифікатором (іменем).

Ця функція виконується в першу чергу, коли користувач робить спробу увійти в мережу.

Користувач повідомляє системі за її запитом свій ідентифікатор, і система перевіряє в своїй базі даних його наявність.

Основні методи ідентифікації користувача в кіберфізичних системах, таких як «Розумний будинок», включають:

1. Використання біометричних даних: це можуть бути відбитки пальців, сканування обличчя, розпізнавання голосу, що дозволяє ідентифікувати користувачів за їхніми фізичними характеристиками.
2. Використання ідентифікаторів: такі як магнітні картки, RFID-мітки або NFC-технології, що можуть бути прикріплені до ключів або телефонів, для ідентифікації користувача.
3. Використання паролів: пароль - це секретний код, який користувач повинен ввести, щоб отримати доступ до системи.
4. Використання додатків: додатки, які встановлюються на смартфони або планшети користувачів, можуть використовуватися для ідентифікації користувача.

Загальна процедура ідентифікації та автентифікації користувача при наданні доступу до АС наведена на рисунку 1.1.

Якщо в процесі автентифікації справжність суб’єкта встановлено, система захисту інформації (СЗІ) повинна визначити його повноваження.

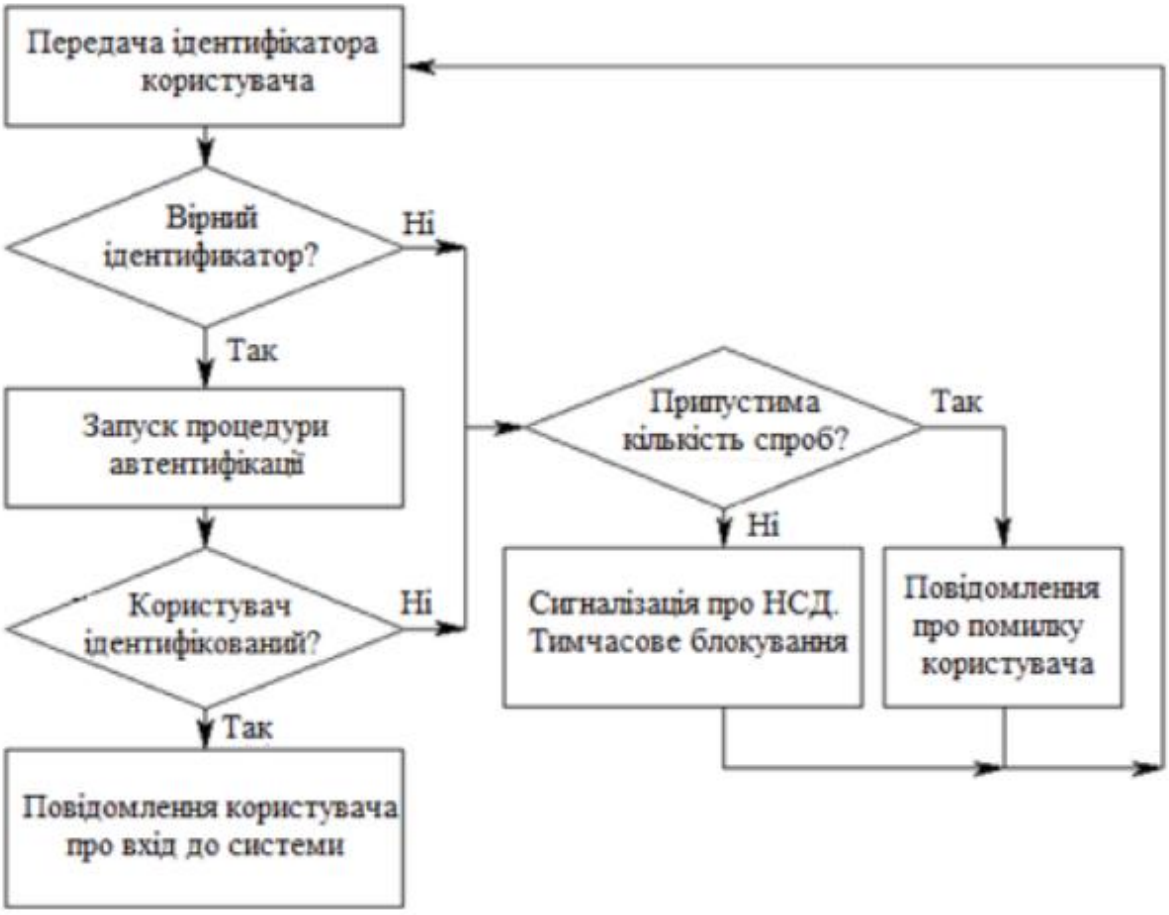


Рисунок 1.1 – Класична процедура ідентифікації

1.2 Аналіз сучасних методів біометричної ідентифікації.

Основні методи біометричної ідентифікації включають:

1. Розпізнавання обличчя: цей метод використовується для ідентифікації особи на основі особливостей її обличчя. Для цього використовуються алгоритми комп'ютерного зору та нейронні мережі.

2. Розпізнавання відбитків пальців: цей метод використовується для ідентифікації особи на основі унікальності її відбитків пальців. Для цього використовуються сенсори відбитків пальців, які зчитують патерн на поверхні пальця та порівнюють його зі збереженим шаблоном в базі даних.

3. Розпізнавання розмірів тіла та форми руки: цей метод використовується для ідентифікації особи на основі її розмірів тіла та форми руки. Для цього використовуються 3D-сенсори та алгоритми комп'ютерного зору.

4. Розпізнавання голосу: цей метод використовується для ідентифікації особи на основі її голосу. Для цього використовуються спеціальні алгоритми, які аналізують голос та порівнюють його зі збереженим шаблоном в базі даних.

5. Розпізнавання рухів: цей метод використовується для ідентифікації особи на основі її рухів. Для цього використовуються спеціальні датчики руху та алгоритми комп'ютерного зору.

1.3 Огляд відомих кіберфізичних систем.

Для огляду використаємо наступні кіберфізичних система формату «Розумний будинок».

Amazon Echo/Alexa - система контролю за будинком, яка використовує голосові команди для керування пристроями у будинку. Пристрій можна підключити до нтернету, щоб керувати його за допомогою мобільного додатку. Однією з переваг цієї системи є її простота використання, але вона може мати проблеми з розпізнаванням голосу та потребує постійного з'єднання з Інтернетом.

Google Nest - це система "розумного будинку", яка дозволяє контролювати температуру, освітлення та безпеку у будинку за допомогою мобільного додатку або голосових команд. Однією з переваг цієї системи є її інтеграція з Google Assistant, але вона може бути дорогим варіантом, особливо якщо потрібно встановлювати додаткові пристрої.

Apple HomeKit - це система "розумного будинку", яка дозволяє керувати пристроями у будинку з допомогою iPhone або iPad. Ця система є досить простою у використанні, але вона може мати обмежені можливості порівняно з іншими системами.

Samsung SmartThings - це кіберфізична система для будинку, яка дозволяє керувати різними пристроями з одного місця за допомогою мобільного додатку або

голосового помічника. Ця система включає в себе гнучку платформу, що підтримує різноманітні протоколи зв'язку, такі як Wi-Fi, Bluetooth, Z-Wave та Zigbee, що дозволяє злити в єдину систему різноманітні речі, що знаходяться в будинку - від освітлення та клімат-контролю до домашньої безпеки та електроніки. Крім того, Samsung SmartThings має можливість інтегруватися з іншими популярними рішеннями розумного будинку, такими як Amazon Alexa та Google Assistant, для забезпечення ще більшої гнучкості та зручності управління вашим будинком.

1.3.1 Кіберфізична система Amazon Echo / Alexa

Кіберфізична система Amazon Echo / Alexa використовує різні методи ідентифікації користувача, зокрема голосову ідентифікацію та ідентифікацію з використанням унікального коду користувача.

Голосова ідентифікація використовує вбудований мікрофон у пристрої Amazon Echo для розпізнавання голосу користувача. Для того, щоб Alexa розпізнала голос користувача, йому спочатку необхідно налаштувати свій голосовий профіль, в якому буде зберігатися інформація про його голосові характеристики. Коли користувач використовує команду голосом, Amazon Echo порівнює голос користувача з його голосовим профілем і визначає, чи є це його голос.

Крім того, Amazon Echo також використовує унікальний код користувача, щоб ідентифікувати його. Кожен пристрій Echo має свій власний унікальний ідентифікатор, який пов'язаний з обліковим записом користувача Amazon. Коли користувач користується пристроєм, Amazon Echo автоматично ідентифікує його за допомогою цього ідентифікатора.

Щоб забезпечити додаткову безпеку, користувач може налаштувати підтвердження голосом для покупок та інших дій, що вимагають авторизації. У цьому випадку Amazon Echo буде запитувати користувача про підтвердження дії, наприклад, запитувати пароль або іншу форму ідентифікації користувача.

Ідентифікація користувача в кіберфізичній системі Amazon Echo / Alexa складається з декількох етапів:

1) користувач ініціює комунікацію з системою, вимовляючи фразу "Alexa" або "Echo" та запитуючи щось;

2) система Echo / Alexa сприймає голосовий сигнал і відправляє його до серверів Amazon;

3) сервери Amazon застосовують алгоритми глибинного навчання та машинного навчання для розпізнавання та ідентифікації голосу;

4) якщо система може ідентифікувати голос як голос користувача, який вже має обліковий запис, то вона повертає дані цього облікового запису;

5) якщо голос не може бути ідентифікований, система запитує користувача додаткову інформацію для ідентифікації, таку як пароль або PIN-код;

6) якщо користувач не може бути ідентифікований, система Echo / Alexa обмежує доступ користувача до конфіденційної інформації та деяких функцій.

У кіберфізичній системі Amazon Echo / Alexa також є можливість створювати та керувати різними профілями користувачів, дозволяючи кільком користувачам використовувати систему з окремими налаштуваннями та обмеженнями доступу.

1.3.2 Кіберфізична система Google Nest

Кіберфізична система Google Nest розумного будинку ідентифікація користувача відбувається за допомогою голосового асистента Google Assistant. Коли користувач говорить до пристрою, голосовий асистент впізнає його голос і порівнює його з голосом, який вже зареєстрований у системі.

Крім того, Google Nest має функцію розпізнавання осіб. За допомогою цієї функції система може розпізнавати обличчя користувачів, які були додані до списку розпізнавання в програмному забезпеченні. Це дозволяє системі автоматично запускати індивідуальні налаштування для кожного користувача, коли він знаходиться в зоні дії камери розпізнавання.

Загалом, ідентифікація користувача в кіберфізичній системі розумного будинку Google Nest базується на голосовому та обличчєвому розпізнаванні, що дозволяє системі взаємодіяти з користувачами із забезпеченням безпеки та конфіденційності даних.

Покроковий текстовий опис роботи ідентифікації в кіберфізичній системі Google Nest:

1. Збір біометричних даних: для ідентифікації користувача система Google Nest використовує біометричні дані, такі як сканування обличчя та голосу. При встановленні системи Google Nest користувачі можуть додати свої біометричні дані до системи, щоб забезпечити ідентифікацію на основі цих даних.

2. Застосування машинного навчання: система Google Nest використовує машинне навчання для аналізу та порівняння біометричних даних користувачів. За допомогою цієї системи аналізу можна застосувати, який користувач намагається отримати доступ до системи.

3. Використання ідентифікаторів: для ідентифікації користувача система Google Nest може використовувати ідентифікатори, такі як NFC-технології або магнітні картки. Ці ідентифікатори можуть бути присвоєні конкретному користувачу, тому система може застосовуватися, хто намагається отримати доступ до системи на основі ідентифікатора.

4. Використання паролів: користувачі системи Google Nest можуть використовувати паролі дляідентифікації. Система може перевірити правильність введеного пароля та дозволити або заборонити доступ до системи на цій основі.

5. Аналіз поведінки: система Google Nest може аналізувати поведінку користувачів, щоб застосувати, хто намагається отримати доступ до системи. Наприклад, система може дізнатися, коли користувач постійно переходить до системи, які пристрої він зазвичайвмикає та вимикає, та інші ознаки поведінки.

1.3.3 Кіберфізична система Apple HomeKit

Кіберфізична система Apple HomeKit розумного будинку, ідентифікація користувача відбувається за допомогою функції "Додавання користувачів" (Add User) в додатку HomeKit на пристроях Apple.

Користувач може додавати інших користувачів до своєї домашньої мережі та надавати їм доступ до своїх підключених пристроїв. Кожен користувач повинен мати власний обліковий запис Apple ID, щоб мати доступ до додатку HomeKit та підключених до нього пристроїв.

При додаванні нового користувача до домашньої мережі, головний користувач може встановлювати рівні доступу та обмеження для кожного з них. Також, при доступі до підключених пристроїв, система запитує підтвердження ідентифікації користувача через Touch ID або Face ID, якщо такі функції доступні на пристрої.

Загалом, ідентифікація користувача в кіберфізичній системі розумного будинку Apple HomeKit забезпечується за допомогою функції "Додавання користувачів" та авторизації за допомогою Touch ID або Face ID. Така система дозволяє забезпечити безпеку та конфіденційність даних, що використовуються в системі розумного будинку.

Ідентифікація користувача в кіберфізичній системі Apple HomeKit складається з декількох етапів:

1) аутентифікація в додатку: користувач повинен авторизуватись в додатку HomeKit за допомогою свого Apple ID, який ідентифікує користувача. Якщо користувач ще не має Apple ID, він повинен створити його;

2) створення будинку: після аутентифікації в додатку, користувач може створити дім, додати пристрої і запустити їх. Кожен дім пов'язаний з Apple ID, який було використано для авторизації;

3) додавання користувачів: додавання інших користувачів дозволяє надавати їм доступ до керування будинком. Для цього користувач повинен запрошувати інших користувачів в додаток HomeKit, вказуючи їх Apple ID;

4) аутентифікація пристроїв: перед додаванням пристроїв до будинку, користувач повинен спочатку аутентифікувати їх за допомогою спеціальних ідентифікаторів, які називаються сертифікатами HomeKit. Ці сертифікати генеруються пристроями, які підтримують технологію HomeKit;

5) використання Siri: користувач може взаємодіяти з будинком через Siri, голосовий помічник від Apple. Для цього, користувач повинен дозволити Siri доступ до додатку HomeKit і налаштувати команди голосового керування;

6) безпека: Apple HomeKit забезпечує безпеку даних користувача, використовуючи шифрування в транспортному та у рівні додатку. Також він підтримує аутентифікацію двох факторів для забезпечення більш високого рівня безпеки.

1.3.4 Кіберфізична система Samsung SmartThings «Розумний будинок»

Кіберфізична система Samsung SmartThings «Розумний будинок», має можливість ідентифікації користувача за допомогою різних біометричних методів, включаючи розпізнавання обличчя та розпізнавання голосу.

Ідентифікація користувача за допомогою розпізнавання обличчя виконується за допомогою камер, розташованих у приміщенні. Система збирає зображення облич користувачів і порівнює їх зі збереженими зразками в базі даних. Якщо знайдено збіг, система ідентифікує користувача.

Ідентифікація користувача за допомогою розпізнавання голосу виконується за допомогою мікрофонів, розташованих у приміщенні. Кожен користувач може навчити систему розпізнавати його голос, проходячи короткий тренувальний процес. Після навчання система порівнює звукові дані, отримані від мікрофонів, зі збереженими зразками в базі даних. Якщо знайдено збіг, система ідентифікує користувача.

Для забезпечення безпеки даних користувачів, система Samsung SmartThings використовує шифрування та автентифікацію користувачів за допомогою пароля.

Крім того, система має можливість зміни налаштувань доступу для кожного користувача окремо, що дозволяє контролювати рівень доступу до різних функцій системи в залежності від прав користувача.

Ідентифікація користувача в кіберфізичній системі Samsung SmartThings може бути виконана за допомогою розпізнавання обличчя та розпізнавання голосу. Давайте розглянемо кожен з цих методів покроково.

Розпізнавання обличчя:

1) камери, розташовані в приміщенні, збирають зображення обличчя користувачів;

2) зображення обробляються і порівнюються зі збереженими зразками в базі даних;

3) якщо знайдено збіг, система ідентифікує користувача;

4) якщо збіг не знайдено, система може запропонувати користувачеві ввести пароль для авторизації.

Розпізнавання голосу:

1) мікрофони, розташовані в приміщенні, збирають звукові дані голосу користувачів;

2) кожен користувач може навчити систему розпізнавати його голос, проходячи короткий тренувальний процес;

3) звукові дані обробляються і порівнюються зі збереженими зразками в базі даних;

4) якщо знайдено збіг, система ідентифікує користувача;

5) якщо збіг не знайдено, система може запропонувати користувачеві ввести пароль для авторизації.

Зауважимо, що система Samsung SmartThings використовує шифрування та автентифікацію користувачів за допомогою пароля для забезпечення безпеки даних користувачів. Крім того, система має можливість зміни налаштувань доступу для кожного користувача окремо, що дозволяє контролювати рівень доступу до різних функцій системи в залежності від прав користувача.

1.4 Висновок

Ідентифікація користувача в кіберфізичних системах Amazon Echo/Alexa, Google Nest, Apple HomeKit та Samsung SmartThings використовує різні методи та технології.

Amazon Echo/Alexa використовує голосову ідентифікацію, яка базується на розпізнаванні голосу користувача. Користувач повинен налаштувати голосовий профіль та повторити кілька фраз для розпізнавання голосу. Крім того, Amazon Echo/Alexa може використовувати інші методи ідентифікації, такі як розпізнавання обличчя та використання пін-коду.

Google Nest використовує кілька методів ідентифікації, зокрема голосову, обличчя та розташування пристроїв. Голосова ідентифікація базується на розпізнаванні голосу, подібно до Amazon Echo/Alexa, але також використовує додаткову інформацію, таку як акцент, тембр голосу та інші. Розпізнавання обличчя відбувається за допомогою камери пристрою та аналізу зображень. Розташування пристроїв визначається за допомогою датчиків руху та інших датчиків.

Apple HomeKit використовує ідентифікацію користувача за допомогою системи аутентифікації Touch ID або Face ID на пристроях Apple. Крім того, користувач може налаштувати авторизовані пристрої для використання в системі HomeKit, що дозволяє обмежити доступ до системи.

Samsung SmartThings використовує ідентифікацію на основі обличчя та візуальну ідентифікацію. У порівнянні з Amazon Echo/Alexa та Google Nest, які використовують голосову ідентифікацію, цей метод забезпечує більш точну та безпечну ідентифікацію користувача.

Загалом, у всіх трьох кіберфізичних системах, що розглядались, ідентифікація користувача здійснюється шляхом розпізнавання голосу та інших характеристик користувача. Однак, є деякі різниці у тому, як вони здійснюють процес ідентифікації.

Amazon Echo / Alexa використовує мультимодальну ідентифікацію, включаючи голосове, зображення та інші характеристики користувача. Google Nest використовує голосове розпізнавання, а також може використовувати інші джерела інформації, такі як рух користувача, для підвищення точності ідентифікації. Apple HomeKit використовує технології шифрування та аутентифікації, щоб забезпечити безпеку взаємодії між девайсами та користувачами, але надійність ідентифікації базується переважно на голосовому розпізнаванні. Samsung SmartThings використовує багатофакторну аутентифікацію, включаючи PIN-код та ідентифікацію на основі голосу, які можуть бути посилені використанням додаткових факторів, таких як відбитки пальців.

Отже, кожна КФС має свої переваги та недоліки у використанні різних методів ідентифікації. Для кожного окремого випадку важливо враховувати характеристики користувачів та особливості використовуваних пристроїв, а також розглянути можливості вдосконалення системи ідентифікації для підвищення безпеки та зручності використання.

2. МОДЕЛЮВАННЯ ПРОЦЕСУ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА КІБЕРФІЗИЧНОЇ СИСТЕМИ «РОЗУМНИЙ БУДИНОК»

2.1 Розробка математичної моделі процесу ідентифікації користувача

2.1.1 Параметри, що впливають на процес ідентифікації користувача

Параметри, що впливають на процес ідентифікації користувача. До таких параметрів можна віднести зовнішні фактори, такі як шум, освітлення, а також внутрішні фактори, такі як характеристики біометричного методу, обраного для ідентифікації. До зовнішніх факторів можна віднести такі параметри:

- шум - будь-який звуковий або електричний сигнал, який несе додаткову інформацію та заважає коректному розпізнаванню голосу або інших біометричних даних;
- освітлення - якість та яскравість освітлення може впливати на якість зображення, що використовується для розпізнавання обличчя;
- відстань - відстань між користувачем та сенсором або камерою також може впливати на якість розпізнавання.

До внутрішніх факторів можна віднести такі параметри:

- характеристики біометричного методу - кожен біометричний метод має свої унікальні особливості, які можуть впливати на точність розпізнавання. Наприклад, розпізнавання голосу може бути ускладнене для людей з деякими мовними дефектами або акцентом;
- кількість біометричних даних - чим більше даних використовується для ідентифікації, тим точніше може бути процес розпізнавання;
- якість біометричних даних - якість зібраних даних, таких як зображення обличчя або звукові записи голосу, також може впливати на точність розпізнавання.

Ці параметри важливі для успішної ідентифікації користувача в кіберфізичній системі, і їх будемо враховувати при розробці та впровадженні систем ідентифікації.

2.1.2 Вибір підходящих методів для збору даних біометричних характеристик користувачів

Вибір підходящих методів для збору даних біометричних характеристик користувачів, які будуть використовуватися для ідентифікації. Це можуть бути:

Розпізнавання обличчя: метод збору біометричних даних, що ґрунтується на аналізі особливостей обличчя користувача. Цей метод можна використовувати для ідентифікації користувачів в реальному часі і без їх участі. Для цього використовується камера, яка фіксує обличчя користувача та порівнює його з зразком, збереженим у системі.

Візуальне розпізнавання обличчя можна реалізувати за допомогою глибокого навчання, а саме за допомогою згорткових нейронних мереж (Convolutional Neural Networks, CNN). Ось приклад математичної моделі для програми візуального розпізнавання обличчя:

1. Попередня обробка: Вхідне зображення нормалізується та масштабується до певного розміру (наприклад, 224x224 пікселів) .

2. Згортковий шар: Застосовуються згорткові фільтри для виявлення різних особливостей зображення. В результаті отримуємо набір активаційних мап:

$$A = f(W \cdot X + b), \tag{2.1}$$

де A - активаційна мапа;

W - ваги згорткового фільтра;

X - вхідне зображення;

b – зсув;

f - функція активації (наприклад, ReLU).

3. Пулінговий шар: Застосовуються операції пулінгу для зменшення розмірності активаційних мап та виокремлення найважливіших особливостей.

4. Повнозв'язні шари: Вихідні дані з попередніх шарів передаються повнозв'язним шарам для визначення співвідношення між різними особливостями та виявлення обличчя:

$$Z = f(N \cdot A + b), \tag{2.2}$$

де Z - вихідні дані;

N - ваги повнозв'язного шару;

A - активаційна мапа;

b – зсув;

f - функція активації;

5. softmax-шар: вихідні дані передаються softmax-шару для отримання ймовірностей належності до різних класів (ідентифікаторів користувачів):

$$P = \text{softmax}(Z). \tag{2.3}$$

6. Ідентифікація користувача: Користувач ідентифікується як той, чия ймовірність максимальна:

$$user\_id = \text{argmax}_i(\text{P}). \tag{2.4}$$

Ця математична модель візуального розпізнавання обличчя може бути використана для розробки програми ідентифікації користувачів в кіберфізичній системі «Розумний будинок». Вона дозволяє виявляти та розпізнавати обличчя користувачів у реальному часі та забезпечувати точність і надійність ідентифікації.

Відбитки пальців: метод збору біометричних даних, що ґрунтується на аналізі особливостей відбитків пальців користувача. Цей метод є досить точним і надійним, тому він широко використовується в різних системах ідентифікації.

Розпізнавання відбитків пальців - це процес ідентифікації особи за її унікальними відбитками пальців. Один з підходів до створення математичної

моделі для розпізнавання відбитків пальців полягає в використанні особливостей (характеристичних точок) відбитка пальця.

Ось приклад такої математичної моделі:

1. Попередня обробка: вхідне зображення відбитка пальця піддається нормалізації, згортанню, бінаризації та скелетизації для покращення якості та виділення характеристичних особливостей.

2. Виявлення особливостей візерунку пальця: застосовуються алгоритми, такі як Poincaré Index, для виявлення особливостей візерунку (наприклад, закінчень та розгалужень) відбитка пальця. Кожна особливість має свої координати (x, y) та орієнтацію (θ).

3. Відповідність особливостей візерунку пальця: для порівняння відбитків пальців використовуються алгоритми відповідності, такі як алгоритм заснований на трикутниках або глобальні алгоритми порівняння. Відповідність між двома відбитками пальців визначається як сума вагових коефіцієнтів відповідних особливостей візерунку:

$$P = \Sigma \, w_{ij}, \tag{2.5}$$

де w_ij - ваговий коефіцієнт для відповідності між особливостями візерунка пальця i та j.

4. Оцінка схожості: відстань між двома відбитками пальців визначається як зворотне значення суми вагових коефіцієнтів відповідних особливостей візерунку:

$$D = \frac{1}{S}. \tag{2.6}$$

5. Ідентифікація користувача: якщо відстань між двома відбитками пальців менша за певний пороговий рівень, відбитки пальців вважаються співпадаючими, і особу можна ідентифікувати.

$$user\_id = \{i \mid D(I, query) < threshold\}, \quad (2.7)$$

де і - ідентифікатор користувача;

query - відбиток пальця, який потрібно ідентифікувати;

threshold - порогове значення відстані для ідентифікації користувачів;

Голосовий ідентифікатор: метод збору біометричних даних, що ґрунтується на аналізі особливостей голосу користувача. Цей метод можна використовувати для ідентифікації користувачів віддалено, за допомогою мікрофону. Важливим фактором при використанні цього методу є те, щоб голос користувача був досить стійким і не залежав від зовнішніх факторів, таких як застуда або пошкодження мікрофону.

Математичної моделі для ідентифікації голосу на основі гауссових сумішей (GMM) та мел-частотних кепстральних коефіцієнтів (MFCC).

1. Попередня обробка: відбувається конвертація аудіо сигналу в набір рамок із перекриванням. Зазвичай використовують вікна тривалістю 20-30 мс з 10-15 мс перекривання. Вікно зазвичай програється по сигналу для виділення короткочасних характеристик сигналу.

2. Обчислення MFCC: для кожної рамки обчислюються MFCC, які є компактними і дискретними представленнями спектра сигналу. MFCC отримують шляхом перетворення Фур'є, застосування мел-шкали та перетворення кепстру.

3. Опис векторів для навчання: зібрані дані (MFCC) від кількох відомих користувачів утворюють набір ознак для навчання GMM. Кожен користувач матиме свій власний набір ознак.

4. Навчання GMM: для кожного користувача створюється його власна GMM, яка найкращим чином апроксимує розподіл його MFCC векторів. GMM можна представити як:

$$p(x) = \sum_i w_i \cdot N(x, \mu_i, \Sigma_i), \quad (2.8)$$

де x - вектор ознак;

w_i - ваги компонентів суміші;

$N(x, \mu_i, \Sigma_i)$ - гауссова щільність ймовірності з математичним сподіванням μ_i та матрицею коваріації Σ_i. GMM навчається за допомогою алгоритму Expectation-Maximization (EM).

5. Ідентифікація голосу: під час ідентифікації голосу, MFCC вектори нового аудіосигналу порівнюються з усіма GMM користувач ів, навченими на етапі 4. Для кожної GMM обчислюється ймовірність генерування даного набору MFCC векторів. Це можна зробити, використовуючи логарифмічну ймовірність:

$$L_i = \sum(\log(p(x \mid w_i, \mu_i, \Sigma_i))) \tag{2.9}$$

де L_i - логарифмічна ймовірність для і-го користувача;

x - вектор ознак;

w_i, μ_i, Σ_i - відповідні параметри GMM.

6. Визначення користувача. Ідентифікований користувач визначається як той, чия GMM максимізує логарифмічну ймовірність:

$$user\_id = argmax_i(L_i) \tag{2.10}$$

Застосування порогового значення може допомогти уникнути помилкової ідентифікації користувачів.

У цій математичній моделі використовуються такі поняття, як мел-частотні кепстральні коефіцієнти (MFCC), гауссові суміші (GMM) та алгоритм Expectation-Maximization (EM) для навчання моделі.

Ця модель дозволяє ідентифікувати користувачів на основі їхніх голосових характеристик, що може бути використано в розумних будинках та інших кіберфізичних системах для забезпечення безпеки та зручності користувачів.

2.1.3 Зібрати даних для побудови математичної моделі

Для збору даних про обличчя можна використовувати камери відеоспостереження або фотоапарати, для збору даних про ретину ока - пристрої для сканування ретини ока, для збору даних про голос - мікрофони.

Важливо забезпечити якість даних, збираних для моделі. Для цього можна використовувати спеціальні програмні засоби, які дозволяють підтверджувати якість зібраних даних, наприклад, програми для перевірки якості зображення. Також важливо забезпечити конфіденційність та безпеку зібраних даних, щоб уникнути можливого їх витоку та недопущення можливого зловживання з боку зловмисників.

2.1.4 Статистичний аналіз зібраних даних

Статистичний аналіз зібраних даних, щоб визначити стійкість та точність використовуваних біометричних методів. Для цього можна використовувати різноманітні методи аналізу, такі як методи машинного навчання або статистичний аналіз.

Правильно, проведення статистичного аналізу є важливим етапом в розробці систем ідентифікації з використанням біометричних методів. Для визначення стійкості та точності можна використовувати різні показники, такі як False Acceptance Rate (FAR) та False Rejection Rate (FRR), що вказують на те, якою часткою користувачів система помилково відповідає на запит або неправильно відкидає запит.

Також можна використовувати показники, такі як Receiver Operating Characteristic (ROC) та Equal Error Rate (EER), що дозволяють оцінити точність та стійкість системи ідентифікації. Для проведення статистичного аналізу можна використовувати різноманітні інструменти, такі як програми для аналізу даних, бібліотеки машинного навчання та інші.

2.1.5 Побудова теоретичної математичної моделі

Побудова теоретичної математичної моделі процесу ідентифікації користувача кіберфізичної системи на основі зібраних даних та статистичного аналізу.

Створення комплексної математичної моделі підсистеми ідентифікації користувача для розумного будинку, яка використовує розпізнавання обличчя, відбитків пальців та сітківки ока, можна здійснити шляхом інтеграції відповідних моделей та алгоритмів.

Спочатку, розробимо функції для кожного методу ідентифікації:

1. F_face(query) - функція розпізнавання обличчя, яка повертає схожість між query (запитом) та збереженими зображеннями обличь користувачів.
2. F_fingerprint(query) - функція розпізнавання відбитків пальців, яка повертає схожість між query (запитом) та збереженими відбитками пальців користувачів.
3. F_retina(query) - функція розпізнавання сітківки ока, яка повертає схожість між query (запитом) та збереженими зображеннями сітківки ока користувачів.

Тепер об'єднаємо ці функції в одну комплексну функцію ідентифікації:

$$F\_identification(query\_face, query\_fingerprint, query\_retina) = (F\_face(query\_face) + F\_fingerprint(query\_fingerprint) + F\_retina(query\_retina)) \ / \ 3. \quad (2.11)$$

Ця функція розраховує середню схожість між запитами та збереженими даними для кожного методу ідентифікації.

Наступним кроком є визначення порогового значення для ідентифікації користувачів. Якщо середня схожість перевищує цей поріг, особу вважають ідентифікованою:

$$user\_id = \{i \mid F\_identification(query\_face, query\_fingerprint, query\_retina) > treshold\} \quad (2.12)$$

де i - ідентифікатор користувача;

query_face, query_fingerprint та query_retina - запити для розпізнавання обличчя, відбитків пальців та сітківки ока відповідно;

threshold - порогове значення середньої схожості для ідентифікації користувачів.

Для вдосконалення цієї комплексної математичної моделі можна розглянути такі підходи:

4. Застосування ваг для кожного методу ідентифікації: через різні рівні надійності та точності різних методів ідентифікації, можна застосувати ваги для кожного методу, щоб врахувати їх вплив на загальну схожість:

$$F\_identification(query\_face, query\_fingerprint, query\_retina) = \frac{(w1 \cdot F\_face(query\_face) + w2 \cdot F\_fingerprint(query\_fingerprint) + w3 * F\_retina(query\_retina))}{(w1 + w2 + w3)} \quad (2.13)$$

де w1, w2, w3 - ваги для розпізнавання обличчя, відбитків пальців та сітківки ока відповідно.

5. Використання метрик схожості або рішення про ідентифікацію: замість використання середньої схожості, можна використовувати інші метрики схожості або рішення про ідентифікацію, які дозволяють краще враховувати різні рівні точності та надійності методів ідентифікації.

6. Застосування машинного навчання: використання алгоритмів машинного навчання для визначення оптимальних параметрів моделі, таких як ваги та порогові значення, може допомогти підвищити ефективність системи ідентифікації користувачів.

7. Забезпечення приватності та захисту даних: розробка та впровадження стратегій збереження, передачі та обробки даних про користувачів, забезпечуючи приватність та захист, є важливим аспектом для розумного будинку.

Таким чином, комплексна математична модель підсистеми ідентифікації користувача розумного будинку, яка використову є розпізнавання обличчя, відбитків пальців та сітківки ока, може допомогти в реалізації більш надійної, безпечної та ефективної системи ідентифікації користувачів.

Щоб забезпечити гладку інтеграцію цієї комплексної математичної моделі з іншими підсистемами розумного будинку, розробники можуть враховувати такі аспекти:

1) інтеграція з підсистемами контролю доступу: комплексну модель ідентифікації користувачів з підсистемами контролю доступу, щоб надавати користувачам доступ до різних приміщень та функцій розумного будинку на основі їх ідентифікації;

2) адаптивність до змін умов середовища: можливість адаптації системи ідентифікації користувачів до змін умов середовища, таких як освітлення, щоб підтримувати високу точність і надійність розпізнавання;

3) сповіщення та моніторинг: механізми сповіщення та моніторингу, які дозволяють операторам системи та користувачам відслідковувати події, пов'язані з ідентифікацією користувачів, і вчасно реагувати на можливі проблеми;

4) розширюваність та гнучкість: можливість розширення та модифікації комплексної моделі ідентифікації користувачів, щоб враховувати нові технології, методи та вимоги безпеки.

Використання такої комплексної математичної моделі підсистеми ідентифікації користувачів у розумному будинку допоможе створити зручну, безпечну та інтуїтивно зрозумілу систему для користувачів. Це покращить їхній досвід користування розумним будинком та забезпечить ефективне управління доступом, енергоефективність та автоматизацію різних систем та пристроїв у розумному будинку.

При розробці такої комплексної математичної моделі важливо також зосередитися на забезпеченні інтероперабельності між різними пристроями та платформами, щоб уникнути обмежень, пов'язаних з використанням пропрієтарних технологій або некомпатибільності пристроїв. Це дозволить забезпечити гладке взаємодію між різними компонентами розумного будинку та сприяти широкому впровадженню інтелектуальних технологій в різних секторах життя.

Окрім того, враховуйте правила та стандарти приватності та захисту даних, такі як GDPR або інші відповідні національні та міжнародні регулювання, щоб забезпечити належний рівень захисту особистих даних користувачів.

На заключний етап розробки такої комплексної математичної моделі підсистеми ідентифікації користувачів розумного будинку важливо провести ретельне тестування та валідацію моделі для забезпечення її надійності та точності. Це може включати випробування на різних сценаріях, перевірку роботи моделі з різними пристроями та платформами, а також відпрацювання процесів виявлення та реагування на можливі проблеми.

Побудова математичної моделі процесу ідентифікації користувача кіберфізичної системи на основі зібраних даних та статистичного аналізу може бути проведена в кілька етапів:

1) визначення вектору ознак: на цьому етапі вибираються показники, що впливають на процес ідентифікації користувача. Наприклад, для ідентифікації людини за обличчям можуть використовуватися такі ознаки, як форма обличчя, розмір і положення очей, ніс та рот;

2) побудова навчальної вибірки: для цього зібрані дані про користувачів системи за певний період часу. Вибірка повинна бути достатньою, щоб мати можливість побудувати достовірну математичну модель. Наприклад, якщо для ідентифікації користувача використовується голосовий ідентифікатор, то для побудови моделі необхідно мати достатньо записів голосу кожного користувача;

3) використання методів машинного навчання: на цьому етапі використовуються методи машинного навчання, такі як навчання з вчителем, навчання без вчителя або підсилене навчання. За допомогою цих методів

формується математична модель, яка може передбачати ідентифікацію користувача на основі вектора ознак;

4) тестування моделі: після побудови моделі необхідно протестувати її на нових даних. Для цього можна використовувати тестову вибірку, яка не використовувалася для побудови моделі. Також можна використовувати метрики точності, такі як чутливість, специфічність, точність та F-міра, для оцінки стійкості та точності моделі.

Після успішного тестування моделі на нових даних можна використовувати її для ідентифікації користувачів кіберфізичної системи. Однак, слід пам'ятати, що ніяка математична модель не є 100% точною, тому важливо забезпечувати безпеку кіберфізичної системи і використовувати додаткові методи аутентифікації та захисту, такі як паролі, ключі доступу та двофакторна аутентифікація.

2.2 Розгляд варіантів взаємодії між підсистемами «Розумний будинок» та ідентифікації користувача

Ідентифікація користувача є важливим елементом в системі «Розумний будинок», оскільки дозволяє забезпечити безпеку та персоналізацію різних функцій. Розглянемо деякі варіанти взаємодії між підсистемами «Розумний будинок». та ідентифікацією користувача:

2.2.1 Візуальне розпізнавання обличчя

Цей метод можна використовувати для ідентифікації користувачів при вході в будинок або певних кімнат. Система може зберігати зображення облич користувачів, які мають доступ до будинку або до певних зон в будинку. Коли користувач підходить до камери входу, система може порівняти його обличчя з зображеннями, що зберігаються у системі. Якщо система розпізнає користувача, вона може надати доступ до будинку або певних зон.

Візуальне розпізнавання обличчя є одним з методів ідентифікації користувача в системі «Розумний будинок». Для цього можуть бути використані камери відеоспостереження, які розміщені в приміщеннях будинку. Основні етапи реалізації візуального розпізнавання обличчя в системі «Розумний будинок». включають наступне:

1) збір відеоданих: камери відеоспостереження збирають відеодані з приміщень будинку;

2) обробка відеоданих: відеодані піддаються обробці для визначення обличчя користувача;

3) виділення рис обличчя: система виокремлює особливі риси обличчя, такі як очі, ніс, рот, які використовуються для подальшої ідентифікації;

4) порівняння зі збереженими образами: система порівнює отримані риси обличчя зі збереженими образами обличчя користувачів, які заздалегідь були занесені в базу даних;

5) прийняття рішення: на основі порівняння система приймає рішення щодо ідентифікації користувача та відповідної реакції системи.

Важливим етапом реалізації візуального розпізнавання обличчя є збереження образів обличь користувачів в базу даних, що потребує забезпечення конфіденційності та безпеки даних. Також необхідно враховувати можливість помилок при ідентифікації, пов'язаних зі зміною вигляду обличчя користувача (наприклад, зміна зачіски, використання окулярів тощо) або зі змінними умовами освітлення приміщення.

2.2.2 Біометричний ідентифікатор голосу

Цей метод можна використовувати для ідентифікації користувачів, коли вони звертаються до системи з голосовими командами. Кожен користувач може навчити систему розпізнавати його голос, щоб отримувати персоналізовані відповіді на свої запити.

Біометричний ідентифікатор голосу - це метод ідентифікації користувача за характеристиками його голосу. Для реалізації цього методу в системі «Розумний будинок». можуть використовуватися мікрофони, які збирають звукові дані, що аналізуються на наявність унікальних характеристик голосу.

Основні переваги біометричного ідентифікатора голосу полягають у тому, що він може бути використаний навіть у випадку, якщо користувач не може бути фізично присутній біля пристрою для ідентифікації. Крім того, цей метод не потребує додаткового обладнання, такого як камери або сканери відбитків пальців, що робить його зручним для використання в повсякденному житті.

Процес ідентифікації користувача за голосом може бути реалізований за допомогою алгоритмів машинного навчання, які дозволяють аналізувати вхідні звукові дані та порівнювати їх зі збереженими характеристиками голосу користувачів, що вже ідентифіковані в системі. Оптимальна точність ідентифікації може бути досягнута шляхом оптимізації алгоритмів та використання достатньої кількості зразків голосу для навчання моделей машинного навчання.

2.2.3 Фізіологічні методи

Іншим варіантом може бути використання фізіологічних методів, таких як сканування відбитків пальців або ретини ока. Кожен користувач може зареєструвати свої відбитки пальців або сканування ретини ока в системі, що дозволяє ідентифікувати його при доступі до будинку або певних зон в будинку.

Фізіологічні методи ідентифікації користувача в системі «Розумний будинок». можуть включати такі параметри, як відбитки пальців, сканування радужної оболонки ока, відбитки долоні, сканування жилки під шкірою та інші. Ці методи базуються на унікальних фізіологічних з високою точністю.

Характеристиках кожної людини, що дозволяє ідентифікувати користувача Взаємодія між підсистемами «Розумний будинок». та фізіологічними методами ідентифікації користувача може бути реалізована шляхом встановлення датчиків, які зчитують фізіологічні параметри користувача, та їх подальшої обробки та

порівняння з даними, збереженими у системі. Для цього можуть використовуватися спеціальні алгоритми, які забезпечують високу точність ідентифікації та захист від шахрайства.

2.2.4 Датчики присутності

Іншим варіантом може бути використання датчиків присутності для ідентифікації користувача розміщені в різних місцях будинку, таких як вхідні двері, вікна, кімнати та інші зони, які потребують контролю доступу та активують інші методи ідентифікації користувача.

Датчики присутності можуть бути використані для ідентифікації користувача в системі «Розумний будинок». Датчики присутності можуть визначати, чи знаходиться людина в певній кімнаті або в певній зоні будинку, і дозволяти системі приймати рішення щодо доступу до певних функцій.

Наприклад, якщо система «Розумний будинок». має функцію контролю доступу до певних приміщень або пристроїв, датчики присутності можуть використовуватися для ідентифікації того, хто знаходиться в цих зонах, і дозволяти або забороняти доступ до цих приміщень або пристроїв в залежності від наявності авторизації.

Також, датчики присутності можуть бути використані для персоналізації налаштувань системи в залежності від поточного користувача. Наприклад, система може автоматично змінювати налаштування освітлення, температури або звуку в залежності від того, хто перебуває в кімнаті.

Отже, датчики присутності можуть допомогти системі «Розумний будинок». в ідентифікації користувача та забезпеченні безпеки та персоналізації різних функцій.

2.3 Розробка алгоритмів та процедур для реалізації процесу ідентифікації користувача

Розробка алгоритмів та процедур для реалізації процесу ідентифікації користувача є важливим етапом в розробці системи «Розумний будинок». Для цього можна використовувати різноманітні методи біометричної ідентифікації, такі як розпізнавання обличчя, відбитків пальців, голосу, ретини та інші.

Основні етапи розробки алгоритмів та процедур для ідентифікації користувача в системі «Розумний будинок».

2.3.1 Вибір методів ідентифікації

Необхідно визначитися з тими методами біометричної ідентифікації, які будуть використовуватися в системі, з урахуванням особливостей обраної архітектури системи та конкретних умов експлуатації.

Вибір методів біометричної ідентифікації для нашої системи будемо використовувати (ґідентифікація голосом та обличчя)ґ разом з паролем може бути ефективним варіантом для забезпечення безпеки та персоналізації системи «Розумний будинок». Проте, перед розробкою алгоритмів та процедур для реалізації процесу ідентифікації користувача, необхідно провести оцінку технічних та функціональних вимог до системи, а також врахувати потенційні ризики та можливість шахрайства.

Щодо ідентифікації голосом, можна використовувати методи акустичної моделі голосу, які базуються на вимірюванні фізичних характеристик голосу, таких як тон, інтонація та частота голосу. При цьому, необхідно забезпечити надійність і точність розпізнавання голосу в різних умовах (наприклад, з урахуванням шуму, різного віку, статі тощо).

Ідентифікація обличчя, у свою чергу, може базуватися на методах візуального аналізу, які використовуються для виявлення та розпізнавання ключових рис обличчя. Цей метод може бути ефективним, якщо в системі будуть

використовуватися камери високої якості з високим розширенням та швидкістю реакції.

Однак, незважаючи на переваги цих методів, необхідно також забезпечити можливість використання пароля, який може бути використаний в якості альтернативного методу ідентифікації користувача. Для цього необхідно розробити відповідні процедури перевірки пароля, які забезпечать високий рівень безпеки системи.

2.3.2 Збір даних

Необхідно зібрати достатню кількість даних для побудови математичної моделі та використання її для ідентифікації користувача.

Збір даних є важливим етапом при розробці системи ідентифікації користувача. Для розробки ефективної математичної моделі необхідно зібрати достатню кількість даних, які будуть використовуватися для тренування алгоритмів машинного навчання.

У випадку біометричної ідентифікації голосом та обличчя, необхідно зібрати зразки голосу та зображення обличчя користувачів. Для кожного користувача необхідно зібрати достатню кількість зразків, щоб математична модель була ефективною. Наприклад, для ідентифікації голосу необхідно записати декілька фраз, які будуть використовуватися для ідентифікації, в різних умовах (з різними шумами, в різний час доби, тощо).

При створенні математичної моделі для збору даних програми ідентифікації голосу, вам потрібно враховувати різні аспекти, такі як характеристики сигналу голосу, шумові забруднення, індивідуальні особливості голосу та інше.

Ось приклад такої математичної моделі:

1. Попередня обробка сигналу голосу:

Фільтрація шуму:

$$H(w) = \frac{Y(w)}{X(w)}, \quad (2.14)$$

де H(w) - передаточна функція фільтра;

Y(w) - вихідний сигнал голосу;

X(w) - вхідний сигнал голосу.

Підвищення частоти дискретизації:

$$y(n) = x\left(n \cdot \frac{L}{M}\right), \quad (2.15)$$

де y(n) - сигнал з підвищеною частотою дискретизації;

x(n) - початковий сигнал голосу;

L та M - коефіцієнти інтерполяції та децимації.

2. Виділення характеристик сигналу голосу:

Оцінка основного тонального періоду (фундаментальної частоти) голосу:

$$F0(n) = argmax \cdot R\_x(\tau), \quad (2.16)$$

де R_x(τ) - автокореляційна функція сигналу голосу;

τ - затримка часу.

Виділення спектральних характеристик (наприклад, мел-частотні кепстральні коефіцієнти (MFCC)):

$$MFCC(k) = \sum n \left[\log\left(S(n,k)\right) \cdot \cos\left(\pi \cdot \left(k - \frac{1}{2}\right) \cdot \frac{n}{N}\right)\right], \quad (2.17)$$

де S(n, k) - спектрограма сигналу голосу;

N - кількість точок у спектрограмі.

3. Моделювання статистичних розподілів характеристик голосу.

Гауссівська суміш моделей (GMM):

$$p(x) = \sum\_i w\_i \cdot N(x \mid \mu\_i, \sum\_i), \quad (2.18)$$

де x - вектор характеристик голосу;

w_i - ваги компонентів суміші;

N(x | μ_i, Σ_i) - багатовимірний нормальний розподіл з параметрами μ_i (математичне сподівання) та Σ_i (коваріаційна матриця).

4. Класифікація та ідентифікація голосу:

Використання алгоритмів машинного навчання, таких як опорні векторні машини (SVM) або нейронні мережі (NN), для класифікації та ідентифікації голосу на основі виділених характеристик:

$$y = f(x, \theta), \quad (2.19)$$

де y - мітка класу голосу;

x - вектор характеристик голосу;

θ - параметри моделі машинного навчання (наприклад, ваги нейронної мережі або рішаюча межа для опорних векторних машин).

5. Оцінка та оптимізація якості моделі:

Використання метрик оцінки якості, таких як точність (accuracy), повнота (recall), F1-міра (F1-score) тощо, для оцінки ефективності розробленої математичної моделі.

Застосування технік оптимізації гіперпараметрів, таких як решітчатий пошук (grid search) або випадковий пошук (random search), для покращення якості моделі.

Ця комплексна математична модель охоплює всі етапи розробки системи ідентифікації голосу від попередньої обробки сигналу до оцінки та оптимізації моделі. За допомогою цієї моделі можна розробити ефективну та надійну систему ідентифікації голосу для застосування в розумному будинку.

Створення математичної моделі для збору даних програми розпізнавання обличчя включає кілька етапів, таких як попередня обробка зображення, виявлення

обличчя, вирівнювання обличчя, витягування ознак та класифікація. Давайте розглянемо кожен етап:

1. Попередня обробка зображення:

Перетворення зображення з кольорового до сірого масштабу:

$$I\_gray = 0.299 \cdot R + 0.587 \cdot G + 0.114 \cdot B, \quad (2.20)$$

де R, G, B - масиви інтенсивності червоного, зеленого та синього каналів відповідно.

Застосування фільтрації для зменшення шуму:

$$I\_filtered = F(I\_gray), \quad (2.21)$$

де F - фільтр (наприклад, Гауссовий або медіанний).

2. Виявлення обличчя:

Виявлення області обличчя за допомогою алгоритмів виявлення об'єктів, таких як Viola-Jones або глибокі нейронні мережі:

$$face\_bbox = D(I\_filered), \quad (2.22)$$

де D - алгоритм виявлення обличчя;

face_bbox - координати прямокутника, що охоплює обличчя.

3. Вирівнювання обличчя:

Вирівнювання зображення обличчя з врахуванням положення очей, носа та рота:

$$I\_aligned = A(I\_filtered, face\_bbox, facial\_landmarks), \quad (2.23)$$

де A - алгоритм вирівнювання обличчя;

facial_landmarks - координати характерних точок обличчя (наприклад, кутики очей, ніс, рот).

4. Витягування ознак:

Витягування характеристик обличчя за допомогою методів, таких як PCA (головні компоненти), LBP (локальні бінарні візерунки) або глибокі нейронні мережі:

$$features = E(I\_aligned), \tag{2.24}$$

де E - алгоритм витягування ознак.

5. Класифікація:

Використання алгоритмів машинного навчання, таких як k-найближчих сусідів (k-NN), опорних векторів машин (SVM), або глибоких нейронних мереж, для порівняння та класифікації характеристик обличчя:

$$identity = C(features, training\_data), \tag{2.25}$$

де C - алгоритм класифікації;

training_data - набір даних з ознаками та відповідними мітками класів для навчання класифікатора;

identity - ідентифікований клас або користувач.

6. Для створення математичної моделі, що об'єднує всі ці етапи, можна записати модель у вигляді послідовності функцій:

$$identity = C(E(A(D(F(I\_gray), face\_bbox, facial\_landmarks)), training\_data), \tag{2.26}$$

Ця модель представляє загальний підхід до створення системи розпізнавання обличчя, яка може бути адаптована до конкретних вимог та обмежень кіберфізичної системи «Розумний будинок». В залежності від конкретної

реалізації, різні алгоритми можуть бути використані для кожного етапу, і додаткові кроки можуть бути внесені для покращення ефективності та надійності системи.

Для створення математичної моделі збору даних програми розпізнавання відбитків пальців можна розглянути такі етапи:

1. Захоплення зображення відбитка пальця:

$$Z = capture(fingerprint\_sensor), \quad (2.27)$$

де Z - зображення відбитка пальця, отримане від сенсора fingerprint_sensor.

2. Попередня обробка зображення:

$$P = preprocess(Z), \quad (2.28)$$

де P - попередньо оброблене зображення відбитка пальця, яке може включати корекцію контрасту, видалення шуму та інші операції, щоб підготувати зображення до подальшої обробки.

3. Виділення характеристик відбитка пальця:

$$F = extract\_features(P), \quad (2.29)$$

де F - набір характеристик відбитка пальця, таких як сідла, гілки, відрізки тощо.

Збір даних для програми розпізнавання відбитків пальців полягає у створенні набору даних, який складається зі зразків відбитків пальців різних користувачів та їх відповідних ідентифікаторів.

Математична модель для збору даних може бути представлена як послідовність функцій:

$$F\_i = extract\_features \cdot (preprocess(capture(fingerprint\_sensor\_i))), \quad (2.30)$$

де F_i - набір характеристик відбитка пальця і-го користувача, отриманий від сенсора fingerprint_sensor_i.

Після отримання характеристик для кожного користувача, вони можуть бути зібрані у набір даних для подальшого використання в системі розпізнавання відбитків пальців.

Для створення математичної моделі збору даних програми розпізнавання сітківки ока можна розглянути такі етапи:

1. Захоплення зображення сітківки ока:

$$R = capture(retina\_scanner), \tag{2.31}$$

де R - зображення сітківки ока, отримане від сканера retina_scanner.

2. Попередня обробка зображення:

$$P = preprocess(R), \tag{2.32}$$

де P - попередньо оброблене зображення сітківки ока, яке може включати корекцію контрасту, видалення шуму та інші операції, щоб підготувати зображення до подальшої обробки.

3. Виділення характеристик сітківки ока:

$$F = extract\_features(P), \tag{2.33}$$

де F - набір характеристик сітківки ока, таких як кільця та кластери капілярів.

Збір даних для програми розпізнавання сітківки ока полягає у створенні набору даних, який складається зі зразків сітківок ока різних користувачів та їх відповідних ідентифікаторів.

Математична модель для збору даних може бути представлена як послідовність функцій:

$$(F\_i = extract\_features(preprocess(capture(retina\_scanner\_i))), \quad (2.34)$$

де F_i - набір характеристик сітківки ока і-го користувача, отриманий від сканера retina_scanner_i.

Після отримання характеристик для кожного користувача, вони можуть бути зібрані у набір даних для подальшого використання в системі розпізнавання сітківки ока.

Для ідентифікації за допомогою пароля, необхідно зберігати хеші паролів користувачів в базі даних.

При введенні пароля користувачем, його пароль буде перевірятися на відповідність збереженому хешу в базі даних.

Збір даних може бути проведений за допомогою спеціальних датчиків та камер, які будуть встановлені в приміщеннях. Також можливо використовувати існуючі джерела даних, наприклад, відео- та аудіозаписи з камер та мікрофонів, які вже встановлені в приміщенні.

Важливо забезпечити безпеку та конфіденційність зібраних даних. Для цього можна використовувати різні методи шифрування, доступ до даних повинен бути обмежений та захищений від несанкціонованого доступу.

2.3.3 Перед процеси даних

Для поліпшення точності процесу ідентифікації необхідно провести перед процеси даних, такий як фільтрація шуму, видалення артефактів та інших забруднень.

Існує декілька способів фільтрації шуму та видалення артефактів в зібраних даних для поліпшення точності ідентифікації користувача. Деякі з них:

1. Фільтрація за допомогою середньої або медіанної фільтрації: ці методи полягають у використанні статистичного аналізу для вилучення шуму та артефактів зі зібраних даних.

Середня фільтрація:

Цей метод фільтрації передбачає розрахунок середнього значення в околі пікселів зображення. Математична модель для середнього фільтра може бути представлена наступним чином:

Припустимо, що I(x, y) - це вхідне зображення, де x та y - координати пікселів. Окіл розміру k × k для пікселя I(x, y) можна представити як:

$$N(x,y) = \{I(x+i,y+j)| -\frac{k}{2} \leq i,j \leq \frac{k}{2}\}. \quad (2.35)$$

Середнє значення N(x, y) обчислюється як:

$$M(x,y) = \frac{1}{k^2} \cdot \sum\sum I(x+i,y+j), \quad (2.36)$$

де сума береться по i та j від -k/2 до k/2. Фільтроване зображення отримується шляхом заміни кожного пікселя I(x, y) на M(x, y).

Медіанна фільтрація:

Цей метод фільтрації передбачає визначення медіани в околі пікселів зображення. Математична модель для медіанного фільтра може бути представлена наступним чином:

Припустимо, що I(x, y) - це вхідне зображення, де x та y - координати пікселів. Окіл розміру k × k для пікселя I(x, y) можна представити як:

$$N(x,y) = \{I(x+i,y+j)| -\frac{k}{2} \leq i,j \leq \frac{k}{2}\}. \quad (2.37)$$

Медіана значень N(x, y) обчислюється як:

$$Med(x,y) = median\big(N(x,y)\big), \quad (2.38)$$

де median - це значення, яке розділяє впорядкований набір даних на дві рівні частини. Фільтроване зображення отримується шляхом заміни кожного пікселя I(x, y) на Med(x, y).

2. Видалення забруднень за допомогою кластерного аналізу: цей метод полягає в групуванні даних за схожістю та вилученні забруднень, які не відповідають визначеним кластерам.

3. Видалення артефактів за допомогою фільтрації Калмана: цей метод використовує математичну модель для відновлення оцінки сигналу та вилучення артефактів.

Фільтр Калмана - це оптимальний рекурсивний фільтр, що забезпечує оцінки стану динамічної системи, мінімізуючи середньоквадратичну помилку. Фільтр Калмана може бути використаний для видалення артефактів із зображень або сигналів.

Припустимо, що ми маємо послідовність даних X(t) з артефактами, де t - часовий індекс. Метою є оцінити "істинний" сигнал Y(t), використовуючи фільтрацію Калмана. Математична модель фільтрації Калмана може бути описана наступним чином:

Динамічну модель системи:

$$Y(t) = A \cdot Y(t-1) + B \cdot U(t) + w(t), \quad (2.39)$$

де A - матриця переходу стану;

Y(t-1) - попередній стан системи;

B - матриця керування;

U(t) - вектор керування;

w(t) - вектор шуму процесу з коваріаційною матрицею Q.

Визначте модель спостереження:

$$X(t) = H \cdot Y(t) + v(t), \quad (2.40)$$

де H - матриця спостереження;

Y(t) - поточний стан системи;

v(t) - вектор шуму спостереження з коваріаційною матрицею R.

Ініціалізуйте фільтр Калмана з початковими значеннями Y(0) та коваріаційною матрицею P(0).

Алгоритм фільтра Калмана, який складається з двох етапів:

а) Етап прогнозу:

$$Y'(t) = A \ * \ Y(t-1) + B * U(t), \quad (2.41)$$

$$P'(t) = \ A * P(t-1) * A\hat{}T + Q. \quad (2.42)$$

б) Етап корекції:

$$K(t) = P'(t) \cdot H^T \cdot (H * P'(t) \cdot H^T + R)^{-1}, \quad (2.44)$$

$$Y(t) = Y'(t) + K(t) \cdot \ (X(t) - H \cdot Y'(t)), \quad (2.45)$$

$$P(t) = (I - K(t) \cdot H) \cdot P'(t), \quad (2.46)$$

де Y'(t) та P'(t) - прогнозовані значення стану та коваріаційної матриці;

K(t) - матриця коефіцієнтів Калмана;

I - одинична матриця.

Повторюються кроки а) та б) для кожного спостереження X(t) в послідовності даних.

Вихідним сигналом фільтра Калмана є оцінка "істинного" сигналу Y(t) без артефактів.

Таким чином, фільтр Калмана може бути використаний для видалення артефактів з послідовності даних, забезпечуючи оптимальну оцінку сигналу на основі динамічної моделі системи та моделі спостереження.

Зауважте, що ефективність видалення артефактів за допомогою фільтра Калмана залежить від правильної моделі системи та властивостей шуму.

4. Використання методів машинного навчання: цей метод використовує навчання на основі попередньо зібраних даних та створення моделі, яка може відрізняти шум від корисних сигналів.

Вибір конкретного методу залежить від типу даних, що збираються, а також від конкретних умов експлуатації системи ідентифікації користувача.

2.3.4 Можливість використання методів машинного навчання

Для побудови математичної моделі та забезпечення точності ідентифікації користувача можна використовувати методи машинного навчання, такі як нейронні мережі, SVM та інші.

Для використання методів машинного навчання для побудови математичної моделі ідентифікації користувача, необхідно спочатку підготувати дані та навчити модель.

Підготовка даних включає в себе збір необхідних даних, очищення та обробку даних, а також розбиття даних на тренувальний та тестовий набори.

Після цього необхідно вибрати та навчити модель машинного навчання. Для цього можна використовувати різні методи машинного навчання, такі як нейронні мережі, SVM та інші.

Після навчання моделі необхідно провести її валідацію на тестовому наборі та провести оцінку точності моделі.

Отриману модель можна використовувати для ідентифікації користувача на основі вхідних даних, таких як голосові, обличчя та пароль.

Використання методів машинного навчання є досить ефективним підходом до розв'язання задачі ідентифікації користувача. Наприклад, нейронні мережі можуть бути використані для аналізу голосу чи обличчя користувача, SVM може використовуватися для класифікації даних і т.д. Проте важливо враховувати, що для успішної реалізації методів машинного навчання потрібно мати достатню кількість даних для навчання моделі та налагодження параметрів алгоритмів.

Також потрібно відслідковувати можливі перекриття ідентифікаторів користувачів та забезпечувати адекватність відповіді системи на такі випадки.

2.4 Висновок

В даному розділі ми розглянули математичні моделі обробки, покращення та фільтрації вхідних даних в систему ідентифікації.

На основі розглянутих математичних моделей створили математичну модель підсистеми ідентифікації користувача РБ, яку будемо використовувати про подальшій розробці.

3. МЕТОД ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА КІБЕРФІЗИЧНОЇ СИСТЕМИ «РОЗУМНИЙ БУДИНОК»

3.1 Визначення вимог до методу ідентифікації користувача

Для ефективного та точного визначення методу ідентифікації користувача необхідно визначити наступні вимоги:

1. Надійність і точність ідентифікації користувача.
2. Швидкість ідентифікації користувача.
3. Масштабованість методу ідентифікації користувача.
4. Зручність та легкість використання методу ідентифікації користувача для забезпечення комфорту користувачів.
5. Захищеність від зловживання користувачами та зловмисниками.
6. Сумісність з існуючими системами безпеки в будинку.

Розглянемо детальніше вище вказані вимоги.

3.1.1 Надійність і точність ідентифікації користувача

Надійність та точність ідентифікації користувача є ключовими вимогами до методу ідентифікації в кіберфізичній системі «Розумний будинок». Надійність визначається як здатність методу визначати коректного користувача при кожному використанні системи, тобто відсутність помилок та фальшивих результатів. Точність визначається як здатність методу давати правильні результати, які максимально відповідають дійсності.

Для досягнення високої надійності та точності ідентифікації користувача необхідно враховувати наступні фактори:

1. Використання надійних технологій ідентифікації, таких як відбитки пальців, розпізнавання обличчя, розпізнавання голосу тощо.
2. Забезпечення безпеки даних користувачів та ідентифікаційної системи, що забезпечує виключення можливості несанкціонованого доступу до даних.

3. Використання кількох методів ідентифікації для забезпечення вищої точності та зменшення ризику помилки.

4. Оцінка та вдосконалення методу ідентифікації на основі статистичних даних, отриманих з використанням системи протягом тривалого часу.

5. Застосування алгоритмів машинного навчання та штучного інтелекту для автоматичного виявлення та виправлення помилок в процесі ідентифікації користувача.

3.1.2 Швидкість ідентифікації користувача

Швидкість ідентифікації користувача - це ще одна важлива вимога до методу ідентифікації в кіберфізичній системі «Розумний будинок». Швидкість ідентифікації повинна бути достатньою для того, щоб не створювати затримок в роботі системи, особливо у випадку аварійних ситуацій, коли потрібно швидко визначити, хто знаходиться в будинку.

Однак, в той же час, швидкість ідентифікації не повинна негативно впливати на точність та надійність ідентифікації користувача. Таким чином, необхідно забезпечити баланс між швидкістю і точністю.

Для досягнення швидкості ідентифікації користувача можуть використовуватись такі методи, як сканування відбитків пальців, розпізнавання обличчя, розпізнавання голосу або використання RFID-карток. Крім того, можна використовувати розподілену обчислювальну систему для прискорення обробки даних ідентифікації.

3.1.3 Масштабованість методу ідентифікації користувача

Щодо масштабованості методу ідентифікації користувача, важливо мати на увазі можливість розширення кількості користувачів, яких система може ідентифікувати, без значного погіршення швидкості та надійності ідентифікації. Крім того, метод повинен бути масштабований відносно різних типів датчиків і

пристроїв, що використовуються в системі. Наприклад, метод ідентифікації повинен бути здатний працювати з різними типами біометричних даних, таких як відбитки пальців, обличчя або голос. До вимог до масштабованості також можна віднести здатність методу працювати з різними типами пристроїв, таких як сенсорні екрани, клавіатури, мікрофони тощо.

3.1.4 Зручність та легкість використання методу ідентифікації користувача для забезпечення комфорту користувачів

Зручність та легкість використання методу ідентифікації користувача є дуже важливою вимогою для забезпечення комфорту користувачів кіберфізичної системи «Розумний будинок». Метод ідентифікації повинен бути простим та зрозумілим для користувача, не вимагати від нього складних дій та процедур. Крім того, метод повинен бути гнучким та адаптивним до різних потреб користувачів, щоб забезпечити їм максимальний комфорт та зручність у використанні кіберфізичної системи.

Наприклад, одним зі способів забезпечення зручності та легкості використання методу ідентифікації може бути використання технологій розпізнавання обличчя, відбитків пальців або голосу, які є зручними для багатьох користувачів та не вимагають від них додаткових зусиль. Крім того, метод повинен бути таким, щоб користувачі могли легко додавати нові облікові записи, видаляти їх та змінювати параметри ідентифікації без необхідності використання складних інтерфейсів та процедур.

3.1.5 Захищеність від зловживання користувачами та зловмисниками

Щоб забезпечити захищеність від зловживання користувачами та зловмисниками, метод ідентифікації користувача повинен відповідати наступним вимогам:

1) необхідна аутентифікація користувача перед початком використання системи. Для цього можуть використовуватись паролі, підписи, біометричні дані тощо;

2) необхідно контролювати доступ до системи та її функцій. Для цього можна використовувати різні рівні доступу, наприклад, адміністраторський та користувацький;

3) необхідно відслідковувати та контролювати дії користувачів у системі. Наприклад, вести журнал подій або моніторинг доступу до різних функцій системи;

4) метод ідентифікації повинен бути стійким до атак, таких як підбір паролю, фішинг, деніал-оф-сервіс, віруси та інші;

5) метод ідентифікації повинен бути оновлюваним та масштабованим, щоб забезпечити захист від нових загроз, а також для можливості розширення функціональності системи;

6) повинна бути забезпечена конфіденційність даних користувача, що використовуються для ідентифікації. Для цього можуть використовуватись різні методи шифрування та зберігання даних в безпечних місцях.

3.1.6 Сумісність з існуючими системами безпеки в будинку.

Однією з вимог до методу ідентифікації користувача кіберфізичної системи «Розумний будинок». є його сумісність з існуючими системами безпеки в будинку. Це означає, що метод ідентифікації повинен бути здатним інтегруватись з іншими системами безпеки в будинку, наприклад з системами контролю доступу або системами відеоспостереження, щоб забезпечити єдину систему безпеки зі зв'язком між компонентами.

Це важливо для забезпечення безпеки в будинку і запобігання можливих кібератак або зловживань користувачами. Якщо метод ідентифікації не є сумісним з існуючими системами безпеки, це може створити додаткові уразливості в системі, що можуть бути використані зловмисниками для доступу до будинку або

зловживання користувачами для отримання неприпустимого доступу до певних функцій системи «Розумний будинок».

Отже, сумісність з існуючими системами безпеки в будинку є важливою вимогою до методу ідентифікації користувача кіберфізичної системи «Розумний будинок».

3.2. Вибір оптимального методу ідентифікації

Для реалізації методу ідентифікації користувача в підсистемі кіберфізичної системи «Розумний будинок» можна використовувати різні технології та пристрої, залежно від вимог та потреб користувачів.

Реалізація методу ідентифікації користувача в підсистемі кіберфізичної системи «Розумний будинок» може бути здійснена за допомогою розпізнавання обличчя, голосу, відбитку пальця та паролю, або комбінації цих методів для підвищення рівня безпеки та точності ідентифікації користувача.

3.2.1 Розпізнавання обличчя

Розпізнавання обличчя передбачає використання камери, що знаходиться в розумному будинку, для захоплення зображення обличчя користувача та подальшого порівняння його з вже збереженими в базі даних зображеннями обличчями ідентифікованих користувачів.

Розташування камери в розумному будинку може бути важливим аспектом при використанні розпізнавання обличчя для ідентифікації користувачів. Крім того, важливо врахувати конфіденційність користувача та його приватність, тому камера не повинна бути спрямована на області приватних просторів, таких як спальні чи ванні кімнати.

Розташування камери для розпізнавання обличчя залежить від конкретного випадку використання. У разі використання розумного телефону як ключа до розумного будинку, камера може розташовуватися на фронтальній частині

телефону для зйомки обличчя користувача при вході до будинку. У разі використання розумної камери в розумному будинку, камера може бути розташована на вхідних дверях або на стелі, щоб забезпечити максимальний охоплюючий кут зйомки. Важливо забезпечити, щоб камера була розташована в такому місці, щоб забезпечити оптимальну якість зображення обличчя та захист від зовнішнього освітлення та перешкод. Також важливо врахувати вимоги до захисту персональних даних, щоб забезпечити конфіденційність даних користувачів та захист від зловживань.

3.2.2 Розпізнавання голосу та відбиток пальця

Розпізнавання голосу та відбиток пальця також можуть бути використані для ідентифікації користувачів. Для голосового розпізнавання можуть використовуватись мікрофони, розташовані в розумному будинку, а для відбитку пальця - сканер відбитків пальців, що може бути встановлений на вхідній двері чи інших важливих місцях в будинку.

Також важливим аспектом реалізації методу ідентифікації користувача є його сумісність з існуючими системами безпеки в будинку. Наприклад, якщо в будинку вже встановлена система відеоспостереження з камерами, то використання цих камер для розпізнавання обличчя користувачів може бути ефективним рішенням. Однак, при використанні існуючих систем безпеки важливо врахувати їхню сумісність з системою ідентифікації користувачів та забезпечити відповідний рівень захисту від несанкціонованого доступу

Розпізнавання голосу передбачає використання мікрофона для запису голосу користувача та подальшого порівняння з вже збереженими в базі даних голосовими зразками ідентифікованих користувачів.

Розпізнавання відбитку пальця передбачає використання датчика відбитків пальців для отримання відбитка пальця та його подальшого порівняння з вже збереженими в базі даних відбитків пальців ідентифікованих користувачів.

Для забезпечення додаткового рівня безпеки може бути використаний метод ідентифікації за допомогою пароля, який може бути введений користувачем на клавіатурі або на смартфоні за допомогою спеціального додатку.

Підсистема ідентифікації користувача в кіберфізичній системі «Розумний будинок» повинна бути реалізована з урахуванням вимог до зручності та легкості використання для забезпечення комфорту користувачів, а також з урахуванням вимог до захищеності від зловживання користувачами та зловмисників.

3.3. Проектування алгоритмів та програмного забезпечення для обробки даних із апаратних компонентів

На рисунку 3.1 показано блок-схему яка відображає загальний процес обробки даних із апаратних компонентів:

1) збір даних. Зчитування даних від апаратних компонентів (камера, мікрофон, сенсор відбитків пальців, пристрій введення паролів) ;

2) попередня обробка даних. На цьому етапі збираються дані з різних апаратних компонентів, таких як камери, мікрофони, сенсори відбитків пальців та пристрої для введення паролів. Дані очищуються від шуму, нормалізуються та приводяться до стандартного формату;

3) визначення особливостей. На основі попередня обробка даних, алгоритми виявляють ключові характеристики (особливості) для кожного методу ідентифікації. Наприклад, для розпізнавання обличчя можуть використовуватися особливості, пов'язані з формою та розташуванням основних елементів обличчя (очі, ніс, рот). Для голосової ідентифікації можуть використовуватися особливості, пов'язані з тембром, висотою та інтонацією голосу користувача;

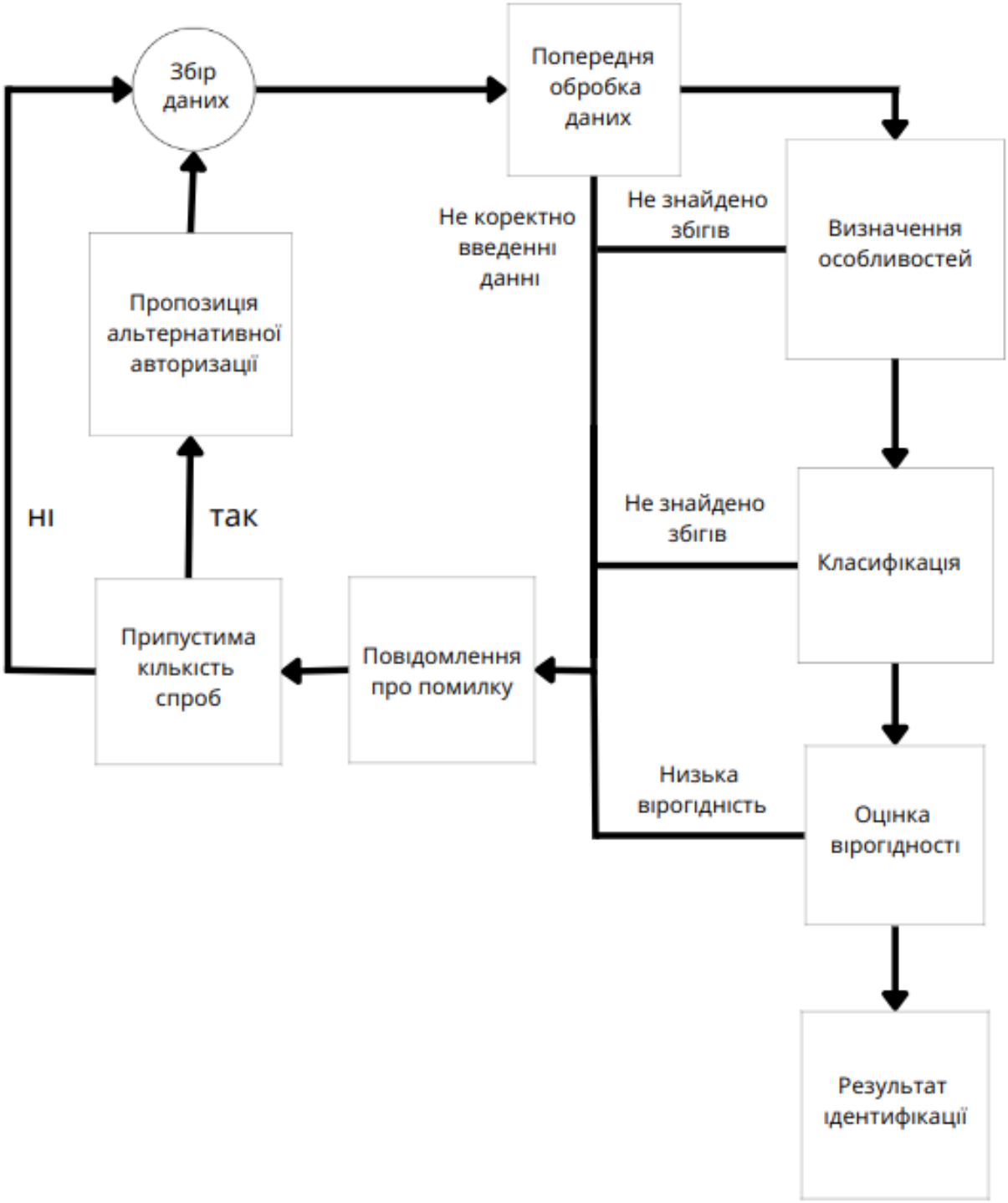


Рисунок 3.1 Загальний процес обробки даних із апаратних компонентів

4) класифікація та сумісність. Застосовуються алгоритми класифікації для визначення ступеня схожості між отриманими особливостями та збереженими шаблонами користувачів. За результатами порівняння визначається, якому користувачеві відповідають введені дані;

5) оцінка вірогідності. На основі аналізу сумісності, алгоритми оцінюють вірогідність ідентифікації. Якщо вірогідність перевищує певний поріг, користувач вважається ідентифікованим.

3.4 Адаптація системи ідентифікації до різних сценаріїв використання та умов

Інтеграція методу ідентифікації у кіберфізичну систему «Розумний будинок». та налаштування порядку використання різних методів ідентифікації та параметрів розпізнавання передбачають ретельний аналіз потреб користувачів, вибір оптимальних методів, розробку алгоритмів, тестування та постійне оновлення системи для забезпечення максимальної зручності та безпеки.

3.4.1 Визначення потреб користувачів

Введемо систему ідентифікації, яка використовує розпізнавання обличчя та голосу в різних ситуаціях. При вході до будинку, система може спочатку використовувати розпізнавання обличчя для швидкої та ефективної ідентифікації користувача. Якщо освітлення недостатнє або користувач має на голові якісь аксесуари (наприклад, окуляри або капелюх), система автоматично переключається на розпізнавання голосу, попросивши користувача сказати унікальну фразу або пароль.

Коли користувач перебуває всередині розумного будинку, система може адаптуватися до його потреб, використовуючи різні методи ідентифікації в залежності від конкретної ситуації. Наприклад, під час перегляду телевізора система може використовувати розпізнавання голосу для управління різними пристроями, такими як телевізор, пристрій для стрімінгу або система освітлення.

Також можливо, що система навчиться передбачати потреби користувача на основі його поведінки та звичок, автоматично адаптуючи рівень ідентифікації для

кожної ситуації. Наприклад, якщо користувач зазвичай вимикає освітлення перед сном, система може автоматично використовувати менш нав'язливий метод ідентифікації, такий як розпізнавання голосу, щоб не порушувати його комфорт.

Таким чином, адаптація системи ідентифікації до різних сценаріїв використання та умов передбачає ретельний аналіз потреб користувачів, розробку адаптивної та персоналізованої системи, а також інтеграцію різних методів ідентифікації для забезпечення максимальної зручності та безпеки користувачів кіберфізичної системи «Розумний будинок».

Для досягнення цієї мети, розробники можуть використовувати ряд технік та підходів, таких як машинне навчання, штучний інтелект та аналіз даних для постійного вдосконалення та оптимізації системи ідентифікації. Це може включати збір даних про користувачів (з дотриманням політики конфіденційності) для аналізу та визначення закономірностей у поведінці користувачів, а також розробку алгоритмів, які дозволять системі автоматично адаптуватися до різних сценаріїв та умов.

Крім того, важливо розглянути можливі обмеження технологій та апаратного забезпечення, а також потенційні проблеми з безпекою та конфіденційністю. Для забезпечення безпеки системи ідентифікації можуть бути використані різні методи захисту, такі як шифрування даних, аутентифікація на рівні пристрою та регулярне оновлення програмного забезпечення.

У результаті, адаптація системи ідентифікації до різних сценаріїв використання та умов вимагає глибокого розуміння потреб користувачів, використання передових технологій та методів аналізу даних, а також ретельної розробки та впровадження системи для забезпечення зручності, ефективності та безпеки користувачів кіберфізичної системи «Розумний будинок».

3.4.2 Вибір методів ідентифікації

Розглянемо сценарій, у якому користувачі "Розумного будинку" мають різні вікові категорії та технічний досвід. Враховуючи потреби користувачів, система ідентифікації може використовувати комбінацію наступних методів ідентифікації:

1) розпізнавання обличчя: це може бути основним методом ідентифікації для молодих та середнього віку користувачів, які зазвичай зручні з використанням сучасних технологій;

2) розпізнавання голосу: для додаткової безпеки та зручності може бути додано голосове розпізнавання. Це може бути корисним для користувачів, які не хочуть використовувати розпізнавання обличчя або якщо система не може розпізнати користувача через низьке освітлення або інші фактори;

3) відбитки пальців: для осіб похилого віку або тих, хто вважає технологію розпізнавання обличчя або голосу занадто складною, можуть бути запропоновані відбитки пальців. Це забезпечить простоту використання та додаткову безпеку;

4) паролі: у якості резервного методу ідентифікації, користувачам може бути запропоновано введення пароля. Це може стати в нагоді, якщо інші методи ідентифікації не спрацьовують або як додатковий рівень захисту для особливо важливих дій, таких як управління системами безпеки або доступ до конфіденційної інформації.

Таким чином, адаптація системи ідентифікації до різних сценаріїв використання та умов полягає у налаштуванні системи таким чином, щоб вона могла пропонувати різні методи ідентифікації в залежності від потреб користувачів та обставин.

3.4.3 Первинна настройка параметрів розпізнавання

Первинна настройка параметрів розпізнавання передбачає встановлення порогових значень вірогідності для кожного методу ідентифікації та параметрів, які відповідають ступеню безпеки та зручності користувачів.

Приклад реалізації адаптації системи ідентифікації з первинними налаштуванням параметрів розпізнавання:

1) аналіз потреб користувачів: зібрати інформацію про потреби користувачів з метою визначення оптимальних порогових значень та параметрів для кожного методу ідентифікації;

2) встановлення порогових значень: для кожного методу ідентифікації (наприклад, розпізнавання обличчя, голосу, відбитків пальців, паролів) встановити порогові значення вірогідності, які гарантують надійність ідентифікації та мінімізують помилки. Ці порогові значення можуть варіюватися в залежності від ступеня безпеки та зручності, які потрібно забезпечити для конкретних сценаріїв використання;

3) налаштування параметрів розпізнавання: на основі аналізу потреб користувачів та наявних апаратних компонентів, встановити параметри розпізнавання для кожного методу ідентифікації. Ці параметри можуть включати рівень чутливості, кількість спроб розпізнавання, інтервал між спробами тощо;

4) тестування та налаштування: провести тестування системи ідентифікації з різними користувачами та сценаріями використання, щоб перевірити ефективність налаштувань порогових значень та параметрів розпізнавання. За результатами тестування вносити корективи у налаштування, якщо це необхідно, для досягнення оптимального балансу між безпекою та зручністю;

5) моніторинг та адаптація: систематично оцінювати роботу системи ідентифікації в реальних умовах та адаптувати налаштування порогових значень та параметрів розпізнавання відповідно до змін умов використання, потреб користувачів або технологічних можливостей.

Таким чином, адаптація системи ідентифікації до різних сценаріїв використання та умов передбачає гнучкий підхід до налаштування порогових значень і параметрів розпізнавання, що враховує потреби користувачів, наявність апаратних компонентів та забезпечує оптимальний баланс між безпекою та зручністю в процесі ідентифікації.

3.4.4 Розробка алгоритму визначення порядку використання методів ідентифікації

При розробці алгоритму визначення порядку використання методів ідентифікації, важливо забезпечити гнучкість та адаптацію до різних ситуацій і контекстів.

Ось приклад реалізації такого алгоритму:

1) оцінка контексту: система аналізує поточні умови та контекст, такі як освітлення, рівень шуму та інші фактори, що можуть впливати на ефективність методів ідентифікації;

2) визначення доступних методів ідентифікації: система перевіряє наявність апаратних компонентів для кожного методу ідентифікації, таких як камера для розпізнавання обличчя, мікрофон для розпізнавання голосу тощо;

3) визначення пріоритетів методів ідентифікації: система встановлює пріоритети для доступних методів ідентифікації залежно від контексту, забезпечуючи оптимальний баланс між надійністю та зручністю для користувачів;

4) каскадна або паралельна ідентифікація: система може використовувати методи ідентифікації послідовно (каскад) або одночасно (паралельно), в залежності від встановлених пріоритетів та контексту;

5) аналіз результатів ідентифікації: система оцінює результати кожного методу ідентифікації та вирішує, чи потрібно використовувати додаткові методи для підтвердження ідентичності користувача;

6) динамічний вибір методів ідентифікації: якщо результати попередньої ідентифікації не є впевненими, система може динамічно змінювати порядок або

комбінацію методів ідентифікації, щоб забезпеч щоб забезпечити більш надійну ідентифікацію користувача;

7) зберігання та аналіз історії ідентифікації: система зберігає дані про успішні та невдалих спроб ідентифікації та аналізує їх для виявлення можливих тенденцій або проблем. Це допомагає в подальшому оптимізувати алгоритм та забезпечити більш ефективну ідентифікацію користувачів;

8) навчання та адаптація: система постійно вчитиметься та адаптується до змін контексту, поведінки користувачів, технічних обмежень тощо, щоб підтримувати надійність ідентифікації на високому рівні.

3.4.5 Інтеграція з системою «Розумний будинок»

Забезпечення взаємодії ідентифікаційної підсистеми з іншими компонентами кіберфізичної системи «Розумний будинок». Це може включати розробку API, протоколів зв'язку та взаємодії з контролерами пристроїв та іншими підсистемами (освітлення, опалення, системи безпеки тощо).

3.5. Забезпечення конфіденційності та захисту даних користувачів

Загрози розумним будинкам, пов’язані з конфіденційністю, є одними з найбільш значних ризиків, на які необхідно звернути увагу. Однак великий перелік кібератак може поставити під загрозу функціональність систем розумного будинку. Забезпечення безпеки особистої інформації мешканців розумного будинку є життєво важливою вимогою для усунення загроз, пов’язаних із широким визнанням таких систем.

Дані, що передаються через бездротову мережу IoT, поділяються на системні та дані користувачів. Ці категорії даних відрізняють необхідні заходи безпеки. Один потребує конфіденційності даних, а інший вимагає конфіденційності даних.

3.5.1 Конфіденційність даних

Конфіденційність у бездротовій системі стосується належного приховування вмісту пакетів даних, які включають або контрольні повідомлення, або інформацію про функціональність інтелектуальних пристроїв, а також запобігання несанкціонованому доступу зловмисників . Впровадження криптографічних методів є поширеним способом захисту цих повідомлень у системі IoT. Складність передових методів шифрування змушує зловмисників знайти секретні ключі для розкриття відкритих текстів і гарантує, що інформація системи не буде виявлена тими, хто не має доступу . З іншого боку, недоліком методів шифрування є те, що вони залишають контекстні дані мережевих повідомлень незахищеними. Прикладами таких даних є ідентифікаційні дані смарт-пристрою, місцезнаходження та час активності. Цей тип даних надає зловмисникам багатий ресурс для отримання важливої інформації про систему, яка може мати більшу цінність, ніж її вміст.

3.5.2 Приватність даних

Приватність даних означає, що захищена інформація належить людині, а не пристрою чи системі. Мешканці інтелектуальної будівлі діляться великою кількістю даних про свої справи із системою, а численні вбудовані датчики в різноманітних розумних пристроях відповідають за збір даних про повсякденну діяльність користувачів (ADL).

Ці всеосяжні накопичені дані дозволяють інтелектуальним механізмам системи оцінювати ситуацію користувачів і створювати послуги відповідно до їхніх бажаних потреб. Подібним чином здатність системи отримувати дані надає зловмисникам цінний ресурс для виявлення конфіденційної інформації про мешканців .

Виходячи з визначення, приватність означає право людини зберігати своє особисте життя або особисту інформацію в таємниці або відомою лише невеликій

групі людей, яке захищено законом у більшості країн. Мотиви хакерів порушувати права на конфіденційність своїх жертв варіюються від комерційної вигоди до особистої ворожнечі . У деяких випадках уряди порушують приватне життя громадян шляхом незаконного спостереження.

У разі атак FATS системи виявлення вторгнень не допомагають через пасивний характер атаки. Зловмисник тихо збирає дані та зловживає ними; катастрофічні результати шпигування з'являються, коли жертвам стає занадто пізно відреагувати належним чином.

Крім того, методи шифрування не можуть захистити інформацію, яку зловмисники збирають отримати, оскільки дані витікають через контекстні аспекти бездротової передачі.

Таким чином, наведені вище ситуації підкреслюють необхідність надійного проактивного механізму захисту в домашніх системах для захисту інформації користувачів. Рисунок 3.2 демонструє різницю між конфіденційністю та приватністю з точки зору типу даних.

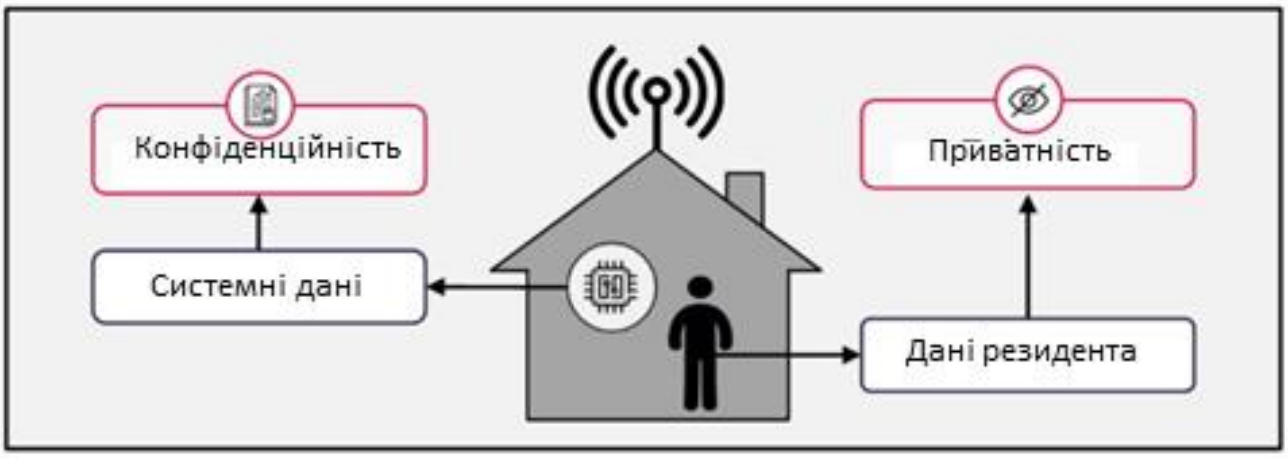


Рисунок 3.2 Типи домашніх даних і відповідні заходи безпеки

3.5.3. Методи забезпечення конфіденційності та захисту даних

Для забезпечення конфіденційності та захисту даних користувачів у розумному будинку можна використовувати наступні методи:

1) шифрування даних. Використання сильних криптографічних алгоритмів для шифрування даних перед їх передачею між пристроями та системами розумного будинку. Це забезпечує конфіденційність даних та запобігає несанкціонованому доступу до інформації;

2) аутентифікація та авторизація. Встановлення сильних механізмів аутентифікації та авторизації для контролю доступу до системи та даних. Це може включати використання багатофакторної аутентифікації, де користувачі повинні надати декілька форм перевірки своєї особи, перш ніж отримати доступ до системи або даних;

3) мережева безпека. Впровадження рівня мережевої безпеки для забезпечення безпеки передачі даних між пристроями та системами розумного будинку. Це може включати використання захищених протоколів зв'язку, файрволів та інших механізмів безпеки мережі;

4) політики конфіденційності та регулятивні вимоги. Розробка та впровадження політик конфіденційності, що відповідають законодавчим та регулятивним вимогам щодо зберігання, обробки та передачі персональних даних. Це включає отримання відповідних згод користувачів на обробку їх даних та дотримання принципів мінімізації даних, які обробляються та зберігаються;

5) регулярне оновлення. Регулярне оновлення для програмного забезпечення та операційних систем розумних пристроїв та систем розумного будинку. Це допомагає запобігти вразливостям, які можуть бути експлуатовані зловмисниками для отримання доступу до системи або даних користувачів;

6) моніторинг та аудит. Встановлення процедур моніторингу та аудиту для виявлення незвичайних та підозрілих активностей та спроб вторгнення в систему. Це допомагає виявити можливі атаки або порушення безпеки на ранніх стадіях та вживати відповідних заходів щодо їх усунення;

7) інформаційна безпека. Організація процесів інформаційної безпеки, які включають розробку політик безпеки, навчання користувачів з питань безпеки та свідомості про можливі загрози, а також регулярне тестування системи на вразливості та відповідність політикам безпеки;

8) фізична безпека. Забезпечення фізичної безпеки розумних пристроїв та систем розумного будинку, що включає контроль доступу до приміщень, де розміщені обладнання та сервери, а також захист від стихійних лих, таких як пожежі, повені та інші катастрофи;

9) резервне копіювання та відновлення даних. Регулярне резервне копіювання даних та розробка планів відновлення даних у випадку втрати або пошкодження інформації. Це допомагає забезпечити доступність та цілісність даних користувачів у разі будь-яких проблем з системою або атаки зловмисників.

Забезпечення конфіденційності та захисту даних користувачів у розумних будинках є важливим завданням, що вимагає комплексного підходу. Використання цих методів і заходів безпеки допоможе забезпечити, що інформація та особисті дані користувачів залишаються безпечними та конфіденційними, а також запобігти потенційним атакам та загрозам. Важливо пам'ятати, що кібербезпека є безперервним процесом, який вимагає постійного моніторингу, оновлення та адаптації до нових загроз та вразливостей.

3.6 Архітектура підсистеми

Для створення архітектури кіберфізичної ідентифікації в системі розумного будинку можна використовувати різні методи біометричної ідентифікації, такі як розпізнавання обличчя, голосу, відбитків пальців та сітківки ока. На основі попередніх досліджень ми прийшли до такої архітектури підсистеми (Рисунок 3.3):

1. Сенсори / пристрої зчитування:
- камера для розпізнавання обличчя;
- мікрофон для розпізнавання голосу;
- сканер відбитків пальців;
- сканер сітківки ока.
2. Модуль перед обробки даних:
- фільтрація та покращення зображень / сигналів;
- виявлення обличчя / очей / пальців на зображеннях;

- вирізання та масштабування регіонів інтересу.

3. Модуль витягу властивостей:

- розрахунок особливостей для кожного методу ідентифікації (наприклад, MFCC для голосу, HOG або CNN для обличчя, особливості сітківки для сітківки ока, особливості відбитків пальців для відбитків пальців).

4. Модуль порівняння / класифікації:

- порівняння властивостей з базою даних користувачів;
- застосування алгоритмів класифікації для визначення, чи є особа користувачем системи.

5. Модуль прийняття рішень:

- обробка результатів порівняння / класифікації;
- визначення довірчого рівня ідентифікації;
- врийняття рішення про надання доступу або відмову.

6. База даних користувачів:

- зберігання біометричних шаблонів користувачів;
- забезпечення інформації для порівняння / класифікації в модулі порівняння / класифікації.

7. Інтерфейс користувача:

- відображення статусу ідентифікації (успішно / не успішно);
- введення або оновлення біометричних даних для зареєстрованих користувачів;
- налаштування параметрів системи ідентифікації та доступу.

8. Модуль управління доступом:

- керування доступом до приміщень та пристроїв на основі результатів ідентифікації;
- відстеження та реєстрація спроб доступу.

9. Зв'язок з іншими системами розумного будинку:

- надсилання сигналів про статус ідентифікації та контролю доступу до інших систем розумного будинку, таких як система безпеки, освітлення, температурний контроль тощо.

– зберігання біометричних шаблонів користувачів;

– забезпечення інформації для порівняння / класифікації в модулі порівняння / класифікації.

Рисунок 3.3 - Архітектура підсистеми ідентифікації

3.7 Висновок

В даному розділі був проведений аналіз критеріїв та методів які необхідні для сучасної підсистеми авторизації.

За результатами проведеного дослідження було була запропонована архітектура підсистеми ідентифікації користувача в кіберфізичній системі «Розумний будинок».

4. ПІДСИСТЕМА ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА КІБЕРФІЗИЧНОЇ СИСТЕМИ «РОЗУМНИЙ БУДИНОК»

4.1 Моделювання підсистеми ідентифікації користувача на основі запропонованого алгоритму

Система ідентифікації користувача буде включати наступні компоненти для ідентифікації за відбитком пальця, обличчям, голосом і паролем:

1) Модуль ідентифікації за відбитком пальця:
- сенсор відбитків пальців;
- блок обробки даних відбитків пальців;
- база даних відбитків пальців.

2) Модуль ідентифікації обличчям:
- камера;
- блок обробки даних обличчя;
- база даних обличь.

3) Модуль ідентифікації за голосом:
- мікрофон;
- блок обробки даних голосу;
- база даних голосових зразків.

4) Модуль ідентифікації за паролем:
- пристрій введення паролів (клавіатура, сенсорний екран) ;
- блок обробки даних паролів;
- база даних паролів.

5) Центральний контролер:
- блок об'єднання результатів ідентифікації;
- модуль визначення ступеня довіри;
- блок прийняття рішення про доступ.

Архітектура підсистеми ідентифікації користувача буде мати структуру модуля, де кожен модуль може працювати незалежно від інших, але результати їх роботи можуть поєднуватися для підвищення точності ідентифікації. Центральний

контролер буде об'єднувати дані з різними ідентифікаціями модулів, аналізувати оцінки довіри до кожного з них і приймати остаточне рішення щодо надання доступу користувачам.

4.2 Вибір апаратно-програмного забезпечення для реалізації підсистеми ідентифікації користувача.

Підбір апаратно-програмного забезпечення для реалізації підсистеми ідентифікації користувача буде здійснюватись з урахуванням таких вимог, як надійність, точність, швидкість роботи та сумісність з іншими компонентами кіберфізичної системи «Розумний будинок».

1) сенсор відбитків пальців: вибір сенсора відбитків пальців з високою роздільною здатністю, швидкістю роботи та можливістю працювати в різних умовах (вологість, температура) ;

2) камера: вибір камери з високою роздільною здатністю, широким кутом огляду та інфрачервоним підсвічуванням для роботи в умовах поганого освітлення;

3) мікрофон: вибір мікрофона з високою чутливістю, можливістю розпізнавати голос на відстані та функцією шумоподавлення;

4) пристрій введення паролів: вибір надійного пристрою для введення паролів, такого як клавіатура або сенсорний екран, з захистом від несанкціонованого доступу;

5) програмне забезпечення: вибір або розробка програмного забезпечення, яке дозволить об'єднати роботу різних модулів ідентифікації, забезпечити аналіз ступеня довіри та прийняття рішення щодо доступу. Програмне забезпечення повинно бути сумісне з іншими компонентами кіберфізичної системи «Розумний будинок» ;

6) обчислювальна платформа: вибір потужної обчислювальної платформи, здатної ефективно обробляти дані від різних модулів ідентифікації. Обчислювальна платформа повинна підтримувати роботу з нейронними мережами та мати достатній ресурс для паралельної обробки даних.

4.3 Прототип реалізації підсистеми ідентифікації користувача кіберфізичної системи

Використовуючи алгоритм розроблений в попередніх розділах ми можемо створити прототип підсистеми ідентифікації користувача кіберфізичної системи «Розумний будинок»

Для реалізації можливо використовувати наступні бібліотеки та інструменти:

1. OpenCV та Android Fingerprint API: для роботи з зображеннями облич та відбитками пальців;
2. TensorFlow або PyTorch: для реалізації нейронних мереж, які використовуються для класифікації та розпізнавання;
3. MaryTTS: для обробки аудіо та розпізнавання голосу;
4. Scikit-learn: для класифікації та обробки даних.

Прототип реалізації представлений в Додатку А.

Додавання підтримки голосового розпізнавання за допомогою MaryTTS та підтримки ідентифікації за відбитком пальця за допомогою Android Fingerprint API потребує додаткових налаштувань та інтеграції з проектом. Оскільки ці рішення базуються на різних платформах (MaryTTS працює на сервері, а Android Fingerprint API на Android-пристрої), їх реалізація може суттєво відрізнятися.

Для реалізації голосової ідентифікації за допомогою MaryTTS, спочатку вам потрібно встановити сервер MaryTTS та інтегрувати його з проектом на Java. Після налаштування сервера та налаштування з'єднання з проектом, можемо використовувати MaryTTS для синтезу та аналізу голосу, а також для порівняння збережених характеристик голосу користувачів з новими даними.

Щодо ідентифікації за відбитком пальця, слід інтегрувати Android Fingerprint API з проектом на платформі Android. Це потребує створення Android-додатка, який використовує FingerprintManager або BiometricPrompt (залежно від версії Android) для роботи з відбитками пальців користувачів. Після успішної

ідентифікації за відбитком пальця, результати можуть передаватися на сервер для подальшої обробки та аналізу.

Нам доведеться розробити детальніше програмне забезпечення на основі відповідних бібліотек та інструментів, а також провести тестування та налагодження, перш ніж підсистема буде готова до використання в реальному середовищі. Ось додаткові критерії щодо кожного кроку реалізації:

1) збір даних. Залежно від використовуваних апаратних компонентів, можуть знадобитися драйвери та програмне забезпечення для зчитування даних від камери, мікрофону, сенсора відбитків пальців та пристрою введення паролів;

2) попередня обробка даних. Використаємо функції з OpenCV та MaryTTS для очищення та нормалізації даних зображень та аудіо. Зверніть увагу на особливості різних модальностей даних, таких як розміри зображень, формати аудіофайлів та кодування символів для паролів;

3) видобуток особливостей. Розробити алгоритми для видобутку особливостей з попередньо оброблених даних. Ви можете використовувати готові до використання моделі, такі як моделі розпізнавання обличчя з OpenCV, або створити власні моделі з TensorFlow або PyTorch для голосової ідентифікації та інших методів ідентифікації;

4) класифікація та сумісність. Використаємо алгоритми класифікації з Scikit-learn для порівняння особливостей з шаблонами користувачів, збереженими в базі даних. Застосуйте стратегії, такі як вагові коефіцієнти або голосування, для об'єднання результатів ідентифікації з різних методів;

5) оцінка вірогідності. На основі порівняння та класифікації, розрахуйте вірогідність ідентифікації для кожного користувача. Ви можете використовувати метрики схожості, такі як відстань Хеммінга або косинусна схожість, для оцінки ступеня схожості між особливостями та шаблонами користувачів;

6) прийняття рішення. На основі вірогідності, вирішити, чи слід надавати доступ користувачеві. Встановіть поріг вірогідності, який буде використовуватись для прийняття рішення про надання доступу. Це може бути фіксований поріг або динамічний поріг, залежно від потреб системи;

7) надання та відмова доступу. Реалізуйте процедури для надання доступу користувачеві в разі успішної ідентифікації або відмови доступу, якщо вірогідність ідентифікації нижча за поріг. Залежно від вашої системи «Розумний будинок», це може включати надання доступу до різних пристроїв, послуг або функцій, а також журналювання спроб ідентифікації та сповіщення адміністратора системи про невдачі;

8) тестування та налагодження. Протестуйте реалізовану підсистему ідентифікації користувача, щоб переконатися, що вона працює належним чином та відповідає вашим вимогам щодо безпеки та зручності використання. За потреби налагоджуйте алгоритми, поріг вірогідності та інші параметри для покращення ефективності та надійності ідентифікації.

Розробка підсистеми ідентифікації користувача для кіберфізичної системи «Розумний будинок» - це складний процес, який вимагає глибокого розуміння різних методів ідентифікації, алгоритмів, технологій та платформ. Окрім того, важливо забезпечити безпеку даних користувачів та приватність інформації, що передається між компонентами системи.

Після успішного тестування та налагодження підсистеми, розгляньте можливості її розширення або інтеграції з іншими підсистемами вашої кіберфізичної системи «Розумний будинок».

Під час розробки підсистеми ідентифікації користувача варто врахувати ще такі критерії:

1) безпека даних. Потрібно забезпечити захист даних користувачів під час передачі між компонентами системи та зберігання в базі даних. Використовуйте криптографічні методи для шифрування даних та забезпечення їх конфіденційності;

2) протоколи аутентифікації. Потрібно розглянути можливість використання стандартних протоколів аутентифікації, таких як OAuth або SAML, для спрощення процесу ідентифікації користувачів та підтримки сумісності з іншими системами;

3) резервне копіювання та відновлення. Потрібно розробити стратегію резервного копіювання та відновлення даних ідентифікації користувачів для забезпечення безперебійної роботи системи в разі втрати даних або апаратних збоїв;

4) моніторинг та сповіщення. Потрібно встановити систему моніторингу для відстеження стану підсистеми ідентифікації користувача та оповіщення адміністратора системи або відповідних осіб про будь-які відхилення від норми, невдачі аутентифікації або можливі атаки на систему. Використовуйте інструменти моніторингу та сповіщення, щоб забезпечити швидке виявлення та реагування на проблеми безпеки;

5) аудит та нотування. Потрібно забезпечити зберігання журналів ідентифікації користувачів для аналізу роботи системи, виявлення аномалій або розслідування інцидентів безпеки. Використовуйте автоматизовані інструменти аудиту та аналізу для перевірки журналів та виявлення можливих проблем;

6) оновлення та підтримка. Потрібно підтримувати підсистему ідентифікації користувача в актуальному стані, оновлюйте програмне забезпечення та компоненти відповідно до випуску оновлень та виправлень від постачальників. Слідкуйте за новими технологіями, алгоритмами та методами ідентифікації, щоб вдосконалювати систему та підвищувати її ефективність;

7) масштабування. Потрібно залишити можливість масштабування підсистеми ідентифікації користувача для підтримки зростання кількості користувачів та пристроїв у вашій кіберфізичній системі «Розумний будинок». Масштабування може включати вдосконалення архітектури системи, а також використання хмарних ресурсів або розподілених обчислень для розподілу обробки даних і навантаження на систему.

Успішна реалізація підсистеми ідентифікації користувача забезпечить безпечний та ефективний спосіб доступу до вашої кіберфізичної системи «Розумний будинок», враховуючи зручність користувачів та вимоги до безпеки.

З метою підвищення ефективності та надійності підсистеми, регулярно переглядайте та оцінюйте її роботу, адаптуйте та оптимізуйте алгоритми та

параметри відповідно до змін у вимогах до безпеки, технологій або потреб користувачів.

Також важливо забезпечити прозорість та приватність для користувачів системи, інформуючи їх про методи ідентифікації, що використовуються, та забезпечуючи можливість відстежувати та контролювати використання своїх персональних даних. Розгляньте можливість надання користувачам налаштувань та опцій управління своїми даними аутентифікації, такими як зміна або скидання паролів, відновлення доступу в разі втрати пристрою або інших проблем.

Дотримуйтесь рекомендацій щодо безпеки, розроблених авторитетними організаціями та стандартними органами, такими як NIST, ISO та інші, а також національні та місцеві законодавчі вимоги щодо захисту даних та приватності.

Таке дотримання допоможе забезпечити надійну роботу вашої підсистеми ідентифікації користувача та зменшити ризики, пов'язані з її використанням.

4.4 Тестування та оптимізація ефективності запропонованої підсистеми ідентифікації користувача

4.4.1 Розробка тестових сценаріїв

Визначимо різні сценарії, які охоплюють різні аспекти підсистеми ідентифікації, такі як позитивні та негативні випробування, випробування на спроби злому, випробування на забезпечення конфіденційності та безпеки даних.

Сценарій №1: Реєстрація нового користувача

- крок 1: Запустити систему ідентифікації користувача;
- крок 2: Вибрати опцію "Реєстрація нового користувача";
- крок 3: Заповнити форму реєстрації з інформацією про нового користувача;
- крок 4: Зареєструвати дані ідентифікації (відбитки пальців, обличчя, голос, пароль) ;
- крок 5: Перевірити успішність реєстрації, збереження даних та здатність системи розпізнавати нового користувача.

Сценарій №2: Ідентифікація зареєстрованого користувача

- крок 1: Запустити систему ідентифікації користувача;
- крок 2: Зареєстрований користувач повинен надати дані ідентифікації (відбитки пальців, обличчя, голос, пароль) ;
- крок 3: Перевірити, чи система успішно розпізнає користувача та надає йому доступ до кіберфізичної системи «Розумний будинок».

Сценарій №3: Ідентифікація користувача з некоректними даними

- крок 1: Запустити систему ідентифікації користувача;
- крок 2: Користувач намагається отримати доступ, використовуючи неправильні дані (наприклад, чужий відбиток пальця, фотографію обличчя або невірний пароль) ;
- крок 3: Перевірити, чи система відмовляє у доступі користувачеві з некоректними даними.

Сценарій №4: Відновлення доступу користувача

- крок 1: Запустити систему ідентифікації користувача;
- крок 2: Користувач намагається отримати доступ, але забув пароль або не може надати інші дані ідентифікації;
- крок 3: Користувач обирає опцію "Відновлення доступу";
- крок 4: Система пропонує альтернативні методи ідентифікації (наприклад, відправка коду підтвердження на електронну пошту або телефон) ;
- крок 5: Користувач отримує код підтвердження та вводить його в систему;
- крок 6: Після успішної ідентифікації, користувач може встановити новий пароль або оновити інші дані ідентифікації;
- крок 7: Перевірити здатність системи надати користувачеві доступ після відновлення ідентифікаційних даних.

Сценарій №5: Видалення користувача з системи

- крок 1: Запустити систему ідентифікації користувача;
- крок 2: Адміністратор системи вибирає опцію "Управління користувачами";

– крок 3: Адміністратор знаходить потрібного користувача та видаляє його з системи;

– крок 4: Перевірити успішність видалення користувача та забезпечити, що він більше не має доступу до кіберфізичної системи «Розумний будинок».

4.4.2 Тестування часу відповіді підсистем авторизації

Під час тестування було виявлено що час відповіді нашої підсистеми є швидшим ніж в вище перелічених це відображено на Рисунок 4.1.

Середній час відповіді в підсистемах:

1) Amazon Echo/Alexa, 1,72 секунд;
2) Google Nest, 2,45 секунд;
3) Apple HomeKit 2,62 секунд;
4) Samsung SmartThings 3,32 секунд;
5) наша підсистема 1,25 секунд.

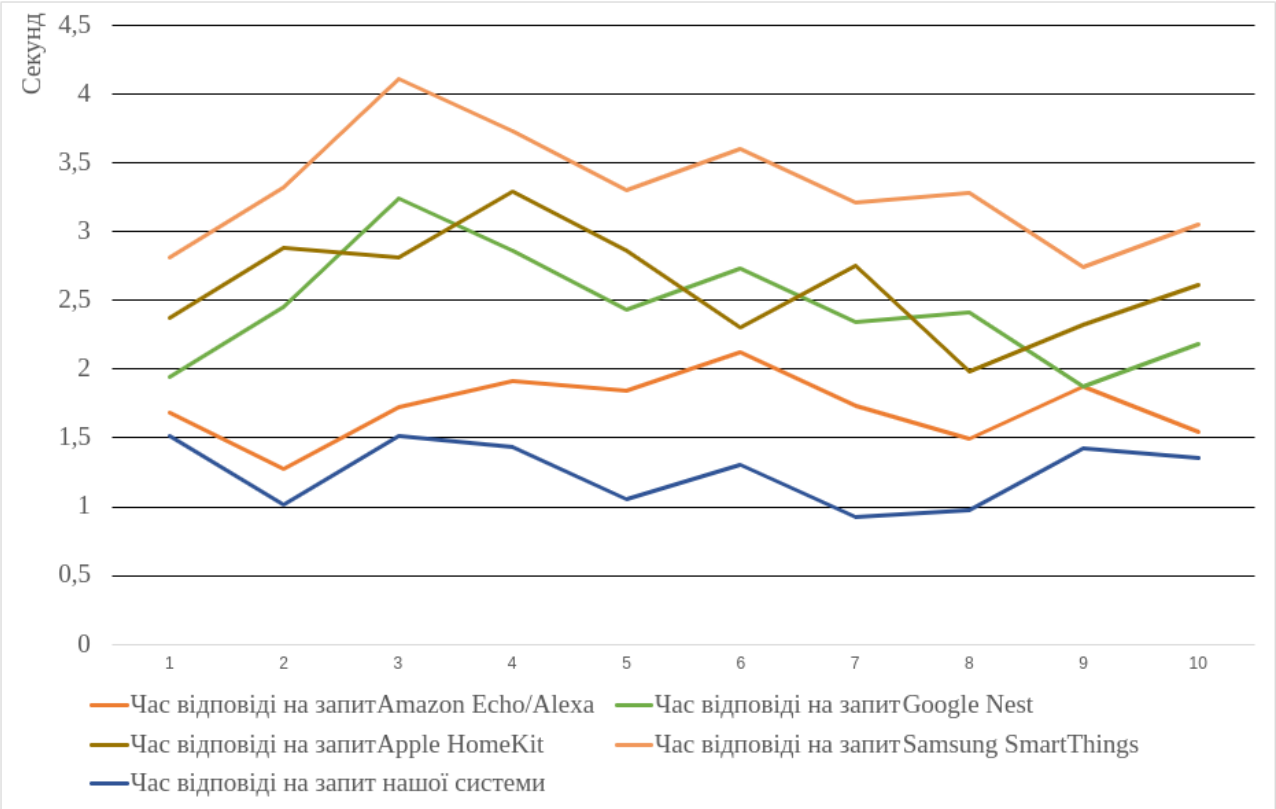


Рисунок 4.1 – Порівняння часу відповіді при авторизації

4.4.3 Тестування захисту підсистем авторизації

Під час тестування авторизації за підбитком пальця використовувався наступний масив даних:

```
fingerprint_data = [
{"id": 1, "fingerprint": [0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9, 1.0]},
{"id": 2, "fingerprint": [0.2, 0.1, 0.4, 0.3, 0.6, 0.5, 0.8, 0.7, 1.0, 0.9]},
{"id": 3, "fingerprint": [0.3, 0.1, 0.2, 0.4, 0.5, 0.7, 0.6, 0.9, 0.8, 1.0]},
{"id": 4, "fingerprint": [0.4, 0.3, 0.2, 0.1, 0.6, 0.5, 0.8, 0.7, 1.0, 0.9]},
{"id": 5, "fingerprint": [0.5, 0.4, 0.3, 0.2, 0.1, 0.6, 0.7, 0.8, 0.9, 1.0]},
…
]
```

fingerprint_data представляє собою список словників, де кожен словник містить унікальний ідентифікатор id та відповідний відбиток пальця fingerprint. Відбиток пальця представлено як список числових значень, які можуть відображати характеристики відбитка пальця, такі як особливості поверхні пальця, співвідношення сірих відтінків та ін.

Використовуючи масив даних було про тестовано та перевірено якість системи авторизації на прикладі аналізу відбитку пальця. Також була підтверджена надійність системи.

4.5. Висновок

Використання запропонованої підсистеми ідентифікації користувача в кіберфізичній системі «Розумний будинок» має ряд можливостей та переваг:

1) безпека: багаторівнева ідентифікація користувача, яка включає розпізнавання обличчя, відбитків пальців, голосу та паролів, підвищує рівень безпеки системи. Це ускладнює можливість несанкціонованого доступу та забезпечує більш надійний контроль доступу до різних функцій розумного будинку;

2) зручність: система ідентифікації користувача забезпечує зручний доступ до різних функцій розумного будинку. Користувачі можуть використовувати різні методи ідентифікації залежно від їх особистих вподобань та ситуації. Наприклад, голосове керування може бути корисним для осіб з обмеженими можливостями або коли руки зайняті;

3) індивідуальні налаштування: ідентифікація користувача дозволяє системі розумного будинку автоматично налаштовуватись на конкретного користувача та його потреби. Це може включати автоматичну регуляцію освітлення, клімату, мультимедійних систем та інших пристроїв відповідно до вподобань користувача;

4) легкість інтеграції: запропонована підсистема ідентифікації користувача може бути легко інтегрована з існуючими пристроями та системами розумного будинку. Також вона сумісна з різними платформами та протоколами, що полегшує її впровадження та розвиток;

5) скорочення ризику помилок: завдяки автоматизованому процесу ідентифікації користувача, ймовірність помилок, пов'язаних з неправильним введенням паролів або втратою ключів, зводиться до мінімуму. Це допомагає запобігти ситуаціям, коли користувачі можуть опинитися заблокованими або втратити доступ до своїх пристроїв та систем;

6) гнучкість: завдяки модульній архітектурі, підсистему ідентифікації користувача можна легко налаштувати та розширювати для підтримки нових методів ідентифікації або інтеграції з іншими системами;

7) забезпечення приватності: зикористання біометричних даних, таких як відбитки пальців та обличчя, дозволяє підсистемі ідентифікації користувача забезпечити високий рівень приватності, оскільки ці дані є унікальними для кожного користувача. Шифрування даних та секретність ключів також забезпечують додатковий рівень захисту приватності користувачів.

ВИСНОВОК

У роботі за результатами виконаних теоретичних та практичних досліджень створена теоретична модель ідентифікації користувача кіберфізичній системі «Розумний будинок».

У першому розділі ми розглянули існуючі прототипи та їх можливості.

У другому розділі була створена математична модель яка охарактеризувала загальні особливості нашої системи.

У третьому розділі були конкретизовані характеристики майбутньої системи ідентифікації користувача.

У четвертому розділі був створений алгоритм та можлива програмна реалізація ідентифікації в кіберфізичній системі, алгоритми тестування даної системи.

В майбутньому впровадження результатів роботи можуть дозволити збільшити точність та надійність системи ідентентифікації в кіберфізичних системах.

За темою дипломної роботи опублікована одна стаття у фаховому науковому виданні “Computer Systems & Information Technologies 2022” .

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Ciprian-Radu R., Olimpiu H., Takacs I. A., Gheorghe O. Smart Monitoring of Potato Crop: A Cyber-Physical System Architecture Model in the Field of Precision Agriculture. *Conference Agriculture for Life, Life for Agriculture*. 2015. №6. P. 73–79.

2. Hovorushchenko T. O, Aleksov S. V, Talapchuk S. I, Shpylyuk O. V, Magdin V. V. Overview of the Methods and Tools for Situation Identification and Decision-Making Support in the Cyberphysical System "Smart House". *Computer Systems & Information Technologies.* 2022. №4. P. 20-26.

3. Georgakopoulos D., Jayaraman P. P. Internet of things: from internet scale sensing to smart services. *Computing*. 2016 №98. P. 1041–1058

4. Robles R.J, Kim T.H. Applications, systems and methods in smart home technology: A Review. *Int. J. Adv. Sci. Technol.* 2010 №15. P. 37–48.

5. Stojkoska B.L.R, Trivodaliev K.V. A review of Internet of Things for smart home: Challenges and solutions. *J. Clean. Prod.* 2017 №140 P. 1454–1464.

6. Abrishamchi M.A., Cheok A.D., Abdullah A.H., Bielawski K.S. In-Home Surveillance Systems and Privacy Considerations for Malaysians: A Survey. *Int. J. Innov. Comput.* 2018 №8 P. 47–51.

7. Liu X. A., survey on clustering routing protocols in wireless sensor networks. *Sensors.* 2012 №12. P. 11113–11153.

8. Wang P., Yao C., Zheng Z., Sun G., Song L. Joint Task Assignment, Transmission, and Computing Resource Allocation in Multilayer Mobile Edge Computing Systems. *IEEE IoT J.* 2018. №6. P. 2872–2884.

9. Ren. J., He Y., Huang G., Yu G., Cai Y., Zhang Z. An edgecomputing based architecture for mobile augmented reality. *IEEE Netw.* 2019. №33. P. 162–169.

10. Cherchi R., Colistra G., Pilloni V., Atzori L. Energy consumption management in Smart Homes: An M-Bus communication system. *In Proceedings of the 2014 International Conference on Telecommunications and Multimedia (TEMU).* 2014 P. 28–30

11. Hu Q., Li F. Hardware Design of Smart Home Energy Management System with Dynamic Price Response. IEEE Trans. Smart Grid 2013. №4. P. 1878–1887.

12. Jo, H.; Kim, S.; Joo, S. Smart heating and air conditioning scheduling method incorporating customer convenience for home energy management system. *Trans. Consum. Electron*. 2013. №59. P. 316–322.

13. Peruzzini M., Germani M., Papetti A., Capitanelli A. Smart Home Information Management System for Energy-Efficient Networks. *In Collaborative Systems for Reindustrialization.* 2013. V. 408. P. 393–401.

14. Han D.M., Lim J.H. Smart home energy management system using IEEE 802.15.4 and ZigBee. *IEEE Trans. Consum. Electron.* 2010. №56. P. 1403–1410.

15. Han D.M., Lim, J.H. Design and implementation of smart home energy management systems based on ZigBee. *IEEE Trans. Consum. Electron.* 2010. №56. P.1417–1425.

16. Atzori L., Iera A., Morabito G. The Internet of Things: A Survey, Computer Networks. 2010. V. 54. № 15. P. 2787–2805.

17. Friedli M, Kaufmann L, Paganini F, Kyburz R, Energy Efficiency of the Internet of Things - Technology and Energy Assessment Report. *International Energy Agency*. 2016. V. 1.

18. Gubbi J, Buyya R, Marusic S, Palaniswami M, Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*. 2013. V. 29, № 7. P. 1645–1660.

19. Bag G, Pang Z, Johansson M. E, Min X, Zhu S, Engineering friendly tool to estimate battery life of a wireless sensor node. *Journal of Industrial Information Integration*, 2016. V. 4. P. 8–14.

20. Kau L. J., Dai B. L., Chen C. S., Chen S. H., A cloud network based power management technology for smart home systems. *International Conference on Systems, Man, and Cybernetics (SMC)*. 2012, P. 2527–2532.

21. Martinez B., Monton M., Vilajosana I., Prades J. D., The Power of Mod- ´ els: Modeling Power Consumption for IoT Devices. *Sensors Journal*. 2015, №.10. P. 5777–5789.

22. Jayakumar H., Lee K., Lee W. S., Raha A., Kim Y., Raghunathan V., Powering the Internet of Things. *International Symposium on Low Power Electronics and Design (ISLPED).* 2014. P. 375– 380.

23. Kaup F., Gottschling P., Hausheer D., PowerPi: Measuring and modeling the power consumption of the Raspberry Pi. *Conference on Local Computer Networks*. 2014. P. 236–243.

24. Cardin O. Classification of cyber-physical production systems applications: proposition of an analysis framework. *Computers in Industry*. 2019. V.104. P. 11–21.

25. Boubekeur M. Industrial applications for cyber-physical systems. *First International Conference on Embedded & Distributed Systems*. 2017. P. 17-18. DOI: 10.1109/EDIS.2017.8284020.

26. Grispos G., Glisson W.B., Choo K. R. Medical Cyber-Physical Systems Development: A Forensics-Driven Approach. In Proceedings of IEEE. *ACM Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE 2017). USA.* 2017. P. 108-114. http://dx.doi.org/10.1109/CHASE.2017.48.

27. Jiafu Wan, Hehua Yan, Hui Suo, Fang Li. Advances in CyberPhysical Systems. Research School of Computer Science and Engineering. *South China University of Technology Guangzhou*. *China* DOI: 2011.11.001. 10.3837/tiis.

28. Sankavaram C, Kodali A, Pattipati K, An integrated health management process for automotive cyber-physical systems. *International Conference on Computing*. *Networking and Communications (ICNC).* 2013. P. 82-86, doi: 10.1109/ICCNC.2013.6504058.

29. Kyoung-Dae Kim, Behrad Bagheri P.R., Shanhu Yang, Hung-An Kao, Jay Lee. An Overview and Some Challenges in Cyber-Physical Systems Some Challenges in Cyber-Physical Systems. *Cyber-physical Systems Architecture for SelfAware Machines in Industry 4.0 Environment, IFAC-Papers On Line.* 2015. № 48. P. 1622-1627, ISSN 2405-8963, https://doi.org/10.1016/j.ifacol.2015.06.318.

30. Hailing Fu., Zahra Sharif-Khodaei, Ferri Aliabadi M. H. An energyefficient cyber-physical system for wireless on-board aircraft structural health monitoring. *Mechanical Systems and Signal Processing*. 2019. №. 128. P. 352-368, ISSN 0888-3270.

31. Insup Lee, Oleg Sokolsky. Medical Cyber Physical Systems. *47th Design Automation Conference* №10. P.743-748. http://dx.doi.org/10.1145/1837274.1837463.

32. Arthur Gatouillat, Youakim Badr, Bertrand Massot, Ervin Sejdić. Internet of Medical Things: A Review of Recent Contributions Dealing with Cyber-Physical Systems in Medicine. *IEEE internet of things journal, IEEE*. 2018. №5. P.3810 - 3822.10.1109/JIOT.2018.2849014. hal-01836236.

33. Silva L.C., Almeida H.O., Perkusich A., Perkusich M. A Model-Based Approach to Support Validation of Medical Cyber-Physical Systems. *Sensors.* 2015. P.27625-27670. https://doi.org/10.3390/s151127625.

34. Li W., Meng W., Su C., Kwok L. F. Towards false alarm reduction using fuzzy if-then rules for medical cyber physical systems. *IEEE Access*. 2018. №6. P. 6530-6539.

35. AlZubi A.A., Al-Maitah M., Alarifi A. Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques. *Soft Comput 25.* 2021. P.12319–12332 https://doi.org/10.1007/s00500-021-05926-8.

36. Guo K., Li N., Kang J., Zhang J. Towards efficient federated learning- based scheme in medical cyber-physical systems for distributed data. *Software: Practice and Experience.* 2021. №51. P. 2274-2289.

37. FENG, Jianshe, Development of An Integrated Framework for Cyber Physical System (CPS)-Enabled Rehabilitation System. *International Journal of Prognostics and Health Management*. 2021. №12.

38. Silva, L. C, Perkusich, M, Bublitz, F. M, Almeida, H. O, & Perkusich A. A model-based architecture for testing medical cyber-physical systems. *In Proceedings of the 29th Annual ACM Symposium on Applied Computing.* 2014. P. 25- 30.

39. Грудзинський Ю.Є. Технології сучасних кіберфізичних систем: навч. посіб. для студ. *КПІ ім. Ігоря Сікорського*, 2020. №327. с. 77

40. Montaner H., Silla F., Fröning H. A new degree of freedom for memory allocation in clusters. *Cluster Comput*. 2012. № 15. P. 101–123. DOI: https://doi.org/10.1007/s10586-010-0150-7

41. Baklouti M., Krichene H., Abid M., Synchronous Communication-Based Many-Core SoC. *Arab J.* 2017. С. 845–857. DOI: https://doi.org/10.1007/s13369-016-2373-2

42. Zhao J., Xu C., Zhang T. A Bandwidth-Aware Hybrid Cache Hierarchy Design with Nonvolatile Memories. *J. Comput. Sci. Technol.* 2016. № 31. С. 20–35. DOI: https://doi.org/10.1007/s11390-016-1609-7

43. Maurya A.K, Modi K., Kumar V. Energy-aware scheduling using slack reclamation for cluster systems. *Cluster Comput*. 2020. № 23. С. 911–923. DOI: https://doi.org/10.1007/s10586-019-02965-7

44. Kostenetskii P.S., Sokolinsky L.B. Simulation of hierarchical multiprocessor database systems. *Program Comput Soft.* 2013. №39. С. 10–24. DOI: https://doi.org/10.1134/S0361768813010040

45. Josephson J., Ramesh R. A novel algorithm for real time task scheduling in multiprocessor environment. *Cluster Comput*. 2019. № 22. С. 13761–13771. DOI: https://doi.org/10.1007/s10586-018-2083-5

46. Otoom M., Paul J.M., Workload Mode Identification for Chip Heterogeneous Multiprocessors. *Int J Parallel Prog*. 2012. № 40. С. 184–224. DOI: https://doi.org/10.1007/s10766-011-0175-4

47. De Silva L.C., Morikawa C., Petra, I. M. State of the art of smart homes. *Eng. Appl. Artif. Intell*. 2012. №25. P.1313–1321.

48. Zhang D., Shah N., Papageorgiou L. G. Efficient energy consumption and operation management in a smart building with microgrid. *Energy Convers. Manag*. 2013. №74. P. 209–222.

49. Pedrasa M., Spooner T., MacGill I. Coordinated Scheduling of Residential Distributed Energy Resources to Optimize Smart Home Energy Services. *IEEE Trans. Smart Grid.* 2010. №1. P.134–143.

50. Gu H., Diao Y., Liu W., Zhang X. The design of smart home platform based on Cloud Computing. *In Proceeding of the International Conference on the Design of Smart Home Platform Based on Cloud Computing, Harbin, China.* 2011. P. 12–14

51. Płaczek, B., Bernaś, M. Uncertainty-based information extraction in wireless sensor networks for control applications. *Ad Hoc Netw*. 2014. №14. P.106–117.

52. Greer C., Burns M., Wollman D., Griffor E. Cyber-physical systems and Internet of Things / *NST Special Publication 1900*. 2019. №202. P.52. https:// doi.org/10.6028/NIST.SP.1900-202.

53. Krening S., Feigh M. Interaction algorithm effect on human experience with reinforcement learning. *ACM Transactions on Human-Robot Interaction*, 2018. №82 P.1–22.

54. Ibarra-Esquer J. E., González-Navarro F. F., Flores-Rios B. L., Burtseva L., Astorga-Vargas M. A., Tracking the evolution of the internet of things concept across different application domains. *Sensors*. 2017. № 17(6). P. 1379. http://www.doi.org/10.3390/s17061379.

55. Minerva R., Biru A., Rotondi D. Towards a definition of the Internet of Things (IoT) // *IEEE Internet Initiative*. 2015. №1. P. 1-86. https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Issue1_14MAY15.pdf.

56. Iskandar N., Diah M., Ismail M. Identifying Artificial Intelligence Pathfinding Algorithms for Platformer Games. *IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS).* 2020. P. 74-80, doi: 10.1109/I2CACIS49202.2020.9140177.

57. Albert M. K. The Past, Present and Future of Cyber-Physical Systems: A Focus on Models. *EECS Department, University of California, Berkeley, CA 94720-1770, USA.* 2015. P.15

58. Ibarra-Esquer J.E, González-Navarro F.F, Flores-Rios B.L, Burtseva L, AstorgaVargas M.A. Tracking the evolution of the internet of things concept across different application domains. *Sensors*. 2017. № 17(6). P. 1379. http://www.doi.org/10.3390/s1706137/.

59. Elbsir H. E., Kassab M., Bhiri S., Bedoui M. H., Evaluation of LoRaWAN Class B efficiency for downlink traffic. *16th International Conference on Wireless and*

Mobile Computing, Networking and Communications (WiMob). 2020. P.105-110, doi: 10.1109/WiMob50308.2020.9253405.

60. Rawat D., Rodrigues J., Stojmenovic I., Sanfelice R.G. Analysis and Design of Cyber-Physical Systems. A Hybrid Control Systems Approach. Cyber-Physical Systems: From Theory to Practice / *CRC Press*. 2016. ISBN 978-1-4822-6333-6.

61. Park K. J., Zheng R., Liu X. Cyber-physical Systems: Milestones and Research Challenges. *Editorial Computer Communications.* 2012. № 36(1). P. 1-7. https://doi.org/10.1016/j.comcom.2012.09.006.

62. Fitz T., Theiler M., Smarsly K. A metamodel for cyberphysical systems. *Advanced Engineering Informatics*. 2019. V. 41.Article 100930.

63. Galin D. Software quality. Concepts and practice. / Publisher: *Wiley-IEEE Press.* 2018. P. 720

64. Garst Smith Howard T. Software quality assurance: A guide for developers and auditors / Publisher: *CRC Press Inc*. 2020. P. 480.

65. Suryn W. Software quality engineering. A practitioner's approach / Publisher: *Wiley-IEEE Computer Society Pr*. 2014. P. 208

66. ISO/IEC 25023:2016 Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE). Measurement of system and software product quality [Electronic resource] // *ISO.org*. Mode of acces: https://www.iso.org/uk/standard/35747.html.

67. Khaitan S. K., McCalley J. D., Design techniques and applications of cyberphysical systems / *A survey IEEE Systems Journal*. 2014. № 9(2). P. 350-365. https://doi.org/10.1109/JSYST.2014.2322503.

68. Faraone J., Gambardella G., Boland D., Fraser N., Blott M., Leong PHW. Customizing low-precision deep neural networks for FPGAs. / *28th International Conference on Field Programmable Logic and Applications (FPL), IEEE*. 2018. P. 97–102

69. Lee, Ming-Chang. Software Quality Factors and Software Quality Metrics to Enhance Software Quality Assurance. *British Journal of Applied Science & Technology*. 2014 № 4. P.10 9734/BJAST/2014/10548.

70. Олеськів О. Вимірювальна техніка та метрологія. Міжвідомчий науково-технічний збірник / *Видавництво Національного університету «Львівська політехніка»*. 2015. № 76. С. 132– 137.

71. Lu Y. Industry 4.0: A survey on technologies, applications and open research issues. *Journal of Industrial Information Integration*. 2017. № 6. P. 1-10. https://doi.org/10.1016/j.jii.2017.04.005.

72. Zhang W., Asiri A. M., Liu D. Nanomaterial-Based Biosensors for Environmental and Biological Monitoring of Organophosphorus Pesticides and Nerve Agents . *TrAC Trends in Analytical Chemistry*. 2014. P. 1–10.

73. Tracy T., Fu Y., Roy I., Jonas E., Glendenning P. Towards Machine Learning on the Automata Processor. *High Performance Computing. ISC High Performance 2016. Lecture Notes in Computer Science.* 2016. V.9697. P. 200-218. doi:10.1007/978-3-319-41321- 1_11.

74. Kim Y., Shin D., Lee J., Lee Y., Yoo H. A 0.55V 1.1mW artificialintelligence processor with PVT compensation for micro robots. *2016 IEEE International Solid-State Circuits Conference (ISSCC)*. 2016. P. 258-259. doi: 10.1109/ISSCC.2016.7418005.

75. Ma H. Internet of Things: Objectives and Scientific Challenges. *Journal of Computer Science and Technology*. 2011. № 26(6). P. 919-924. https://doi.org/10.1007/s11390-011-1189-5.

76. Мартинюк О.Р., Яшина О.М., Радельчук Г.І., Кустовський Р.С. Порівняння програмних метрик для оцінки якості програмних продуктів. *Вісник ХНУ: серія Технічні науки*. 2021. №5. С.166-169.

77. Pushkar O., Hrabovskyi Y. Methodology for developing an intelligent user interface for educational publications in the e-learning system. *Development Management*. 2019. V. 17. № 3. P. 23-34

78. Ghiani G., Manca M., Paternò F. Authoring context-dependent crossdevice user interfaces based on trigger/action rules. *Proceedings of the 14th international conference on mobile and ubiquitous multimedia. ACM*. 2015. P. 313– 322.

79. Pillai, A.S., Singh, K., Saravanan, V. A genetic algorithm-based method for optimizing the energy consumption and performance of multiprocessor systems. *Soft Comput.* 2018. № 22. С. 3271–3285. DOI: https://doi.org/10.1007/s00500-017-2789-y

80. Gavrilov, V.S., Kazennov, G.G. Method of simulation the asymmetric memory access for solving synchronization problems in multiprocessor systems. Russ Microelectron 2014. № 43. С. 496–500. DOI: https://doi.org/10.1134/S1063739714070087

81. Furugyan, M.G. Scheduling in Multiprocessor Systems with Additional Restrictions. *J. Comput. Syst. Sci. Int*. 2018. № 57. С. 222–229. DOI: https://doi.org/10.1134/S1064230718020077

82. Lv, F., Cui, HM., Wang, L. Dynamic I/O-Aware Scheduling for Batch-Mode Applications on Chip Multiprocessor Systems of Cluster Platforms. *J. Comput. Sci. Technol*. 2014. № 29. С. 21–37. DOI: https://doi.org/10.1007/s11390- 013-1409-2

83. Regnier, P., Lima, G., Massa, E. Multiprocessor scheduling by reduction to uniprocessor: an original optimal approach. *Real-Time Syst.* 2013. № 49. С. 436–474. DOI: https://doi.org/10.1007/s11241-012-9165-x

ДОДАТОК А

Базові принципи реалізації підсистеми ідентифікації користувача на Java з використанням OpenCV, MaryTTS та Android Fingerprint API

```
import org.opencv.core.Core;
import org.opencv.core.Mat;
import org.opencv.core.MatOfRect;
import org.opencv.core.Point;
import org.opencv.core.Rect;
import org.opencv.core.Scalar;
import org.opencv.core.Size;
import org.opencv.imgcodecs.Imgcodecs;
import org.opencv.imgproc.Imgproc;
import org.opencv.objdetect.CascadeClassifier;
public class UserIdentificationSystem {
  public static void main(String[] args) {
      System.loadLibrary(Core.N
ATIVE_LIBRARY_NAME);
      // Завантаження зображення та ініціалізація детектора обличчя
      Mat image = Imgcodecs.imread("path/to/image.jpg");
      CascadeClassifier faceDetector = new
CascadeClassifier("path/to/opencv/data/haarcascades/haarcascade_frontalface_alt.xml")
;
      // Детектування обличчя
      MatOfRect faceDetections = new MatOfRect();
      faceDetector.detectMultiScale(image, faceDetections);
      // Обробка результатів детектування обличчя
      for (Rect rect : faceDetections.toArray()) {
```

```
            Imgproc.rectangle(image, new Point(rect.x, rect.y), new Point(rect.x + rect.width,
rect.y + rect.height), new Scalar(0, 255, 0));
        }
        // Збереження результатів
        Imgcodecs.imwrite("path/to/output.jpg", image);
        MaryTTS
    }
}
```

ДОДАТОК Б

Копія наукової публікації

INTERNATIONAL SCIENTIFIC JOURNAL *ISSN 2710-0766*
«COMPUTER SYSTEMS AND INFORMATION TECHNOLOGIES»

UDC 004.9: 347.151
https://doi.org/10.31891/csit-2022-4-3

TETIANA HOVORUSHCHENKO, SERGII ALEKSOV,
SNIZHANA TALAPCHUK, OLEKSII SHPYLYUK, VIKTOR MAGDIN
Khmelnytskyi National University

OVERVIEW OF THE METHODS AND TOOLS FOR SITUATION IDENTIFICATION AND DECISION-MAKING SUPPORT IN THE CYBERPHYSICAL SYSTEM «SMART HOUSE»

The technology of a smart house is mostly understood as a system that combines a number of subsystems that provide comfortable living conditions for residents in the room and make it possible to significantly reduce energy costs. A house is called smart if it has a certain computer or control system for managing engineering equipment. "Smart House" should be designed so that all services can be integrated with each other with minimal costs (in terms of finances, time and effort), and their maintenance would be organized in an optimal way.

The "Smart House" system should competently allocate resources, reduce operating costs and provide a clear control and management interface. Such an intelligent system should be able to recognize specific planned and emergency situations occurring in the home and respond to them (make decisions) in accordance with the given program. Therefore, today the urgent task is to recognize the situation and support decision-making in the "Smart House" cyber-physical system.

The conducted overview of methods and tools for situation identification and decision-making support in the "Smart House" cyber-physical system showed that: in existing solutions, situation recognition occurs only for one of the groups of the system of managed housing functions or does not occur at all; existing solutions provide decision-making support for only one of the groups of the system of managed housing functions or do not provide it at all; the available solutions do not provide for the possibility of assessing the sufficiency of information for decision-making in the "Smart House" cyber-physical system.

Therefore, there is a need to develop such methods and tools for situation identification and decision-making support in the "Smart House" cyber-physical system, which would: perform situation recognition for all 5 groups of the system of managed housing functions; provide the decision-making support for all 5 groups of the system of managed housing functions; perform an assessment of the sufficiency of information for making all decisions in the "Smart House" cyber-physical system, which will be the focus of the authors' further efforts.

Keywords: cyber-physical system "Smart House", system of managed housing functions, housing microclimate management; housing lighting control; housing security system; management of multimedia systems of housing; control of household appliances and power grid of housing.

ТЕТЯНА ГОВОРУЩЕНКО, СЕРГІЙ АЛЕКСОВ,
СНІЖАНА ТАЛАПЧУК, ОЛЕКСІЙ ШПИЛЮК, ВІКТОР МАГДІН
Хмельницький національний університет

ОГЛЯД МЕТОДІВ І ЗАСОБІВ РОЗПІЗНАВАННЯ СИТУАЦІЇ ТА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ У КІБЕРФІЗИЧНІЙ СИСТЕМІ «РОЗУМНИЙ БУДИНОК»

Під технологією розумного будинку здебільшого розуміють систему, що об'єднує в собі ряд підсистем, які забезпечують комфортні умови проживання мешканців у приміщенні та надають змогу суттєво зменшити витрати енергоносіїв. Будинок називається розумним, якщо в ньому наявна певна комп'ютерна чи контролююча система управління інженерним оснащенням. «Розумний будинок» повинен бути спроектований так, щоб всі сервіси могли інтегруватися один з одним з мінімальними витратами (з точки зору фінансів, часу і трудомісткості), а їх обслуговування було б організовано оптимальним чином.

Система «Розумний будинок» повинна грамотно розподіляти ресурси, знижувати експлуатаційні витрати і забезпечувати зрозумілий інтерфейс контролю і управління. Така інтелектуальна система повинна вміти розпізнавати конкретні заплановані та надзвичайні ситуації, що відбуваються у помешканні, і реагувати на них (приймати рішення) відповідно до заданої програми. Отже, на сьогодні актуальним завданням є розпізнавання ситуації та підтримки прийняття рішень у кіберфізичній системі «Розумний будинок».

Проведений огляд методів і засобів розпізнавання ситуації та підтримки прийняття рішень у кіберфізичній системі «Розумний будинок» показав, що: в наявних рішеннях розпізнавання ситуацій відбувається лише для однієї з груп системи керованих функцій житла або не відбувається взагалі; наявні рішення передбачають підтримку прийняття рішень лише для однієї з груп системи керованих функцій житла або не передбачають її взагалі; в наявних рішеннях не передбачається можливість оцінювання достатності інформації для прийняття рішень у кіберфізичній системі «Розумний будинок».

Отже, виникає необхідність в розробленні таких методів і засобів розпізнавання ситуації та підтримки прийняття рішень у кіберфізичній системі «Розумний будинок», які б: виконували розпізнавання ситуацій для всіх 5 груп системи керованих функцій житла; передбачали підтримку прийняття рішень для всіх 5 груп системи керованих функцій житла; виконували оцінювання достатності інформації для прийняття всіх рішень у кіберфізичній системі «Розумний будинок», на що й будуть спрямовані подальші зусилля авторів.

Ключові слова: кіберфізична система «Розумний будинок», система керованих функцій житла, керування мікрокліматом житла; керування освітленням; система безпеки; керування системами мультимедіа; керування побутовою технікою та електромережею.

INTERNATIONAL SCIENTIFIC JOURNAL ISSN 2710-0766
«COMPUTER SYSTEMS AND INFORMATION TECHNOLOGIES»

Introduction

"Smart House" is a living environment of a modern type, organized for people to live with the help of automation and high-tech devices that form an intelligent control system to ensure the coordinated and automatic operation of all engineering networks of the house [1]. The technology of a smart house is mostly understood as a system that combines a number of subsystems that provide comfortable living conditions for residents in the room and make it possible to significantly reduce energy costs [2]. A house is called smart if it has a certain computer or control system for managing engineering equipment [2]. "Smart House" should be designed so that all services can be integrated with each other with minimal costs (in terms of finances, time and effort), and their maintenance would be organized in an optimal way [3].

The "Smart House" system competently allocates resources, reduces operating costs and provides a clear control and management interface. Such an intelligent system should be able to recognize specific planned and emergency situations occurring in the home and respond to them according to a given program: one of the systems, according to the programmed algorithm, can control the behavior of others [1].

An important feature and property of the "Smart House", which distinguishes it from other ways of organizing the living environment, is that it is the most progressive concept of human interaction with the living space, when the resident of the house chooses one of the programmed scenarios, and the automated control system in accordance with external and internal conditions sets the parameters and monitors the operating modes of all engineering systems and electrical devices [1].

The system of managed housing functions consists of *five main groups* [1]:

1) housing microclimate management;
2) housing lighting control;
3) housing security system;
4) management of multimedia systems of housing;
5) control of household appliances and power grid of housing.

Creating and maintaining an optimal *home microclimate* is the most important condition for high efficiency, productive rest and health of residents of a house or apartment. The climate control system in the room makes it possible to set the optimal level of temperature, humidity, the amount of fresh air inflow, control the operation of the air filtration system, and create an individual climate system for each family member, in particular, for a child [1].

Lighting control of the residential environment is divided into control of three types of lighting: natural, artificial and light dynamics (Fig. 1). In order to regulate the illumination of the premises by natural daylight and shade the windows in the evening, the "Smart House" system controls the positions of the blinds and shutters, as well as the mechanical opening and closing of the curtains. The intelligent system for managing artificial lighting sources regulates the brightness and number of lighting devices for each individual room or functional zone, depending on the time of day, weather conditions, and the type of activity of the residents at a specific time. One of the important possibilities of the "smart house" is the creation of dynamic light scenarios, when pressing one button turns on the optimal lighting for a particular situation [1, 4, 5].

Fig. 1. Typical implementation of a lighting control system

INTERNATIONAL SCIENTIFIC JOURNAL ISSN 2710-0766
«COMPUTER SYSTEMS AND INFORMATION TECHNOLOGIES»

The security system in the "Smart House" system has several areas of protection: protection against intrusion, protection against water and gas leaks, fire safety, video surveillance system, alarm buttons and simulation of the presence of the owners at home [1, 5, 6].

In addition to the service function, the "Smart House" is also equipped with *internal multimedia systems* for the entertainment of the owners of the house and their guests: multiroom (multi-zone audio and video distribution system), media server, home theater (Fig. 2) [1].

Fig. 2. Typical implementation of the "multiroom" system

The management of household appliances and the electrical network is an important part of the overall complex of intelligent management of the housing environment. The following components can be attributed to it: scenarios for switching on or off the equipment, control of individual sockets or their groups, control of household appliances (Fig. 3) [1, 7].

Fig. 3. Typical implementation of remote control in the house

Systems of intelligent control of the housing environment have a wide range of functional purposes, perform numerous operations according to many scenarios [1, 8].

A homeowner doesn't need to have deep programming knowledge to operate such a powerful system, as all scenarios are pre-programmed and configured to suit the needs of the family. It is enough for home owners to control the functions of the "Smart House" through control devices with an intuitive interface [1, 9, 10].

Therefore, today *the urgent task* is to recognize the situation and support decision-making in the "Smart House" cyber-physical system.

Overview of the methods and tools for situation identification and decision-making support in the cyberphysical system "Smart House"

Let's conduct an overview of known methods and tools for situation identification and decision-making support in the "Smart House" cyber-physical system, highlighting their advantages and disadvantages.

INTERNATIONAL SCIENTIFIC JOURNAL ISSN 2710-0766
«COMPUTER SYSTEMS AND INFORMATION TECHNOLOGIES»

In the paper [2], fuzzy logic algorithms are used to determine the comfortable conditions of stay in the "Smart House" system, in particular, to calculate the comfortable temperatures. A basic term set is formed for each linguistic variable. For example, for the variables "temperature inside the room", "air temperature of the atmosphere", such a set consists of four terms: "cold", "neutral", "warm", "hot". After the selection of linguistic variables, term sets are formed and membership functions are constructed, production rules for the model are compiled. This technique makes it possible to determine how to adjust the temperature to comfortable values by evaluating the internal and external air temperature using the rules of fuzzy logic.

The study [11] developed the rolling-horizon optimization model with a recurrent neural network-driven predicting, which is developed for interactively prediction of uncertainty and optimization of battery energy storage operations in residential smart houses in an iterative fashion. The proposed model can be used for optimizing battery energy storage operations in residential smart houses and for efficiently utilizing solar power.

Home energy management systems are used for management of energy consumption in smart houses. The research [12] presented home energy management strategy (OHEM-algorithm) based on the improved binary particle swarm optimization, which intended for optimization of customer satisfaction and electric cost, for getting the accurate, optimal, and desirable solutions for power consumption in the smart homes, for lower the cost of electricity and the user's conformity.

The paper [13] proposes a Smart Apartment Building model, in which multiple distributed power sources are shared by multiple consumers for reducing the operation costs and carbon emissions through the implementation of highly efficient operation methods.

The paper [14] proved that the fuzzy logic with Multi-class Support Vector Machine (SVM) method, which is realized as the fuzzy trapezoidal membership function for each sample within the hyper-sphere and as a linear function of the selected sample's distance in the non-linear SVM hyperplane, is effective in selection of the rules to make decision to the control in temperature and humidity.

Paper [15] made the OTP-based door opening system using Arduino and GSM, which generates the one-time password on mobile phone for unlocking the door and is much safer than the traditional key-based system.

Paper [16] develops the Internet-of-Things-based indoor, comfortable, environmental, and real-time monitoring system for the smart house, which consists of the temperature-and humidity-sensing module and the lightness module. In this system, improved particle swarm optimization (IPSO) is used for creating the ideal and comfortable environment.

The paper [17] investigated the appliance of electrical use as a means for detecting the presence/absence of residents (for example, people suffering from dementia, elderly people living alone, home quarantine) with using the several machine learning algorithms.

The research [18] is devoted to the full state feedback and feed forward control method for determination of the best control theory for control of the servo motor in the smart window systems, which is ised for improving the air circulation and for better automation of the air circulation.

The paper [19] presents the Internet-of-Things-based smart kitchen system, which automatically detects the temperature, monitors the humidity level, includes built-in gas detection sensors for detection of gas leaks in the kitchen, provides the remotely control of the appliances (ovens, freezers, and air conditioners) using the mobile phone. This system is realized on an Arduino board with the Internet connection. The system's goal is remotely control devices (switches, fans, and lights) by any Android smartphone.

The paper [20] presents an Emergy-based methodological approach for assessing the effectiveness of integration of the IoT-based sensing systems into smart buildings for reducing their environmental impacts and energy consumption.

The research [21] focused on the addition of nodes into the IoT-based smart home infrastructure, on the design, implementation and testing the hardware and software of the ESP-Mesh-based smart home system (using the ESP8266) with 3 different nodes – mechanical (door lock), temperature & humidity sensors, electrical (fan, generic power switch, or power plug).

Paper [22] proposed the new data driven method for accurate indirect heat accounting in apartment buildings, which provided the measurements or estimations of the difference of temperature between the indoor environment and the heat transfer fluid, because of which the heating bill's error is reduced by 20%–50%.

The paper [23] proposes a development method and TOPPERS Embedded-Component System on the basis of the embedded components for devices for improving the development efficiency of smart homes' electrical equipment, increasing the electrical equipment's scalability and reducing the developmental complexity.

The paper [24] investigated to the development of the voice-activated home automation system, which integrates the Artificial Intelligence, Internet of Things, Natural Language Processing, Blockchain for a cost-effective and efficient interacting with household equipment.

The paper [25] proposed the method of optimal energy consumption in the smart houses on the basis of the optimal scheduling the household appliances, considering demand side management and techno-economic indices in electrical grids.

The paper [26] is devoted to the development of Internt-of-Things-based system for control heating and cooling within the residential housing, which accurately identifies whether it should be cooled or heated, so that energy is not wasted.

The paper [27] proposed Smart Exterior Home Management System for automatically managing the house's exterior activities without the human efforts (automating the water motor, notifications of the house members about receeiving the posts or deliveries, car parking shed and gate, ring a calling bell, if any person is detected near the main door of the house).

The paper [28] proposed the secure user authentication and key agreement scheme using physical unclonable functions for preventing the security problems, used Real-or-Random model and Burrows-Abadi-Needham logic for verification of the session key security and mutual authentication, used too the Automated Validation of Internet Security Protocols and Applications tool for simulation of the scheme resistance to security attacks.

The paper [29] proposed an automatic control heating and domestic hot water system into a single-family house with installing sensors, PID regulators and actuators, with monitoring control system in the SIEMENS TIA Portal software tool via intelligent interface. This approach increases energy efficiency and reduces the energy costs in the building.

Paper [30] expanded a Secure Smart Home Automation System using Arduino UNO and Wi-Fi technology using Face recognition gadgets with the purpose of the implementation of greater protection to the users and greater effectiveness of the software tool, greater luxury and greater usefulness for the old humans or handicapped.

The paper [31] aims to develop software, which is capable of controlling all electrical devices of a house based on a Raspberry-based control system with the smartphone tools for ensuring the adequate securities.

Results & Discussion

The conducted overeview of methods and tools for situation identification and decision-making support in the "Smart House" cyber-physical system showed that:

1) in existing solutions, recognition of situations occurs only for one of the groups of the system of managed housing functions or does not occur at all;

2) existing solutions provide decision-making support for only one of the groups of the system of managed housing functions or do not provide for it at all;

3) the existing solutions do not provide for the possibility of assessing the sufficiency of information for decision-making in the "Smart House" cyber-physical system.

So, based on the critical analysis of methods and tools for situation identification and decision-making support in the cyber-physical system "Smart House", during which the above-mentioned shortcomings were highlighted, there is a need to develop such methods and tools for situation identification and decision-msking support in the cyber-physical system "Smart house", which would: perform recognition of situations for all 5 groups of the system of managed housing functions; provide the decision-making support for all 5 groups of the system of managed housing functions; evaluate the sufficiency of information for making all decisions in the "Smart House" cyber-physical system (Fig. 4).

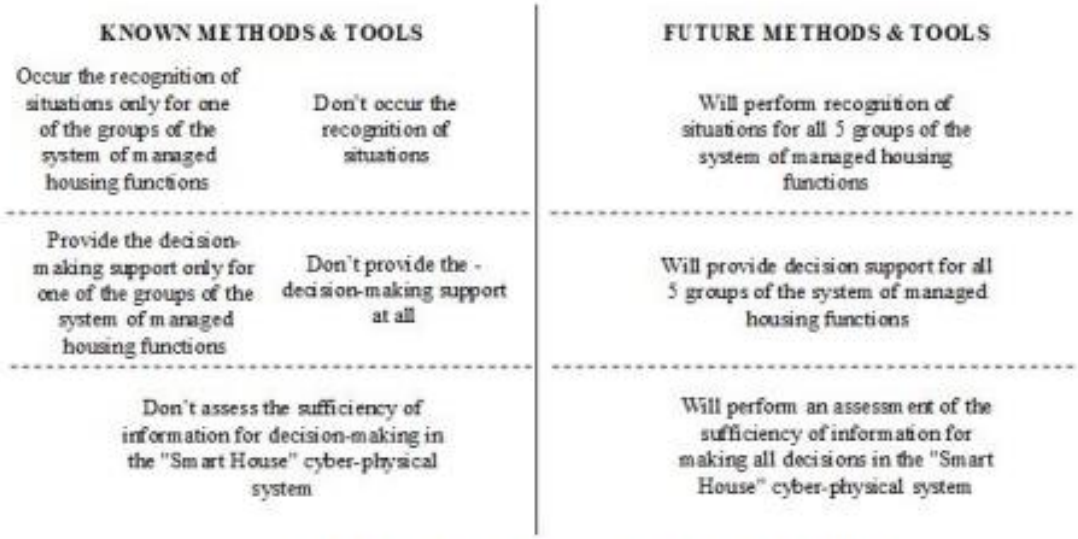


Fig. 4. The role of the proposed approach in the cyber-physical system "Smart House"

Conclusions

The "Smart House" system should competently allocate resources, reduce operating costs and provide a clear control and management interface. Such an intelligent system should be able to recognize specific planned and emergency situations occurring in the home and respond to them (make decisions) in accordance with the given program. Therefore, today the urgent task is to recognize the situation and support decision-making in the "Smart House" cyber-physical system.

The conducted overview of methods and tools for situation identification and decision-making support in the "Smart House" cyber-physical system showed that: in existing solutions, situation recognition occurs only for one of the groups of the system of managed housing functions or does not occur at all; existing solutions provide decision-making support for only one of the groups of the system of managed housing functions or do not provide it at all; the available solutions do not provide for the possibility of assessing the sufficiency of information for decision-making in the "Smart House" cyber-physical system.

Therefore, there is a need to develop such methods and tools for situation identification and decision-making support in the "Smart House" cyber-physical system, which would: perform situation recognition for all 5 groups of the system of managed housing functions; provide the decision-making support for all 5 groups of the system of managed housing functions; perform an assessment of the sufficiency of information for making all decisions in the "Smart House" cyber-physical system, which will be the focus of the authors' further efforts.

References

1. M. Maslova. "Smart House": bibliographic index. URL: https://zounb.zp.ua/wp-content/uploads/2021/07/Rozumnij-budinok-pokazhchik-6.04.21-s-oblozhkoj.pdf.
2. I. Yurchak, P. Vyshynskyi. Application of Fuzzy Logic Algorithms in Smart Home Systems. Computer Systems and Networks. 2018. Vol. 905. Pp. 142-148.
3. S. Kukunin. Development of a holistic methodology for the organization of "Smart House" type systems within the framework of the "Internet of Things" paradigm. Computer-integrated technologies: education, science, production. 2020. Vol. 38. Pp. 40-45.
4. I. Shostak, M. Danova, O. Feoktystova. An approach to the robotization of the functioning processes of the "Smart House" system based on the Internet of Things. The XIII International Scientific and Practical Conference "Integrated intelligent robotic complexes": Proceedings (Kyiv (Ukraine), May 19-20, 2020). Kyiv, 2020. Pp. 48-49.
5. V. Teslyuk, Kh. Beregovska, V. Beregovskyi. Model of operation of subsystems of lighting and protection of an intelligent building. Scientific bulletin of NLTU of Ukraine. 2013. Vol. 23. Issue 10. Pp. 297-303.
6. O. Boreiko, V. Teslyuk, O. Berezsky. Development of components of the "Intelligent House" video surveillance system based on Raspberry Pi. Modeling and information technologies. 2014. Vol. 71. Pp. 66-71.
7. I. Dontsov, O. Bezvesilna. Use of artificial intelligence in home automation and energy saving. The XI All-Ukrainian Scientific and Practical Conference of the Students and PhD Students "A look into the future of instrument building": Proceedings (Kyiv (Ukraine), May 15-16, 2018). Kyiv, 2018. Pp. 505-508.
8. O. Polyakova. Classification of functional constituent elements of the system of intelligent management of the environment in housing design. Bulletin of the Kyiv National University of Technology and Design. Technical sciences. 2016. Vol. 4 (100). Pp. 133-140.
9. D. Fedorov. Increasing the comfort of life with the help of "Safe House" intelligent machines. Scientific notes of the Small Academy of Sciences of Ukraine. Pedagogical sciences. 2018. Vol. 12. Pp. 179-185.
10. I. Sribna, A. Aleksandrov. Interactive automatic system "Smart House". Communication. 2019. Vol. 3. Pp. 55-58.
11. S. Abedi, S. Kwon. Rolling-horizon optimization integrated with recurrent neural network-driven forecasting for residential battery energy storage operations. International Journal of Electrical Power and Energy Systems. 2023. Volume 145. Article number 108589.
12. A. Mohammad, S. Ansari, F. Ali, I. Ashraf. Home Energy Management System with Improved Binary PSO. Lecture Notes in Electrical Engineering. 2023. Vol. 926. Pp. 873 – 881.
13. K. Tamashiro, E. Omine, N. Krishnan, A. Mikhaylov, A. M. Hemeida, T. Senjyu. Optimal components capacity based multi-objective optimization and optimal scheduling based MPC-optimization algorithm in smart apartment buildings. Energy and Buildings. 2023. Vol. 2781. Article number 112616.
14. K. Devi Thangavel, U. Seerengasamy, S. Palaniappan, R. Sekar. Prediction of factors for Controlling of Green House Farming with Fuzzy based multiclass Support Vector Machine. Alexandria Engineering Journal. 2023. Vol. 62. Pp. 279 – 289.
15. P. Srinivasan, R. Sabeenian, B. Thiyaneswaran, M. Swathi, G. Dineshkumar. OTP-Based Smart Door Opening System. Lecture Notes on Data Engineering and Communications Technologies. 2023. Vol. 131. Pp. 87 – 98.
16. W.-T. Sung, S.-J. Hsiao. Creating Smart House via IoT and Intelligent Computation. Intelligent Automation and Soft Computing. 2023. Vol. 35. Issue 1. Pp. 415 – 430.
17. A. Lentzas, D. Vrakas. Machine learning approaches for non-intrusive home absence detection based on appliance electrical use. Expert Systems with Applications. 2022. Vol. 21030. Article number 118454.
18. R. A. Lestari, U. Y. Oktiawati. Full state feedback and feed forward control of servo smart window using MATLAB/Simulink. Indonesian Journal of Electrical Engineering and Computer Science. 2022. Vol. 28. Issue 3. Pp. 1355 – 1362.
19. C. A. U. Hassan, J. Iqbal, M. Khan, S. Hussain, A. Akhunzada, M. Ali, A. Gani, M. Uddin, S. Ullah. Design and Implementation of Real-Time Kitchen Monitoring and Automation System Based on Internet of Things. Energies. 2022. Vol. 15. Issue 18. Article number 6778.
20. T. Kumar, R. Srinivasan, M. Mani. An Emergy-based Approach to Evaluate the Effectiveness of Integrating IoT-based Sensing Systems into Smart Buildings. Sustainable Energy Technologies and Assessments. 2022. Vol. 52. Article number 102225.
21. S. Fuada, Hendriyana. UPISmartHome V.2.0 – A Consumer Product of Smart Home System with an ESP8266 as the Basis. Journal of Communications. 2022. Vol. 17. Issue 7. Pp. 541 – 552.
22. Y. Stauffer, F. Saba, R. Carrillo, M. Boegli, A. Malengo, A. Hutter A. Smart sensors network for accurate indirect heat accounting in apartment buildings. Journal of Building Engineering. 2022. Vol. 461. Article number 103534.
23. J. Y. Jiang, F. Qi, H. Oyama, H. Nagashima, T. Azumi. ECHONET Lite Framework Based on Embedded Component Systems. ECTI Transactions on Computer and Information Technology. 2022. Vol. 16. Issue 1. Pp. 74-83.
24. S. Ansar, K. Jaiswal, S. Aggarwal, S. Shukla, J. Yadav, N. Soni. Smart Home Personal Assistants: Fueled by Natural Language Processor and Blockchain Technology. The 2022 2nd International Conference on Interdisciplinary Cyber Physical Systems: Proceedings (Chennai, May 9-10, 2022). Chennai, 2022. Pp. 113-117.
25. I. Muda, N. Dwijendra, T. Awsi, B. Bashar, M. Majeed. Optimal Energy Scheduling of Appliances in Smart Buildings Based on Economic and Technical Indices. Environmental and Climate Technologies. 2022. Vol. 26. Issue 1. Pp. 561 – 573.

26. W. Yaici, E. Entchev, M. Longo. Internet of Things (IoT)-Based System for Smart Home Heating and Cooling Control. The 2022 IEEE International Conference on Environment and Electrical Engineering and 2022 IEEE Industrial and Commercial Power Systems Europe: Proceedings (Prague, June 28 – July 1, 2022). Prague, 2022. Code 182192.

27. C. Prasad, Y. Srikanth, P. R. Rao, K. Sreedhar. Smart exterior home management system using Arduino Uno and Tinkercad. AIP Conference Proceedings. 2022. Vol. 2418. Article number 030039.

28. Y. Cho, J. Oh, D. Kwon, S. Son, J. Lee, Y. Park. A Secure and Anonymous User Authentication Scheme for IoT-Enabled Smart Home Environments Using PUF. IEEE Access. 2022. Vol. 10. Pp. 101330 – 101346.

29. K. Osman, M. Petic, T. Alajbeg, M. Stefic. Comparison of the theoretical mathematical model and the experimental approach in the development of an automatic control system in a smart family house. The 2022 7th International Conference on Smart and Sustainable Technologies: Proceedings (Split, July 5-8, 2022). Split, 2022. Code 182191.

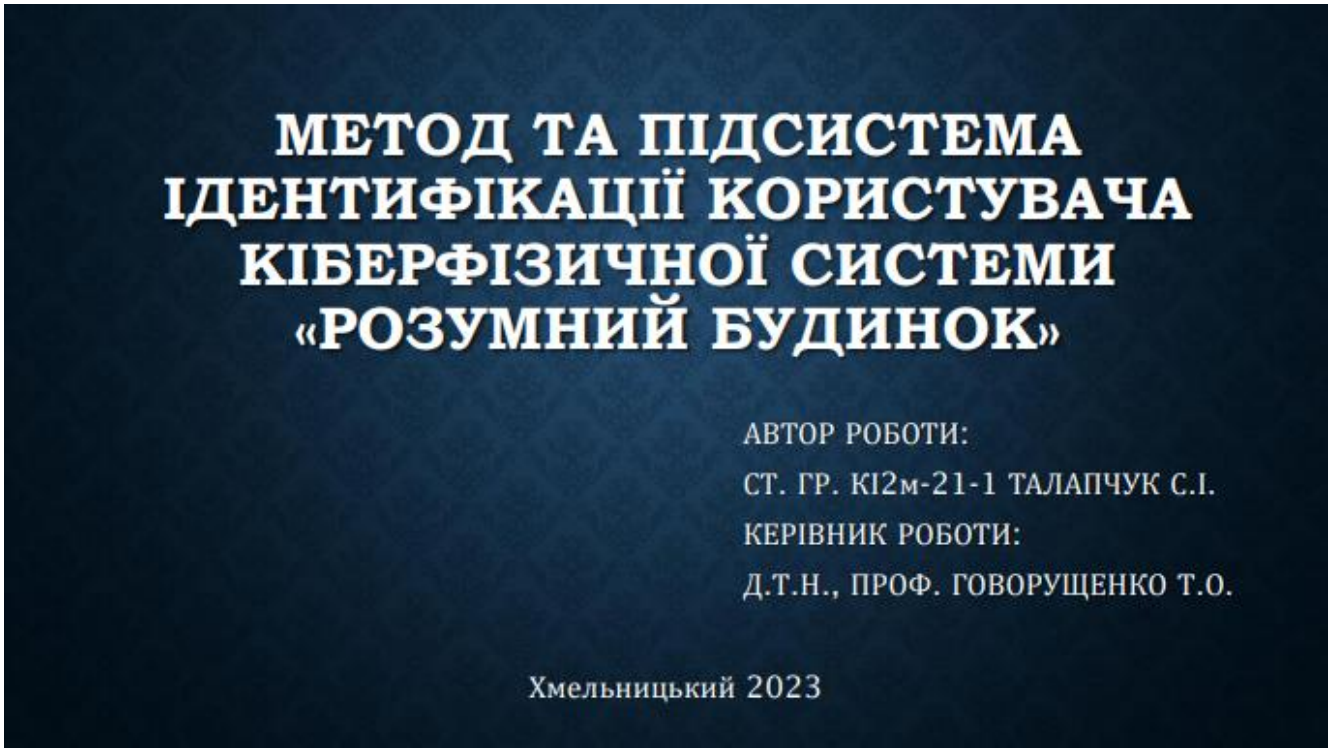
30. A. Nirmala, V. Asha, P. Chandra, H. Priya, S. Raj. IoT based Secure Smart Home Automation System. The 2022 IEEE Delhi Section Conference: Proceedings (Online, February 11-13, 2022). Online, 2022. Code 178847.

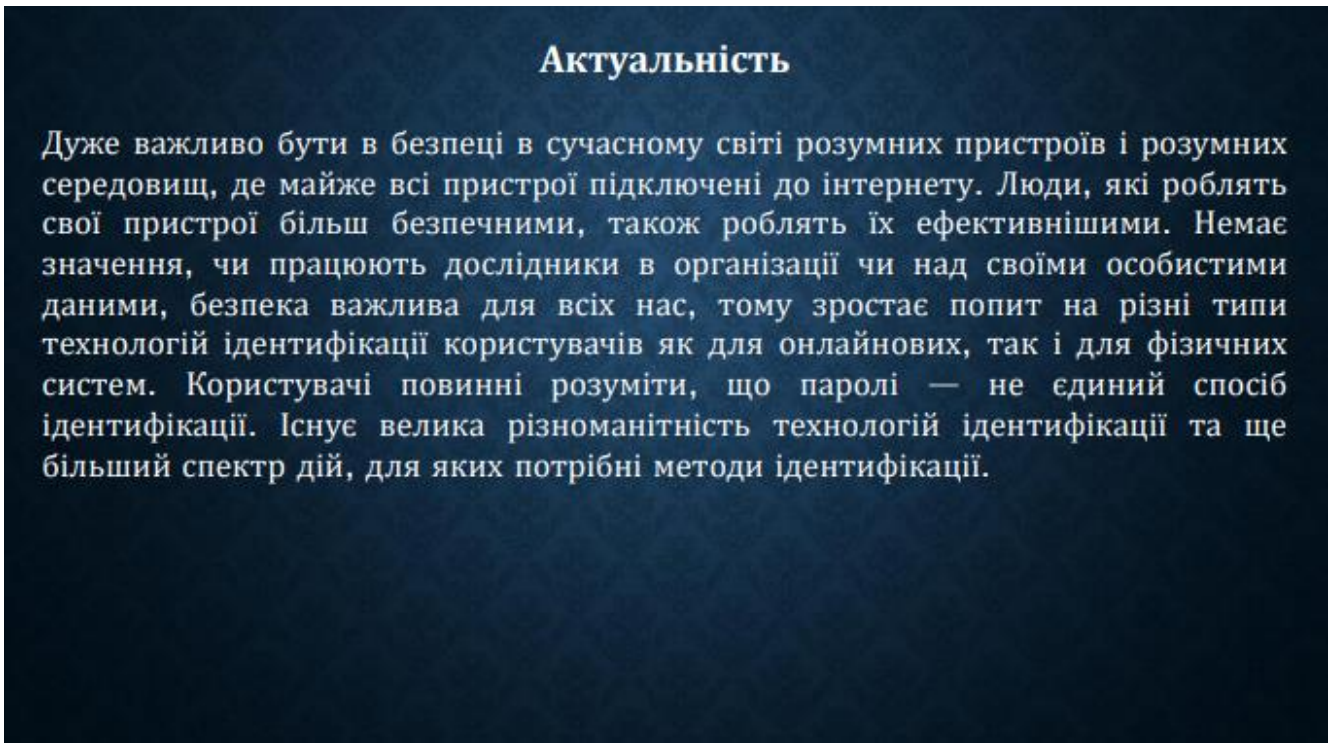
31. Y. Tjandi, M. Paloboran, M. Yahya, A. Idkhan. Raspberry-based control system for the future house. Tehnicki Vjesnik. 2021. Vol. 28. Issue 6. Pp. 2115 – 2120.

Tetiana Hovorushchenko Тетяна Говорущенко	DrSc (Engineering), Professor, Head of Computer Engineering & Information Systems Department, Khmelnytskyi National University https://orcid.org/0000-0002-7942-1857 e-mail: govorushchenko@gmail.com	Доктор технічних наук, професор, завідувач кафедри комп'ютерної інженерії та інформаційних систем, Хмельницький національний університет
Sergii Aleksov Сергій Алексов	PhD student of Computer Engineering & Information Systems Department, Khmelnytskyi National University e-mail: aleksov@gmail.com	Аспірант кафедри комп'ютерної інженерії та інформаційних систем, Хмельницький національний університет
Snizhana Talapchuk Сніжана Талапчук	MSc student of Computer Engineering & Information Systems Department, Khmelnytskyi National University e-mail: snizhanatalapchuk@gmail.com	Магістрантка кафедри комп'ютерної інженерії та інформаційних систем, Хмельницький національний університет
Oleksii Shpylyuk Олексій Шпилюк	Student of Computer Engineering & Information Systems Department, Khmelnytskyi National University e-mail: oleksa280804@gmail.com	Студент кафедри комп'ютерної інженерії та інформаційних систем, Хмельницький національний університет
Viktor Magdin Віктор Магдін	Junior researcher of the Scientific and Research Department, Khmelnytskyi National University e-mail: vityok555@gmail.com	Молодший науковий співробітник науково-дослідної частини, Хмельницький національний університет

ДОДАТОК В

Презентація дипломної роботи





- Мета дослідження – підвищення ефективності ідентифікації користувача кіберфізичної системи «Розумний будинок»
- Об’єкт дослідження – процес ідентифікації користувача кіберфізичної системи «Розумний будинок»
- Предмет дослідження – метод та підсистема ідентифікації користувача кіберфізичної системи «Розумний будинок»

ОТРИМАНІ НАУКОВІ РЕЗУЛЬТАТИ

- **Метод ідентифікації користувача кіберфізичної системи «Розумний будинок»**, який забезпечує верифікацію наданих під час автентифікації користувачем даних (відбиток пальця, скан сітківки ока, тощо) та висновок про можливість доступу до тих чи інших ресурсів та підсистем кіберфізичної системи «Розумний будинок» на основі такої верифікації.
- **Архітектура підсистеми ідентифікації користувача кіберфізичної системи «Розумний будинок»**, спрямована на перевірку даних користувача, наданих під час автентифікації, а також на формування висновку про ідентифікацію користувача та його роль і права доступу.

ОТРИМАНІ ПРАКТИЧНІ РЕЗУЛЬТАТИ

Підсистема ідентифікації користувача кіберфізичної системи «Розумний будинок», спрямована на перевірку даних користувача, наданих під час автентифікації (відбиток пальця, скан сітківки ока, результати алкотесту, тощо), а також на формування висновку про ідентифікацію користувача та про можливість доступу до тих чи інших ресурсів та підсистем кіберфізичної системи «Розумний будинок» на основі такої верифікації.

ЗАДАЧІ ДОСЛІДЖЕННЯ:

1. ПРОВЕСТИ АНАЛІЗ ВІДОМИХ МЕТОДІВ ТА РІШЕНЬ ДЛЯ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА КІБЕРФІЗИЧНОЇ СИСТЕМИ «РОЗУМНИЙ БУДИНОК»;
2. МОДЕЛЮВАННЯ ПРОЦЕСУ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА КІБЕРФІЗИЧНОЇ СИСТЕМИ «РОЗУМНИЙ БУДИНОК»;
3. ЗАПРОПОНУВАТИ МЕТОД ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА КІБЕРФІЗИЧНОЇ СИСТЕМИ «РОЗУМНИЙ БУДИНОК»;
4. НА ОСНОВІ ЗАПРОПОНОВАНОГО МЕТОДУ РОЗРОБИТИ ПІДСИСТЕМУ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА КІБЕРФІЗИЧНОЇ СИСТЕМИ «РОЗУМНИЙ БУДИНОК».

Ідентифікації користувача та її види

Ідентифікація - це процедура розпізнавання користувача за його ідентифікатором (іменем).
Загальна процедура ідентифікації та автентифікації користувача при наданні доступу до АС наведена на рисунку 1.
Основні методи ідентифікації користувача в кіберфізичних системах, таких як "Розумний будинок", включають:

- Використання біометричних даних: це можуть бути відбитки пальців, сканування обличчя, розпізнавання голосу, що дозволяє ідентифікувати користувачів за їхніми фізичними характеристиками.
- Використання ідентифікаторів: такі як магнітні картки, RFID-мітки або NFC-технології, що можуть бути прикріплені до ключів або телефонів, для ідентифікації користувача.
- Використання паролів: пароль - це секретний код, який користувач повинен ввести, щоб отримати доступ до системи.
- Використання додатків: додатки, які встановлюються на смартфони або планшети користувачів, можуть використовуватися для ідентифікації користувача.

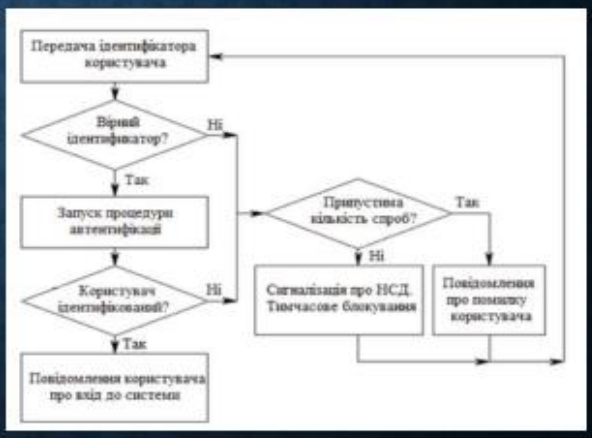


Рисунок 1 - Класична процедура ідентифікації

АНАЛІЗ ВІДОМИХ МЕТОДІВ ТА РІШЕНЬ ДЛЯ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА КІБЕРФІЗИЧНОЇ СИСТЕМИ «РОЗУМНИЙ БУДИНОК»

Amazon Echo/Alexa - система контролю за будинком, яка використовує голосові команди для керування пристроями у будинку. Пристрій можна підключити до інтернету, щоб керувати його за допомогою мобільного додатку. Однією з переваг цієї системи є її простота використання, але вона може мати проблеми з розпізнаванням голосу та потребує постійного з'єднання з Інтернетом.

Google Nest - це система "розумного будинку", яка дозволяє контролювати температуру, освітлення та безпеку у будинку за допомогою мобільного додатку або голосових команд. Однією з переваг цієї системи є її інтеграція з Google Assistant, але вона може бути дорогим варіантом, особливо якщо потрібно встановлювати додаткові пристрої.

Apple HomeKit - це система "розумного будинку", яка дозволяє керувати пристроями у будинку з допомогою iPhone або iPad. Ця система є досить простою у використанні, але вона може мати обмежені можливості порівняно з іншими системами.

Samsung SmartThings - це кіберфізична система для будинку, яка дозволяє керувати різними пристроями з одного місця за допомогою мобільного додатку або голосового помічника. Ця система включає в себе гнучку платформу, що підтримує різноманітні протоколи зв'язку, такі як Wi-Fi, Bluetooth, Z-Wave та Zigbee, що дозволяє злити в єдину систему різноманітні речі, що знаходяться в будинку - від освітлення та клімат-контролю до домашньої безпеки та електроніки.

МОДЕЛЮВАННЯ ПРОЦЕСУ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА КІБЕРФІЗИЧНОЇ СИСТЕМИ “РОЗУМНИЙ БУДИНОК”

Обробка голосу:

- фільтрація шуму: $H(w) = \frac{Y(w)}{X(w)}$;
- підвищення частоти дискретизації: $y(n) = x\left(n \cdot \frac{L}{M}\right)$;
- оцінка основного тонального періоду голосу: $F0(n) = argmax \cdot R\_x(\tau)$;
- виділення спектральних характеристик: $MFCC(k) = \sum n \left[\log(S(n,k)) \cdot \cos(\pi \cdot (k - \frac{1}{2}) \cdot \frac{n}{N})\right]$;
- гауссівська суміш моделей: $p(x) = \sum\_i w\_i \cdot N(x \mid \mu\_i, \sum\_i)$.

Перед процеси даних:

- фільтрація за допомогою середньої фільтрації: $N(x,y) = \{I(x+i, y+j) | -\frac{k}{2} \leq i,j \leq \frac{k}{2}\}$;
- середнє значення N: $M(x,y) = \frac{1}{k^2} \cdot \sum\sum I(x+i, y+j)$;
- динамічну модель системи: $Y(t) = A \cdot Y(t-1) + B \cdot U(t) + w(t)$;
- визначення моделі спостереження: $X(t) = H \cdot Y(t) + v(t)$;
- етап прогнозу: $Y'(t) = A * Y(t-1) + B * U(t)$, $P'(t) = A * P(t-1) * A\text{^}T + Q$;
- етап корекції: $K(t) = P'(t) \cdot H^T \cdot \left(H * P'(t) \cdot H^T + R\right)^{-1}$,

$Y(t) = Y'(t) + K(t) \cdot (X(t) - H \cdot Y'(t))$, $P(t) = (I - K(t) \cdot H) \cdot P'(t)$;

МЕТОД ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА КІБЕРФІЗИЧНОЇ СИСТЕМИ «РОЗУМНИЙ БУДИНОК»

Ефективне та точне визначення методу ідентифікації користувача за допомогою вимоги:

- Надійність і точність ідентифікації користувача.
- Швидкість ідентифікації користувача.
- Масштабованість методу ідентифікації користувача.
- Зручність та легкість використання методу ідентифікації користувача для забезпечення комфорту користувачів.
- Захищеність від зловживання користувачами та зловмисниками.
- Сумісність з існуючими системами безпеки в будинку.

Загальний процес обробки даних із апаратних компонентів

1. ***Збір даних***. Зчитування даних від апаратних компонентів.
2. ***Попередня обробка даних***. На цьому етапі збираються дані з різних апаратних компонентів, таких як камери, мікрофони, сенсори відбитків пальців та пристрої для введення паролів. Дані очищуються від шуму, нормалізуються та приводяться до стандартного формату.
3. ***Визначення особливостей***. На основі попередня обробка даних, алгоритми виявляють ключові характеристики (особливості) для кожного методу ідентифікації. Наприклад, для розпізнавання обличчя можуть використовуватися особливості, пов'язані з формою та розташуванням основних елементів обличчя.
4. ***Класифікація та сумісність***. . Застосовуються алгоритми класифікації для визначення ступеня схожості між отриманими особливостями та збереженими шаблонами користувачів. За результатами порівняння визначається, якому користувачеві відповідають введені дані
5. ***Оцінка вірогідності***. На основі аналізу сумісності, алгоритми оцінюють вірогідність ідентифікації. Якщо вірогідність перевищує певний поріг, користувач вважається ідентифікованим.

Конфіденційність та приватність даних

Конфіденційність у бездротовій системі стосується належного приховування вмісту пакетів даних, які включають або контрольні повідомлення, або інформацію про функціональність інтелектуальних пристроїв, а також запобігання несанкціонованому доступу зловмисників . Впровадження криптографічних методів є поширеним способом захисту цих повідомлень у системі IoT. Складність передових методів шифрування змушує зловмисників знайти секретні ключі для розкриття відкритих текстів і гарантує, що інформація системи не буде виявлена тими, хто не має доступу . З іншого боку, недоліком методів шифрування є те, що вони залишають контекстні дані мережевих повідомлень незахищеними. Прикладами таких даних є ідентифікаційні дані смарт-пристрою, місцезнаходження та час активності. Цей тип даних надає зловмисникам багатий ресурс для отримання важливої інформації про систему, яка може мати більшу цінність, ніж її вміст.

Приватність даних означає, що захищена інформація належить людині, а не пристрою чи системі. Мешканці інтелектуальної будівлі діляться великою кількістю даних про свої справи із системою, а численні вбудовані датчики в різноманітних розумних пристроях відповідають за збір даних про повсякденну діяльність користувачів (ADL). Ці всеосяжні накопичені дані дозволяють інтелектуальним механізмам системи оцінювати ситуацію користувачів і створювати послуги відповідно до їхніх бажаних потреб. Подібним чином здатність системи отримувати дані надає зловмисникам цінний ресурс для виявлення конфіденційної інформації про мешканців .

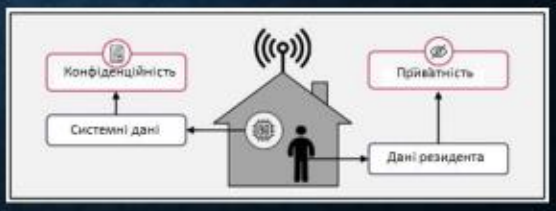


Рис. 2 Типи домашніх даних і відповідні заходи безпеки

На основі попередніх досліджень ми прийшли до такої архітектури підсистеми:

1. Сенсори / пристрої зчитування:
   - Камера для розпізнавання обличчя;
   - Мікрофон для розпізнавання голосу;
   - Сканер відбитків пальців;
   - Сканер сітківки ока.
2. Модуль перед обробки даних:
   - Фільтрація та покращення зображень / сигналів;
   - Виявлення обличчя / очей / пальців на зображеннях;
   - Вирізання та масштабування регіонів інтересу.
3. Модуль витягу властивостей:
   - Розрахунок особливостей для кожного методу ідентифікації (наприклад, MFCC для голосу, HOG або CNN для обличчя, особливості сітківки для сітківки ока, особливості відбитків пальців для відбитків пальців).
4. Модуль порівняння / класифікації:
   - Порівняння властивостей з базою даних користувачів;
   - Застосування алгоритмів класифікації для визначення, чи є особа користувачем системи.
5. Модуль прийняття рішень:
   - Обробка результатів порівняння / класифікації;
   - Визначення довірчого рівня ідентифікації;
   - Прийняття рішення про надання доступу або відмову.
6. База даних користувачів:
   - Зберігання біометричних шаблонів користувачів;
   - Забезпечення інформації для порівняння / класифікації в модулі порівняння / класифікації.
7. Інтерфейс користувача:
   - Відображення статусу ідентифікації (успішно / не успішно);
   - Введення або оновлення біометричних даних для зареєстрованих користувачів;
   - Налаштування параметрів системи ідентифікації та доступу.
8. Модуль управління доступом:
   - Керування доступом до приміщень та пристроїв на основі результатів ідентифікації;
   - Відстеження та реєстрація спроб доступу.
9. Зв'язок з іншими системами розумного будинку:
   - Надсилання сигналів про статус ідентифікації та контролю доступу до інших систем розумного будинку, таких як система безпеки, освітлення, температурний контроль тощо.
   - Зберігання біометричних шаблонів користувачів;
   - Забезпечення інформації для порівняння / класифікації в модулі порівняння / класифікації.

Архітектура підсистеми ідентифікації

ПІДСИСТЕМА ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА КІБЕРФІЗИЧНОЇ СИСТЕМИ “РОЗУМНИЙ БУДИНОК”

Використовуючи алгоритм розроблений в попередніх розділах ми можемо створити прототип підсистеми ідентифікації користувача кіберфізичної системи “Розумний будинок”

Для реалізації можливо використовувати наступні бібліотеки та інструменти:

1) OpenCV та Android Fingerprint API: для роботи з зображеннями обличя та відбитками пальців;
2) TensorFlow або PyTorch: для реалізації нейронних мереж, які використовуються для класифікації та розпізнавання;
3) MaryTTS: для обробки аудіо та розпізнавання голосу;
4) Scikit-learn: для класифікації та обробки даних.

Базові принципи реалізації підсистеми ідентифікації користувача на Java з використанням OpenCV, MaryTTS та Android Fingerprint API

```
public class UserIdentificationSystem {
  public static void main(String[] args) {
    System.loadLibrary(Core.N
ATIVE_LIBRARY_NAME);
    // Завантаження зображення та ініціалізація детектора обличчя
    Mat image = Imgcodecs.imread("path/to/image.jpg");
    CascadeClassifier faceDetector = new CascadeClassifier("path/to/opencv/data/haarcascades/haarcascade_frontalface_alt.xml");
    // Детектування обличчя
    MatOfRect faceDetections = new MatOfRect();
    faceDetector.detectMultiScale(image, faceDetections);
    // Обробка результатів детектування обличчя
    for (Rect rect : faceDetections.toArray()) {
      Imgproc.rectangle(image, new Point(rect.x, rect.y), new Point(rect.x + rect.width, rect.y + rect.height), new Scalar(0, 255, 0));
    }
    // Збереження результатів
    Imgcodecs.imwrite("path/to/output.jpg", image);
    MaryTTS
  }
}
```

Тестування системи

Під час тестування було виявлено що час відповіді нашої підсистеми є швидшим ніж в вище перелічених це відображено на Рис. 2.
Середній час відповіді в підсистемах:

- Amazon Echo/Alexa, 1,72 секунд;
- Google Nest, 2,45 секунд;
- Apple HomeKit 2,62 секунд;
- Samsung SmartThings 3,32 секунд;
- наша підсистема 1,25 секунд.

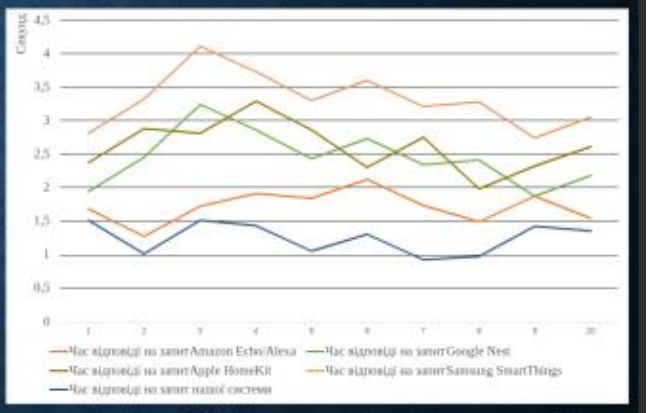


Рисунок 2 – Порівняння часу відповіді при авторизації

Під час тестування авторизації за підбитком пальця використовувався наступний масив даних:

```
fingerprint_data = [
{"id": 1, "fingerprint": [0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9, 1.0]},
{"id": 2, "fingerprint": [0.2, 0.1, 0.4, 0.3, 0.6, 0.5, 0.8, 0.7, 1.0, 0.9]},
{"id": 3, "fingerprint": [0.3, 0.1, 0.2, 0.4, 0.5, 0.7, 0.6, 0.9, 0.8, 1.0]},
{"id": 4, "fingerprint": [0.4, 0.3, 0.2, 0.1, 0.6, 0.5, 0.8, 0.7, 1.0, 0.9]},
{"id": 5, "fingerprint": [0.5, 0.4, 0.3, 0.2, 0.1, 0.6, 0.7, 0.8, 0.9, 1.0]},
...
]
```

fingerprint_data представляє собою список словників, де кожен словник містить унікальний ідентифікатор id та відповідний відбиток пальця fingerprint. Відбиток пальця представлено як список числових значень, які можуть відображати характеристики відбитка пальця, такі як особливості поверхні пальця, співвідношення сірих відтінків та ін.

Використовуючи масив даних було про тестовано та перевірено якість системи авторизації на прикладі аналізу відбитку

ВИСНОВОК

У роботі за результатами виконаних теоретичних та практичних досліджень створена теоретична модель ідентифікації користувача кіберфізичній системі “Розумний будинок”.

У першому розділі ми розглянули існуючі прототипи та їх можливості.

У другому розділі була створена математична модель яка охарактеризувала загальні особливості нашої системи.

У третьому розділі були конкретизовані характеристики майбутньої системи ідентифікації користувача.

У четвертому розділі був створений алгоритм та можлива програмна реалізація ідентифікації в кіберфізичній системі, алгоритми тестування даної системи.

В майбутньому впровадження результатів роботи можуть дозволити збільшити точність та надійність системи ідентентифікації в кіберфізичних системах.

За темою дипломної роботи опублікована одна стаття у фаховому науковому виданні “Computer Systems & Information Technologies 2022” .

ДЯКУЮ ЗА УВАГУ

UNICHECK

Ім'я користувача:
Кафедра КІ

ID перевірки:
1014910864

Дата перевірки:
04.05.2023 07:22:48 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
04.05.2023 07:38:15 EEST

ID користувача:
100005591

Назва документа: Талапчук_Метод та підсистема ідентифікації користувача кіберфізичної системи "Розумни...

Кількість сторінок: 91 Кількість слів: 17096 Кількість символів: 141383 Розмір файлу: 451.99 KB ID файлу: 1014607175

1.38%
Схожість

Найбільша схожість: 0.73% з джерелом з Бібліотеки (ID файлу: 1014424613)

0.61% Джерела з Інтернету	68	Сторінка 93
1.2% Джерела з Бібліотеки	80	Сторінка 93

0.05% Цитат

Цитати	6	Сторінка 94
Посилання	1	Сторінка 94

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи	6

Thu May 04 06:22:43 EEST 2023, Медзатий Дмитро Миколайович, Хмельницький національний університет, ХНУ

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 0.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 9%**

	Документ		Сумарний збіг по Базі Даних	
ID: 112979 Назва: МКР Метод та підсистема ідентифікації користувача кіберфізичної системи “Розумний будинок” Додано в БД: 2023-05-04 Автора: С.І. Талапчук Керівники: Т.О.Говорущенко Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	114099	915	1542 (1%)	24 (3%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Талапчук Сніжана Іванівна

Тема: Метод та підсистема ідентифікації користувача кіберфізичної системи «Розумний будинок»

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи:

Кількість сторінок записки 83

1. Короткий зміст роботи та прийнятих рішень: Метою кваліфікаційної роботи є підвищення ефективності ідентифікації користувача кіберфізичної системи «Розумний будинок».

2. Висновок про відповідність роботи дипломному завданню: Робота повністю, відповідає поставленому завданню.

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: В першому розділі проведено аналіз відомих методів та рішень для ідентифікації користувача кіберфізичної системи «Розумний будинок». В другому розділі проведено моделювання процесу ідентифікації користувача кіберфізичної системи «Розумний будинок». В третьому розділі розроблено правила і метод ідентифікації користувача кіберфізичної системи «Розумний будинок». Вперше розроблено метод ідентифікації користувача кіберфізичної системи «Розумний будинок», який забезпечує верифікацію наданих під час автентифікації користувачем даних (відбиток пальця, скан сітківки ока, тощо) та висновок про можливість доступу до тих чи інших ресурсів та підсистем кіберфізичної системи «Розумний будинок» на основі такої верифікації. В четвертому розділі розроблено підсистему ідентифікації користувача кіберфізичної системи «Розумний будинок». Вперше розроблено архітектуру підсистеми ідентифікації користувача кіберфізичної системи «Розумний будинок», яка забезпечує перевірку даних користувача, наданих під час автентифікації, а також формування висновку про ідентифікацію користувача та його роль і права доступу.

4. Позитивні сторони роботи: отримання двох пунктів наукової новизни.

5. Негативні сторони роботи:

6. Оцінка графічного оформлення та пояснювальної записки роботи: Пояснювальна записка оформлена коректно, згідно діючих стандартів оформлення документації.

7. Відгук про роботу в цілому: Робота виконана на високому науково-технічному рівні.

8. Інші зауваження: _____

9. Оцінка дипломної роботи: добре.

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) д. т. н., професор, завідувач кафедри ТМіТ ХНУ Пученко С. К.

"05" 05 2023 р. _____ (підпис)

Завідувачу кафедри КІІС
д-р.техн.наук, проф. Говорущенко Т. О.

Талапчук_Сніжані Іванівні
ПІБ здобувача вищої освіти

ФІТ, 2 курсу, групи КІ2м-21-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 01.07.2022, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений(а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

22 квітня 2023 року

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ
КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОМАЦІЙНИХ СИСТЕМ
ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: «Метод та підсистема ідентифікації користувача кіберфізичної системи «Розумний будинок»»

Автор: Талапчук Сніжана Іванівна

Спеціальність: 123 – Компютерна інженерія

Освітня програма: освітньо-наукова

Науковий керівник: Говорущенко Тетяна Олександрівна, д.т.н, професор

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділах аналізу існуючих методів, які не описують безпосередньо авторське дослідження, а є прикладами існуючих рішень;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
3) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з 10-40 джерелами на один фрагмент речення;
4) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 1.38% і адресується до 148 першоджерела, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ Т.О. Говорущенко

Гарант ОП _____ О. С. Савенко

Завідувач кафедри КІІСч _____ Т. О. Говорущенко