https://doi.org/10.31891/2219-9365-2025-81-32
УДК 004.93.1

ФОРКУН Юрій
Хмельницький національний університет
https://orcid.org/0000-0002-7906-4191
forkvnjv@khnu.km.ua
МАКАРИШКІН Денис
Хмельницький національний університет
https://orcid.org/0000-0003-3447-811X
makaryshkinde@khmnu.edu.ua
АНТОНЮК Владислав
Хмельницький національний університет
ЛЮБЧИК Віталій
ТОВ «Карат»
https://orcid.org/0000-0003-0053-5542
vitaly1612@gmail.com

ДОСЛІДЖЕННЯ МЕТОДІВ АВТОМАТИЗОВАНОГО КЕРУВАННЯ РЕЄСТРАЦІЄЮ ЛЮДЕЙ У ПРИМІЩЕННІ

В статті проведено дослідження методів реєстрації людей, що є основою систем контролю доступом. Дані системи призначені для персоналізації доступу у приміщення з обмеженим доступом. В основі цих систем полягає застосування комплексу взаємопов'язаного обладнання, що керує ідентифікацією контролем доступу у приміщення. Такі системи поділяються на автономні і мережеві. У статті розглянуті особливості кожного виду систем, їх переваги і недоліки.

Проаналізовано системи, що постачаються провідними світовими виробниками. Наведено основні особливості функціонування, переваги та недоліки. Розглянуто архітектури побудови програмних засобів контролю доступом. До них відносяться монолітні і мікросервісні архітектури. Описані особливості їх алгоритмів, переваги і недоліки. Наведено їх порівняння.

Ключові слова: керування, автоматизація, методи, архітектура, алгоритми.

FORKUN Yuriy, MAKARYSHKIN Denys, ANTONYUK Vladyslav
Khmelnytskyi National University
LIUBCHYK Vitalii
Karat LTD

RESEARCH OF METHODS OF AUTOMATED MANAGEMENT OF REGISTRATION OF PEOPLE IN THE ROOM

The article studies the methods of registering people, which form the basis of modern access control systems. These systems are designed to personalize and regulate access to premises with restricted entry. They ensure that only authorized personnel or individuals with specific permissions can enter certain areas, thereby enhancing security and minimizing unauthorized access risks.

The foundation of such systems lies in the use of a complex of interconnected equipment and software that together manage identification processes and access control mechanisms. These systems are broadly classified into two main types: autonomous and networked. Autonomous systems function independently, without requiring a central control unit, making them simpler and more reliable for smaller-scale implementations. In contrast, networked systems operate under centralized control, allowing for seamless integration with broader security infrastructure and providing enhanced monitoring and reporting capabilities.

The article examines the specific features of each type of access control system, analyzing their advantages and disadvantages. Autonomous systems are typically easier to install and maintain but may lack the scalability and flexibility of networked solutions. Networked systems, on the other hand, offer better management options and integration with other security measures, yet they require more complex deployment and ongoing support.

Additionally, the article reviews the leading global manufacturers supplying such systems, presenting an analysis of their key operational features, strengths, and weaknesses. Various architectures used in the development of access control software are also considered. These architectures generally fall into two categories: monolithic and microservice-based.

Monolithic architectures, though simpler and more straightforward, can pose scalability challenges, whereas microservice-based architectures allow for greater flexibility and modularity. The article explores the algorithms underlying these architectures, their respective benefits and drawbacks, and provides a comparative analysis of their effectiveness in real-world applications.

Keywords: management, automation, methods, architecture, algorithms.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Завдання присвячене вирішенню прикладної проблеми, створенню системи управління доступом. Це, безумовно, має відношення до цього завдання, оскільки питання безпеки як в особистому, так і в

державному секторі є перш за все, аналіз різноманітних систем цього типу, які діють на даний момент, має ряд особливостей їх застосування.

Перший з них – це опис описаних функцій, включаючи точність цих систем, простоту їх використання для користувача та здатність обробляти персональні дані. Оскільки ці три параметри мають найбільший зв'язок один з одним і безпосередньо впливають на кінцеву ефективність розробленої системи.

До цього моменту більшість компаній вже почали використовувати свої системи безпеки – СКУД (системи контролю та управління доступом). Зрештою, використання біометричних систем ідентифікації на підприємстві може призвести до значного підвищення безпеки компанії та її співробітників. У зв'язку зі стрімким зростанням вимог підприємств до систем біометричного розпізнавання найближчим часом очікується зростання інтересу до технологій розпізнавання осіб.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

У 21 столітті постало питання організації захисту персональних даних і взагалі доступу до власності, важливих об'єктів і т.д. Ситуація стала дуже серйозною. Оскільки доступ до даних або об'єктів через неавторизованих осіб може призвести до жахливих результатів. У результаті було прийнято рішення про новий підхід до вирішення питань контролю доступу. Це рішення, яке пропонували люди вже досить давно. Були спроби застосувати різні варіанти, зокрема: коди доступу, які легко підробити, або отримати доступ до цієї інформації третьою стороною, магнітне зчитування стрічок або чіпів, але це рішення потребує зберігання особистої ідентифікаційної інформації, що призвело до низка питань щодо безпечного керування даними від імені користувача, контрольні картки, які мають непрямий характер, тощо. Як наслідок, тепер, коли загальна тенденція до використання обличчя як засобу ідентифікації почала поширюватися, за належного підходу до цього типу контролю та управління доступом його можна вважати найефективнішим рішенням для захисту людей. [1]

Система контролю та управління доступом (СКУД) – це сукупність програмно-апаратних засобів, яка призначена для обмеження доступу до об'єкта та реєстрації використовуваних точок доступу. Основним завданням контролю та управління доступом до конкретної території (об'єкта) є:

- контроль та обмеження доступу на конкретну територію - це дає змогу визначити чіткі правила для певної групи осіб щодо часу доступу та ступеня доступу, ці правила можна використовувати для визначення відповідальності та надання конкретних деталей щодо об'єкт з підвищеною безпекою.

- ідентифікація того, хто має доступ до певної території – ця інформація важлива, оскільки дозволяє відслідковувати як час роботи, так і проблеми, що виникають. [1]

Додаткові обов'язки:

Облік відпрацьованого часу;

Управління базою даних персоналу та відвідувачів також входить до цієї категорії.

- інтеграція з системою безпеки, приклад:

- з системою відеоспостереження, яка об'єднує системні події, які вже заархівовані, надсилаючи в систему сповіщення про необхідність початку запису та повертаючи камеру на фіксацію наслідків зафіксованої підозрілої події;

- із системою охоронної сигналізації (СОС) це дозволяє отримати доступ до зон обмеженого доступу або зон, які автоматично поставлені під охорону.

- із системою пожежної сигналізації (СПС), яка отримує інформацію про стан пожежних сповіщувачів, автоматичне розмикання евакуаційних дверей і закривання дверей у разі пожежної тривоги. [1]

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

У зв'язку з цим була поставлена мета даної статті – провести аналіз методів та засобів автоматизованого керування реєстрацією людей у приміщенні на основі розпізнавання осіб.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

У цій спробі пропонується використовувати підхід до керування даними та контролю доступу за допомогою використання технології розпізнавання обличчя. Перевага цього підходу полягає в тому, що він зменшує потребу в особистих даних, водночас забезпечуючи користувачеві максимальну легкість і відповідний поріг ефективності.

СККД поділяють на два типи - мережеві та автономні.

Мережеві РК-дисплеї мають атрибут, що кожен об'єкт управління доступом (контролер) пов'язаний із сервером. Тобто він містить принаймні два компоненти: локальну систему автоматизації (виконавчий механізм, пристрій зчитування та пристрій обмеження доступу) і серверну частину, яка обробляє запити на доступ від локальної системи автоматизації (клієнт). Такий стиль ССКД вигідний для великих об'єктів, оскільки регулювати навіть десяток автономних дверей стає вкрай складно. Використовувати мережеві ССКД корисно в таких ситуаціях:

Коли це непрактично або рекомендовано встановити комплексну внутрішню систему автоматизації.

Якщо систему можна розділити на кілька частин і скопіювати в інші системи (наприклад, пристрій з обмеженим доступом), тоді потрібно буде встановити більше обладнання для обробки та зберігання даних, що матиме негативний вплив на підтримку та витрати система.

Коли локальні дані не потрібні, а продуктивність системи невисока, саме час перейти до хмари. в особистих приміщеннях тощо.

Системи контролю доступу до мережі мають значну перевагу, яка полягає в здатності поширювати та диференціювати системи контролю доступу, роблячи їх автономними, легко розширюваними та керованими. Бездротові технології (радіоканали) можна використовувати в системах контролю доступу до мережі. Використання бездротових мереж, як правило, визначається конкретними ситуаціями: важко або неможливо підключити дротовий зв'язок до об'єктів, це збільшує фінансові витрати на встановлення точки доступу. Для радіостанцій доступно багато опцій, але лише деякі з них реально використовуються в системі SKKD.

Bluetooth. Цей тип бездротового пристрою передачі даних схожий на Ethernet щодо аналогового. Його властивість полягає в тому, що немає необхідності використовувати паралельні комунікації для підключення компонентів при використанні протоколу RS-485. Однак це рішення не є ідеальним для великих класів об’єктів через обмежений діапазон і проблеми безпеки, пов’язані з технологією Wi-Fi. Ці проблеми роблять його непридатним для великих установок, відстань до приймача (комп’ютера, який оброблятиме дані), ймовірно, буде виправлено, і проблеми необхідності підключення до іншого користувача буде уникнуто. Це рішення більше підходить для локальної домашньої автоматизації, яка матиме одного користувача та обмежену відстань до приймача. Однак цей тип об’єднання є дуже енергоефективним, що може бути корисним у ситуаціях, коли система переходить у режим очікування для генерування електроенергії.

Wi-Fi. Основною перевагою цієї радіочастоти є велика відстань зв’язку, яка може досягати кількох сотень метрів. Це особливо важливо для з'єднання об'єктів, які знаходяться далеко. Крім того, зменшуються тимчасові та фінансові витрати, пов'язані з прокладанням комунікацій. Крім того, цей тип зв’язку має вищий ступінь безпеки, пов’язаний із переданими пакетами. При правильній конфігурації цього типу підключення ми можемо гарантувати, що пакети досягнуть сервера та користувача, обидва вони мають вирішальне значення для належної роботи автоматизації.

Автономні системи дешевші, простіші в експлуатації, не вимагають прокладання сотень метрів кабелю, додаткових пристроїв, які підключаються до сервера, або самого сервера. І навпаки, негативні аспекти цих типів систем включають неможливість створювати звіти, відсутність інформації про робочий час, відсутність контролю над подіями та неможливість дистанційного керування. Вище були описані різні типи системи цього типу, одна з найбільш істотних небезпек - це неможливість запам'ятати пароль, який описаний вище. Крім того, такі типи систем мають широкі обмеження щодо застосування. Однак навіть цей тип системи має переваги, окрім згаданої вище здатності продовжувати функціонування, коли один із критичних компонентів системи вимкнено, система також стійка до збоїв через втрату зв’язку з сервером, на відміну від мережі. ССКД де втрата зв’язку з сервером призводить до нездатності всієї системи функціонувати, у цьому типі ССКД такої проблеми немає. При виборі автономної системи з високими вимогами безпеки важливо враховувати наступне:

- ✓ зчитувач повинен бути ізольований від контролера, щоб зовнішні дроти, через які можна відкрити замок, були недоступні.
- ✓ контролер повинен мати джерело живлення, якщо зовнішнє джерело живлення виходить з ладу.

У рамках системи автономного доступу також використовуються електронні замки, які передають інформацію по бездротових каналах: у дверях розташований механічний замок з електронним управлінням і вбудованим зчитувальним пристроєм. Замок пов'язаний з концентратором через радіочастотний канал, це вже передає інформацію по дроту на робочу станцію, на якій встановлено програмне забезпечення.

З кожним роком кількість людей, які цікавляться технологіями розпізнавання осіб, значно збільшується. Сьогодні в різних сферах людської діяльності використовується кілька десятків систем розпізнавання.

Лідируючими компаніями з розробки таких систем є: NEC Corporation (Японія), Cognitec Systems GMBH (Німеччина), Neurotechnology (Литва).

Система «FaceVACS-VideoScan»

«FaceVACS-VideoScan» — це просте у використанні настроюване програмне забезпечення для розпізнавання облич у реальному часі, створене компанією Cognitec Systems.

За роботу системи «FaceVACS-Video» відповідає системний компонент під назвою FaceVACS-VideoScan.

- ✓ сервер відеопотоку, який керує потоком відео;
- ✓ сервер відеоспостереження координує всі компоненти системи та виконує основні біологічні операції.

- ✓ обчислювальний вузол, призначений для обчислення розподілу обчислювальних навантажень.
- ✓ Інтерфейс користувача:
- ✓ диспетчер сигналів, який приймає сповіщення про події та керує мобільними пристроями, оперативною базою даних та набором інтеграторів.
- ✓ До цього моменту технологія FaceVACS використовувала алгоритм B10T9 для розпізнавання обличчя. Цей алгоритм стійкий до змін виразу обличчя, повороту обличчя (±15º), часткового закриття, використання сонцезахисних окулярів і змін освітлення.
- ✓ Крім того, система FaceVACS має додаткові можливості:
- ✓ можливість стежити за кількома людьми одночасно;
- ✓ порівняння індивідів ведеться в режимі реального часу.
- ✓ здатність показувати та передавати статистичні дані про потоки.
- ✓ підтримка інтерактивної реєстрації власності;
- ✓ використання C++'sAPI і Web Services'API.

Система "NEC's Face Recognition" компанії "NEC"

Система розпізнавання облич у NEC є однією з найдосконаліших у японській країні, ця система розроблена компанією NEC і розпізнає людей із фільмів десятирічної давнини, навіть якщо людина в окулярах або стоїть обличчям. Усі розпізнані обличчя зберігаються в базі даних, тому, якщо вам потрібно отримати доступ до всієї історії реєстрації відео, ви можете просто відкрити реєстраційну інформацію та переглянути дату й час будь-якого раніше збереженого зображення.

Технологія, відома як NEC, перевершує інші системи розпізнавання як за швидкістю, так і за точністю. Це ефективно в різних сценаріях, у тому числі при роботі з відео низької якості та сильно стисненими зображеннями. NEC оцінює індивідуальні характеристики людини (розмір, форму зіниць, лінії носа та рота та їх розташування відносно інших осіб у базі даних), а потім знаходить схожу особу в базі даних на основі цієї інформації.

Система містить декілька модулів, які реалізують наступні алгоритми:

1. Використовується метод узагальненого узгодження (GMFD), який має високу швидкість виявлення та високу точність розпізнавання облич. Метод GMFD складається з нейронних мереж, які спочатку шукають пари очей.

2. Алгоритм PSM (Perturbation Space Method) допомагає вам вирішити проблеми, пов’язані з визначенням місця розташування людини в кадрі (хтось під кутом або просто за межами кадру).

3. Метод ARBM (Adaptive Regional Blend Matching) зменшує вплив незначних змін обличчя (наприклад, зміни виразу обличчя, наявність окулярів або головного убору) на точність розпізнавання [2].

Система розпізнавання обличчя NeoFace має наступні атрибути:

- Можливість спостерігати та регулювати в реальному часі.
- індивідуальна ідентифікація;
- Багаторазове підтвердження;
- Можливість пошуку подій у базі даних;
- Наявність журналу записаних зображень осіб.
- Відкритість для нових напрямків руху до 45 градусів від попереднього положення;
- Елемент керування «перетягуванням»;
- Велика ємність і необмежений розмір бази даних;
- Незалежно від напрямку погляду та особливостей обличчя (окуляри, борода та виразні рухи обличчя).

Система VeriLook SDK компанії Neurotechnology

VeriLook SDK — система ідентифікації людини, створена компанією Neurotechnology. Це система, яка розпізнає людей за присутністю в кадрі та швидко їх ідентифікує (знаходить до 100 тис. осіб за секунду). VeriLook SDK доступний як повна платформа розробки програмного забезпечення та підтримує різноманітні пристрої на Windows, Linux, Mac OS X, iOS та Android.

Алгоритм VeriLook використовує технологію цифрової обробки зображень на основі глибоких нейронних мереж для локалізації людини.

Основними перевагами системи VeriLook є відсутність необхідності взаємодіяти з пристроями, які сканують обличчя, і швидке впровадження біометричних функцій, які ідентифікують людей, у програмах клієнтів. Крім того, є кілька інших переваг:

- ✓ Одночасна обробка кількох осіб.
- ✓ Класифікація за статтю. Стать можна позначити для кожної особи на портреті.
- ✓ Розпізнавання облич у реальному часі. VeriLook визначає, чи людина на відео насправді жива чи це фотографія.
- ✓ Розпізнавання емоцій. VeriLook розглядає шість основних емоцій: гнів, відраза, страх, щастя, сум і здивування;

✓ Особистісні характеристики. VeriLook можна налаштувати для розпізнавання певних атрибутів під час збору обличчя - усмішка, відкритий рот, закриті очі, окуляри, борода чи вуса;

✓ Визначення краси зовнішнього вигляду обличчя. Поріг якості можна використовувати під час реєстрації фізичних осіб, щоб гарантувати, що в базі даних зберігаються лише найбільш кваліфіковані шаблони.

✓ Кілька прикладів однієї особи. Ці зразки можна оцінювати з різних точок зору та в різний час, що сприяє підвищенню якості порівняння.

✓ Здатність розпізнавати. Параметри VeriLook також доступні для порівняння 1 до 1 (перевірка), а також у режимі багаторазового порівняння.

✓ Маленький дизайн обличчя. Шаблон особи може мати розмір 4 байти;

✓ Переваги загального режиму. Цей метод створює різноманітні узагальнені атрибути обличчя з кількох зображень самого об’єкта.

Алгоритм VeriLook здатний розпізнавати межі, які спостерігалися в інфрачервоному спектрі.

Основні елементи СККД.

Ці методи досить різноманітні, включаючи турнікети, двері з електромагнітним ключем тощо.

- Електромагнітні замки - більшість із них вимикаються, коли до них подається живлення, тому вони популярні для використання на шляхах евакуації при пожежі.

- Турнікети - механізм перемикання між поворотним і ковзним рухом за допомогою штифтів, які запобігають руху. Він може не прикривати, а лише сповільнювати швидкість руху при необхідності. Якщо процес верифікації користувача ще можливий.

- Електромеханічні замки – вони досить стійкі до злому (якщо замок механічно потужний), вони також мають механічне скидання (це означає, що якщо ви натиснете на замок, він буде відчинено, доки ви не відчините двері).

- Шлюзові кабіни: вони працюють у банках, у режимних установах (у компаніях, які мають підвищену стурбованість безпекою).

- Ворота та шлагбауми - в основному, вони розташовуються на в'їздах на територію компанії, на автостоянках і паркінгах, на під'їздах до господарських будівель, у дворах житлових будинків. Основною вимогою є здатність витримувати кліматичні умови та можливість автоматизації (через систему контролю доступу). При проектуванні організації контролю доступу до системи пред'являються додаткові вимоги - додаткові можливості включають можливість зчитування табличок, розмір яких перевищує термін експлуатації, розпізнавання номерів автомобілів (при поєднанні з системою відеоспостереження).

Найпоширеніші види виконання - це карта, брелок, ярлик. Є основним компонентом системи контролю доступу, який зберігає код, який використовується для визначення прав власника («ідентифікація»). Це може бути картка пам’яті Touch, безконтактна картка (наприклад, RFID) або картка з магнітною смугою. Код, який вводиться з клавіатури, також може служити відмінністю. Сьогодні їх не дуже складно попсувати. Зіставляється з біометричними показниками, якими є: відбиток пальця, малюнок сітківки або райдужної оболонки ока, тривимірне зображення людини, малюнок капілярних ліній на долоні.

Надійність (стійкість до підробок) системи контролю доступу в першу чергу залежить від типу використовуваного ідентифікатора: найпоширеніші безконтактні картки підробляються на обладнанні, яке легко визначити. Як наслідок, ці ідентифікатори не підходять для об’єктів, які потребують більш широкого захисту. Більш фундаментальна відмінність у безпеці полягає в тому, що RFID забезпечують вищий рівень безпеки, код картки зберігається в захищеній зоні та зашифрований. Однак цей метод все ще не є надійним, оскільки не потрібно розшифровувати мітку, а ви можете лише відтворити її зашифроване значення на іншій платформі. Зрештою, більш точним методом, як було сказано раніше, є біометричний показник. Не всі біометричні показники легко зчитуються, тому необхідно використовувати такий, який не потребує додаткового обладнання, окрім простої камери або іншого пристрою для зчитування інформації та отримання інформації за короткий проміжок часу. Це риси сітківки ока, підпис обличчя на фотографії. Однак це ставить питання щодо збереження даних, оскільки це особиста інформація, відмінна від обличчя, і може бути використана в іншій системі. Сьогодні навіть у мобільних телефонах є зчитувач відбитків пальців, ця інформація важлива, тому підробляти її не варто. На відміну від обличчя, дані надзвичайно важко підробити за допомогою тривимірної карти тегів, тому що для цього потрібно буде використовувати обладнання, а використання простої фотокартки унеможливить доступ до системи. без обличчя. Крім того, зчитувач у системі використовує подібну технологію, і використання простої фотокартки призведе до неможливості надати доступ без обличчя.

Це є невід’ємною частиною системи: контролер визначає, чи дозволено власнику ідентифікатора проходити через точку доступу, система зберігає коди для прав доступу ідентифікатора в списку, а контролер визначає, чи має власник права. Коли людина зчитує (подає читачеві) код, відбувається порівняння між ними, і на основі результатів порівняння приймається рішення. Для роботи контролера потрібне живлення, тому контролери зазвичай мають окрему батарею, яка підтримує його роботу протягом кількох годин або днів у разі збою живлення. Однак у дуже складних системах контролер частіше бере

участь у процесі керування без фактичної обробки даних, він приймає рішення на основі результатів сервера, які можуть бути отримані після обробки певного набору даних. Контролер є центральною частиною локальної системи автоматизації, він обробляє сигнали датчиків і передає команди виконавчим механізмам.

Це пристрій, який отримує ідентифікаційний код і передає його на контролер. Варіанти зчитувача залежать від типу ідентифікатора: для «планшета», який складається з двох електричних компонентів (один є «кишеньковим»), для картки, яка складається з електронної плати та антени, у У цьому випадку читач повинен вставити телевізійну камеру в зображення. Якщо зчитувач розміщений на дорозі (ворота, зовнішній в'їзд у будівлю та під'їзд до стоянки), то він повинен витримувати кліматичне навантаження перепадів температур, опадів, а особливо, якщо місцевість має суворий клімат, то читач має вміти це витримати. Якщо існує ризик руйнування, важлива також механічна потужність (сталевий корпус). Окремо можна вибрати зчитувачі, які ідентифікують об'єкти на відстані до 50 м. Ці типи систем корисні на шосе, автострадах і в'їздах до блокпостів. Зчитувачі, ідентифіковані як такі, зазвичай мають активну мітку (містять вбудований акумулятор). Для відбитків рук або пальців це ультразвукові датчики, які створюють чітке зображення (відбиток) відповідного методу авторизації. У цих методах зображення характеризується специфічними та вимогливими вимогами, що вимагає використання ультразвукових датчиків для створення відбитка. У випадках, коли використовується обличчя, необхідна камера глибини як засіб перевірки.

Після вивчення існуючих рішень і підходів були визначені вимоги, які б відповідали даним умовам. Щоб система була застосована, мають бути виконані наступні передумови.

- Можливість зв'язку з усіма периферійними пристроями через одну універсальну точку доступу;
- Швидкість системи;
- Здатність до збільшення;
- Можливість зберігати та додавати інформацію про нових та існуючих користувачів;
- Можливість перепроектувати систему без переривання її функціонування;
- Масштабність системи як у вертикальному, так і в горизонтальному напрямках;
- Стабільність системи.

Після того, як всі вимоги були виконані, ми мали можливість спостерігати всю проблему та вибирати підходи до її вирішення.

Як компонент системи контролю та управління доступом, наявність руху документується дискретним датчиком руху; фото зображення. Вплив керування - це сигнал, який посилає контролер після обробки фотографії через модель, цей сигнал потім передається у вигляді двійкового числа на вихід. У нашому прикладі живлення є, але воно не надсилається на плату керування приводу.

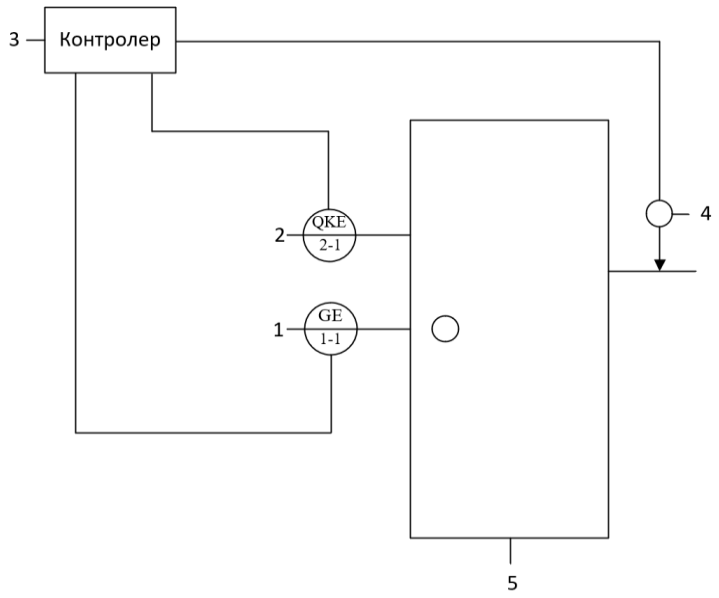

Рис. 1. Функціональна схема керування СККД

На функціональній схемі СККД (рис. 1.) зображено 5 основних компонентів системи:

1. Датчик руху, який являє собою інфрачервоний випромінювач і приймач.
2. Камера, яка документує зображення.
3. Контролер повинен взаємодіяти з системою.
4. Механізм замикання.

5. Пристрій блокування фізичного доступу.

Система працює за такими принципами: людина, яка бажає увійти в приміщення, наближається до наявного фізичного бар'єру, спрацьовує датчик руху та надходить сигнал на контролер. Контролер інтерпретує цей сигнал і наказує камері зробити знімок. Камера зробить знімок і поверне його до контролера, який потім обробить фотографію за допомогою моделі. Після отримання результату (% подібності) контролер визначає, чи слід надати чи заборонити доступ, якщо вони це зроблять, вони надішлють сигнал виконавчому механізму (виконавчий механізм зазвичай закритий).

Зараз використовується багато різних шаблонів архітектури програмного забезпечення. Давайте розглянемо три, які можуть допомогти у вирішенні нашої проблеми:

конструкція «моноліт».

- Дизайн «Малі послуги».
- Дизайн «Клієнт-сервер».

Обговоримо кожен із цих підходів докладніше.

Монолітна архітектура — це традиційний дизайн програмного забезпечення, що складається з одного модуля, який функціонує автономно та незалежно від інших програм. Моноліт часто характеризують як великий і неінтуїтивно зрозумілий, ці два слова добре описують загальну архітектуру розробки програмного забезпечення.

Монолітна архітектура - це окрема велика мережа, яка має єдиний базовий код і використовується для об'єднання всіх бізнес-завдань. Щоб внести зміни в цю програму, ви повинні спочатку оновити весь стек через кодову базу, а потім випустити та розгорнути оновлену версію сервіс-орієнтованого інтерфейсу. Це виключає можливість робити оновлення та займає багато часу.

Моноліти корисно використовувати на ранніх стадіях проектів, щоб полегшити розгортання коду без необхідності витрачати надто багато розумової енергії на підтримку коду. Це полегшує негайний випуск усього в монолітній програмі.

Рисунок 2 ілюструє схему монолітної конструкції. Це демонструє, що всі складові компоненти включені в одну програмну програму. Тобто все виконується одним механізмом, який знаходиться в одному місці як єдина служба.

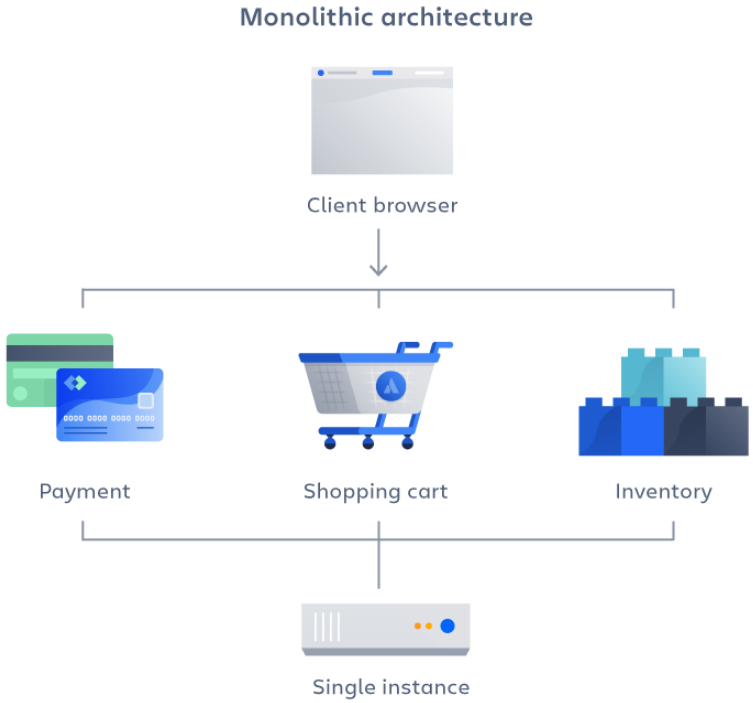

Рис. 2. Схематичне зображення монолітної архітектури

Переваги цієї конструкції:

- Легкий монтаж. Використання одного виконуваного файлу або каталогу спрощує розгортання.

розвиток. Простіше створити програму, якщо вона створена з єдиним базовим кодом.

Продуктивність. У централізованій базі коду та сховищі один API часто може служити інтерфейсом для кількох мікросервісів.

- Скорочене тестування. Монолітна програма — це єдиний централізований компонент, який забезпечує швидше тестування всієї системи, ніж розподілена програма.

Легке усунення несправностей. Весь код знаходиться в одному місці, що полегшує виконання запитів і виявлення проблем.

Недоліки такої конструкції:

Зниження швидкості росту. Велика надійна програма, яка є складною та уповільнює процес розробки, є великою.

Масштабованість. Окремі компоненти не можуть бути змінені.

Міцність. Збій в одному з модулів може негативно вплинути на доступність програми.

- Недостатня гнучкість. Можливості цілісних програм обмежені застосовуваними технологіями.

- Перешкоди для впровадження технологій. Будь-які зміни в інфраструктурі чи мові програмування вплинуть на всю програму, що зазвичай вимагає збільшення витрат і часу.

Реалізація. Внесення незначних змін вимагатиме перетворення всієї монолітної програми.

Наступний тип архітектурної реалізації - "Мікросервіси". Архітектура мікросервісів (або просто «мікросервіси») — це стиль архітектури, який базується на незалежному виконанні кількох сервісів. Ці служби мають власну логіку та базу даних, призначену для конкретної мети. Розгортання, тестування та масштабування є внутрішніми для кожної служби. Мікросервіси розкладають великі бізнес-завдання на численні індивідуальні бази коду. Мікросервіси не зменшують складність, але вони роблять будь-яку складність очевидною та більш керованою, розбиваючи завдання на менші процеси, які не залежать один від одного та сприяють ширшій картині. На малюнку 3. показано склад компонентів цієї архітектури.

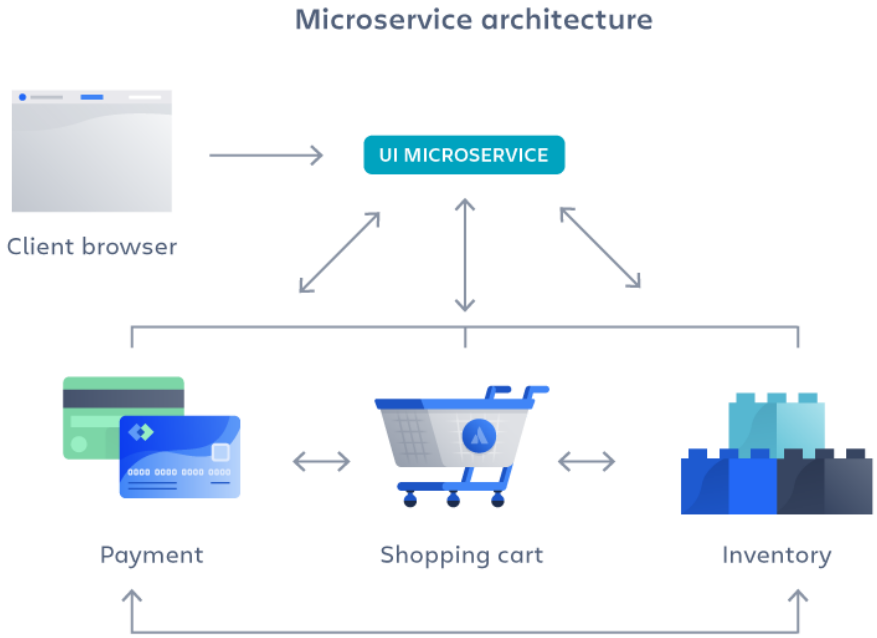

Рис. 3. Діаграма “Мікросервісної” архітектури

Опишемо наступний тип архітектурного натхнення - "Мікросервіси". Архітектура мікросервісів (або просто «мікросервіси») — це стиль архітектури, який базується на незалежному виконанні кількох сервісів. Ці служби мають власну логіку та базу даних, призначену для конкретної мети. Розгортання, тестування та масштабування є внутрішніми для кожної служби. Мікросервіси розкладають великі бізнес-завдання на численні індивідуальні бази коду. Мікросервіси не зменшують складність, але вони роблять будь-яку складність очевидною та більш керованою, розбиваючи завдання на менші процеси, які не залежать один від одного та сприяють ширшій картині. На малюнку 3. показано склад компонентів цієї архітектури.

✓ Простота обслуговування та тестування. Команди можуть вивчати нові функції та повертатися до попередньої версії, якщо щось неефективне. Це зменшує складність оновлень коду та прискорює випуск нових функцій для громадськості. Крім того, легко знаходити та виправляти помилки та проблеми в окремих службах.

✓ Розгортання, яке не залежить від хоста. Мікросервіси розглядаються як окремі компоненти, що дозволяє легко і швидко реалізувати окремий розподіл окремих функцій.

✓ Гнучкість технологій. Використовуючи дизайн мікросервісів, команди мають можливість використовувати інструменти на основі своїх уподобань.

✓ Висока надійність. Вносячи зміни в певний сервіс, можна не побоюватися, що програма вийде з ладу.

- ✓ Переваги цього варіанту:
- ✓ Збільшення розвитку зростання. Мікросервіси ускладнюють монолітну архітектуру порівняно з іншими проектами, оскільки існує більше сервісів, створених кількома командами в різних місцях. Якщо ріст не регулюється належним чином, це сповільнить розвиток і знизить ефективність роботи.
- ✓ Зростання вартості інфраструктури. Кожен новий мікросервіс може мати власні витрати, пов’язані з набором тестів, інструкціями щодо розгортання програмного забезпечення, інфраструктурою для розміщення програмного забезпечення, інструментами для моніторингу програмного забезпечення тощо.
- ✓ Додаткові витрати, пов'язані з організацією. Команди потребують додаткового спілкування та співпраці, щоб полегшити оновлення та взаємодію.
- ✓ Проблеми з налагодженням. Кожен мікросервіс має власний набір журналів, що ускладнює усунення неполадок. Крім того, можуть виникнути додаткові ускладнення, якщо одна бізнес-процедура виконується на кількох машинах.
- ✓ Відсутність стандартизації. Без спільної платформи може виникнути ситуація, коли перелік мов, стандартів для ведення журналів та інструментів для моніторингу збільшиться.
- ✓ Відсутні запити щодо власності майнових питань. У міру створення нових послуг збільшується кількість команд, які в них беруть участь. Зрештою, важче визначити, які послуги може надати команда та до кого слід звертатися по допомогу.

Розглянемо останню зі списку з наведених архітектур - “Клієнт - серверна”. “Клієнт - сервер” - поняття що об’єднує в собі два окремих шари, а саме:

- Клієнт - це локальний комп'ютер (або інший пристрій з обчислювальними можливостями), який діє як віртуальний користувач, цей пристрій запитує дані або певну групу дій від сервера.

- Сервер: потужний комп'ютер або спеціальне системне обладнання, яке призначене для виконання конкретного завдання під час виконання комп'ютерних програм. Він виконує роботу з обслуговування за запитами клієнтів, надає користувачам доступ до певних ресурсів системи, зберігає інформацію або працює з базою даних.

Атрибути цієї моделі полягають у тому, що користувач запитує певну дію від сервера, яка обробляється автоматично, а кінцевий результат надсилається клієнту. Сервер здатний обслуговувати декілька клієнтів одночасно.

Якщо одночасно надходить більше ніж один запит, ці запити поміщаються в окрему чергу, і сервер виконуватиме їх у порядку. Іноді запити мають свої пріоритети. Деякі більш важливі запити завжди виконуватимуться за принципом першої важливості.

Параметри, реалізовані на сервері:

- Зберігання, захист і доступ до даних;
- Робота над заявками клієнтів,

Порядок повернення клієнту.

Параметри, які можна змінити на клієнті:

- Інтерфейс, який надає користувачеві графічний досвід;
- Запит на допомогу сервера і подальша доставка запиту;
- Отримання результатів запитів і відправка додаткових команд (запити на додавання, оновлення інформації або видалення групи даних).

Такий тип системи дозволяє брати участь у кількох ідентичних проектах, що в нашому випадку сприяє розширенню системи та дозволить використовувати її в майбутньому в різних компаніях. Крім того, у поєднанні з попередньо визначеною базою даних це дозволяє легко налаштовувати різні компоненти системи, не змінюючи код програми, натомість вносячи лише зміни в базу даних.

У результаті, вивчивши всі вищезазначені підходи до розробки програмного забезпечення для нашої системи автоматизації, включаючи швидкість, можливість налаштування та простоту побудови та обслуговування, ми можемо зробити висновок, що найефективнішим підходом буде «архітектура клієнт-сервер». ".

Оскільки ми обрали клієнт-серверний дизайн програми, міні-комп’ютер буде виконувати роль клієнта, а сервер буде реалізований на Python і функціонуватиме як передача даних між базою даних, нейронною мережею та клієнтом.

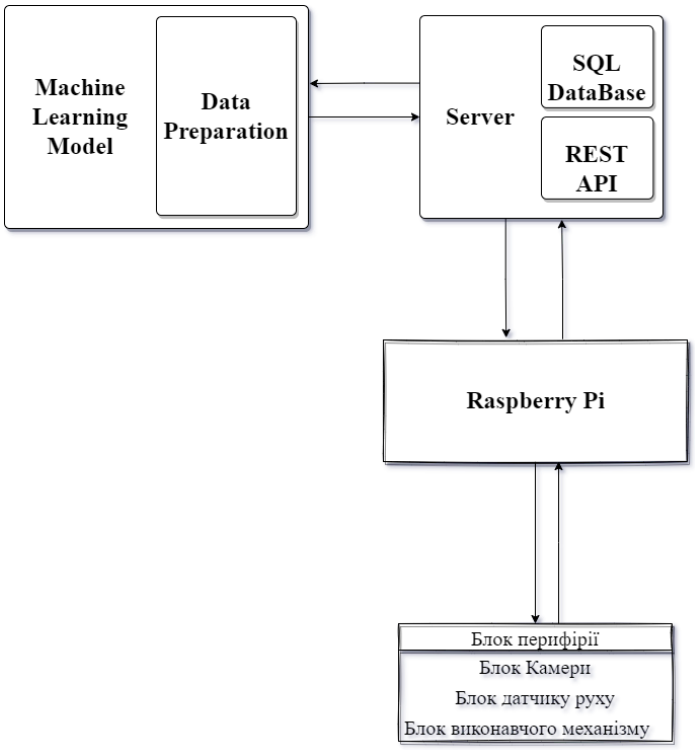

Рис. 4. Блок схема архітектури застосунку

Схема складається з чотирьох основних блоків.

- Raspberry Pi – блок, що відноситься до клієнтського компонента
- Сторона сервера
- Модель машинного навчання (модель ML) – блок, який містить модель для розпізнавання та навчання, а також попередньої обробки даних.
- Периферійний блок - зовнішні компоненти

Компоненти Raspberry Pi та периферійні пристрої — це фізичні компоненти, які розташовані безпосередньо на інсталяції, інші компоненти — це програмні додатки, розташовані на сервері або в «хмарі». Raspberry Pi та його периферійні пристрої взаємодіятимуть один з одним через паралельну шину даних у синхронному режимі. Тобто до отримання сигналу від датчика руху периферійний блок буде залишатися нерухомим.

Завдяки цій взаємодії «Сервер», «Модель машинного навчання» та «Raspberry Pi» будуть виконуватися через Rest API, який є підходом, який використовує HTTP-запити.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

В результаті можна зробити висновок, що система контролю та управління доступом не є останньою розробкою і вже досягнута в цьому напрямку, однак остаточного вирішення проблеми захисту швидкості з точки зору контролю доступу досі немає. Оскільки швидкість у напрямку нахилу велика, починають використовуватися картки або мітки, які можна підробити. При збільшенні глибини захисту починають виникати проблеми з налаштуваннями системи і втрата персональних даних. Наразі в РК-телевізорах відсутні опції з функцією розпізнавання обличчя, хоча вони можуть вирішити проблеми швидкості та безпеки.

Література

1. NEC. Facial Recognition [Електронний ресурс]. // Режим доступу: https:// u.nec.com/solutions/security/technologies/face_recognition.html (дата обращения: 12.05.2018).
2. Neurotechnology. VeriLook SDK [Електронний ресурс]. // Режим доступу: http://www.neurotechnology.com/ (дата звернення: 13.11.2024).
3. Techniques and Challenges of Face Recognition: A Critical Review [Електронний ресурс]. // Режим доступу: https://www.sciencedirect.com/science/article/pii/S1877050918321252 (дата звернення: 13.11.2024).

4. TechniquesandChallengesof Face Recognition: A Critical Review [Електронний ресурс]. // Режим доступу: https://www.sciencedirect.com/science/article/pii/S1877050918321252 (дата звернення: 13.11.2024).
5. AndreaF. Abate, Nappi Nappi, Riccio Riccio, Gabriele Sabatino 2D and 3D face recognition: A survey Pattern Recognition Letters, 28 (14) (2007), pp. 1885-1906
6. FaceNet: A Unified Embedding for Face Recognition and Clustering [Електронний ресурс]. // Режим доступу: https://www.cv-foundation.org/openaccess/content_cvpr_2015/papers/Schroff_FaceNet_A_Unified_2015_CVPR_paper.pdf (дата звернення: 13.11.2024).

References

1. NEC. Facial Recognition [Elektronnyi resurs]. // Rezhym dostupu: https:// u.nec.com/solutions/security/technologies/face_recognition.html (data obrashchenyia: 12.05.2018).
2. Neurotechnology. VeriLook SDK [Elektronnyi resurs]. // Rezhym dostupu: http://www.neurotechnology.com/ (data zvernennia: 13.11.2024).
3. Techniques and Challenges of Face Recognition: A Critical Review [Elektronnyi resurs]. // Rezhym dostupu: https://www.sciencedirect.com/science/article/pii/S1877050918321252 (data zvernennia: 13.11.2024).
4. TechniquesandChallengesof Face Recognition: A Critical Review [Elektronnyi resurs]. // Rezhym dostupu: https://www.sciencedirect.com/science/article/pii/S1877050918321252 (data zvernennia: 13.11.2024).
5. AndreaF. Abate, Nappi Nappi, Riccio Riccio, Gabriele Sabatino 2D and 3D face recognition: A survey Pattern Recognition Letters, 28 (14) (2007), pp. 1885-1906
6. FaceNet: A Unified Embedding for Face Recognition and Clustering [Elektronnyi resurs]. // Rezhym dostupu: https://www.cv-foundation.org/openaccess/content_cvpr_2015/papers/Schroff_FaceNet_A_Unified_2015_CVPR_paper.pdf (data zvernennia: 13.11.2024).