МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ПРИРОДОКОРИСТУВАННЯ

ФАКУЛЬТЕТ МЕХАНІКИ, ЕНЕРГЕТИКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА

другого (магістерського) рівня вищої освіти

на тему: **“Розробка системи аутентифікації користувача з використанням платформи FS2-D”**

Виконав: студент гр. Іт-62

Спеціальності 126 «Інформаційні системи та технології»
(шифр і назва)

Свіца Богдан Васильович
(Прізвище та ініціали)

Керівник: к.т.н., доц. Лиса О.В.
(Прізвище та ініціали)

Рецензенти: д.т.н., проф. Власовець В.М.
(Прізвище та ініціали)

ДУБЛЯНИ-2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ПРИРОДОКОРИСТУВАННЯ
ФАКУЛЬТЕТ МЕХАНІКИ, ЕНЕРГЕТИКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Другий (магістерський) рівень вищої освіти
Спеціальність 126 «Інформаційні системи та технології»

"ЗАТВЕРДЖУЮ"
Завідувач кафедри_____
д.т.н., проф. А.М. Тригуба
"____"_____2023 р.

ЗАВДАННЯ

на кваліфікаційну роботу студенту

Свіца Богдан Васильович

1. Тема роботи: «Розробка системи аутентифікації користувача з використанням платформи FS2-D»

Керівник роботи Лиса Ольга Володимирівна, к.т.н., доцент.
Затверджені наказом по університету від 28.04 2023 року № 133 /к-с.

2. Строк подання студентом роботи 15.12.2023 р.

3. Вихідні дані до роботи: *методики аутентифікації, методи розробки систем аутентифікації, програмне забезпечення*

4. Зміст розрахунково-пояснювальної записки (перелік питань, які необхідно розробити)

Вступ.
1. Аналіз стану аутентифікації користувача та завдання кваліфікаційної роботи.
2. Обгрунтування та вибір методів для розробки системи аутентифікації користувача.
3. Результати розробки системи аутентифікації користувача.
4. Охорона праці та безпека у надзвичайних ситуаціях.
5. Визначення ефективності від використання системи аутентифікації користувача.
Висновки та пропозиції.
Список використаної літератури

5. Перелік ілюстраційного матеріалу (з точним зазначенням обов'язкових слайдів): *способи біометричних систем автентифікації; порівняльна різниця між FaceStation і FaceStation2; конфігурації інтеграції систем; схема інтеграції Biostar2 Web API із веб сервером; комунікація клієнта із сервером без сторонніх SDK з боку BioStart2; програма створення користувача; економічна ефективність.*

6. Консультанти з розділів:

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1, 2, 3, 5	*Лиса О.В., доцент кафедри інформаційних технологій*		
4	*Городецький І.М., доцент кафедри фізики, інженерної механіки та безпеки виробництва*		

7. Дата видачі завдання 30 червня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Приміт-ка
1	*Написання першого розділу*	30.06.23-04.07.23	
2	*Виконання другого розділу та аркушів ілюстраційного матеріалу до нього*	05.07.23-14.08.23	
3.	*Виконання третього розділу та аркушів ілюстраційного матеріалу до нього*	15.08.23-24.09.23	
4.	*Написання розділу «Охорона праці та безпека у надзвичайних ситуаціях»*	25.09.23-10.10.23	
5.	*Оцінення ефективності запропонованої системи*	11.10.23-31.10.23	
6.	*Завершення оформлення розрахунково-пояснювальної записки та презентації*	01.11.23-30.11.23	
7.	*Завершення роботи в цілому*	01.12.23-16.12.23	

Студент _____ Свіца Б.В.
(підпис)

Керівник роботи _____ Лиса О.В.
(підпис)

УДК 621.311.1

Розробка системи аутентифікації користувача з використанням платформи FS2-D. Свіца Б.В. Кафедра інформаційних технологій – Дубляни, Львівський НУП, 2024. Кваліфікаційна робота: 70 с. текст. част., 14 рис., 7 табл., 10 арк. ілюстраційного матеріалу, 30 джерел.

Виконано аналіз систем аутентифікації. Охарактеризовано особливості аутентифікації та авторизації в залежності від виду використання системи: використання ключа, захист паролем, біометрія. Розкрито статичні та динамічні методи біометричної аутентифікації. Сформульовано завдання кваліфікаційної роботи. Здійснено аналіз методів для розробки системи аутентифікації користувача, зокрема методів нейронних мереж (Convolutional Neural Network), статистичних методів розпізнавання облич з використанням прихованих Марківських моделей (ПММ) з дискретним часом, методу головних компонент (principal component analysis, PSA), заснованому на перетворенні Карунена-Лоева, методу гнучкого порівняння на графах, активних моделей зовнішнього вигляду (Active Appearance Models), які шляхом зміни форми моделі підбираються під реальне зображення. Проведено порівняльний аналіз між FaceStation і FaceStation2. Обґрунтовано доцільність використання платформи FS2D з BioStart 2 system в ролі програмного забезпечення, зокрема BioStar2 API, що забезпечує просту взаємодію і інтеграцію із сторонніми застосунками на базі WEB API. Розроблено систему аутентифікації користувача. Подано створену програму та аналіз коду задачі аутентифікації користувача. Розроблено заходи із охорони праці та безпека у надзвичайних ситуаціях. Визначено ефективність від використання розробленої системи аутентифікації користувача.

ЗМІСТ

ВСТУП

У зв'язку з розширенням використання інтернет-технологій та збільшенням кількості цифрових сервісів та платформ зростає актуальність розробки системи аутентифікації користувача. Аутентифікаційні системи допомагають у збереженні конфіденційності особистої інформації та даних користувачів, запобігаючи їхньому несанкціонованому використанню. Зростання кількості онлайн-сервісів, мобільних додатків та інших цифрових платформ вимагає надійних засобів ідентифікації користувачів для забезпечення безпеки та конфіденційності. З користувачами можуть взаємодіяти з різних місць світу за допомогою різноманітних пристроїв. Системи аутентифікації повинні бути гнучкими та забезпечувати доступ до ресурсів з будь-якого місця та пристрою, не збільшуючи ризиків для безпеки.

Забезпечення безпеки ідентифікації користувачів стає критичним завданням в контексті зростання кількості кіберзагроз та кібератак. Зловмисники постійно шукають нові методи для отримання несанкціонованого доступу до систем та особистої інформації користувачів. Актуальна система аутентифікації допомагає запобігти таким атакам та зберегти конфіденційні дані.

Розвиток біометричних методів аутентифікації, таких як відбитки пальців, розпізнавання обличчя та інші, додає нові можливості для забезпечення надійності ідентифікації користувачів. Зростання обсягу регулювань та стандартів безпеки, таких як GDPR в Європі, вимагає від компаній розробляти та впроваджувати ефективні системи аутентифікації для виконання нормативних вимог.

Користувачі стають більш обізнаними та вимогливими стосовно своєї безпеки в інтернеті. Системи аутентифікації повинні бути зручними та швидкими, а також забезпечувати високий рівень захисту.

У зв'язку з цим, розробка та вдосконалення систем аутентифікації є надзвичайно важливою для забезпечення безпеки та конфіденційності у цифровому середовищі. Надійна система аутентифікації допомагає зберігати довіру користувачів до сервісів та платформ, що може позитивно позначитися на репутації

компанії. Правильно розроблена система аутентифікації повинна бути зручною для користувачів, дозволяючи їм легко та швидко виконувати вхід та отримувати доступ до ресурсів. Ефективна аутентифікація може допомогти у попередженні втрат даних, фінансових втрат та інших збитків, пов'язаних із порушенням безпеки.

На підставі викладених фактів можна стверджувати, що тема кваліфікаційної роботи «Розробка системи аутентифікації користувача з використанням платформи FS2-D» є досить актуальною та своєчасною.

Практична цінність системи аутентифікації полягає в її здатності забезпечувати надійний захист від кіберзагроз, дотриманні вимог безпеки та конфіденційності, а також в покращенні користувацького досвіду та управлінні ризиками для бізнесу.

Об’єктом дослідження є комплексний набір технічних та практичних аспектів, пов'язаних із розробкою, впровадженням та використанням систем аутентифікації користувача.

Предмет дослідження є технології автентифікації, авторизації за допомогою систем розпізнавання BioStar2 на базі платформи FaceStation2.

Метою роботи є розробка авторизації за допомогою систем розпізнавання BioStar2 на базі платформи FaceStation2 на мові програмування C# та проведено тестування розроблених програмних модулів.

РОЗДІЛ 1.
АНАЛІЗ СТАНУ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧА ТА ЗАВДАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ

1.1. Аналіз основних понять та процесу аутентифікації

Ідентифікація, аутентифікація та авторизація є загальноприйнятими концепціями, але не у всіх є розуміння їх відмінності. Аутентифікація – це процес визначення, чи є особа чи об'єкт тим, за кого вони себе видають. Технологія автентифікації забезпечує контроль доступу, перевіряючи, чи співпадають облікові дані користувача з авторизованими обліковими даними у базі даних чи на сервері автентифікації.

Зазвичай ідентифікація користувачів використовує ідентифікатор, а автентифікація відбувається, коли користувач подає облікові дані, такі як пароль, що відповідає цьому ідентифікатору. Більшість користувачів знають про використання паролів, які вважаються факторами знань автентифікації. Інші фактори та методи для двофакторної чи багатофакторної автентифікації (MFA) описані нижче.

Аутентифікація має важливе значення, оскільки дозволяє організаціям захищати свої мережі, надаючи доступ лише автентифікованим користувачам до довірених ресурсів. Ці ресурси можуть включати комп'ютерні системи, мережі, бази даних, веб-сайти та інші мережеві або службові додатки.

Після автентифікації користувач або процес переходять до процесу авторизації, щоб визначити, чи має автентифікований суб'єкт доступ до захищеного ресурсу чи системи. Навіть якщо користувач пройшов автентифікацію, він може бути позбавлений доступу, якщо не отримав дозволу на цей доступ.

Терміни "автентифікація" та "авторизація" часто використовуються як синоніми, але їх функції відрізняються. Аутентифікація – це процес визначення ідентичності зареєстрованого користувача перед отриманням доступу, тоді як авторизація – це перевірка права автентифікованого користувача на доступ до

конкретних ресурсів. Контроль доступу визначає, яким користувачам дозволено чи заборонено отримати доступ до цих ресурсів.

Аутентифікація завжди передує авторизації. Аутентифікація користувача зазвичай відбувається при взаємодії з комп'ютерними системами за межами гостьових облікових записів. Користувач вибирає ім'я користувача чи ідентифікатор і подає дійсний пароль для отримання доступу. Аутентифікація дозволяє взаємодіяти з системами, операційними системами, додатками та мережами для доступу до різноманітних ресурсів.

Багато компаній використовують автентифікацію для перевірки користувачів на своїх веб-сайтах. Без відповідних заходів безпеки особисті дані, такі як номери банківських карт та соціального страхування, можуть стати предметом кібератак.

Організації використовують автентифікацію для контролю доступу користувачів до корпоративних ресурсів, комп'ютерів, серверів, додатків та мереж. Для великих організацій використовується система єдиного входу (SSO), яка надає доступ до кількох систем за одним обліковим записом.

Під час автентифікації, введені користувачем облікові дані перевіряються шляхом порівняння з інформацією у файлі бази даних з авторизованими користувачами або на локальній операційній системі, або через сервер аутентифікації. Якщо дані збігаються, і автентифікований суб'єкт має відповідні права на використання ресурсу, процес завершується, і користувач отримує доступ. Права та доступ до папок визначають, яке середовище бачить користувач, а також спосіб взаємодії з ним, включаючи час доступу та інші налаштування, такі як обсяг використовуваних ресурсів.

Традиційно автентифікація виконується системами або ресурсами, які забезпечують доступ. Наприклад, сервер аутентифікації користувачів використовує власну систему паролів, реалізовану локально, і використовує ідентифікатори входу (імена користувачів) та паролі. Вважається, що знання облікових даних для входу гарантує автентичність користувача. Кожен користувач спочатку реєструється, встановлюючи пароль, і повторно його використовує при наступних сеансах.

Тим не менше, протоколи додатків у Інтернеті, такі як HTTP і HTTPS, не зберігають стану, що означає, що кінцеві користувачі перевіряються при кожному доступі до ресурсу через HTTPS. Щоб полегшити цей процес для кінцевих користувачів, захищені системи часто використовують автентифікацію на основі токенів. Користувач автентифікується один раз під час початку сеансу, і система видає підписаний токен, який використовується при кожному запиті від клієнта.

Аутентифікація для систем і процесів може виконуватися через використання облікових даних машини, які служать як ідентифікатор користувача та пароль. Важливим відзначенням є те, що ці облікові дані автоматично передаються від цього пристрою. Також можуть використовуватися цифрові сертифікати, які були видані та перевірені центром сертифікації в рамках інфраструктури відкритого ключа для автентифікації особи під час обміну інформацією через Інтернет.

Аутентифікація користувача за допомогою ідентифікатора користувача та пароля вважається основним типом аутентифікації. Цей тип аутентифікації передбачає введення двох частин інформації: ідентифікатора користувача (ім'я користувача) та пароля. Оскільки це ґрунтується лише на одному факторі, це визначається як однофакторна аутентифікація.

Фактори автентифікації представляють собою дані або атрибути, які використовуються для визначення особи, яка запитує доступ до системи. Раніше розрізняли такі фактори, як: "те, що ви знаєте, те, що у вас є або хто ви". Ці три фактори відповідають факторам знання, володіння та сутності. За останні роки було введено та реалізовано додаткові фактори: місце розташування та час.

Фактори автентифікації, що використовуються в даний час, включають ряд чинників, наприклад чинник знання: «Те, що ви знаєте». Фактором знань можуть бути будь-які облікові дані аутентифікації, які складаються з інформації, яку має користувач, включаючи персональний ідентифікаційний номер (ПІН), ім'я користувача, пароль або відповідь на секретне запитання.

Ще одним аспектом є фактор володіння, означений як "Те, що у вас є". Цей фактор може включати різноманітні облікові дані, що базуються на предметах,

якими користувач може володіти та носити при собі, таких як апаратні пристрої, наприклад токен безпеки чи мобільний телефон. Останній може використовуватися для отримання текстових повідомлень або запуску програми автентифікації, яка генерує одноразовий пароль або PIN-код.

Часто використовується фактор сутності, що базується на певних формах біометричної ідентифікації, таких як відбитки пальців, розпізнавання обличчя, сканування сітківки та інші біометричні дані.

Фактор розташування відповідає на питання "Де ви знаходитесь". Хоча він може бути менш конкретним, іноді використовується як додатковий елемент разом з іншими факторами. Розташування може бути точно визначене за допомогою пристроїв з GPS або менш точно за допомогою перевірки мережевих маршрутів. Цей фактор може доповнювати інші, надаючи можливість відфільтрувати спроби доступу з віддалених географічних областей, що не характерні для звичних місць входу.

Фактор часу відповідає на питання "Коли ви аутентифікуєтеся". Як і фактор розташування, цей фактор сам по собі недостатній, але його можна використовувати як додатковий механізм для відсіювання зловмисників. Також, разом із розташуванням, він може використовуватися для встановлення обмежень на доступ залежно від часу та місця. Сучасні технології, такі як смартфони з GPS, дозволяють зручно використовувати багатофакторну аутентифікацію для більшої безпеки.

Система аутентифікації користувача зазвичай включає в себе процес перевірки та підтвердження ідентичності особи, яка намагається отримати доступ до системи чи ресурсу. Це може бути виконано за допомогою різних методів, включаючи:

1. пароль або PIN-код;
2. фізичний токен або смарт-карта
3. біометричні дані, такі як відбиток пальця чи розпізнавання обличчя.

1.2. Аналіз біометричних систем аутентифікації

Біометрична автентифікація – це процес підтвердження та перевірки автентичності оголошеного користувачем імені через подання свого біометричного зображення, та шляхом перетворення цього зображення відповідно до попередньо встановленого протоколу автентифікації.

Ці системи не слід плутати із системами біометричної ідентифікації, такими як, наприклад, системи розпізнавання осіб водіїв та системи біометричного контролю робочого дня. Біометричні системи аутентифікації працюють в активному, а не пасивному режимі та майже завжди мають на увазі авторизацію. Хоча ці системи не схожі на системи авторизації, вони часто комбінуються (наприклад, вони встановлюють замки з перевіркою відбитків пальців у електронних дверях).

Різні системи безпечного доступу можна розділити на три групи в залежності від того, як користувач збирається використовувати систему:

- Використовуючи ключі. Користувач представляє свій особистий ідентифікатор, що є фізичним зберігачем ключа. Зазвичай використовуються пластикові картки з магнітною смугою, флешки та інші пристрої;

- захист паролем. Користувач використовує секретні дані для отримання доступу (наприклад, PIN-код або пароль);

- біометрія. Користувач представляє біологічний параметр, яка є його частиною. Біометричний клас відрізняється тим, що біологічні характеристики людини піддаються ідентифікації – її індивідуальні особливості (малюнок сітківки, відбитки пальців, малюнок особи і т. д.).

Біометричні системи доступу надійні та зручні для користувача. На відміну від паролів та ключів, які можуть бути втрачені, вкрадені, скопійовані, біометричні системи доступу ґрунтуються на біологічних параметрах, які є невід'ємною частиною користувача, і проблема їхньої безпеки не виникає. Втратити їх практично неможливо. Також неможливо передати ідентифікатор третім особам. В іншому ви можете примусово видалити параметри. У фільмах та анімаціях

неодноразово було показано, що очі та руки можуть бути ампутовані (або використані користувачем як жетон заручника). Ви також можете робити копії, у тому числі приховано рахуючи параметри. Однак багато методів мають захист від використання мертвого органу чи копії. Так, багато сканерів райдужної оболонки також мають інфрачервоний сканер, який визначає, чи є око теплим, макетним чи ні (ви можете ходити, нагріваючи око або використовуючи лінзи з малюнком).

Проводяться дослідження можливості використання короткочасного спалаху та сканування рухової реакції зіниці, але цей метод має потенційні проблеми з використанням наркотичного сп'яніння та офтальмологічних препаратів. Сканери відбитків пальців можуть поєднувати ультразвукове та ємнісне (захищає від копіювання на струменевому принтері, надрукованому провідним чорнилом),сканування (може бути обмануто провідним матеріалом і 3D-принтером). Найбільш надійним методом тут є сканування сітківки, дуже складно зробити макет після смерті судини сітківки перестають перекачувати кров, і сканер здатний це визначити. Повністю насильницьке використання заручника потенційно може бути визначено шляхом аналізу поведінки на відео, наприклад, з використанням нейронних мереж.

Критерії для біометричних властивостей. Вони мають відповідати наступним якостям:

- унікальність: біометрія заперечує існування двох людей з однаковими біологічними та фізичними параметрами;

- універсальність: ця функція має бути присутня для всіх користувачів;

- сталість: для правильної аутентифікації потрібно узгодженість у часі;

- вимірність: система повинна бути здатна вимірювати знак з допомогою будь-якого пристрою для подальшого зберігання бази даних.

- прийнятність: суспільство не повинно бути проти збору та виміру біометричні параметри.

Усі методи біометричної автентифікації поділяються на два види:

- статичні методи;

- динамічні методи.

Біометричні системи аутентифікації можуть сканувати різні параметри користувача і поділяються на кілька підвидів розпізнавання:

- по відбитку пальців;
- по райдужці ока;
- по сітківці ока;
- з геометрії кисті;
- з геометрії обличчя;
- за термограмою обличчя;
- за голосом;
- за рукописним підписом.

Статичні методи

Аутентифікація по відбитку пальця

Цей метод поширений і застосовується у різних інфраструктурах. Завдяки маленькому розміру для інтеграції, використовується навіть у смартфонах ноутбуках і т.д.

Суть методу полягає у скануванні папілярних візерунків, які у всіх людей індивідуальні, і за точками, що відповідають певним малюнкам пальця, створення моделі. Перевагами використання аутентифікації за відбитками пальців є простота використання, швидкість автентифікації та надійність. Також у деяких джерелах сканери відбитків пальців поділяються на 3 класу відповідно до їх фізичних принципів: оптичний, кремнієвий, ультразвуковий.

Аутентифікація по райдужній оболонці очей

Через те, що від народження райдужка людини не змінює свою форму, метод є досить точним.

Розпізнавання людською райдужкою призначене для виключення розпізнавання сітківкою, оскільки вчені виявили, що сітківка має тенденцію змінювати свою структуру з віком, на відміну від райдужної оболонки. Інфрачервоні промені та яскраве світло, що використовуються при розпізнаванні сітківки, що негативно впливали на зір людини, тому вчені були змушені вдосконалити цю технологію. Одним із ключових факторів переходу до

розпізнавання райдужної оболонки є те, що немає двох людей з однаковою структурою райдужної оболонки.

Для отримання інформації про діафрагму чорно-біла камера робить 30 записів за секунду. Низьке світло допомагає камері сфокусуватися на діафрагми. Найбільш чітке зображення оцифровується та зберігається в базі даних користувачів. Тривалість процедури становить декілька секунд. Контактні лінзи будь-якого кольору та окуляри не впливають на якість ідентифікації користувача, оскільки зйомка відбувається у чорно-білому режимі.

Вартість технології є ключовим фактором, який впливає на розподіл. Наразі розробляються різні незалежні організації, які дозволяють технологіям ставати дешевше та простіше в використання. Прихильники технології стверджують, що розпізнавання райдужної оболонки незабаром стане загальною технологією ідентифікації в різних областях.

Аутентифікація сітківки ока

Сітківка ока одне з найзахищеніших місць людського тіла, що надає гарну безпеку від злому, саме тому цей метод популярний у військових. У звичайних громадян представлений метод викликає психологічний дискомфорт, тому що при скануванні сітківки очей має бути не рухомим, коли в нього світить інфрачервоне випромінювання та яскраве світло.

Взаємодія даного методу та користувача з хворими очима може призвести до сліпоти. Але через точність і захищеність даного методу їм не припиняють користуватися.

Аутентифікація з геометрії кисті руки

Простота використання та його недороге використання призводить до широкому використанню представленого методу. Крапок для побудова шаблонної моделі стільки ж скільки в методі відбитка пальця, але при цьому через те, що в сканованому об'єкті більше параметрів такі як довжина фаланг, вигини пальців і т. д. метод є надійнішим.

Для даної аутентифікації відбувається створення тривимірної моделі кисті та наступні порівняння з еталонним варіантом. Недоліком системи є висока ймовірність пошкодження частини тіла, що читається.

Метод аутентифікації пензлем був створений на початку 70-х років і відразу став дуже популярним у різних сферах життя людей.

Аутентифікація з геометрії обличчя

Цей метод полягає у створенні еталонного шаблону тривимірної моделі особи кожному за користувача індивідуально. Державні служби часто користуються цим методом у спрощеній формі, для пошуку підозрюваних, злочинців боржників і т. д. Усі дії відбувається при підключенні до громадських камер, за допомогою яких відбувається сканування осіб у місцях великого скупчення людей.

Аутентифікація та створення шаблону для кожної людини вимагає від дванадцяти до сорока різних елементів. Шаблон має бути проекцією з різних боків, щоб розпізнавати навіть повернене обличчя. Чим більше елементів, що скануються в шаблоні, тим більш точним розпізнавання при зміні зовнішності людини [3].

Аутентифікація за термограмою обличчя

У зв'язку з тим, що в даний час добре розвинена пластична інфраструктура, в якій можна повністю змінити зовнішній вигляд і розпізнавання геометрії обличчя виявився марним. Оскільки у кожної людини розташування теплових полів індивідуально аутентифікація термограмою обличчя більш надійна.

Сканування виконується інфрачервоними камерами, які вимірюють розмір, місце розташування та інтенсивність теплового випромінювання. Цей метод немає широкого застосування через необхідного йому устаткування.

Динамічні методи

Аутентифікація за голосом

Одним із найпростіших у використанні та впровадженні є голосова автентифікація. Представлений спосіб не вимагає великих витрат на обладнання, достатньо звукової карти та мікрофона.

Недоліком цього методу є низький рівень універсальності та адаптації, оскільки людина часто хворіє, а система може не розпізнавати хрипкий голос, також може призвести до різноманітності тональності голосу.

одну й ту саму людину. до негативного результату. Оскільки різноманітність голосових властивостей однієї й тієї ж людини може відрізнятися, що призводить до труднощів у виявленні унікальних характеристик. Цей метод не використовується для захисту важливої інформації [19].

Аутентифікація з рукописного підпису

Підпис у кожного користувача індивідуальний, але при цьому його можна сфальшувати. Еталонний шаблон створюється залежно від необхідного ступеня захисту, чим більше параметрів сканується. Найпростіший спосіб це сканування по фото, запропонований варіант порівнюється із шаблоном. При найвищому рівні сканується безліч точок на підписи, швидкість написання, тиск на ручку і т.д.

Порівняння всіх видів біометричної автентифікації

Вибір систем біометричної аутентифікації великий, але кожен спосіб має як свої плюси, і мінуси. При виборі потрібно чітко розуміти, для яких цілей потрібна система, що вибирається. Порівняння видів між собою представлене у таблиці 1.1.

Таблиця 1.1

Способи біометричних систем автентифікації

Методи	№	Спосіб автенти-фікації	Необхідне обладнання	Плюси	Мінуси	Область застосування
Статичні	1	Аутенти-фікація по відбитку пальців.	Скануюча панель з багаторівневим фотоелементом, у дорогих апаратах з датчиком ступеня натискання та температурним датчиком.	Швидкість аутентифікації, великий вибір апаратів сканування, простота використання, спеціальні модулі для аутентифікації не займають багато місця.	Мало точок для побудови шаблонної моделі, Можна обдурити фізичною копією пальця.	Телефони, ноутбуки, біометричні замки (двері, сейф, і т.д.)

	2	Аутенти-фікація по рогівці ока	Камера швидкісної зйомки вбудована в модуль сканування.	Швидкість сканування, Точність сканування, Високий захист від спроби підробки оригінального об'єкта	Вартість, Складність обладнання та його обслуговування	Об'єкти схильні до високого рівня небезпеки.
	3	Аутенти-фікація сітківки ока	Сканер сітківки ока з інфрачервоним випромінюванням низького ступеня інтенсивності.	Індивідуальність використовуваного об'єкта сканування, Висока точність сканування.	Зміна сітківки протягом життя, Незручність використання, Шкідливість організму.	Надсекретні об'єкти (особливо військові)
	4	Аутенти-фікація з геометрії кисті руки.	Скануючий модуль з камерою та освітлювальний елемент для створення тривимірної моделі	Швидкість сканування та обробки запиту, багато параметрів перевірки, простота використання, вартість.	Висока ймовірність пошкодження сканованої частини тіла, ті ж недоліки, що й у автентифікації по відбитку пальця.	Замки в бізнес-центрах, контрольно-пропускні пункти.
	5	Аутенти-фікація за термограмою обличчя.	Скануючий елемент з інфрачервоними камерами, для створення об'ємної теплової моделі обличчя.	Точність використо-вуваного методу, не обдурити навіть людям з ідентичною зовнішністю, захист від старіння та зміни об'єкта	Мала зацікавленість у цьому методі, Вартість спеціального обладнання, Складність роботи з обладнанням	Охоронні системи, військові об'єкти
	6	Аутенти-фікація з геометрії обличчя.	Камера або модуль дозволяє знімати та створювати тривимірну модель.	Швидкість автентифікації, Простота використання, Висока ступінь точності.	Виникнення проблем при частковій закритості обличчя можна обдурити при використанні	Державні служби, смартфони, банки.

					пластичного втручання	
Динамічні методи	7	Аутенти-фікація на голос.	Мікрофон, обладнання для обробки	Вартість, простота використання, швидкість сканування.	Низький рівень безпеки, При хворобі користувача, можуть виникнути проблеми з автенти-фікацією	Смартфони, двері, сейфи, банки.
	8	Аутенти-фікація з рукописного підпису	Сканер із сенсорною панеллю з датчиком сили натискання.	Простота використання, Швидкість сканування	Можливість підробки, Низький рівень безпеки.	Бізнес підприємства, державні служби, банки.

Біометричні системи аутентифікації постійно вдосконалюються та оптимізуються. Поступово біометрична система захисту стає дешевшою, але при цьому надійнішою. Крім того, вони стають більш доступними в плані використання та обслуговування, малий відсоток системних помилок і збоїв при яких користувач не був авторизований або прийнятий за іншого. Найближчим часом біометричні системи аутентифікації займуть лідируючу нішу в системах захисту.

Усі розглянуті методи мають як плюси, так і мінуси. У цій роботі оптимально підходить метод аутентифікації за допомогою розпізнавання геометрії обличчя.

1.3.Існуючі особливості аутентифікації та авторизації

Процес авторизації включає у себе дії, під час яких адміністратор встановлює права для вже аутентифікованих користувачів і здійснює перевірку дозволів облікового запису, щоб забезпечити, що користувач має відповідний доступ до необхідних ресурсів. При цьому права та привілеї, пов'язані із визначеним обліковим записом, визначаються на рівні дозволів користувача, які можуть знаходитися на локальному пристрої або на сервері аутентифікації. Параметри середовища встановлюються адміністратором для усіх цих змінних.

Автоматизованим системам та процесам також може бути необхідна авторизація для виконання визначених дій у мережі. Онлайн-сервіси резервного копіювання, системи виправлення та оновлення, а також системи віддаленого моніторингу, наприклад у технологіях телемедицини та смарт-сітках, проходять надійну аутентифікацію.

Зазвичай традиційна аутентифікація ґрунтується на використанні файлу паролів, де ідентифікатори користувачів зберігаються поруч із хешами паролів, пов'язаних із кожним користувачем. У процесі входу в систему пароль, надісланий користувачем, хешується та порівнюється із значенням у файлі паролів. Цей метод має свої недоліки, зокрема, вразливість до атак грубої сили та потребу в кількох аутентифікаціях для додатків, що працюють у різних системах. На щастя, інтелектуальніші вимоги до імен користувачів та паролів, такі як мінімальна довжина та складні умови, забезпечують деяку виправдану захищеність. Тим не менше, ці форми аутентифікації ґрунтуються на паролях та знаннях, і, таким чином, виявляються менш безпечними порівняно із системами, що використовують кілька незалежних методів.

Додаткові методи аутентифікації можна поділити на кілька факторів. Використання багатофакторної аутентифікації, що вимагає принаймні два різні фактори, вважається більш надійним та стійким до атак. Сучасні методи, такі як аутентифікація на основі криптографічних методів, визнаються як строгий підхід.

Впровадження двофакторної та багатофакторної аутентифікації, яке включає в себе кілька різних факторів, дозволяє значно підвищити рівень безпеки. Сувора аутентифікація передбачає використання принаймні двох різних типів факторів. Іншими словами, базова аутентифікація, що використовує ім'я користувача та пароль, не є прикладом двофакторної аутентифікації (2FA).

Двофакторна автентифікація зазвичай ґрунтується на поєднанні фактора знання із біометричним або фактором володіння, таким як токен безпеки. Системи двофакторної автентифікації (2FA) часто вимагають від користувача введення коду підтвердження, який надходить текстовим повідомленням на заздалегідь

зареєстрований мобільний телефон, або коду, створеного за допомогою додатка для автентифікації.

Багатофакторна автентифікація передбачає, що користувачі пройдуть аутентифікацію, використовуючи кілька факторів, таких як біометричний (відбиток пальця, розпізнавання обличчя), фактор володіння (фейс-ключ, токен безпеки від програми-аутентифікатора) та, можливо, фактор часу чи місцезнаходження. Багатофакторна автентифікація може включати різні типи аутентифікації, які залежать від двох чи більше факторів. Наприклад, процес аутентифікації, що включає в себе введення пароля разом із двома різними біометричними даними, не вважатиметься трифакторною аутентифікацією. Однак, якщо для цього процесу необхідні фактор знання, фактор володіння та фактор сутності, тоді він може бути розглядений як трифакторна аутентифікація.

Трифакторна аутентифікація (3FA) є одним з типів багатофакторної аутентифікації (MFA) і використовує три різних фактори аутентифікації. Зазвичай, це включає коефіцієнт знання (пароль), фактор володіння (маркер безпеки) та коефіцієнт спадкування (біометричний).

Надається приклади чотирифакторної аутентифікації, яка вимагає не лише трьох основних факторів, але й додаткового елемента, такого як географічне чи тимчасове позначення. Важливо відзначити одноразовий пароль – це автоматично сформований набір числових чи буквено-цифрових символів, який служить для аутентифікації користувача. Даний пароль залишається активним лише протягом одного сеансу входу або транзакції та часто застосовується для нових користувачів чи тих, хто втратив свій основний пароль, щоб забезпечити вхід до системи та перехід до нового пароля.

Хоча деякі системи аутентифікації можуть базуватися виключно на біометричній ідентифікації, біометричні дані зазвичай використовуються як додатковий, другорядний чи третинний фактор аутентифікації. Серед розповсюджених типів біометричної автентифікації варто відзначити сканування відбитків пальців, обличчя чи сітківки та розпізнавання голосу.

Мобільна автентифікація представляє собою процес перевірки користувача через пристрої або перевірку самого пристрою. Це дозволяє користувачам отримувати доступ до безпечних місць та ресурсів з будь-якого місця. Процес мобільної аутентифікації включає багатофакторність, яка може включати в себе одноразові паролі, біометричну аутентифікацію чи перевірку QR-коду. Під час неперервної автентифікації додаток компанії постійно обчислює "оцінку справжності", яка вимірює, наскільки впевнений система, що власник облікового запису – це фізична особа, яка використовує пристрій.

Аутентифікація через API (інтерфейс програмування додатків) ґрунтується на кількох принципах. Основні методи управління аутентифікацією API включають базову автентифікацію HTTP, використання ключів API та принципи OAuth. В базовій аутентифікації HTTP сервер запитує інформацію аутентифікації, таку як ім'я користувача та пароль, від клієнта. Після чого клієнт передає цю інформацію серверу в заголовку авторизації. У випадку аутентифікації ключами API перший користувач отримує унікальне згенероване значення, яке підтверджує його ідентичність. При кожній наступній спробі входу в систему використовується його унікальний ключ для перевірки того, що він той самий користувач, який раніше входив в систему.

Open Authorization (OAuth) – це відкритий стандарт для аутентифікації та авторизації на токенах в Інтернеті. OAuth дозволяє використовувати інформацію облікового запису користувача сторонніми службами, такими як Facebook, без викриття пароля користувача. OAuth виступає посередником від імені користувача, видавши службі токен доступу, який дає можливість спільного використання певної інформації облікового запису.

Процедура аутентифікації користувача та аутентифікації комп'ютера включає ідентифікацію машини, яка може базуватися на облікових даних пристрою, таких як ідентифікатор користувача та пароль, представлені самим пристроєм. Додатково, використання цифрових сертифікатів, виданих та перевірених центром сертифікації, є розповсюдженим явищем і становить частину інфраструктури відкритого ключа, спрямованої на підтвердження ідентифікації під

час обміну інформацією через Інтернет, як, наприклад, у випадку цифрового пароля.

Зі зростанням кількості пристроїв з підтримкою Інтернету, важливим аспектом стає надійна автентифікація машини, спрямована на забезпечення безпечного зв'язку в автоматизованих системах, таких як "Розумний дім", а також у сфері Інтернету речей, де будь-який суб'єкт чи об'єкт може виступати як адресат та обмінюватися даними через мережу. Потрібно розуміти, що кожна точка доступу може стати потенційною точкою вторгнення. Таким чином, кожен мережевий пристрій повинен пройти надійну автентифікацію машини. Навіть у випадку обмеженої активності таких пристроїв, вони повинні бути налаштовані на обмежений доступ для запобігання можливим порушенням безпеки.

Поняття суворої автентифікації визначає будь-який метод аутентифікації користувача або пристрою, який, в суті, є настільки ретельним, щоб гарантувати безпеку системи, яку він захищає, і витримувати будь-які атаки, що можуть виникнути. Це поняття, як правило, має єдиний стандартний визначення. Згідно з Європейським центральним банком та іншими стандартами, сувора автентифікація передбачає використання щонайменше двох взаємозалежних факторів, забезпечуючи таким чином непорушність обох методів, і включає елемент, який не може бути повторно використаний чи легко скопійований через Інтернет. Отже, термін "строга автентифікація" визначається як синонім до двофакторної або багатофакторної автентифікації. Тим не менше, такий підхід призводить до непорозумінь, оскільки деякі види надійної автентифікації ґрунтуються на одному факторі, наприклад, системи, що використовують криптографічно захищені відповіді на запит/відповідь, що, однак, є формою однофакторної автентифікації (SFA).

Аналогічно, деякі види біометричної автентифікації виявляються досить ефективними у своєму використанні. Наприклад, національні стандарти, такі як ДСТУ 9594-8-98, або міжнародний Recommendation X.509 (11/88), використовують криптографічні методи. У цьому стандарті виокремлюються та описуються три процедури суворої аутентифікації: односпрямована, двоспрямована і

триспрямована аутентифікація. В процедурі суворої аутентифікації сторона, що перевіряється, доводить свою справжність через демонстрацію знань секрету за допомогою криптографічних методів. Зазвичай, цей секрет – це секретний ключ, розподілений безпечним способом, який не передається через відкриті канали під час автентифікаційного обміну.

В односторонній автентифікації лише одна сторона підтверджує свою справжність. Порівняно із цим, двостороння автентифікація містить взаємне підтвердження обох сторін – тієї, що перевіряє, і тієї, що підтверджує свою справжність. У випадку тристоронньої автентифікації передача додаткових даних від сторони, що перевіряє, дозволяє уникнути використання міток часу при процедурі аутентифікації [14]. Протоколи, що використовують сувору автентифікацію, можуть базуватися на різноманітних криптографічних методах, таких як симетричні методи шифрування, односпрямовані ключові хеш-функції, асиметричні методи шифрування та цифровий підпис.

Двосторонні та тристоронні процедури входять до категорії взаємної аутентифікації. Взаємна автентифікація або двостороння автентифікація відноситься до взаємного підтвердження обох сторін, які автентифікують одна одну. Це може бути режимом автентифікації за замовчуванням у деяких протоколах, таких як IKE та SSH, і стати необов'язковим в інших, наприклад, TLS. Протокол TLS за замовчуванням підтверджує лише автентифікацію сервера перед клієнтом за допомогою сертифіката X.509, водночас залишаючи автентифікацію клієнта для сервера на рівні додатків. У TLS також пропонується взаємна автентифікація клієнта та сервера за допомогою аутентифікації X.509 на стороні клієнта. Однак, оскільки це вимагає надання сертифікатів клієнтам та може бути менш зручним для користувача, такий підхід рідко використовується у програмах для кінцевих користувачів.

Взаємна автентифікація TLS (mTLS) більш поширена в застосунках для бізнесу (B2B), де обмежена кількість програм та однорідних клієнтів підключаються до конкретних веб-служб. У таких випадках експлуатаційне

навантаження обмежене, а вимоги до безпеки значно вищі порівняно із споживчим середовищем.

Завдяки взаємній автентифікації між установами та клієнтами ускладнюється завдання зловмисників, які намагаються успішно виглядати фінансовими установами для викрадення облікових даних клієнтів. Звісно, належна автентифікація між клієнтами та установами ускладнює завдання зловмисників, які спробують видати себе за клієнтів, намагаючись виглядати як фінансові установи для шахрайства.

У більшості випадків взаємна автентифікація здійснюється на рівні "машина-машина", що надає користувачам можливість виявити випадки, коли віддалена автентифікація завершується невдачею (наприклад, з'являється червоний замок в адресному рядку браузера або неправильно вказане ім'я домену). Крім того, існує нетехнічна взаємна автентифікація, спрямована на полегшення цієї проблеми, що передбачає виконання користувачем завдань, ефективно мотивуючи його до повідомлення та блокування автентифікації у випадку виявлення некоректної кінцевої точки.

Взаємна автентифікація буває двох типів:

- на основі сертифікату;
- на основі імені та пароля користувача.

При взаємній аутентифікації сервер та клієнт аутентифікують один одного. У разі використання взаємної автентифікації на основі сертифікатів виконуються такі дії:

1. Клієнт вимагає доступу до захищеного ресурсу.
2. Веб-сервер представляє сертифікат клієнту.
3. Клієнт перевіряє сертифікат сервера.
4. У разі успіху клієнт надсилає свій сертифікат на сервер.
5. Сервер перевіряє облікові дані клієнта.
6. У разі успіху сервер надає доступ до захищеного ресурсу, запрошеного клієнтом.

Під час взаємної автентифікації на основі імені користувача та пароля виконуються такі дії.

1. Клієнт вимагає доступу до захищеного ресурсу.
2. Веб-сервер представляє сертифікат клієнту.
3. Клієнт перевіряє сертифікат сервера.
4. У разі успіху клієнт надсилає своє ім'я користувача та пароль на сервер, який перевіряє облікові дані клієнта.
5. Якщо перевірка пройшла успішно, сервер надає доступ до захищеного ресурсу, запрошеного клієнтом.

1.4. Завдання кваліфікаційної роботи

Проведене дослідження процесів аутентифікації та авторизації, виділені основні функціональні відмінності процесу аутентифікації, аналіз біометричних систем аутентифікації, їх статичних та динамічних методів, а також порівняння всіх видів біометричної автентифікації вказують на доцільність розроблення, реалізації системи авторизації за допомогою систем розпізнавання BioStar2 на базі платформи FaceStation2 на мові програмування C# та проведення тестування розроблених програмних модулів. Для цього слід вирішити у роботі такі завдання:

➢ провести дослідження процесів аутентифікації та авторизації, для того щоб виділити основні функціональні відмінності;

➢ дослідити реалізації системи аутентифікації на базі F2S платформи, їхню інтеграцію у існуючі системи управління даними;

➢ виконано формалізацію процесу авторизації на основі біометричних даних для побудови алгоритму біометричної автентифікації;

➢ здійснити опис побудови системи розпізнавання обличчя на базі платформи FaceStation2;

➢ реалізувати систему авторизації за допомогою систем розпізнавання BioStar2 на базі платформи FaceStation2 на мові програмування C# та провести тестування розроблених програмних модулів;

➢ розробити заходи стосовно охорони праці та безпеки у надзвичайних ситуаціях;

➢ визначити економічну ефективність від розроблених програмних модулів.

РОЗДІЛ 2.
ОБГРУНТУВАННЯ ТА ВИБІР МЕТОДІВ ДЛЯ РОЗРОБКИ СИСТЕМИ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧА

2.1. Нейронні мережі

Нейронні мережі у системах автентифікації використовуються для розпізнавання та перевірки ідентичності особи на основі її біометричних ознак. Такі системи базуються на здатності нейронних мереж аналізувати та вивчати складні закономірності у великих обсягах біометричних даних.

У світі представлено понад десять видів нейронних мереж (НМ). Одним із найчастіше застосовуваних варіантів є мережа, побудована на багатошаровому персептроні, яка дозволяє розпізнавати надане зображення/сигнал відповідно до попереднього навчання/налаштування мережі.

Навчання нейронних мереж полягає у класифікації міжнейронних зв'язків за вагами та методом градієнтного спуску оптимізації завдання. Під час налаштування нейронних мереж в автоматичному режимі вилучають ключові ознаки, класифікуючи їх за важливістю та видом взаємозв'язку між ними. В результаті навчена нейронна мережа зможе застосувати отриманий у процесі навчання досвід на нові зображення завдяки узагальнюючим здібностям.

Найкращі результати в галузі розпізнавання облич (за результатами аналізу публікацій) показала Convolutional Neural Network або надточна нейронна мережа (далі – ННМ), яка є логічним розвитком ідей таких архітектур НМ як когнітрону та неокогнітрону. Успіх обумовлений можливістю обліку двовимірної топології зображення, на відміну від багатошарового персептрона.

Відмінними рисами ННМ є локальні рецепторні поля (забезпечують локальну двовимірну зв'язність нейронів), загальні ваги (забезпечують детектування деяких рис в будь-якому місці зображення) та ієрархічна організація з просторовими семплінгом (spatial subsampling). Завдяки цим нововведенням ННМ забезпечує

часткову стійкість до змін масштабу, зсувів, поворотів, зміни ракурсу та інших спотворень.

Тестування НММ на базі даних ORL, що містить зображення осіб з невеликими змінами освітлення, масштабу, просторових поворотів, положення та різними емоціями, показало 96% точність розпізнавання. Свій розвиток НММ отримали у розробці DeepFace, яку придбав Facebook для розпізнавання осіб користувачів своєї соціальної мережі. Усі особливості архітектури мають закритий характер.

Плюси нейронних мереж у системах автентифікації: глибокі нейронні мережі можуть досягати високого рівня точності при розпізнаванні біометричних ознак, таких як обличчя, голос, відбитки пальців і т. д; нейронні мережі можуть бути адаптивними до змін в біометричних даних користувача з плином часу, наприклад, з урахуванням змін у вигляді обличчя або голосу; мережі можуть ефективно обробляти та комбінувати інформацію з різних біометричних джерел для поліпшення точності; можливість навчання на реальних даних може поліпшити адаптивність системи до реальних умов та варіацій.

Недоліки нейронних мереж: додавання нової еталонного обличчя до бази даних вимагає повного перенавчання мережі по всьому наявному наборі (досить тривала процедура, залежно від обсягу вибірки від 1 години до кілька днів). Проблеми математичного характеру, пов'язані з навчанням: перенавчання, вибір оптимального кроку оптимізації, потрапляння до локального оптимуму тощо.

2.2. Приховані Марківські моделі

Одним із статистичних методів розпізнавання облич є приховані Марківські моделі (ПММ) з дискретним часом. ПММ використовують статистичні властивості сигналів та враховують безпосередньо їх просторові характеристики. Елементами моделі є: матриця перехідних ймовірностей, початкова ймовірність станів, безліч прихованих станів, безліч станів, що спостерігаються. Кожному відповідає своя ПММ. При розпізнаванні об'єкта перевіряються згенеровані для заданої бази Марківські моделі, і шукається максимальна на всьому проміжку дослідження

ймовірність того, що послідовність спостережень для об'єкта згенерована відповідною моделлю.

Приховані Марківські моделі (ПММ) з дискретним часом мають певні переваги у контексті розпізнавання облич. ПММ дозволяють моделювати динаміку сигналів в часі. Це особливо важливо для розпізнавання облич, оскільки обличчя може змінюватися з часом, наприклад, при рухах або зміні виразів. Модель використовує "приховані стани", які можуть представляти різні стани обличчя (наприклад, вирази обличчя або пози). Це робить модель більш гнучкою і спроможною адаптуватися до різних сценаріїв. ПММ базуються на ймовірнісних моделях, що дозволяє їм ефективно враховувати невизначеність у вхідних даних. Це важливо для реалістичного розпізнавання облич, оскільки вони можуть змінюватися через освітлення, погляд або інші фактори. ПММ можуть враховувати просторові характеристики обличчя, оскільки вони спроможні моделювати структуру та розташування об'єктів на зображенні. ПММ можуть ефективно використовувати локальні властивості сигналів, що може бути корисно при розпізнаванні облич у різних контекстах. Враховуючи ці плюси, ПММ можуть бути досить ефективним методом для розпізнавання облич, особливо коли важливо враховувати часові та просторові аспекти динамічного об'єкта, такого як обличчя.

Недоліки:

- Параметри моделі індивідуальні для кожної бази даних;

- ПММ не розпізнає відмінності, навчання моделям лише прискорює відгук на пошук потрібної моделі [13].

2.3. Метод головних компонент

Одним з розвинених методом є метод головних компонент (principal component analysis, PSA), заснований на перетворенні Карунена-Лоева.

Спочатку застосування PSA було поширене у статистиці, для оптимізації процесу використовувалося зменшення мало значимих ознак, але із збереженням ключової інформації.

У задачі розпізнавання облич його застосовують головним чином для представлення зображення обличчя вектором малої розмірності (головних компонент), який порівнюється потім з еталонними векторами, закладеними в базу даних.

Головною метою методу головних компонентів є значне зменшення розмірності простору ознак таким чином, щоб воно якнайкраще описувало «типові» образи, що належать безлічі облич. Використовуючи цей метод можна виявити різні мінливості в навчальній вибірці зображень облич та описати цю мінливість у базисі кількох ортогональних векторів, які називаються власними (eigenface).

При розпізнаванні облич на навчальній вибірці, виходить власний набір векторів, за допомогою яких здійснюється координування зображень, що надходять, які представляються зваженою комбінацією цих власних векторів. При використанні обмеженої кількості власних векторів можна отримати стислу апроксимацію вхідного зображення особи, яку потім можна зберігати в базі даних у вигляді вектора коефіцієнтів, що є одночасно ключем пошуку в базі даних облич.

PCA дозволяє зменшити розмірність даних, відділивши інформативні функції (головні компоненти) від менш інформативних. Це допомагає зменшити обсяг даних, що обробляється, та може полегшити подальший аналіз. PCA намагається знайти напрямки максимальної дисперсії в даних, що відповідають важливим особливостям даних. Це може бути корисно при розпізнаванні облич, оскільки важливі ознаки обличчя можуть виявитися вздовж цих напрямків. PCA може стати ефективним методом розпізнавання облич, оскільки головні компоненти визначаються структурою даних, незалежно від конкретного виразу обличчя чи пози. Зменшення розмірності за допомогою PCA може допомогти уникнути проблеми перенавчання (overfitting), особливо при роботі з обмеженим обсягом даних. PCA є лінійним методом, що може бути вигідним у випадках, коли дані мають відносно просту лінійну структуру.

Метод головних компонент добре показав себе практично. Однак, у тих випадках, коли на зображенні особи присутні значні зміни у освітленості або виразі

обличчя, ефективність методу значно зменшується. Вся справа в тому, що PSA вибирає підпростір з такою метою, щоб максимально профільтрувати вхідний набір даних, а не втратити ознаки відмінностей між класами осіб.

Загалом, PCA може бути корисним методом для витягування важливих ознак та зменшення розмірності даних при розпізнаванні облич. Однак важливо враховувати, що він може не враховувати нелінійні залежності між ознаками, і для деяких складних завдань розпізнавання облич може бути вигідно використовувати більш складні моделі.

2.4. Метод гнучкого порівняння на графах

Метод полягає в пружному порівнянні графіків, що описують зображення облич. Грані визначаються як графи із зваженими вершинами та ребрами. На етапі розпізнавання один із графіків – еталонний – залишається незмінним, а інший деформується з метою найкращої відповідності першому. У подібних системах розпізнавання графи можуть бути або структурою або прямокутною сіткою, утвореною характерними (антропометричними) вершинами грані.

У вершинах графа обчислюються значення атрибутів; найчастіше використовуються комплексні значення фільтрів Габора чи його впорядкованих наборів – вейвлети Габора (лінії Габора), які розраховуються локально у локальній області вершин графа шляхом порівняння значень яскравості пікселів із фільтрами Габора.

Ребра графа зважуються на відстані між сусідніми вершинами. Різниця (відстань, дискримінаційна характеристика) між двома графіками розраховується за допомогою деякої функції деформації ціни, яка враховує як різницю між значеннями характеристик, розрахованими у вершинах, так і ступінь деформації ребер граф.

Граф деформується шляхом зміщення кожної з його вершин на певну відстань у певних напрямках щодо його вихідного розташування та вибору його положення таким чином, щоб різниця між значеннями атрибутів (відгуками

фільтрів Габора) була у верхній частині деформованого графа та відповідна вершина графа посилань мінімальна. Ця операція виконується послідовно для всіх вершин графа, поки не знайдена найменша загальна різниця між знаками деформованого і еталонного графів. Значення функції ціни деформації в такому положенні графіка, що деформується, буде мірою різниці між вхідним зображенням обличчя і опорним графіком. Цю процедуру релаксаційної деформації слід виконати для всіх контрольних осіб, включених до бази даних системи. Результатом розпізнавання системи є стандарт з найкращим значенням функції ціни деформації.

Графи можуть ефективно виражати взаємозв'язки між об'єктами. У випадку розпізнавання облич, граф може використовуватися для представлення взаємозв'язків між різними частинами обличчя, ключовими точками, або навіть взаємодії з іншими об'єктами. Графи дозволяють гнучко визначати властивості та атрибути об'єктів, а також взаємозв'язки між ними. Це може полегшити використання різноманітних функцій та ознак для розпізнавання облич. Графові структури можуть бути менш чутливими до змін у розміщенні об'єктів або невеликих змін у формі обличчя порівняно з традиційними методами розпізнавання. Глибокі нейронні мережі, які використовують графові структури, можуть ефективно взаємодіяти з графами для розпізнавання облич та витягування корисної інформації з них. Графи можуть об'єднувати інформацію з різних джерел, дозволяючи враховувати контекст та взаємозв'язки для кращого розпізнавання облич.

Більшість статей вказують на 95–97% ефективності розпізнавання навіть за зміни емоційних виразів обличчя та зміни кута читання до 15 градусів. Однак розробники систем пружного порівняння на графіках попереджають про трудомісткі та дорогі обчислення графіків. Наприклад, щоб порівняти вхідне зображення обличчя з 87 еталонними шаблонами, потрібно приблизно 25 секунд при роботі на паралельному комп'ютері з 23 транспуляторами. В інших публікаціях на цю тему час або не вказано або сказано, що він великий.

Недоліки: обчислювальна складова становить високу складність процедури розпізнавання. Слабка навченість при запам'ятовуванні нових стандартів. Лінійна залежність часу роботи від обсягу бази даних осіб [17].

2.5. Активні моделі зовнішнього вигляду

Active Appearance Models (AAM) Активні моделі зовнішнього вигляду (Active Appearance Models, AAM) – це статистичні моделі зображень, які шляхом зміни форми моделі підбираються під реальне зображення. Представлений тип моделей у двовимірному просторі було запропоновано Тімом Кутсом та Крісом Тейлором у 1998 році. На початковому етапі AAM використовувалися для аналізу параметрів зображення обличчя.

AMM містить два типи параметрів: параметри, пов'язані зі статистичною моделлю пікселів зображення або текстурою (параметри зовнішнього вигляду), та параметри, пов'язані з формою (параметри форми). Перед використанням модель має бути штучно навчена на безлічі заздалегідь розмічених зображень. Розмітка зображень виконується вручну. Кожна точка визначається характерною міткою, якою відповідає певний номер, який модель розпізнає під час налаштування нового зображення [17], [13].

AAM можуть адаптуватися до змін у формі та текстурі обличчя, що робить їх ефективними при аналізі зображень з різними позами, виразами обличчя, а також при змінах освітлення. AAM базуються на статистичних властивостях обличчя, що дозволяє їм враховувати різні варіації у формі та текстурі. Це корисно при роботі з різноманітними зображеннями та сценаріями. Модель охоплює як форму, так і текстуру обличчя, дозволяючи здійснювати більш комплексний аналіз та враховувати важливі аспекти визначення обличчя. AAM можуть пристосовуватися до різних джерел даних, що може бути корисно при роботі з різними типами зображень чи даних, такими як фотографії, відео або зображення з різних джерел. Модель може бути налаштована на врахування локальних особливостей обличчя, таких як очі, ніс, рот та інші ключові точки, що може покращити точність

розпізнавання. AAM можуть використовуватися для відслідковування рухів та анімацій обличчя, що робить їх корисними в додатках відслідковування рухів, таких як в інтерфейсах розпізнавання жестів.

Незважаючи на ці плюси, важливо також враховувати обмеження AAM, такі як чутливість до змін в розміщенні ключових точок та обмежена здатність до ефективного врахування нелінійних змін у формі обличчя. Ефективність AAM може бути суттєво залежати від правильної ініціалізації моделі. Неправильна початкова ініціалізація може призвести до невірної адаптації моделі до зображення. AAM можуть бути чутливими до змін в освітленні та виразах обличчя, що може призвести до неправильного визначення ключових точок у випадках, коли обличчя змінює свій вигляд. У випадках зміни розмірів обличчя або часткового приховування ключових точок, AAM може втратити точність визначення контурів обличчя. Тренування та використання AAM може бути витратними з точки зору обчислень, особливо при великій кількості ключових точок та складних обличчях. AAM може виявлятися менш ефективними при обробці ситуацій, де існує значна невизначеність або коли форма обличчя змінюється дуже швидко. Модель може виявити складнощі при врахуванні змін відображення обличчя, таких як велика зміна кута огляду або артифакти, пов'язані з віддзеркаленням.

2.6. Формалізація системи аутентифікації

Обличчя - один із найпростіших способів відрізнити людину від іншої. Навіть малюк може впізнати обличчя матері через кілька днів після народження. Інтуїтивно зрозуміліше впізнати людину в обличчя, ніж за іншими факторами, як-от хода людини, її голос і зріст.

Біометричні системи автентифікації використовують такі фізичні ознаки, як відбитки пальців, обличчя, райдужна оболонка ока та вени як облікові дані. Крім іншого, термінали автентифікації обличчя використовують обличчя як облікові дані, що є найбільш схожим способом розпізнавання людини людиною. Завдяки

такій природі технології автентифікації обличчя люди відчувають себе комфортно під час автентифікації обличчя.

Пристрої розпізнавання відбитків пальців, які найчастіше використовуються для біометричної аутентифікації, оснащені оптичним датчиком. Оскільки автентифікація обличчя використовує камери для ідентифікації особи, оптичний датчик не потрібен. Таким чином, це дозволяє користувачеві виконувати автентифікацію без фізичного контакту. Оскільки термінали автентифікації за обличчям використовують ІЧ-технологію (ІЧ-порт), одним із головних недоліків автентифікації за обличчям є обмеження щодо місця встановлення: термінал автентифікації за обличчям працюватиме погано, якщо його встановити надворі або біля вікон через сильне навколишнє освітлення.

FaceStation 2, найновіший термінал автентифікації обличчя від Suprema, виходить за рамки цього обмеження. Це термінал контролю доступу та обліку робочого часу, який покращує роботу користувача з Android 5.0 Lollipop і найновішим алгоритмом, апаратним і програмним забезпеченням Suprema. Широкий набір функцій і покращена продуктивність забезпечать користувачам абсолютно новий досвід безконтактної біометричної автентифікації.

Покращена технологія автентифікації обличчя та ближній інфрачервоний світлодіод

Обробка навколишнього освітлення має вирішальне значення для продуктивності автентифікації обличчя. Більшість наявних на ринку терміналів автентифікації обличчя мають обмежені місця встановлення, оскільки продуктивність розпізнавання залежить від інтенсивності навколишнього освітлення.

FaceStation 2 має 80 ширококутних ближніх інфрачервоних світлодіодів і 60 вузькокутних ближніх інфрачервоних світлодіодів, тож він може розпізнавати обличчя навіть у середовищі з 25 000 люкс, що еквівалентно середовищу з повним денним освітленням (без прямого сонця). Це дозволяє користувачам встановлювати термінали в приміщеннях біля вікон, вестибюлів і входів у будівлі.

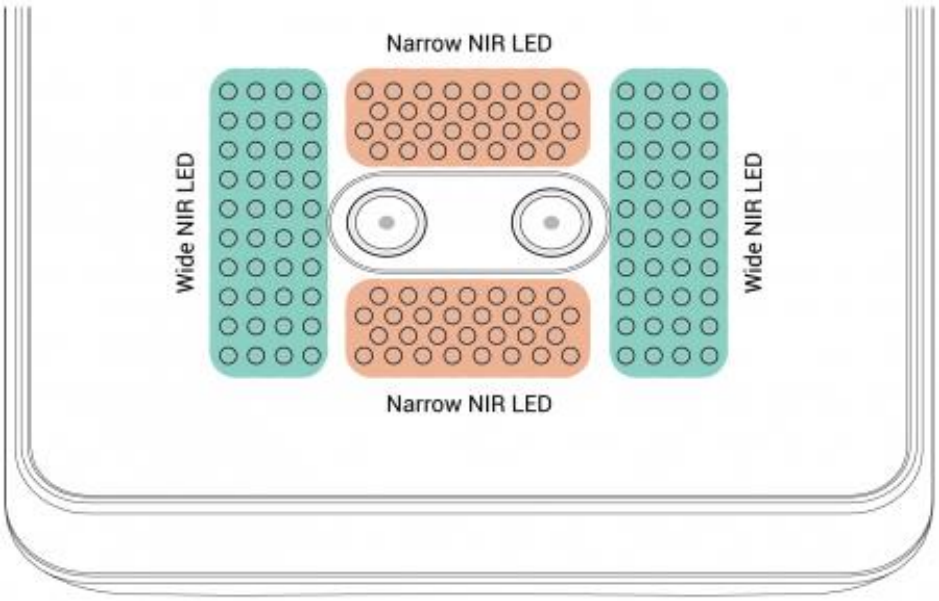

Рис. 2.1 Схема діодів на інтерфейсі станції

Ще одна технологія, застосована FaceStation 2 для підвищення продуктивності, — це аналіз розподілу інтенсивності пікселів. Однією з труднощів використання світлодіодної технології ближнього інфрачервоного діапазону є вплив навколишнього освітлення. Навколишнє освітлення може зробити світлодіодне освітлення ближнього інфрачервоного діапазону марним, оскільки воно містить ультрафіолетові промені. Крім того, тінь на обличчі від навколишнього освітлення може ускладнити алгоритм вилучення рис обличчя.

Аналіз розподілу інтенсивності тривимірних пікселів мінімізує вплив навколишнього освітлення під час отримання зображень обличчя. В результаті термінал отримує зображення в ближньому інфрачервоному діапазоні з мінімальною зміною контрастності. Алгоритму легше розпізнати форму обличчя за допомогою цих рівномірних контрастних зображень, ніж із занадто яскравими або темними зображеннями, тому він може виділити більше різноманітних рис, таким чином створюючи високоякісні шаблони обличчя. Високоякісні шаблони обличчя мають вирішальне значення для продуктивності автентифікації обличчя.

Кут і положення камер на FaceStation 2 визначені таким чином, щоб високим користувачам не потрібно було надто згинати спину. Крім того, різні кути огляду між вбудованою візуальною та інфрачервоною камерами дозволяють користувачам стояти в положенні, яке найбільше підходить для автентифікації обличчя

(користувачі можуть легко знайти себе, спробувавши знайти своє обличчя в правильному місці на екрані) .

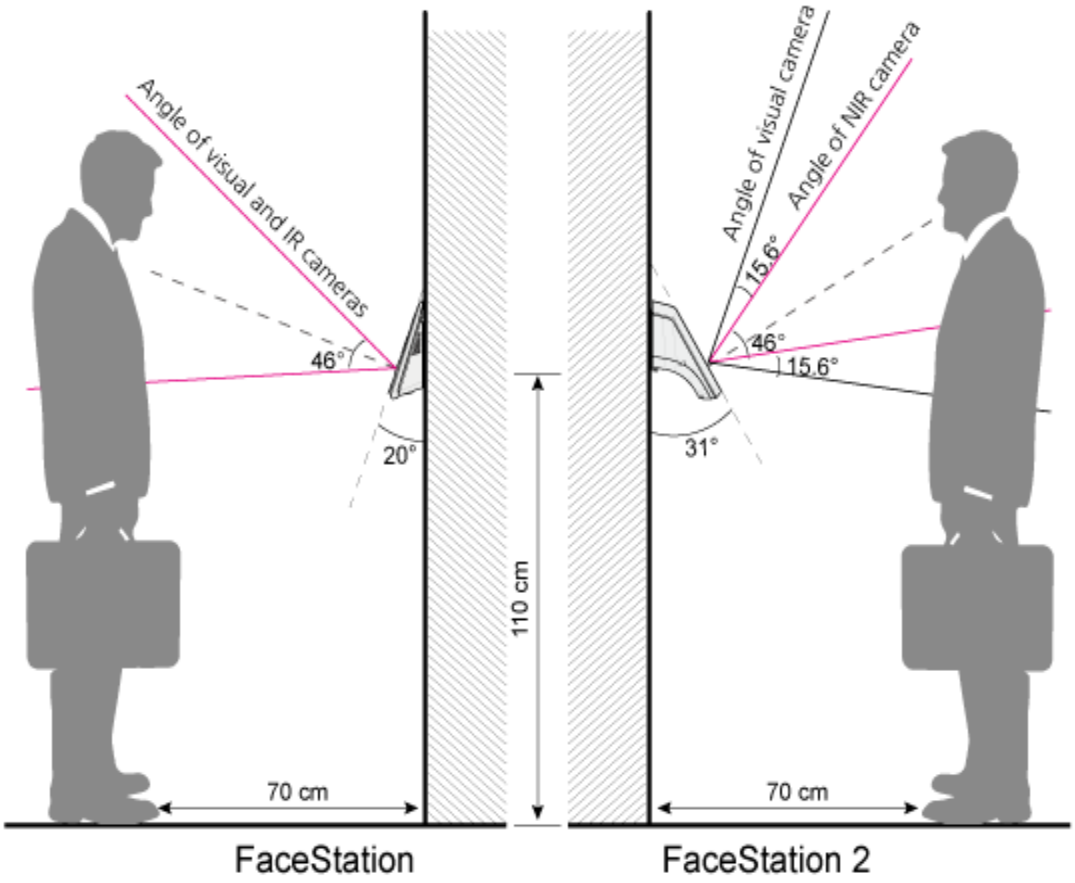

Рис. 2.2 Порівняльна різниця між FaceStation і FaceStation2

FaceStation 2 також працює як відеотелефон SIP (протокол ініціації сеансу), що усуває необхідність встановлення окремого відеотелефону. Якщо SIP-сервер уже встановлено на сайті, ви можете використовувати наявну SIP-інфраструктуру. В іншому випадку клієнти можуть встановити добре відомий SIP-сервер з відкритим кодом, рекомендований і протестований Suprema, щоб використовувати FaceStation 2 як відеотелефон.

Таким чином основними перевагами FSD2 є:

Висока продуктивність:

- Швидкість порівнянь (matching speed): 1:3,000 match/sec
- Group Matching: 1:5,000 match/sec

Найвища робоча освітленість:

- Робоча освітленість від 0 лк до 25000 лк

- Найвища доступна робоча освітленість
- Перекриває повну темряву за будь-яких умов освітлення в приміщенні

Покращена безпека:

- Розпізнавання обличчя в реальному часі: аналіз зображень на основі ІЧ для запобігання
- Підробка за допомогою друкованих зображень і РК-дисплеїв

Покращена безпека за допомогою Android 5.0 Lollipop, Android 5.0 Lollipop, випущений у 2014 році, вніс значні покращення у безпеку операційної системи Android порівняно з попередніми версіями. Android 5.0 вперше включав підтримку 64-бітних пристроїв, що дозволило використовувати більше безпеки на рівні апаратного забезпечення та більшу потужність шифрування. В Android 5.0 вперше був включений SELinux, що представляє собою мандатний модуль безпеки для ядра Linux. SELinux дозволяє обмежити доступ і зменшити можливість вразливостей шляхом введення політик безпеки на рівні ядра. Android 5.0 запровадив стандартне шифрування даних на пристроях за замовчуванням. Це важливий крок у напрямку захисту конфіденційної інформації користувачів в разі втрати чи крадіжки пристрою. Android 5.0 почав використовувати концепцію "RunTime Permissions" (дозволи в часі виконання), що дозволяло користувачам керувати дозволами додатків більш ефективно під час використання. Додаткові функції безпеки, такі як Smart Lock, яка дозволяє використовувати різні методи аутентифікації на основі контексту, а також удосконалені методи блокування екрану, були введені для забезпечення більшої безпеки пристрою. Для корпоративних користувачів Samsung представив технологію безпеки Knox, яка дозволяє визначати області "безпеки" та "персонального використання" на пристрої. З виходом Android 5.0 Google почав надавати регулярні оновлення систем безпеки через Google Play Services, що дозволяє оновлювати важливі компоненти безпеки без необхідності чекати на випуск оновлення всієї операційної системи.

Журнал зображень високої якості,

Multi RFID Card Reading, Здатність одночасного читання інформації з кількох RFID-карток (Radio-Frequency Identification). RFID - це технологія, що

використовує радіочастотне ідентифікаційне зв'язування для автоматичного визначення та взаємодії з об'єктами, які мають RFID-мітки або картки. Суть Multi RFID Card Reading в тому, що система може одночасно зчитувати дані з кількох RFID-карт, які перебувають у зоні зчитування.

Ергономіка та зручність користувача

Конфігурацій систем можуть бути виконані у декількох варіантах:

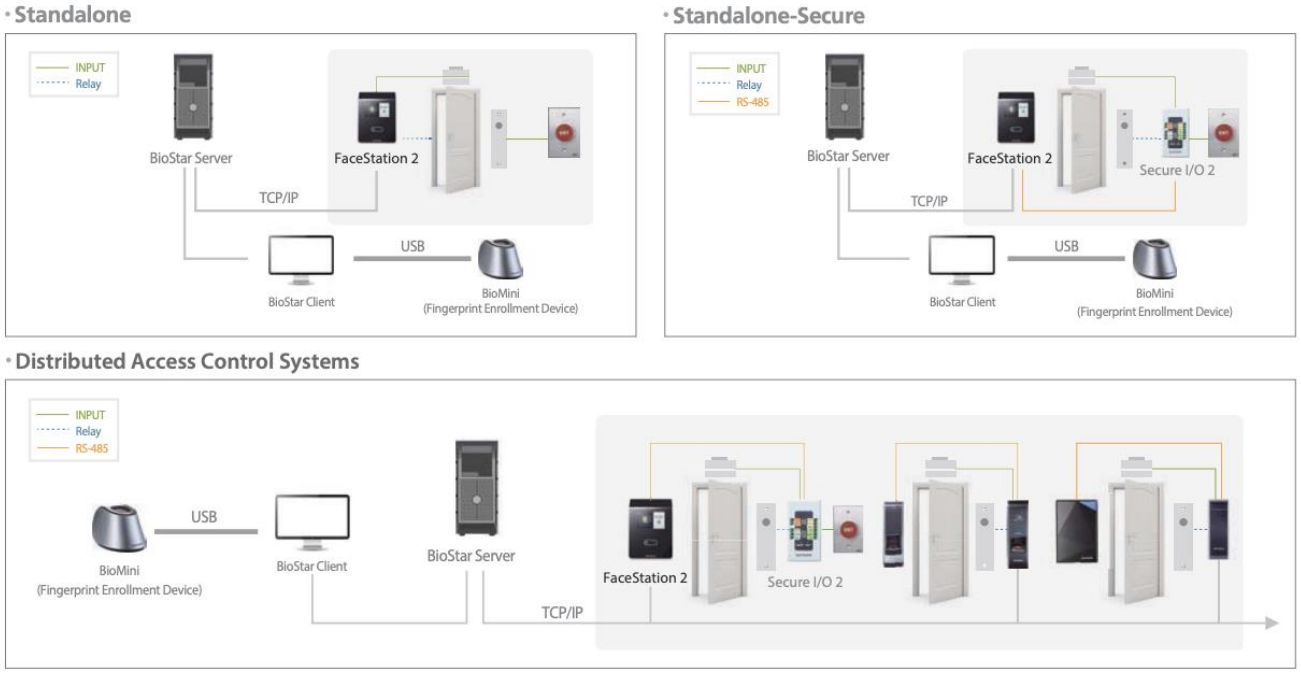

Рис.2.3 Конфігурації інтеграції систем

Незважаючи на велику різноманітність алгоритмів розпізнавання облич, можна виділити загальну структуру процесу. На першому етапі проводиться детектування та локалізація особи на зображенні. На етапі розпізнавання виробляється вирівнювання зображення особи (геометричне і яскравісне), обчислення ознак і безпосередньо розпізнавання – порівняння обчислених ознак із закладеними базу даних стандартами. Основною відмінністю всіх розглянутих алгоритмів це різне обчислення ознак та порівняння їх сукупностей між собою.

РОЗДІЛ 3.
РЕЗУЛЬТАТИ РОЗРОБКИ СИСТЕМИ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧА

3.1. Вибір та реалізація інструментарію розв'язання задачі аутентифікації користувача

Платформа FS2D використовує BioStart 2 system в ролі програмного забезпечення. Згідно із мінімальними вимогами по програмному забезпеченню із офіційно веб сайту компанії розробника існуючі рішення працюють із windows платформами. Тому в ході цієї роботи ми будемо використовувати програмне забезпечення адаптоване під windows машини.

BioStar 2 було розроблено для подолання обмежень розподіленої системи контролю доступу, яка, як стверджується, не є достатньо стабільною та потужною, щоб відповідати системним вимогам рівня підприємства. З точки зору централізованої системи контролю доступу, периферійні пристрої (зчитувач і контролер) часто називають обмеженим рішенням з точки зору загального охоплення системи, оскільки воно сильно залежить від характеристик і можливостей пристрою, які є порівняно нижчими, ніж централізована головна панель керування.

Є два способи використання BioStar API. Один називається Web API (через BioStar Cloud Server), а інший називається Local API. Компанія виробник рекомендує використовувати локальний API.

BioStar 2 Web Client & API.

BioStar 2 адаптував потужну веб-систему, яка дозволяє веб-браузерам бути клієнтами системи. Кінцевим користувачам не потрібно встановлювати спеціальну клієнтську програму, і вони можуть отримати доступ до локального сервера BioStar 2 через будь-який веб-браузер, який підтримує HTML5.

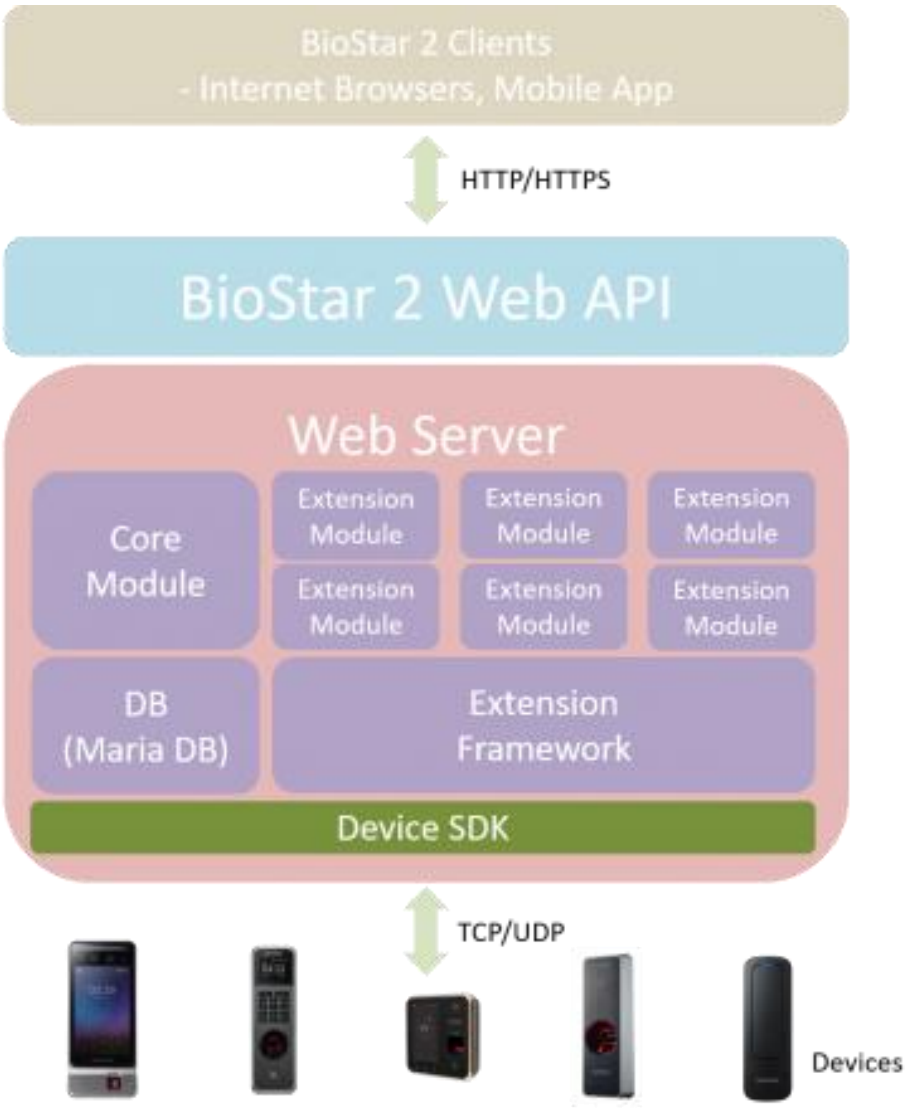

Рис. 3.1 Схема інтеграції Biostar2 Web API із веб сервером

Крім того, його веб-API, наданий у форматі REST/JSON, дозволяє додаткам або програмам сторонніх розробників легше та ефективніше здійснювати систематичну інтеграцію. Крім того, тепер, коли це API рівня сервера, немає потреби створювати власну логіку системи контролю доступу, реалізація якої зазвичай потребує багато часу за допомогою SDK пристрою, і можна більше зосередитися на її прикладних частинах.

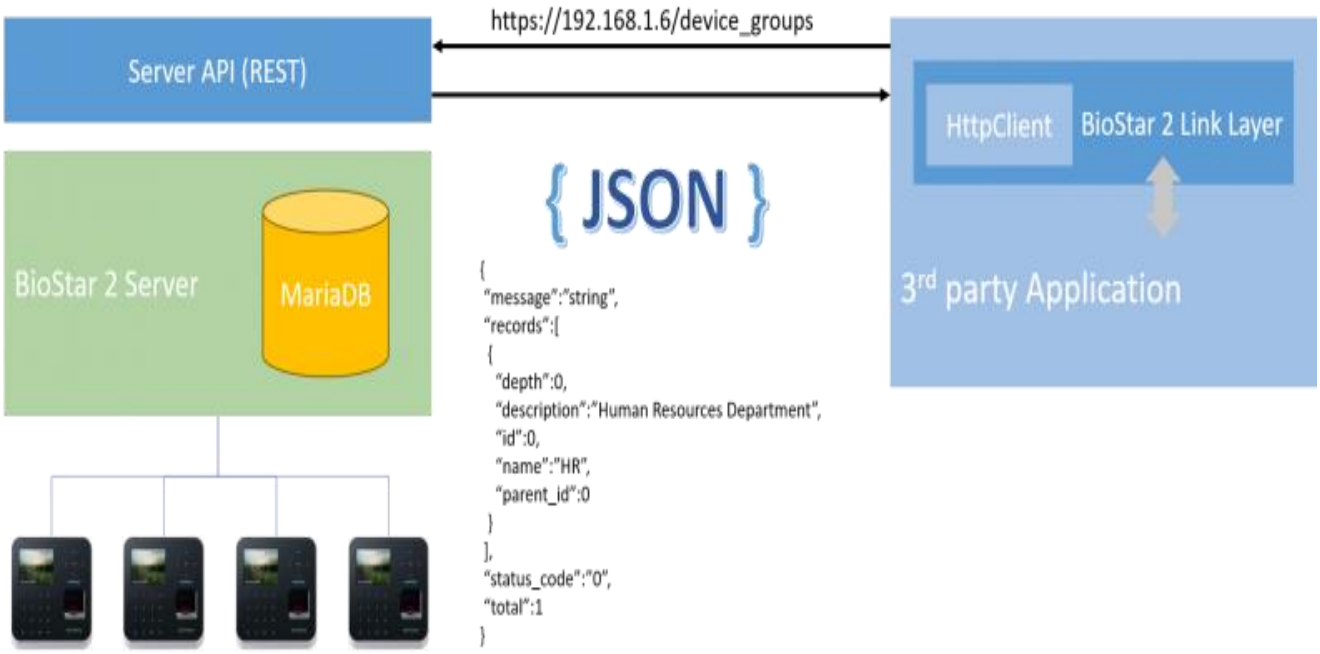

Рис. 3.2. Комунікація клієнта із сервером без сторонніх SDK з боку BioStart2

BioStar2 API це API на серверному рівні, це означає що більше не треба інтегрувати додаткові SDK. Як наслідок більш проста взаємодія і інтеграція із сторонніми застосунками на базі WEB API.

3.2. Результати розв'язання задачі аутентифікації користувача

У цій роботі ми розглянемо зразок програми, створений на базі C# або окремою програмою Windows. Оскільки BioStar API є RESTful API, ми можемо змоделювати повноцінну клієнт-серверну архітектуру.

Функції. Цей зразок програми є консольною програмою Visual C# і містить чотири основні функції: вхід, створення користувача, отримання групи доступу та отримання журналу.

По-перше, ми повинні увійти в систему, перш ніж використовувати будь-які інші функції. Якщо ми введемо «1» і натиснемо Enter, зразок програми ввійде на наш локальний сервер BioStar через сервер BioStar API.

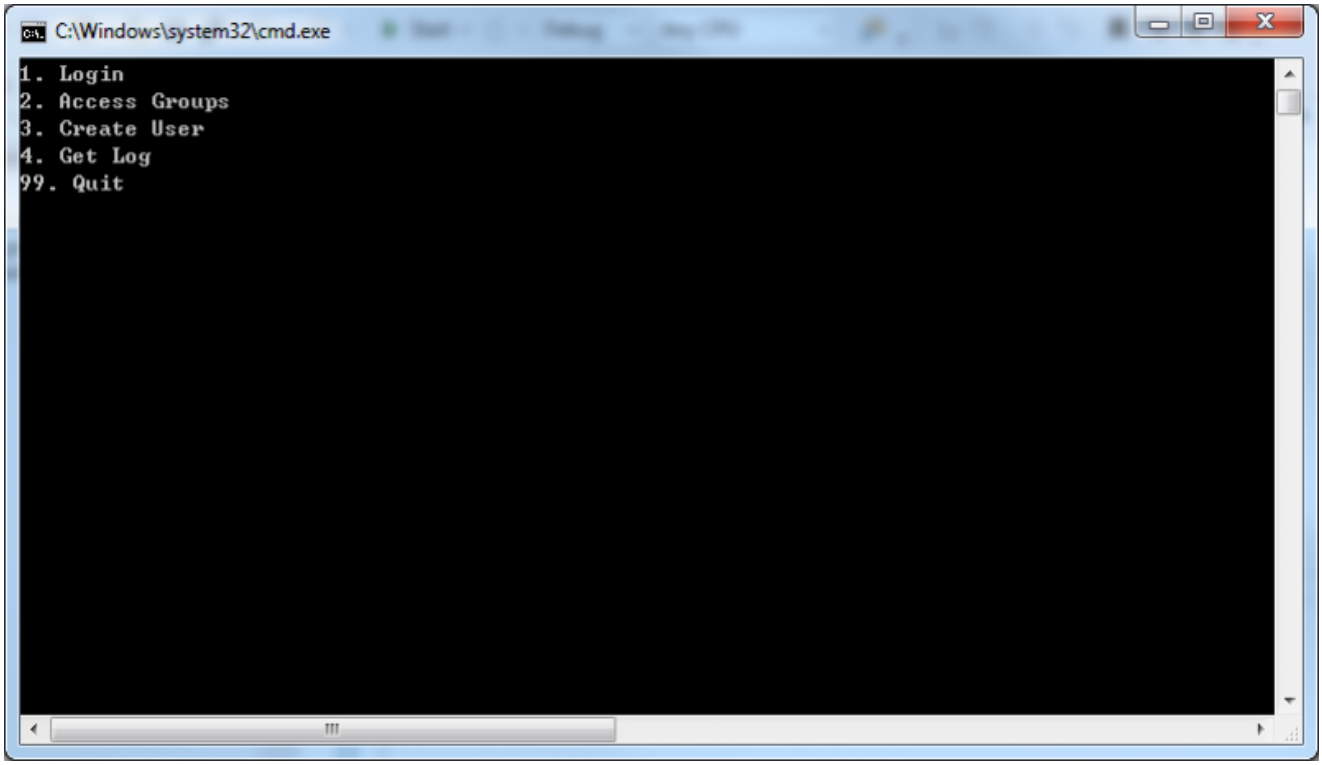

Рис.3.3 Старт програми

Після успішного входу ми отримуємо інформацію про користувача, якого ми використовували для входу. Дані користувача містяться у форматі JSON і містять дуже докладні дані, включаючи шаблони відбитків пальців, як видно на рисунку 3.4. Тепер, коли ми ввійшли в систему , ми можемо використовувати інші функції. Щоб отримати групи доступу, введемо «2» і натиснемо Enter.

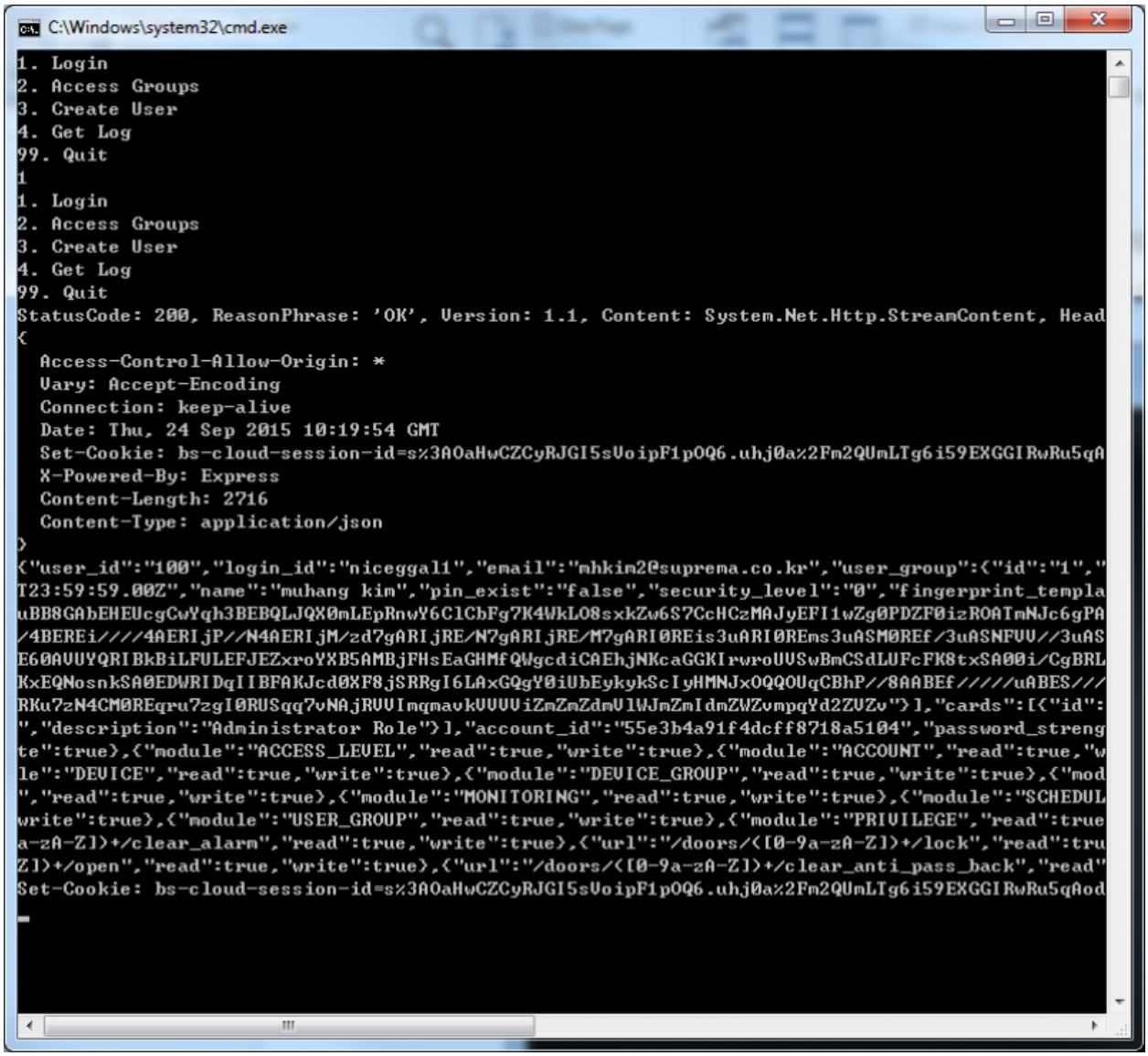

Рис. 3.4. Програма після введення логіну

Рис.3.5. Отримання групи доступу

Як видно на знімку екрана, на сервері BioStar 2 існує лише одна група доступу, а назва групи доступу — «Перша група доступу», і якщо ми подивимося на властивість «user_summary», то побачимо, що в ній є два користувачі . Тепер введемо «3» і натиснемо Enter, щоб створити нового користувача. Нам буде запропоновано ввести ідентифікатор користувача. Я ввів «98» як ідентифікатор користувача та отримав повідомлення про успіх із сервера.

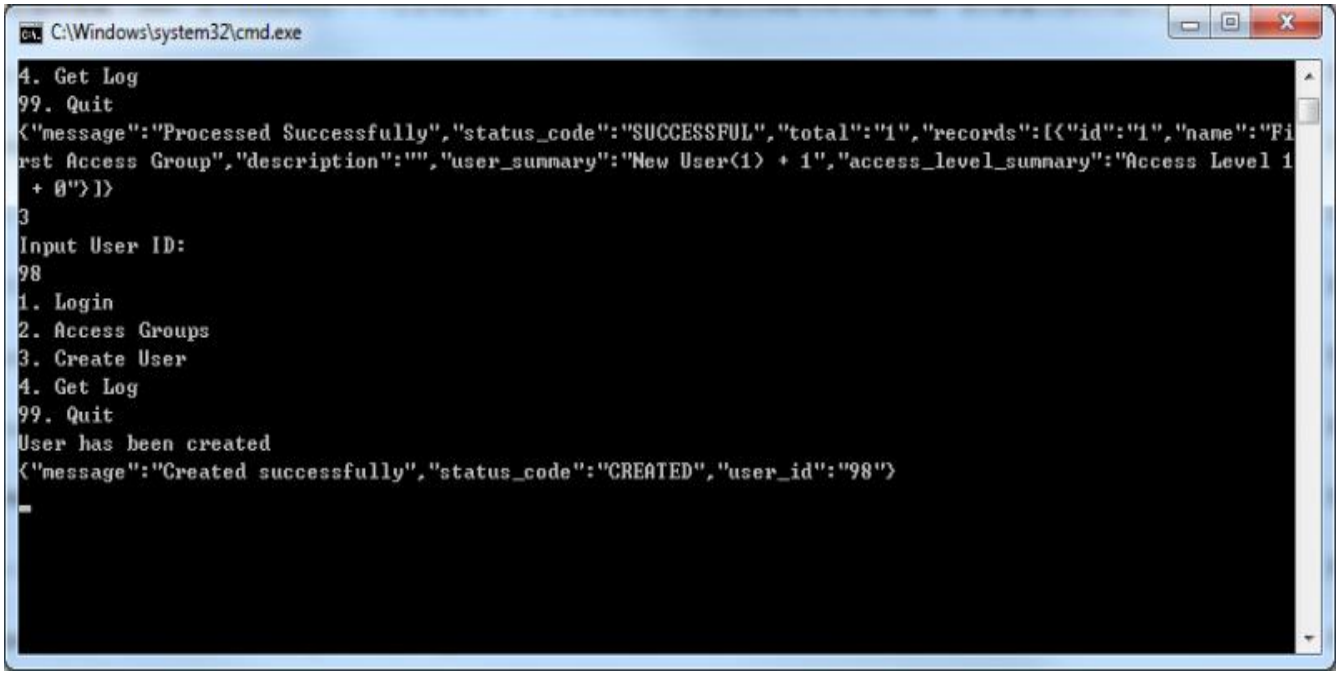

Рис. 3.6. Створення нового користувача

Тепер, давайте отримаємо журнал подій із сервера. Введемо «4» і натиснемо Enter, і ми отримаємо дані журналу з сервера, як показано на знімку екрана нижче (рис.3.7):

Рис.3.7 Отримання списку логів

3.3. Аналіз коду задачі аутентифікації користувача

Найважливішою частиною цього прикладу програми є вхід. Давайте розглянемо функцію нижче:

```
24          static async void LoginTask()
25          {
26              string resourceAddress = "http://127.0.0.1:8795/v2/login";
27
28              HttpClient httpClient = new HttpClient();
29
30              JavaScriptSerializer serializer = new JavaScriptSerializer();
31
32              Dictionary<string, string> dicLoginUser = new Dictionary<string, string>();
33              dicLoginUser.Add("name", "ts22");
34              dicLoginUser.Add("password", "rlaangkd!1");
35              dicLoginUser.Add("user_id", "niceggal1");
36
37              string jsonLoginUser = serializer.Serialize(dicLoginUser);
38
39              StringContent sc = new StringContent(jsonLoginUser, Encoding.UTF8, "application/json");
40              HttpResponseMessage httpResponse = await httpClient.PostAsync(resourceAddress, sc);
41
42
43              if(httpResponse.IsSuccessStatusCode == true)
44              {
45                  Console.WriteLine(httpResponse.ToString());
46                  string httpResponseBody = await httpResponse.Content.ReadAsStringAsync();
47                  Console.WriteLine(httpResponseBody);
48
49
50                  MemoryStream responseMemoryStream = new MemoryStream();
51                  StreamWriter sw = new StreamWriter(responseMemoryStream);
52                  sw.Write(httpResponse.ToString());
53                  sw.Flush();
54
55                  bool isSessionIDContained = httpResponse.Headers.Contains("Set-Cookie");
56                  if (isSessionIDContained == true)
57                  {
58                      IEnumerable<string> sessionEnum = httpResponse.Headers.GetValues("Set-Cookie");
59                      foreach(string element in sessionEnum)
60                      {
61                          Console.WriteLine("Set-Cookie: " + element);
62                          string[] strCookieArr = element.Split(new string[] { "bs-cloud-session-id=" }, StringSplitOptions.None);
63                          string[] strCookieArr2 = strCookieArr[1].Split(new string[] { ";" }, StringSplitOptions.None);
64                          sessionID = strCookieArr2[0];
65                      }
66                  }
67                  else
68                  {
69                      Console.WriteLine("Session ID not found");
70                  }
71              }
72              else
73              {
74                  Console.WriteLine("Failed to log in");
75                  Console.WriteLine(httpResponse.ToString());
76              }
77          }
```

Рис.3.8 Функція логування

Рядок 26: це URL-адреса, яку ми використовуємо для входу на наш локальний сервер BioStar. У випадку локального API префіксом є «http://127.0.0.1:8795/v2/». «login» після префікса вказує на поведінку або дію, яку ми хочемо виконати.

Рядок 27: у цьому прикладі коду ми використовуємо клас HttpClient для надсилання запиту та отримання відповіді від BioStar Cloud.

Рядок 30: Клас JavaScriptSerializer потрібен для перетворення даних у формат JSON або аналізу даних у форматі JSON у будь-який потрібний формат.

Рядки 32-35: ці рядки створюють словник, який складається з ключа рядка та значення рядка. Необхідні три параметри: ім’я субдомену, ідентифікатор і пароль. Поле «ім’я» призначене для імені субдомену, тому встановіть у цьому полі назву свого субдомену.

Рядок 37: цей рядок перетворює словник на рядок у форматі JSON.

Рядок 39: цей рядок встановлює рядок у форматі JSON як вміст запиту HTTP, UTF8 як параметр кодування та JSON як тип медіа.

Рядок 40: ми використовуємо метод HTTP POST, щоб зробити HTTP-запит для входу.

Рядок 45-53: ми виводимо вміст HTTP-відповіді з метою налагодження.

Рядок 55-65: якщо інформація для входу дійсна, ми отримуємо інформацію про сеанс із сервера. Кожного разу, коли ми робимо виклик API, ми повинні розміщувати цю інформацію про сеанс у заголовку HTTP. Отже, рядки з 55 по 65 витягують інформацію про сеанс із заголовка відповіді HTTP для подальшого використання.

```
203         static async void AccessGroupsTask()
204         {
205             if (sessionID == null)
206             {
207                 Console.WriteLine("You must log in first!");
208                 return;
209             }
210 
211             CookieContainer cookieContainer = new CookieContainer();
212 
213             HttpClientHandler handler = new HttpClientHandler();
214             handler.CookieContainer = cookieContainer;
215 
216             HttpClient client = new HttpClient(handler);
217 
218 
219             cookieContainer.Add(new Uri(    "http://127.0.0.1:8795"     ), new Cookie("bs-cloud-session-id", sessionID));
220             HttpResponseMessage httpResponse = await client.GetAsync(     "http://127.0.0.1:8795/v2/access_groups"     );
221 
222             if (httpResponse.IsSuccessStatusCode == true)
223             {
224                 string httpResponseBody = await httpResponse.Content.ReadAsStringAsync();
225                 Console.WriteLine(httpResponseBody);
226             }
227             else
228             {
229                 Console.WriteLine("Retrieving Access Groups Failed");
230                 Console.WriteLine(httpResponse.ToString());
231             }
232         }
```

Рис.3.9 Отримання групи доступу

Рядок 205-209: спочатку нам потрібно перевірити, чи успішно ввійшли в систему та чи збережено ідентифікатор сеансу.

Рядок 211: ми використовуємо клас CookieContainer для надсилання інформації про ідентифікатор сеансу на сервер BioStar.

Рядок 219: розміщуючи ідентифікатор сеансу в файлі cookie, ми повинні вказати URI.

Рядок 220: Отримання груп доступу має здійснюватися за допомогою методу HTTP GET.

```
125     static async void GetLogTask()
126     {
127         if(sessionID == null)
128         {
129             Console.WriteLine("You must log in first!");
130             return;
131         }
132
133         CookieContainer cookieContainer = new CookieContainer();
134
135         HttpClientHandler handler = new HttpClientHandler();
136         handler.CookieContainer = cookieContainer;
137
138         HttpClient httpClient = new HttpClient(handler);
139
140         HttpClient client = new HttpClient(handler);
141         cookieContainer.Add(new Uri( "http://127.0.0.1:8795"      ), new Cookie("bs-cloud-session-id", sessionID));
142
143         string resourceAddress = "http://127.0.0.1/v2/monitoring/event_log/search";
144
145         string startTime = "1970-01-01T00:00:00Z";
146         string endTime = DateTime.UtcNow.ToString("yyyy-MM-ddTHH:mm:ssZ");
147
148         DateTime dtLatestLogTime = new DateTime(1970, 1, 1);
149
150         JavaScriptSerializer serializer = new JavaScriptSerializer();
151
152         for (int logCallIndex = 0; logCallIndex < 1000; logCallIndex++)
153         {
154             endTime = DateTime.UtcNow.ToString("yyyy-MM-ddTHH:mm:ssZ");
155
156             string payload = "{ \"datetime\": [\"" + startTime + "\", \"" + endTime + "\"] }";
157
158
159             StringContent sc = new StringContent(payload, Encoding.UTF8, "application/json");
160             HttpResponseMessage httpResponse = await httpClient.PostAsync(resourceAddress, sc);
```

Рис.3.10. Отримання івентів (подій)

```
162             if (httpResponse.IsSuccessStatusCode == true)
163             {
164                 Console.WriteLine("Succeeded to retrieve log from " + startTime + " to " + endTime);
165                 string httpResponseBody = await httpResponse.Content.ReadAsStringAsync();
166                 Console.WriteLine(httpResponseBody);
167 
168                 endTime = startTime;
169 
170                 Dictionary<string, dynamic> logValues = serializer.Deserialize<Dictionary<string, dynamic>>(httpResponseBody);
171                 foreach(KeyValuePair<string, dynamic> logElement in logValues)
172                 {
173                     if (logElement.Key == "records")
174                     {
175                         foreach (Dictionary<string, dynamic> recordElement in logElement.Value)
176                         {
177                             if(recordElement.ContainsKey("datetime"))
178                             {
179                                 Console.WriteLine(recordElement["datetime"]);
180                                 DateTime dtLogTime = DateTime.Parse(recordElement["datetime"]);
181 
182                                 if(dtLogTime > dtLatestLogTime)
183                                 {
184                                     dtLatestLogTime = dtLogTime;
185                                     startTime = dtLatestLogTime.ToUniversalTime().AddSeconds(1).ToString("yyyy-MM-ddTHH:mm:ssZ");
186                                 }
187                             }
188                         }
189                     }
190                 }
191 
192                 System.Threading.Thread.Sleep(1000);
193             }
194             else
195             {
196                 Console.WriteLine("Log Retrieval Failed from " + startTime + " to " + endTime);
197                 Console.WriteLine(httpResponse.ToString());
198                 break;
199             }
```

Рис.3.10. Отримання івентів (подій) (продовження).

Рядок 152: Ми використовуємо цикл For для повторного отримання подій із сервера через певний інтервал.

Рядки 154-156: під час отримання подій із сервера ми повинні вказати час початку та час завершення. Цього разу, замість використання класу Dictionary, ми створюємо рядок у форматі JSON вручну для демонстраційних цілей.

Рядки 170-188: ми використовуємо клас Dictionary із рядковим ключем і динамічним значенням для аналізу даних у форматі JSON у структуру даних словника. Оскільки події мають форму масиву, ми повинні використовувати динамічний тип значення в словнику.

```
79          static async void CreateUserTask()
80          {
81              if (sessionID == null)
82              {
83                  Console.WriteLine("You must log in first!");
84                  return;
85              }
86
87              CookieContainer cookieContainer = new CookieContainer();
88
89              HttpClientHandler handler = new HttpClientHandler();
90              handler.CookieContainer = cookieContainer;
91
92              HttpClient httpClient = new HttpClient(handler);
93
94              HttpClient client = new HttpClient(handler);
95              cookieContainer.Add(new Uri(    "http://127.0.0.1:8795"     ), new Cookie("bs-cloud-session-id", sessionID));
96
97              string resourceAddress = "http://127.0.0.1:8795/v2/users";
98
99              Console.WriteLine("Input User ID: ");
100             string userInputID = Console.ReadLine();
101
102             JavaScriptSerializer serializer = new JavaScriptSerializer();
103
104             Dictionary<string, string> dicNewUser = new Dictionary<string, string>();
105             dicNewUser.Add("user_id", userInputID);
106
107             string payload = serializer.Serialize(dicNewUser);
108
109             StringContent sc = new StringContent(payload, Encoding.UTF8, "application/json");
110             HttpResponseMessage httpResponse = await httpClient.PostAsync(resourceAddress, sc);
```

Рис.3.11. Створення користувача

Рядок 99-100: ми отримуємо введення користувача для ідентифікатора нового користувача.

Рядки 104-105: Єдиною обов’язковою властивістю, яку ми маємо надати під час створення нового користувача, є ідентифікатор користувача.

На цьому прикладі ми розглянули як можна використовувати BioStart API. Основний ухил на пояснення в даному прикладі припадає на використання локального API.

РОЗДІЛ 4.
ОХОРОНА ПРАЦІ ТА БЕЗПЕКА У НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1. Аналіз небезпечних та шкідливих виробничих чинників під час роботи з комп’ютерною технікою

Однією із характерних особливостей сучасного розвитку суспільства є зростання сфер діяльності людини, в яких використовуються інформаційні технології. Широке розповсюдження отримали персональні комп'ютери. Однак їх використання загострило проблеми збереження власного та суспільного здоров'я, вимагає удосконалення існуючих та розробки нових підходів до організації робочих місць, проведення профілактичних заходів для запобігання розвитку негативних наслідків впливу ПК на здоров'я користувачів.

Заходи з охорони праці користувачів ПК необхідно розглядати в трьох основних аспектах:

1. соціальному;
2. психологічному;
3. та медичному.

У соціальному плані розв'язання цих проблем пов'язане з оптимізацією умов життя, праці, відпочинку, харчування, побуту, розвитком культури, транспорту.

Психологічний аспект. Значне місце у профілактиці розладів здоров'я належить психології праці. Тому заходи, пов'язані з формуванням раціональних виробничих колективів, у яких відсутня психологічна несумісність, сприяють зменшенню нервово-психічного перенапруження, підвищенню працездатності та ефективності праці. Особливої значущості у користувачів відеодисплейних терміналів (ВДТ) набуває психоемоційний стрес, який більшою або меншою мірою проявляється у кожного з них.

Медичний аспект. Значна роль у профілактиці захворювань користувачів ПК відводиться медицині. Існує перелік профілактичних заходів для користувачів ПК, що включає як складові первинної профілактики здоров'я (професійний відбір), так

і вторинної, яка направлена на зниження ймовірності розвитку перевтоми та перенапруження. Ці комплексні заходи спрямовані на відновлення функціонального стану зорового та опорно-рухового апарату.

Гігієнічні вимоги до організації та обладнання робочих місць з ПК Обладнання і організація робочого місця з ВДТ мають забезпечувати відповідність конструкції всіх елементів робочого місця та їх взаємного розташування ергономічним вимогам з урахуванням характеру і особливостей трудової діяльності. Конструкція робочого місця користувача ВДТ має забезпечити підтримання оптимальної робочої пози. Робочі місця з ВДТ слід так розташовувати відносно світлових прорізів, щоб природне світло падало збоку, переважно зліва. При розміщенні робочих столів з ВДТ слід дотримуватись таких відстаней: між бічними поверхнями ВДТ - 1,2 м; від тильної поверхні одного ВДТ до екрана іншого - 2,5 м. Екран ВДТ має розташовуватися на оптимальній відстані від очей користувача, що становить 600...700 мм, але не ближче ніж за 600 мм з урахуванням розміру літерно-цифрових знаків і символів. Розташування екрана ВДТ має забезпечувати зручність зорового спостереження у вертикальній площині під кутом +30° до нормальної лінії погляду працюючого. Клавіатуру слід розташовувати на поверхні столу на відстані 100...300 мм від краю, звернутого до працюючого. У конструкції клавіатури має передбачатися опорний пристрій (виготовлений із матеріалу з високим коефіцієнтом тертя, що перешкоджає мимовільному її зсуву), який дає змогу змінювати кут нахилу поверхні клавіатури у межах 5...15°.

Вимоги до режимів праці і відпочинку при роботі з ПК При організації праці, пов'язаної з використанням ЕОМ і ПЕОМ, для збереження здоров'я працюючих, запобігання професійним захворюванням і підтримки працездатності передбачаються внутрішньозмінні регламентовані перерви для відпочинку. Внутрішньозмінні режими праці і відпочинку містять додаткові нетривалі перерви в періоди, що передують появі об'єктивних і суб'єктивних ознак стомлення і зниження працездатності.

Впродовж робочої зміни мають передбачатися:

- перерви для відпочинку і вживання їжі (обідні перерви);

- перерви для відпочинку і особистих потреб (згідно з трудовими нормами);

- додаткові перерви, що вводяться для окремих професій з урахуванням особливостей трудової діяльності.

За характером трудової діяльності розрізняють три професійні групи, згідно з діючим класифікатором професій (ДК-003-95 і Зміна N1 до ДК-003- 95):1):

1. розробники програм (інженери-програмісти) виконують роботу з ЕОМ та документацією при необхідності інтенсивного обміну інформацією з ЕОМ і високою частотою прийняття рішень. Робота характеризується інтенсивною розумовою творчою працею з підвищеним напруженням зору, концентрацією уваги на фоні нервово-емоційного напруження, вимушеною робочою позою, загальною гіподинамією, періодичним навантаженням на кисті верхніх кінцівок. Робота виконується в режимі діалогу з ЕОМ у вільному темпі з періодичним пошуком помилок в умовах дефіциту часу;

2. оператори електронно-обчислювальних машин виконують роботу, пов'язану з обліком інформації, одержаної з ВДТ за попереднім запитом, або тієї, що надходить з нього, супроводжується перервами різної тривалості, пов'язана з виконанням іншої роботи і характеризується напруженням зору, невеликими фізичними зусиллями, нервовим напруженням середнього ступеня та виконується у вільному темпі;

3. оператор комп'ютерного набору виконує одноманітні за характером роботи з документацією та клавіатурою і нечастими нетривалими переключеннями погляду на екран дисплея, з введенням даних з високою швидкістю. Робота характеризується як фізична праця з підвищеним навантаженням на кисті верхніх кінцівок на фоні загальної гіподинамії з напруженням зору (фіксація зору переважно на документи), нервово-емоційним напруженням.

Правилами встановлюються такі внутрішньо змінні режими праці та відпочинку при роботі з ЕОМ при 8-годинній денній робочій зміні в залежності від характеру праці:

- для розробників програм із застосуванням ЕОМ слід призначати регламентовану перерву для відпочинку тривалістю 15 хвилин через кожну годину роботи за ВДТ;

- для операторів із застосуванням ЕОМ слід призначати регламентовані перерви для відпочинку тривалістю 15 хвилин через кожні дві години;

- для операторів комп'ютерного набору слід призначати регламентовані перерви для відпочинку тривалістю 10 хвилин після кожної години роботи за ВДТ.

У всіх випадках, коли виробничі обставини не дозволяють застосувати регламентовані перерви, тривалість безперервної роботи з ВДТ не повинна перевищувати 4 години. При 12-годинній робочій зміні регламентовані перерви повинні встановлюватися в перші 8 годин роботи аналогічно перервам при 8-годинній робочій зміні, а протягом останніх 4-х годин роботи, незалежно від характеру трудової діяльності, через кожну годину тривалістю 15 хвилин. Для зниження нервово-емоційного напруження, стомлення зорового аналізатора, поліпшення мозкового кровообігу, подолання несприятливих наслідків гіподинамії, запобігання втомі доцільно деякі перерви використовувати для виконання комплексу вправ, які наведені у Державних санітарних правилах і нормах роботи з ПК електронно-обчислювальних машин ДСанПІН 3.3.2.007-98.

Психофізіологічне розвантаження. При проведенні сеансів психофізіологічного розвантаження рекомендується використовувати деякі елементи методу аутогенного тренування, який ґрунтується на свідомому застосуванні комплексу взаємопов'язаних прийомів психічної саморегуляції й виконанні нескладних фізичних вправ із словесним самонавіюванням. Головна увага при цьому приділяється набуванню й закріпленню навичок м'язового розслаблення (релаксації). У рекомендованому сеансі, який має проводитися в кімнаті психофізіологічного розвантаження з відповідним інтер'єром та кольоровим оформленням, виділяються три періоди, що відповідають фазам відновлювального процесу.

Перший період - абстрагування працівників від виробничої обстановки - відповідає фазі залишкового збудження.

Другий період - заспокоєння - відповідає фазі відновлювального гальмування.

Третій період - активізація - відповідає фазі підвищеної збудженості.

Сеанси психологічного розвантаження можуть проводитись за єдиною програмою через індивідуальні навушники і складатись із двох періодів по 5 хвилин кожний:

1) повне розслаблення;

2) активізація працездатності.

У разі потреби, на фоні музичних програм можуть вимовлятися окремі фрази навіювання відпочинку, гарного самопочуття і, на заключному етапі, бадьорості. Після сеансів психофізіологічного розвантаження у працівників зменшується відчуття втоми, з'являються бадьорість, гарний настрій. Загальний стан відчутно поліпшується.

4.2. Моделювання процесу виникнення травм та аварій

Моделювання процесу виникнення травм та аварій під час роботи з комп’ютерною технікою може бути корисним для покращення безпеки та запобігання можливим негативним подіям. Нижче наведено загальний огляд етапів такого моделювання:

1. Визначення сценаріїв травм та аварій:
    - Вивчення історії попередніх інцидентів і аварій на робочих місцях.
    - Аналіз та ідентифікація потенційних сценаріїв травм та аварій.
2. Збір даних:
    - Збір статистичних даних про попередні інциденти.
    - Запис виявлених ризикових факторів та умов, що сприяють травмам і аваріям.
3. Визначення факторів ризику:
    - Аналіз впливу різних чинників на виникнення травм та аварій (наприклад, обладнання, люди, середовище).

- Визначення факторів, які можуть збільшити ризик інцидентів.

4. Розробка математичних моделей:
    - Створення математичних моделей, що відображають взаємозв'язки між різними чинниками та ймовірність виникнення травм та аварій.
    - Використання статистичних методів для аналізу даних та розрахунку ризиків.
5. Валідація моделей:
    - Перевірка правильності моделей на основі реальних інцидентів.
    - Коригування та уточнення моделей на основі нової інформації.
6. Визначення заходів безпеки:
    - Розробка та впровадження заходів безпеки на основі результатів моделювання.
    - Організація тренінгів та навчань з безпеки для персоналу.
7. Моніторинг та аналіз:
    - Систематичний моніторинг безпекових показників.
    - Постійний аналіз даних та моделей для вчасного виявлення нових ризикових факторів.

Моделювання такого роду допомагає вдосконалити безпекові стандарти та процедури, зменшити ймовірність травм та аварій та підвищити загальний рівень безпеки на робочому місці.

4.3. Розробка заходів щодо безпеки у надзвичайних ситуаціях

Забезпечення безпеки населення у надзвичайних ситуаціях включає в себе комплекс заходів та дій для запобігання, мінімізації та виправлення наслідків небезпеки чи кризової ситуації. Основні аспекти забезпечення безпеки під час загроз та надзвичайних ситуацій включають:

Попередження та інформування:

- Системи оповіщення: Розробка та впровадження систем оповіщення через різні канали (сирени, текстові повідомлення, соціальні мережі тощо) для швидкого повідомлення населення про небезпеку.
- Інформаційні кампанії: Проведення освітніх кампаній, які навчають населення діяти в надзвичайних ситуаціях та розпізнавати можливі загрози.

Евакуація та укриття:

- Плани евакуації: Розробка та публікація планів евакуації для населення, шкіл, медичних установ та інших важливих об'єктів.
- Створення укриттів: Розміщення та обладнання спеціальних укриттів для захисту населення від небезпеки.

Системи моніторингу та раннього попередження:

- Метеорологічний моніторинг: Постійне спостереження за погодними умовами для вчасного виявлення можливих стихійних лих та інших природних небезпек.
- Системи виявлення загроз: Використання сучасних технологій для виявлення потенційних загроз, таких як техногенні аварії, терористичні атаки тощо.

Підготовка та тренування:

- Навчання населення: Проведення регулярних навчань та тренувань для населення щодо дій в надзвичайних ситуаціях.
- Тренування служб безпеки: Підготовка та тренування відповідальних служб, включаючи рятувальників, медичний персонал та поліцію.

Комунікація та координація:

- Центри управління кризовими ситуаціями: Створення центрів управління, де представники різних служб можуть координувати свої дії та обмінюватися інформацією.
- Системи комунікації: Забезпечення ефективних систем зв'язку для оперативного обміну інформацією між відповідальними службами та населенням.

Системи медичної допомоги: Розвиток та удосконалення систем медичної допомоги для надання ефективної допомоги потерпілим в надзвичайних ситуаціях.

Забезпечення безпеки населення у надзвичайних ситуаціях вимагає інтегрованого підходу, співпраці різних служб та постійного оновлення планів та технічних рішень для ефективного вирішення різноманітних ситуацій загроз та надзвичайних подій.

РОЗДІЛ 5.
ВИЗНАЧЕННЯ ЕФЕКТИВНОСТІ ВІД ВИКОРИСТАННЯ СИСТЕМИ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧА

Стратегія розвитку існуючого продукту (проектного рішення) з супутніми послугами означає пропонування на ринку модифікованого програмного забезпечення із додатковими послугами (встановлення, супроводження, коригування, адаптування до специфіки конкретного підприємства тощо).

Бюджетування є комплексно обґрунтованою системою розрахунку витрат, пов'язаних з виготовленням та реалізацією продукту, яка дає можливість здійснити аналіз витрат та розробити заходи щодо підвищення рентабельності виробництва. На даному етапі необхідно визначити собівартість продукту, який розробляється та економічно обґрунтувати доцільність. Бюджет витрат на матеріали та комплектуючі наведено в таблиці 5.1.

Таблиця 5.1

Бюджет витрат на матеріали та комплектуючі виробів

Назва матеріалів та комплектуючих	Марка, тип, модель	Фактична кількість, шт.	Ціна за одиницю, грн.	Разом, грн.
Оренда сервера	Heroku	1	6500,0 грн/міс	6500,0
Програмне забезпечення	Windows 10	1	5200,0 грн	5200,0
Система контролю версій	GitHub	1	550,0 грн/міс	550,0
Разом:		1	12250,0	12250,0

Для розробки проекту також потрібні людські ресурси. Проте, щоб реалізувати цей проект не потрібно наймати велику команду. В таблиці 5.2 наведено бюджет витрат на оплату праці.

Таблиця 5.2

Бюджет витрат на оплату праці

Посада, спеціальність	Кількість працівників, осіб	Час роботи, дні	Денна заробітна плата працівників, грн.	Сума витрат на оплату праці, грн.
Основна заробітна плата				
Програміст	2	21	2200	92 400
Тестер	2	7	2100	29 400
Разом				121 800

У таблиці 5.3 представлено бюджет загальновиробничих витрат.

Таблиця 5.3

Бюджет загальновиробничих витрат

Статті витрат	Сума, грн.
Змінні загальновиробничі витрати, у т.ч.:	
- заробітна плата допоміжного персоналу;	
- витрати на МШП;	670
- витрати на електроенергію та технологічні цілі;	5000
- витрати на ремонт;	
- інші змінні витрати;	
Разом змінних витрат:	15450
Постійні загальновиробничі витрати, у т.ч.:	
- заробітна плата допоміжного персоналу;	
- комунальні послуги;	2000
- витрати на оренду;	4580
- витрати на ремонт;	700
- інші постійні витрати;	
Разом постійних витрат:	7280
Разом загальновиробничих витрат:	22730

До адміністративних витрат відносяться загальногосподарські втрати, спрямовані на обслуговування та управління підприємством. Витрати на збут включають витрати, пов'язані з реалізацією (збутом) продукції (товарів, робіт, послуг). Бюджет адміністративних витрат та витрат на збут наведено в таблиці 5.4. Витрати на виробництво продукції у вартісному виразі формують її виробничу собівартість. Цей показник є одним з найважливіших економічних показників господарської діяльності підприємства, у якому дістають відображення зростання продуктивності праці, економія ресурсів.

Таблиця 5.4

Бюджет адміністративних витрат та витрат на збут

Статті витрат	Сума, грн.
Адміністративні витрати, у т.ч.:	
- заробітна плата адміністративного персоналу;	7000
- витрати на МШП;	600
- витрати на відрядження;	
- витрати на ремонт;	
- витрати на паливно-мастильні матеріали;	
- витрати на сплату податків і зборів;	1540
- знос адміністративного обладнання;	700
Разом адміністративних витрат:	9840
Витрати на збут, у т.ч.:	
- заробітна плата менеджерів зі збуту;	16000
- витрати на гарантійний ремонт;	2300
- витрати на відрядження;	
- витрати на гарантійне обслуговування;	6100
- витрати на налагодження і експлуатацію;	3400
- витрати на паливо-мастильні матеріали;	5000
- витрати на рекламу;	7500
Разом витрат на збут:	40300

Для того, щоб можна було зручно переглянути та проаналізувати усі статті витрат, варто скласти таблицю зведеного кошторису витрат на розробку. Зведені витрати представлено в таблиці 5.5.

Таблиця 5.5

Зведений кошторис витрат на розробку проектного рішення

Статті витрат	Сума, грн.
Сировина і матеріали	10550
Купівельні напівфабрикати та комплектуючі вироби	
Зворотні відходи (вираховуються)	
Паливо та електроенергія на технологічні цілі	
Основна заробітна плата	128 100
Додаткова заробітна плата	
Відрахування на соціальне страхування	28182
Витрати на утримання й експлуатацію устаткування	
Загальновиробничі витрати, у т.ч.:	
- змінні;	15450
- постійні;	7280
Разом виробничих витрат:	22730
Адміністративні витрати	9840
Витрати на збут	40300
Інші операційні витрати	
Разом виробничих і операційних витрат:	72870

Для визначення фінансових результатів, необхідно розрахувати вартість (ціну) продукту (проектного рішення), який розробляється. Ціна визначається на основі суми виробничих і операційних витрат з врахуванням рентабельності виробництва 76%.

$$Ц = СБ * Р$$

де Ц – ціна одинці продукту, грн. СБ – собівартість продукту, грн. Р – рентабельність виробництва, %

Ц =72870 *0,76 = 55 381,20грн

У таблиці 5.6 наведено бюджет фінансових результатів.

Таблиця 5.6

Бюджет фінансових результатів

Показники	Сума, грн.
Дохід від реалізації продукції (обсяг 8 шт)	443049,60
Податок на додану вартість	88609,92
Чистий дохід від реалізації продукції	354439,68
Собівартість реалізованої продукції	72870,00
Валовий прибуток	281569,68
Операційні витрати:	
- адміністративні витрати:	9840,00
- витрати на збут;	40300,00
- інші операційні витрати;	
Фінансовий результат від операційної діяльності	231429,68
Податок на прибуток	41657,34
Чистий прибуток (збиток)	189772,34

За результатами проведених досліджень та розрахунків проектне рішення щодо розробки системи є економічно доцільним.

Проведено аналіз витрат, пов’язаних з реалізацією проекту і з’ясовано, що за рівня рентабельності 76% ціна на розроблюване ПЗ становитиме 55 381,20грн. Величина чистого прибутку 189772,34 грн свідчить про доцільність розробки такого продукту.

ВИСНОВКИ І ПРОПОЗИЦІЇ

Проведений аналіз стану аутентифікації користувача, а також усвідомлення важливості цього процесу, оскільки він дозволяє організаціям захищати свої мережі, вказують на доцільність розроблення системи аутентифікації користувача. Відповідно до цього, у кваліфікаційній роботі пропонується розробка системи аутентифікації користувача з використанням платформи FS2-D.

Нами виконано аналіз стану аутентифікації користувача. Встановлено, що організації використовують автентифікацію для контролю доступу користувачів до корпоративних ресурсів, комп'ютерів, серверів, додатків та мереж. Для великих організацій використовується система єдиного входу (SSO), яка надає доступ до кількох систем за одним обліковим записом. Під час автентифікації, введені користувачем облікові дані перевіряються шляхом порівняння з інформацією у файлі бази даних з авторизованими користувачами або на локальній операційній системі, або через сервер аутентифікації. Якщо дані збігаються, і автентифікований суб'єкт має відповідні права на використання ресурсу, процес завершується, і користувач отримує доступ. Протоколи додатків у Інтернеті, такі як HTTP і HTTPS, не зберігають стану, що означає, що кінцеві користувачі перевіряються при кожному доступі до ресурсу через HTTPS. Щоб полегшити цей процес для кінцевих користувачів, захищені системи часто використовують автентифікацію на основі токенів. Користувач автентифікується один раз під час початку сеансу, і система видає підписаний токен, який використовується при кожному запиті від клієнта.

Система аутентифікації користувача зазвичай включає в себе процес перевірки та підтвердження ідентичності особи, яка намагається отримати доступ до системи чи ресурсу. Це може бути виконано за допомогою різних методів, включаючи: пароль або PIN-код; фізичний токен або смарт-карта; біометричні дані, такі як відбиток пальця чи розпізнавання обличчя. Біометрична автентифікація – це процес підтвердження та перевірки автентичності оголошеного користувачем імені

через подання свого біометричного зображення, та шляхом перетворення цього зображення відповідно до попередньо встановленого протоколу автентифікації.

Розглянуті види біометричних способів захисту інформації та поділені на два методи: статичний та динамічний. Усі розглянуті методи мають як плюси так і мінуси. Розглянуто методи розпізнавання осіб, такі як: метод гнучкого порівняння у графах, нейронні мережі, приховані марківські моделі, метод головних компонентів, активні моделі зовнішнього вигляду. Незважаючи на велику різноманітність алгоритмів розпізнавання осіб, можна виділити загальну структуру процесу. На першому етапі проводиться детектування та локалізація особи на зображенні. На етапі розпізнавання виробляється вирівнювання зображення обличчя геометричне і яскравісне), обчислення ознак і безпосередньо розпізнавання – порівняння обчислених ознак із закладеними базу даних еталонами. Основною відмінністю всіх розглянутих алгоритмів це різне обчислення ознак та порівняння їх сукупностей між собою.

Біометричні системи автентифікації використовують такі фізичні ознаки, як відбитки пальців, обличчя, райдужна оболонка ока та вени як облікові дані. Крім іншого, термінали автентифікації обличчя використовують обличчя як облікові дані, що є найбільш схожим способом розпізнавання людини людиною. Пристрої розпізнавання відбитків пальців, які найчастіше використовуються для біометричної аутентифікації, оснащені оптичним датчиком. Оскільки автентифікація обличчя використовує камери для ідентифікації особи, оптичний датчик не потрібен. Таким чином, це дозволяє користувачеві виконувати автентифікацію без фізичного контакту. Оскільки термінали автентифікації за обличчям використовують ІЧ-технологію (ІЧ-порт), одним із головних недоліків автентифікації за обличчям є обмеження щодо місця встановлення: термінал автентифікації за обличчям працюватиме погано, якщо його встановити надворі або біля вікон через сильне навколишнє освітлення.

FaceStation 2, найновіший термінал автентифікації обличчя від Suprema, виходить за рамки цього обмеження. Це термінал контролю доступу та обліку робочого часу, який покращує роботу користувача з Android 5.0 Lollipop і

найновішим алгоритмом, апаратним і програмним забезпеченням Suprema. Обробка навколишнього освітлення має вирішальне значення для продуктивності автентифікації обличчя. Більшість наявних на ринку терміналів автентифікації обличчя мають обмежені місця встановлення, оскільки продуктивність розпізнавання залежить від інтенсивності навколишнього освітлення. FaceStation 2 має 80 ширококутних ближніх інфрачервоних світлодіодів і 60 вузькокутних ближніх інфрачервоних світлодіодів, тож він може розпізнавати обличчя навіть у середовищі з 25 000 люкс, що еквівалентно середовищу з повним денним освітленням (без прямого сонця). Це дозволяє користувачам встановлювати термінали в приміщеннях біля вікон, вестибюлів і входів у будівлі.

Ще одна технологія, застосована FaceStation 2 для підвищення продуктивності, — це аналіз розподілу інтенсивності пікселів. Однією з труднощів використання світлодіодної технології ближнього інфрачервоного діапазону є вплив навколишнього освітлення. Навколишнє освітлення може зробити світлодіодне освітлення ближнього інфрачервоного діапазону марним, оскільки воно містить ультрафіолетові промені. Крім того, тінь на обличчі від навколишнього освітлення може ускладнити алгоритм вилучення рис обличчя.

Аналіз розподілу інтенсивності тривимірних пікселів мінімізує вплив навколишнього освітлення під час отримання зображень обличчя. В результаті термінал отримує зображення в ближньому інфрачервоному діапазоні з мінімальною зміною контрастності. Алгоритму легше розпізнати форму обличчя за допомогою цих рівномірних контрастних зображень, ніж із занадто яскравими або темними зображеннями, тому він може виділити більше різноманітних рис, таким чином створюючи високоякісні шаблони обличчя. Високоякісні шаблони обличчя мають вирішальне значення для продуктивності автентифікації обличчя.

FaceStation 2 також працює як відеотелефон SIP (протокол ініціації сеансу), що усуває необхідність встановлення окремого відеотелефону. Якщо SIP-сервер уже встановлено на сайті, ви можете використовувати наявну SIP-інфраструктуру. В іншому випадку клієнти можуть встановити добре відомий SIP-сервер з

відкритим кодом, рекомендований і протестований Suprema, щоб використовувати FaceStation 2 як відеотелефон.

Встановлено, що основними перевагами FSD2 є: висока продуктивність, найвища робоча освітленість, покращена безпека, покращена безпека за допомогою Android 5.0 Lollipop, Журнал зображень високої якості, Multi RFID Card Reading, ергономіка та зручність користувача

Платформа FS2D використовує BioStart 2 system в ролі програмного забезпечення. Згідно із мінімальними вимогами по програмному забезпеченню із офіційно веб сайту компанії розробника існуючі рішення працюють із windows платформами. Тому в ході цієї роботи ми використовували програмне забезпечення адаптоване під windows машини. BioStar 2 було розроблено для подолання обмежень розподіленої системи контролю доступу.

Є два способи використання BioStar API. Один називається Web API (через BioStar Cloud Server), а інший називається Local API. Компанія виробник рекомендує використовувати локальний API. BioStar2 API це API на серверному рівні, це означає що більше не треба інтегрувати додаткові SDK. Як наслідок більш проста взаємодія і інтеграція із сторонніми застосунками на базі WEB API.

Оскільки BioStar API є RESTful API, ми змогли змоделювати повноцінну клієнт-серверну архітектуру.

Створена програми є консольною програмою Visual C# і містить чотири основні функції: вхід, створення користувача, отримання групи доступу та отримання журналу.

Дані користувача містяться у форматі JSON і містять дуже докладні дані, включаючи шаблони відбитків пальців.

У роботі подано створену програму та аналіз коду задачі аутентифікації користувача. На рисунках представлено програмні коди функції логування, отримання групи доступу, отримання івентів (подій), створення користувача.

У роботі розроблено заходи із охорони праці та безпеки у надзвичайних ситуаціях під час з комп’ютерною технікою. Розрахована ефективність використання інформаційної системи аутентифікації.

Система аутентифікації знижує ризик незаконного доступу до конфіденційної інформації та забезпечує захист від кіберзагроз, таких як хакерські атаки та фішинг. Системи аутентифікації постійно вдосконалюються та оптимізуються. Поступово система захисту стає дешевшою, але при цьому надійнішою. Крім того, вони стають більш доступними в плані використання та обслуговування, є малий відсоток системних помилок і збоїв при яких користувач не був авторизований або прийнятий за іншого.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Архітектури рекурентної нейронної мережі довгострокової пам'яті для великомасштабного акустичного моделювання (2014), Хасім Сак та ін., Google Research
2. Бібліотека “Stanford Core NLP” [Електронний ресурс]. — Дата візиту 30.09.2023. — Режим доступу до ресурсу: https://stanfordnlp.github.io/CoreNLP/index.html.
3. Монолітна архітектура розроблення ПЗ [Електронний ресурс]. — Дата візиту 30.09.2023. — Режим доступу до ресурсу: http://microservices.io/patterns/monolithic.html.
4. Надо Д. Огляд розпізнавання та класифікації названих сутностей / Д. Надо, С. Секіне // Національна дослідницька рада Канади – 2016.
5. Д. Фленаган, JavaScript: повне керівництво, 2008
6. Analysis market recognition technology [Электронный ресурс]. // TrendForce. https://www.trendforce.com/
7. Angular 101: Pros, cons, features and more [Електронний ресурс] - Режим доступу до ресурсу: https://www.pluralsight.com/blog/software development/angular-101
8. Brunelli R., Poggio T. Face recognition through geometrical features – Computer Vision—ECCV'92. – Springer Berlin/Heidelberg, 1992.
9. J. Chan, Learn CSS in one day and learn it well, 2015
10. Elisabeth Freeman, Head First HTML with CSS & XHTML, 2005
11. D. McFarland, CSS: The Missing Manual, 2006
12. A. Freeman, Pro Angular 6, 2018
13. Husken, M.: Strategies and benefits of fusion of 2d and 3d face recognition. In: Proceedings of the IEEE Workshop on Face Recognition Grand Challenge Experiments./ Husken, M., Brauckmann, B., Gehlen, S., von der Malsburg //IEEE Press, Los Alamitos Computer Society Digital Library,:.2005. – 174 p.

14. Hrytsyk V. V. Modeling and synthethis of complex symmetrical images / V. V. Hrytsyk, K. M. Berezska, O. M. Berezsky // International journal of pattern recognition and artificial intelligence. – 2004. – V. 18, № 2. – P. 175–195.
15. JavaScript [Електронний ресурс] – Режим доступу до ресурсу: https://developer.mozilla.org/en-US/docs/Web/JavaScript
16. Lienhart, R. An extended set of Haar-like features for rapid object detection / Maydt, J. ICIP02, 2002 – 250
17. Liu, C. Using Dimensionality Enhancement Techniques to Improve Face Recognition./ Liu, C // IEEE: Workshop on Face Recognition Grand Challenge Experiments, 2006. – 737 p.
18. Main Disadvantages of Python Programming Language [Електронний ресурс] – Режим доступу до ресурсу: https://www.pythonistaplanet.com /disadvantages-of-python/
19. Neurotechnology. VeriLook SDK: http://www.neurotechnology.com/
20. Otander J. CMUSphinx tutorial for developers. URL: https://cmusphinx.github.io/wiki/tutorial/
21. Peter N. Belhumeur Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection / David J. Kriegman, 1997 – 64
22. L. Richardson, RESTful Web APIs: Services for a Changing World, 2013
23. Suprema knowledge center. BioStar 2 Distributed System https://kb.supremainc.com/
24. Suprema knowledge center. Fundamental https://kb.supremainc.com/knowledge/doku.php?id=en:trn_ec_main
25. B. Syed, Beginning Node.js, 2014
26. The Zen Of Python, Explained [Електронний ресурс] - Режим доступу до ресурсу: https://inventwithpython.com/blog/2018/08/17/the-zen-of-pythonexplained
27. Turati C. et al. Newborns' face recognition: Role of inner and outer facial features //Child development. – 2006. – Т. 77. – №. 2. – С. 297-311

28. TypeScript Documentation [Електронний ресурс] - Режим доступу до ресурсу: https://www.typescriptlang.org/docs/home.html
29. D. Vanderkam, Effective TypeScript: 62 Specific Ways to Improve Your TypeScript, 2019
30. Wiskott L. et al. Face recognition by elastic bunch graph matching //IEEE Transactions on pattern analysis and machine intelligence. – 1997.