УДК 004.

С. В. Сідак
О. О. Ковалюк

АВТОМАТИЗАЦІЯ ПРОЦЕСУ АВТЕНТИФІКАЦІЇ ТА АВТОРИЗАЦІЇ ПЕРСОНАЛУ НА ПІДПРИЄМСТВІ ІЗ ВИКОРИСТАННЯМ ХМАРНИХ ТЕХНОЛОГІЙ

Вінницький національний технічний університет

Анотація

У цьому дослідженні було розглянуто процес автентифікації та авторизації, а також автоматизацію процесу автентифікації та авторизації персоналу на підприємстві із використанням хмарних технологій, також проведено їх класифікацію та порівняння.

Ключові слова: авторизація, автентифікація, хмарні технології, біометричні дані, автоматизація процесу.

Abstract

This research considered the process of authentication and authorization, as well as the automation of the process of authentication and authorization of personnel in enterprises using cloud technologies, as well as their classification and comparison.

Keywords*: authorization, authentication, cloud technologies, biometric systems, process automation.*

Вступ

Авторизація та автентифікація[1] – терміни, які характеризують суміжні, проте несхожі поняття. Автентифікація – це процедура перевірки достовірності того, що користувач саме той, за кого себе видає. Авторизація ж – це надання прав на певні дії. Тобто дані поняття є взаємопов'язаними: спочатку відбувається автентифікація – підтвердження того, ким є суб'єкт автентифікації, а потім авторизація – надання прав на виконання дій.

Перші згадки про автентифікацію почали з'являтися у 60-роках XX століття[2], коли у деяких університетах почали з'являтися комп'ютери, які використовувалися всімами студентами. У Массачусетському технологічному інституті існувала Сумісна система розподілу часу (Compatible Time-Sharing System), яка дозволяла сумісно використовувати комп'ютер, саме у ній було запроваджено першу систему автентифікації – для доступу до своїх файлів, користувач повинен був ввести пароль, який, щоправда, зберігався у текстовому файлі у файловій системі.

Потреба у контролі доступу виникає, коли необхідно запобігти несанкціонованому доступу до об'єкту захисту. Контролювати доступ можна як до фізичних об'єктів – як от різноманітні зони на підприємстві чи кімнати до яких можуть мати доступ лише кваліфіковані спеціалісти, так і дані на сервері, як от частини сайту, на які можуть заходити авторизовані користувачі із певними ролями (відкрита частина сайту – доступна неавторизованим користувачам, частина із можливістю додавати записи на сайт – вимагає наявності ролі – зареєстрований користувач та адміністративна частина – можливість редагувати та видаляти).

Існують різні способи авторизації та автентифікації та відповідно різні системи, побудовані на них. У ході даного дослідження було розроблено систему для автоматизації процесу автентифікації та авторизації персоналу на підприємстві, із використанням хмарних технологій.

Автоматизація процесу автентифікації та авторизації дозволяє покращити точність, а також запобігти виникненню помилок, які можуть бути спричинені людським фактором. Окрім цього покращити безпеку, шляхом детального контролю та аудиту всіх дій персоналу, пов'язаних із отриманням доступу, які відбувалися на підприємстві. Зручність способу полягає у можливості розширеного налаштування та можливості зберігати дані як на віддаленому сервері – так і локально, на підприємстві, що дозволяє зробити систему ізольованою, та запобігти можливим атакам ззовні.

Результати дослідження

Автентифікація та авторизація є невід'ємною складовою будь якої сучасної системи, а автентифікація та авторизація персоналу на підприємстві дозволяє підвищити рівень безпеки, а також запобігти

несанкціонованому доступу до інформаційної бази підприємства. Автоматизація цього процесу надає можливість покращити якість ідентифікації осіб та за рахунок цього підвищити точність розпізнавання і запобігти можливим помилкам, пов'язаним із людським фактором.

Системи авторизації та автентифікації персоналу можна умовно поділити на 5 видів:

- Автентифікація та авторизація із відсутнім захистом
- Автентифікація та авторизація із використанням статичного паролю
- Автентифікація та авторизація із використанням одноразового паролю
- Автентифікація та авторизація із використанням фізичного ключа
- Автентифікація та авторизація із використанням біометрії

До недоліків автоматизованих систем автентифікації та авторизації можна віднести:

- Вартість імплементації – розробка надійної системи автентифікації та авторизації, а також обладнання, необхідне для її впровадження та супроводу коштуватиме недешево.
- Незручності для кінцевого користувача – користувачі, які звикли працювати без використання автентифікації та авторизації можуть відчувати певні незручності, пов'язані із необхідністю проходити процес автентифікації та авторизації перед доступом до ресурсів.
- Неточність автентифікації та авторизації користувача, при використанні ненадійного обладнання.
- Можливість компрометації користувацьких паролів або біометричних даних[3].

До переваг автоматизованих систем автентифікації та авторизації можна віднести:

- Висока точність та надійність автентифікації та авторизації, порівняно з іншими методами автентифікації та авторизації
- Швидкість ідентифікації – при використанні обладнання належного рівня, можна побудувати систему, яка буде відповідати найвищим вимогам щодо швидкодії
- Універсальність систем – після імплементації автоматизованої системи автентифікації та авторизації персоналу, її можна широко використовувати для захисту різноманітних ресурсів на підприємстві, із доданням мінімальних змін до існуючих
- Підвищена безпека, порівняно з аналогами, а також детальний журнал всіх дій, які відбувалися у системі, із можливістю зберігання та доступу до цих даних як локально, так і у мережі інтернет

Для успішної автоматизації даного процесу необхідно не тільки розробити програмну, але і спроектувати апаратну частину системи. Тобто система повинна складатися із апаратної частини, яка дозволяє отримати дані користувача та програмної – яка проводить обробку даних, та залежно від валідності даних, обробляє їх відповідним чином та сповіщає апаратну частину про успіх або невдачу процесу обробки даних.

Умовно систему можна поділити на три частини – прикладну, серверну та частину роботи із даними, кожна з яких має свої обов'язки:

1. Отримання даних
2. Обробка даних
3. Зберігання даних

Прикладна частина – обчислювальний модуль сканування, який відповідає за отримання даних, їх обробку та відправку на сервер для подальшої обробки. Не має особливої архітектури, є звичайним додатком, який використовує бібліотеку, розроблену на мові python, для взаємодії із сканером та передачі даних. Структурну схему приладу зображено на рисунку 1.

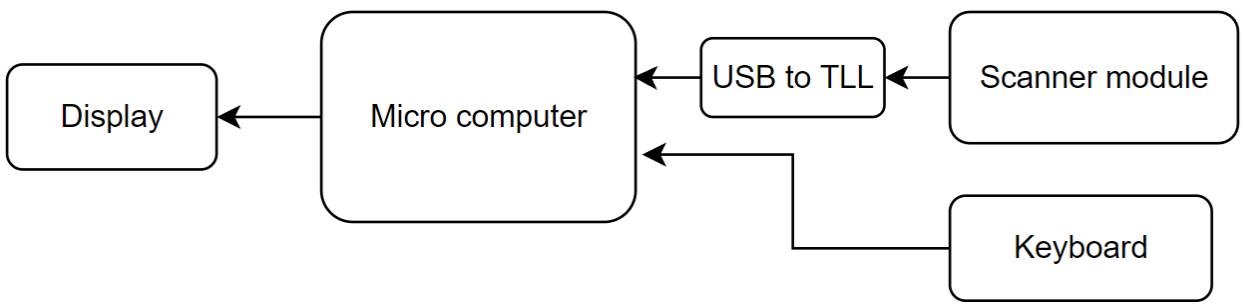

Рисунок 1 – Структурна схема

У ході дослідження при виборі мікрокомп'ютера, було проаналізовано багато моделей, серед яких

моделі від Arduino, Nvidia, Raspberry Pi, Intel, Coral та інші. У результаті для порівняння було відібрано три пристрої – raspberry pi 4, Nvidia Jetson та Asus Tinker Board та проведено їх порівняння. Детальніші дані наведено у таблиці 1.

Таблиця 1 – Порівняння мікроком'ютерів за характеристиками та ціною

	Raspberry pi 4 b	**Nvidia Jetson nano**	**ASUS TINKER BOARD**
SoC	Cortex-A72 @ 1.5GHz	ARM® A57 @ 1.43 GHz	ARM Cortex-A17 1.8GHz
К-ть ядер процесора	4	4	4
GPU	Broadcom VideoCore 4	128-core NVIDIA Maxwell	Mali-T764
Відеовиходи	2 micro-HDMI, 4k	HDMI	HDMI
RAM	2 GB	2 GB	2 GB
ROM	microSD	microSD	microSD
Network	Gigabit Ethernet	Gigabit Ethernet	Ethernet 10/100/1000
USB ports	2 USB 3.0 / 2 USB 2.0	SB 1x USB 3.0 Type A, 2x USB 2.0 Type A, USB 2.0 M-B	4 x USB 2.0
Бездротові інтерфейси	Bluetooth 5.0, Wi-Fi 2.4 GHz / 5.0 GHz	WiFi 2.4GHz	Bluetooth, WiFi 2.4GHz
Живлення	5V 3A	5V 2A	5V 2A
Ціна	45$	59$	$60

Опираючись на дані таблиці, а також на доступність мікрокомп'ютерів та складових до них у нашому регіоні, було вирішено обрати Raspberry Pi 4, який має багатий набір бездротових інтерфейсів, підтримує вивід зображення на два монітори у великій роздільній якості, а також має нижчу вартість, порівняно із конкурентами. Також у якості інших складових системи було обрано:

- R307 Fingerprint Scanner Module[4] модуль сканеру відбитків пальця, сумісний із Raspberry Pi 4;
- CP2102 USB to TTL converter - для підключення модулю сканера відбитків пальців по usb було вирішено використати конвертер.

Серверна частина складається із Web Api, та angular клієнту, які розгорнуті в azure app service, із використанням хмарних технологій.

Рівень бази даних – це реляційна SQL база даних, розгорнута у хмарному середовищі, із можливістю налаштування доступу, реплікації, масштабування та інших функцій. На рисунку 2 зображено архітектуру системи автоматизації процесу.

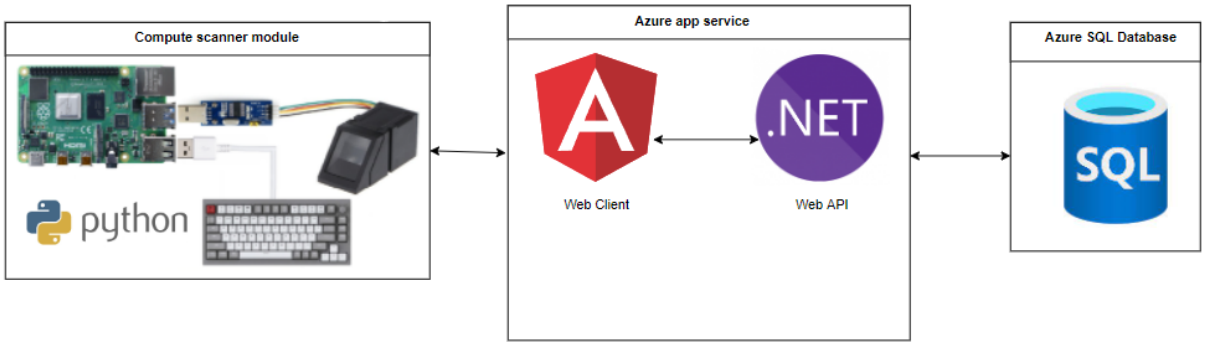

Рисунок 2 – Архітектура системи автоматизації процесу

Обчислювальний модуль сканування – працює на застосунку, написаному на мові програмування python, бекенд та фронтенд частини системи розгортаються у хмарному середовищі Azure app service, а у якості сховища даних також використовується хмарна технологія – Azure SQL Database.

Наразі існують вже розроблені системи автентифікації та авторизації персоналу серед них:

- Veriff – це програмне забезпечення, яке надає комплексні рішення у сфері безпеки та обліку персоналу та дозволяє ідентифікувати особу у реальному часі, використовуючи різноманітні критерії для

оцінки достовірності особи;

• PalmId – це продукт, який надає апаратне забезпечення, для автентифікації персоналу, із використанням біометрії.;

• Regula Face Matching Module – це продукт, основним спрямуванням якого є робота із документами. Має функції сканування та ідентифікації документів, проте окрім цього, має функцію ідентифікації користувачів із використанням розпізнавання обличчя (face matching) та розпізнавання у реальному часі (liveness detection), автентифікація та авторизації особи виконується шляхом порівняння знятого реального зображення особи, із зображенням у документі, який посвідчує особу.

Висновки

Дане дослідження показало процес автоматизації автентифікації та авторизації персоналу на підприємстві із використанням хмарних технологій, було проаналізовано системи авторизації та автентифікації, проведено їх аналіз та порівняння переваг і недоліків. Також було проаналізовано складові частини для реалізації апаратної та програмної частини, запропоновано структурну схему приладу для зчитування користувацьких даних. Запропоновано архітектуру системи.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Solving Identity Management in Modern Applications: Demystifying OAuth 2.0, OpenID Connect, and SAML 2.0 / Yvonne Wilson, Abhishek Hingnikar - 2019. 340 p.

2. A Developer’s History of Authentication [Електронний ресурс] – Режим доступу до ресурсу: https://workos.com/blog/a-developers-history-of-authentication

3. Biometric Authentication Definition, trends, pro and cons, use cases and myths [Електронний ресурс] – Режим доступу до ресурсу: https://www.onespan.com/topics/biometric-authentication

4. R307 Fingerprint Module [Електронний ресурс] – Режим доступу до ресурсу: https://www.rajguruelectronics.com/Product/1276/R307%20Fingerprint%20Module.pdf

Сідак Степан Васильович — студент групи 2АКІТ-18б, Факультет комп’ютерних систем і автоматики, Вінницький національний технічний університет, Вінниця, e-mail: sbezsm@gmail.com
Ковалюк Олег Олександрович *– к.т.н., доцент кафедри комп’ютерних систем управління, Вінницький національний технічний університет, м. Вінниця, e-mail: oleh.kovalyuk@vntu.edu.ua.*

Sidak Stepan V. — student of group 2AKIT-18b, Faculty of Computer Systems and Automation, Vinnytsia National Technical University, Vinnytsia, e-mail: sbezsm@gmail.com
Kovaliuk Oleh O. *– Ph.D., Associate Professor of the Department of Computer Control Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: oleh.kovalyuk@vntu.edu.ua.*