



ЗАСТОСУВАННЯ КРИПТОГРАФІЧНИХ МЕТОДІВ ШИФРУВАННЯ В  
РОЗРОБЦІ ВЕБ-СЕРВІСУ ДЛЯ БЕЗПЕЧНОГО ЗБЕРІГАННЯ ЧУТЛИВИХ  
ДАНИХ  
APPLICATION OF CRYPTOGRAPHIC ENCRYPTION METHODS IN THE  
DEVELOPMENT OF A WEB SERVICE FOR SECURE STORAGE OF SENSITIVE  
DATA

Виконала студентка КН-4

Бойко Інна Іванівна

Науковий керівник - старший викладач

Кирієнко Оксана Валентинівна



## **Метою кваліфікаційної роботи є:**

Розробка веб-сервісу для управління персоналом з підвищеним рівнем безпеки шляхом застосування сучасних криптографічних методів, впровадження механізму управління ключами та усунення критичних загроз, пов'язаних із зберіганням чутливих даних.

# Аналіз рівня захищеності вибраного веб-сервісу організації

## Виявлені вразливості

відсутність  
шифрування  
чутливих даних

використання  
застарілого  
програмного  
забезпечення

використання  
протоколу TLS  
1.0

# Постановка завдання

1

Аналіз та впровадження криптографічного алгоритму для шифрування чутливої інформації в базі даних

2

Розробка прототипу веб-сервісу з актуальним програмним забезпеченням для усунення низки вразливостей

# Критерії оцінки алгоритмів шифрування

## Безпека

Безпекова стійкість  
(Security strength)

## Продуктивність

Execution time

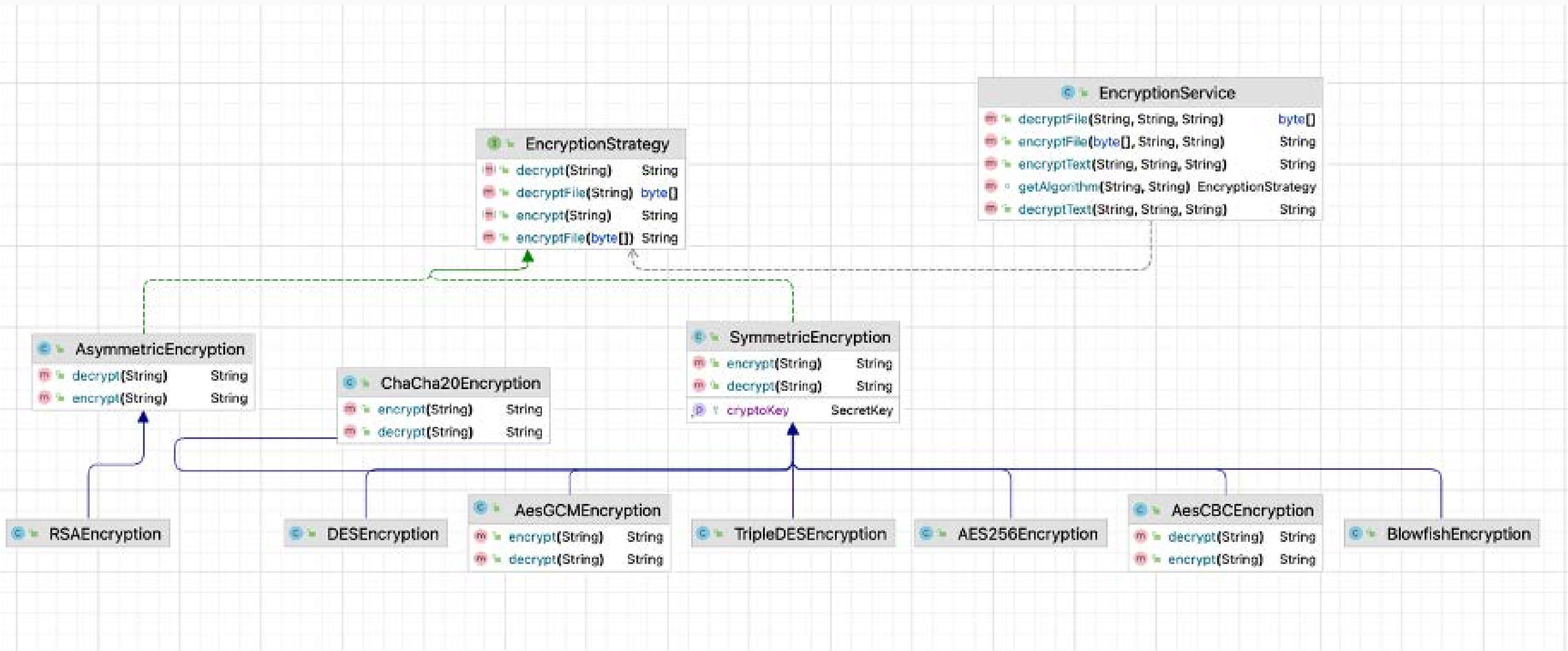
# Безпечова стійкість (Security strength)

Attack Steps Metric

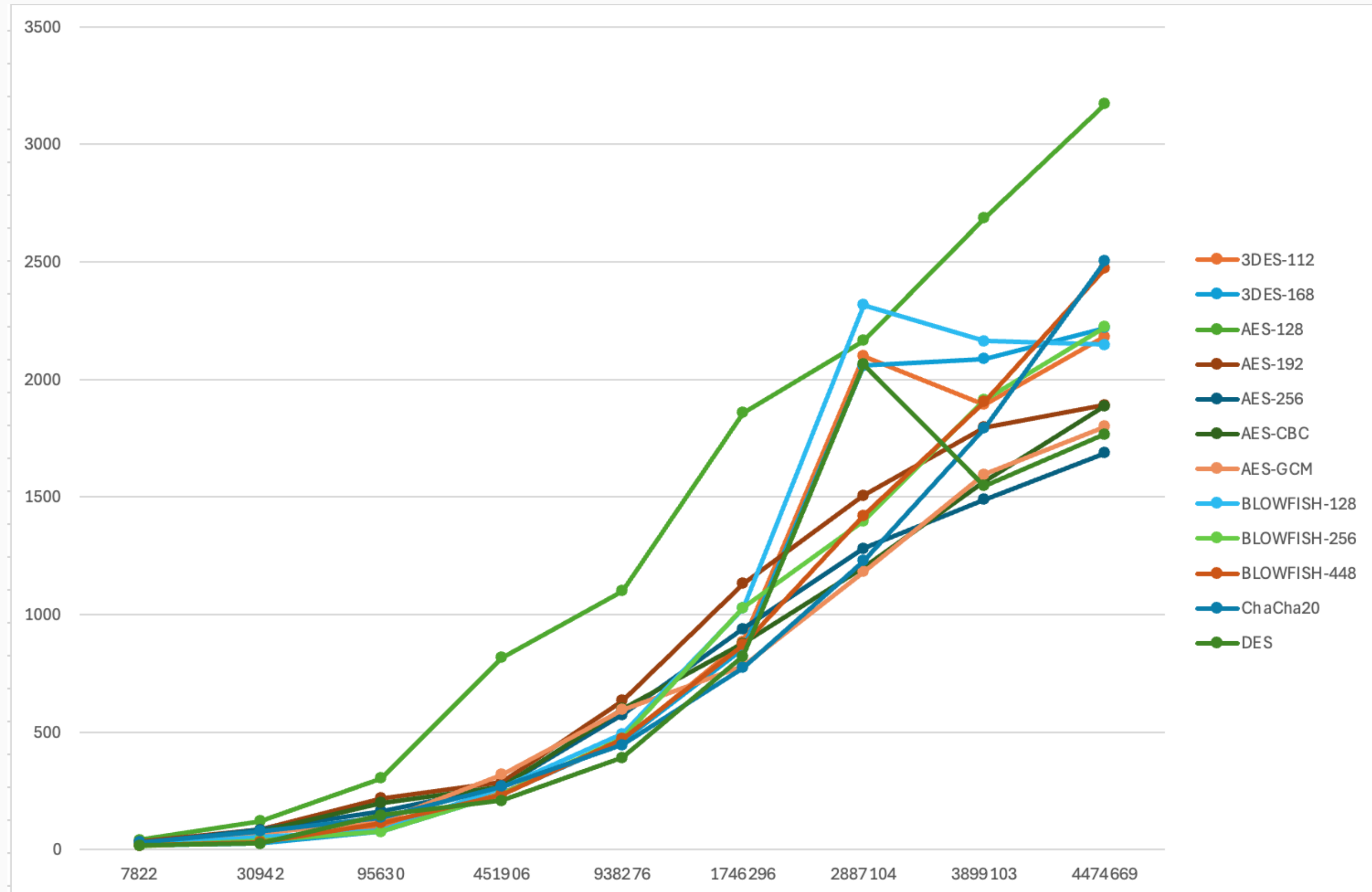
Attack Time Metric

Алгоритм	Розмір ключа(у бітах)	Security Strength (у бітах)	Attack Steps Metric	Attack Time Metric (у роках)
BLOWFISH-128	128	32	$2^{32}$	2,5 (секунд)
BLOWFISH-256	256	32	$2^{32}$	2,5 (секунд)
BLOWFISH-448	448	32	$2^{32}$	2,5 (секунд)
DES	56	56	$2^{56}$	1,31
3DES-112	112	112	$2^{112}$	$9.45 \cdot 10^{16}$
3DES-168	168	112	$2^{112}$	$9.45 \cdot 10^{16}$
AES-128	128	128	$2^{128}$	$6,19 \cdot 10^{21}$
ECIES-256	128	128	$2^{128}$	$6,19 \cdot 10^{21}$
RSA-2048	2048	128	$2^{128}$	$6,19 \cdot 10^{21}$
AES-192	192	192	$2^{192}$	$1.14 \cdot 10^{41}$
ECIES-384	192	192	$2^{192}$	$1.14 \cdot 10^{41}$
CHACHA20	256	256	$2^{256}$	$2.11 \cdot 10^{60}$
AES-256	256	256	$2^{256}$	$2.11 \cdot 10^{60}$
AES-CBC	256	256	$2^{256}$	$2.11 \cdot 10^{60}$
AES-GCM	256	256	$2^{256}$	$2.11 \cdot 10^{60}$
ECIES-521	256	256	$2^{256}$	$2.11 \cdot 10^{60}$

# Execution time



# Throughput



# Execution time



# Обраний криптографічний алгоритм - AES - GCM

Безпекова стійкість  
256 біт

Забезпечення безпеки  
та цілісності даних

Один з найкращий  
показників  
продуктивності серед  
тестованих алгоритмів

AES-NI

## Реалізовано:

- вибраний алгоритм шифрування
- керування криптографічними ключами
- захищена передача даних за TLS 1.3

Secrets / secret / key / 4284 / aes-gcm

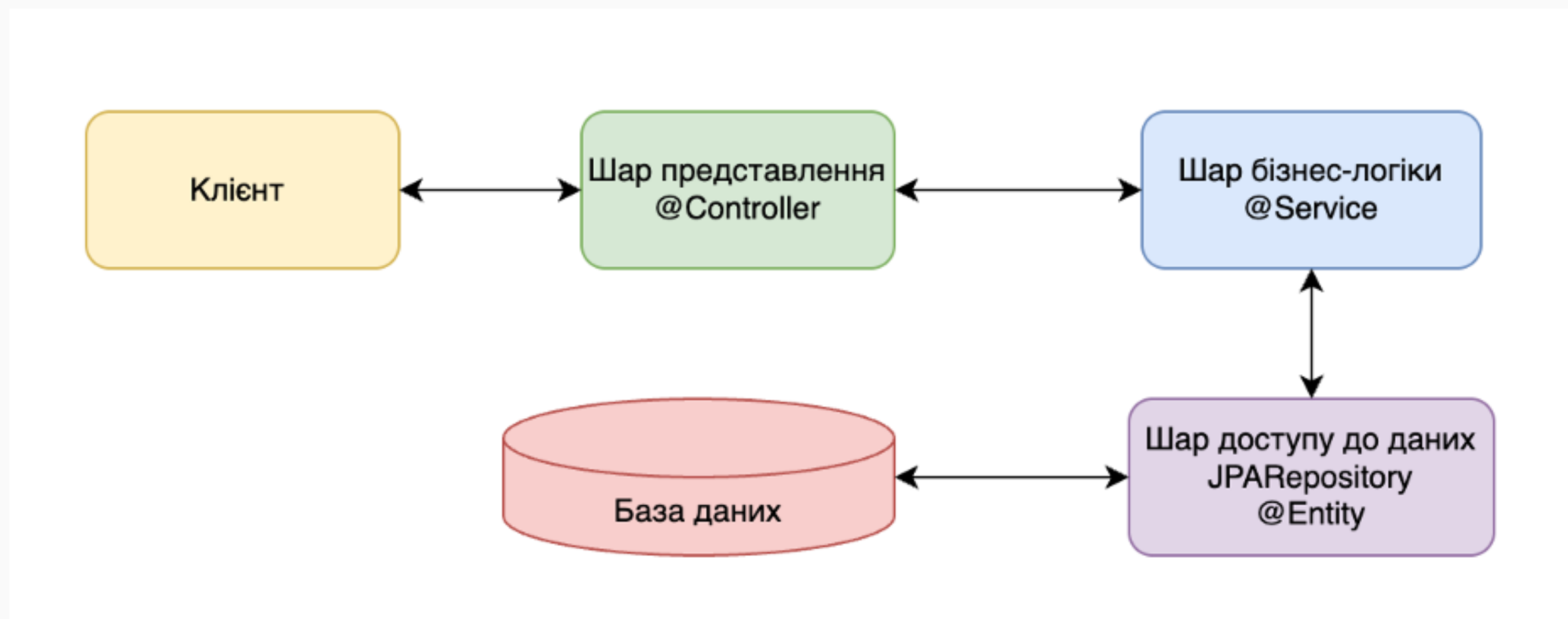
### key/4284/aes-gcm

Overview **Secret** Metadata Paths Version History

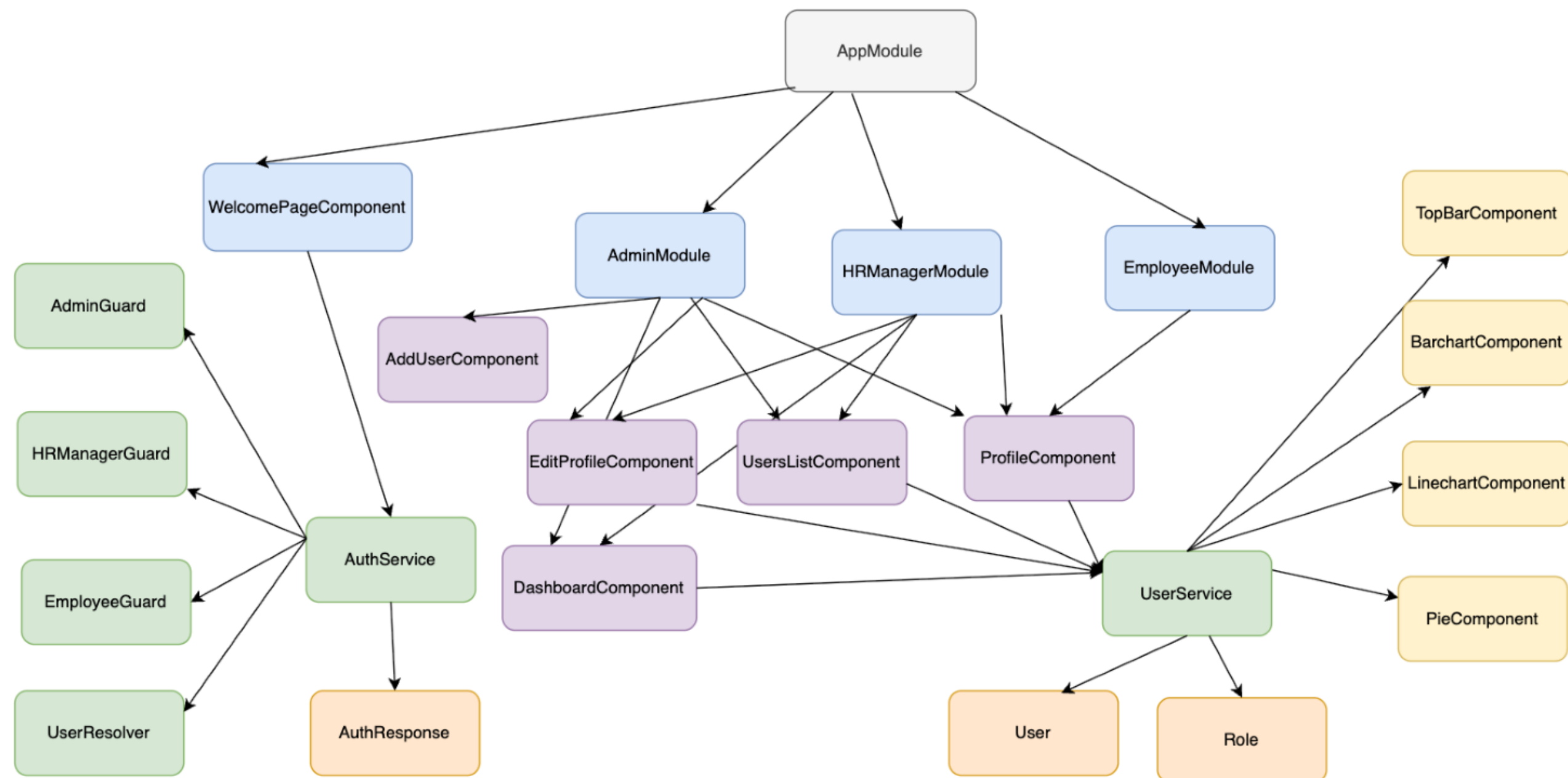
JSON Delete Destroy Copy Version 1 Create new version +

Key	Value	Version 1 created May 18, 2025 07:53 PM
key	.....	

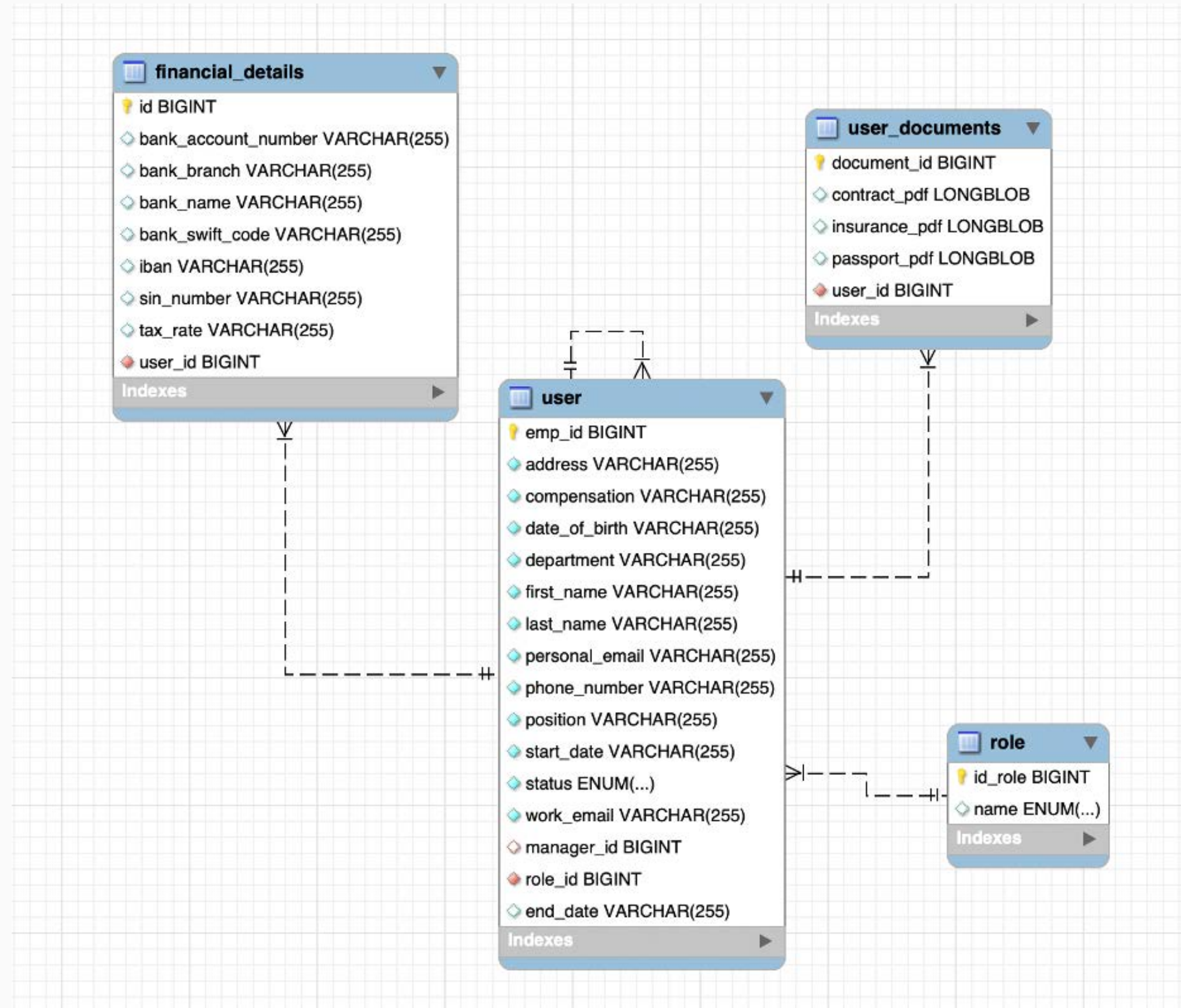
# Розроблена архітектура веб-сервісу керування персоналом



# Розроблена архітектура веб-сервісу керування персоналом



# База даних



# Розроблений веб-сервіс управління персоналом

15/19

## Welcome to HR System


Please sign in to continue

Email\*

Password\*

Sign-In

Sign-In with Google

 Вхід через Google

## Увійдіть

Перейти в додаток [hrsystem-56590.firebaseio.com](https://hrsystem-56590.firebaseio.com)

Електронна адреса або телефон

Забули електронну адресу?

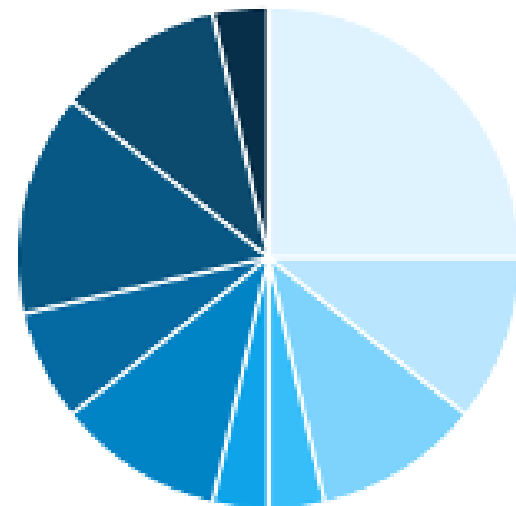
Створити обліковий запис

Далі

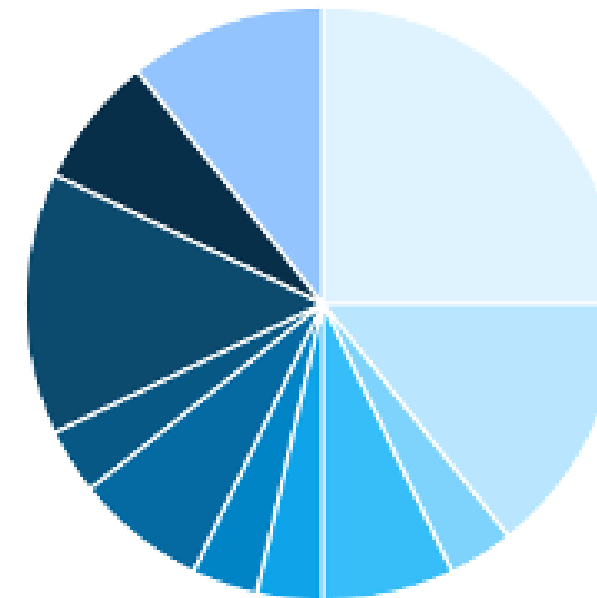
## Dashboard

Total number of employees : 28

Number of employees by department



Employee tenure distribution



ID	First Name	Last Name	Work Email	Position	Department	Manager	Personal Email	Phone	A
4284	Inna	Boiko	innaa.boikooo@gmail.com	Software Engineer	Human Resouces		inna.boiko@gmail.com	+380-50-123-4567	B
4290	Idsjflds	Idsjflds	kfsdkf.khskdfjk@gmail.com	HR manager	Human Resources		sdkfks.sdkfks@hotmail.com	4738282393323	B
4289	Ashley	Joham	ahley.joham@gmail.com	HR manager	Human Resources		ahley.joham@hotmail.com	4738282393323	B
4291	Alayna	Gleichner	alayna.gleichner@yahoo.com	Financial Accountant	Finance & Accounting		alayna_gleichner@gmail.com	543-231-5555	5
4292	Stephanie	Marquardt	stephanie.marquardt@gmail.com	Financial Accountant	Finance & Accounting		stephanie.marquardt@yahoo.com	1-399-385-0350	6
4293	Garett	Towne	garett.towne@yahoo.com	Legal Counsel	Legal		garett_towne@gmail.com	543-231-5555	5
4294	Daniella	Schiller	daniella.schiller@yahoo.com	Financial Accountant	Finance & Accounting		daniella_schiller@gmail.com	543-231-5555	S

Items per page:

10

1 - 10 of 28

&lt;&lt; &lt; &gt; &gt;&gt;

Add user

### Personal Information

**Id:** 4292

**First Name:** Stephanie

**Last Name:** Marquardt

**Work Email:** stephanie.marquardt@gmail.com

**Personal Email:** stephanie.marquardt@yahoo.com

**Phone:** 1-399-385-0350

**Date of Birth:** 1990-04-12

**Address:** 667 Koch Camp, New Hobartstad, OR 95837

### Work Information

**Department:** Finance & Accounting

**Position:** Financial Accountant

**Compensation:** 79000

**SIN :** 123-45-6789

**Bank Name:** PrivatBank

**Bank Account Number:** 26008012345678

**Bank Branch:** Головне відділення

**Bank SWIFT Code:** PBANUA2X

**IBAN:** UA12345678012345678901234567

### Documents

 Insurance: [Download](#)

 Passport: [Download](#)

 Contract: [Download](#)

[Update Profile](#)

## Висновок:

- виконаний аналіз та вибір найкращого алгоритму шифрування
- впровадження методів захисту для зменшення кількостей вразливостей в розробленому веб-сервісі

**Дякую за  
увагу!**