Додаток А

Звіт результатів перевірки на унікальність тексту в базі хнуре

StrikePlagiarism.com

Дата звіту 6/13/2025
Дата редагування ---

Звіт не був оцінений

Звіт подібності

метадані

Назва організації
Kharkiv National University of Radio Electronics
Заголовок
2025_M_ПІ_ІПЗм_23_4_Козинець_М_С_скорочений
Автор Науковий керівник / Експерт
Козинець Максим СергійовичОпена Опійник
підрозділ
каф. ПІ

Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високе значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.

3.54% 3.54% КП 1

1.06% 1.06% КЦ

25	8967	72324
Довжина фрази для коефіцієнта подібності 2	Кількість слів	Кількість символів

Тривога

У цьому розділі ви знайдете інформацію щодо текстових спотворень. Ці спотворення в тексті можуть говорити про МОЖЛИВІ маніпуляції в тексті. Спотворення в тексті можуть мати навмисний характер, але частіше характер технічних помилок при конвертації документа та його збереженні, тому ми рекомендуємо вам підходити до аналізу цього модуля відповідально. У разі виникнення запитань, просимо звертатися до нашої служби підтримки.

Заміна букв		12
Інтервали		0
Мікропробіли		0
Білі знаки		0
Парафрази (SmartMarks)		18

Подібності за списком джерел

Нижче наведений список джерел. В цьому списку є джерела із різних баз даних. Колір тексту означає в якому джерелі він був знайдений. Ці джерела і значення Коефіцієнту Подібності не відображають прямого плагіату. Необхідно відкрити кожне джерело і проаналізувати зміст і правильність оформлення джерела.

10 найдовших фраз — Колір тексту

ПОРЯДКОВИЙ НОМЕР	НАЗВА ТА АДРЕСА ДЖЕРЕЛА URL (НАЗВА БАЗИ)	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	https://science.lpnu.ua/sites/default/files/journal-paper/2019/apr/15997/vis673ism-205-213.pdf	64 0.71 %
2	https://science.lpnu.ua/sites/default/files/journal-paper/2019/apr/15997/vis673ism-205-213.pdf	21 0.23 %
3	http://ena.lp.edu.ua:8080/bitstream/ntb/10543/1/59.pdf	20 0.22 %
4	https://hub.kyivstar.ua/news/tmarni-trend-yak-rozvivatimut-sya-cloud-tehnologi-ta-navishho-von-biznesu/	18 0.20 %

Рисунок А.1 – Результати перевірки на антиплагіат (сторінка 1)

5	ТІ-Порівняльний аналіз використання алгоритмів геометричної трансформації для покращення продуктивності в мобільних додатках [redacted] 7/12/2024 Kyiv National University of Technologies and Design (НДЧ)	16 0.18 %
6	http://ena.lp.edu.ua:8080/bitstream/ntb/10543/1/59.pdf	15 0.17 %
7	https://openarchive.nure.ua/bitstream/document/12600/1/2020_M_Shl_Berestovy_OO.pdf	14 0.16 %
8	https://science.lpnu.ua/sites/default/files/journal-paper/2019/apr/15997/vis673ism-205-213.pdf	13 0.14 %
9	ВИКОРИСТАННЯ SERVERLESS МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ ДЛЯ ВІДПРАВКИ ДАНИХ НА SFTP СЕРВЕР [redacted] 6/27/2024 Lesya Ukrainka Volyn National University (Кафедра комп'ютерних наук та кібербезпеки)	12 0.13 %
10	https://userua.org.ua/yaki-formaty-grafichnyh-failiv-vy-znayete	11 0.12 %

з бази даних RefBooks (0.00 %)

ПОРЯДКОВИЙ НОМЕР	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)

з домашньої бази даних (0.00 %)

ПОРЯДКОВИЙ НОМЕР	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)

з програми обміну базами даних (0.59 %)

ПОРЯДКОВИЙ НОМЕР	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	2022_61230000_Choba_Oleksii_Volodymyrovych_96004 [redacted] 10/26/2024 National University "Lviv Politechnika" (National University Lviv Politechnika)	25 (4) 0.28 %
2	ТІ-Порівняльний аналіз використання алгоритмів геометричної трансформації для покращення продуктивності в мобільних додатках [redacted] 7/12/2024 Kyiv National University of Technologies and Design (НДЧ)	16 (1) 0.18 %
3	ВИКОРИСТАННЯ SERVERLESS МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ ДЛЯ ВІДПРАВКИ ДАНИХ НА SFTP СЕРВЕР [redacted] 6/27/2024 Lesya Ukrainka Volyn National University (Кафедра комп'ютерних наук та кібербезпеки)	12 (1) 0.13 %

з Інтернету (2.94 %)

ПОРЯДКОВИЙ НОМЕР	ДЖЕРЕЛО URL	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	**https://science.lpnu.ua/sites/default/files/journal-paper/2019/apr/15997/vis673ism-205-213.pdf**	**98 (3) 1.09 %**
2	http://ena.lp.edu.ua:8080/bitstream/ntb/10543/1/59.pdf	82 (8) 0.91 %
3	https://dukt.edu.ua/repozitorii/ukb/2024/%D0%93%D0%BE%D0%BB%D0%BE%D0%B2%D0%BA%D0%BE.pdf	22 (3) 0.25 %
4	https://userua.org.ua/yaki-formaty-grafichnyh-failiv-vy-znayete	21 (3) 0.23 %
5	https://hub.kyivstar.ua/news/hmarni-trendi-yak-rozvivatimut'sya-cloud-tehnologii-ta-navishho-voni-biznesu/	18 (1) 0.20 %
6	https://openarchive.nure.ua/bitstream/document/12600/1/2020_M_Shl_Berestovy_OO.pdf	14 (1) 0.16 %

Рисунок А.2 – Результати перевірки на антиплагіат (сторінка 2)

Додаток Б

ЕКСПЕРИМЕНТАЛЬНІ ДАНІ ТА ПОКАЗНИКИ ЕФЕКТИВНОСТІ СИСТЕМИ

Таблиця Б.1 – Експериментальні дані та показники ефективності системи (виконано самостійно)

Формат зображення	Алгоритм шифрування	Система зберігання	Час шифрування (мс)	Час дешифрування (мс)	Ентропія (біт)	Кореляція	Швидкість (зобр./сек)	Час доступу (мс)
JPEG	AES-256	Гібридна (Cloud-Local)	140	120	7.89	0.015	3.85	46
JPEG	AES-256	Блокчейн	140	120	7.89	0.015	3.85	51
JPEG	AES-256	Багатовимірна	140	120	7.89	0.015	3.85	43
JPEG	RSA	Гібридна (Cloud-Local)	210	190	7.78	0.017	2.5	60
JPEG	RSA	Блокчейн	210	190	7.78	0.017	2.5	65
JPEG	RSA	Багатовимірна	210	190	7.78	0.017	2.5	57
JPEG	XOR	Гібридна (Cloud-Local)	110	98	7.52	0.025	4.81	40
JPEG	XOR	Блокчейн	110	98	7.52	0.025	4.81	45
JPEG	XOR	Багатовимірна	110	98	7.52	0.025	4.81	37
JPEG	DNA	Гібридна (Cloud-Local)	180	160	7.91	0.014	2.94	55
JPEG	DNA	Блокчейн	180	160	7.91	0.014	2.94	60
JPEG	DNA	Багатовимірна	180	160	7.91	0.014	2.94	52
JPEG	Fisher-Yates	Гібридна (Cloud-Local)	125	113	7.62	0.021	4.2	43
JPEG	Fisher-Yates	Блокчейн	125	113	7.62	0.021	4.2	48
JPEG	Fisher-Yates	Багатовимірна	125	113	7.62	0.021	4.2	40

Продовження таблиці Б.1

PNG	AES-256	Гібридна (Cloud-Local)	141	121	7.9	0.014	3.82	46
PNG	AES-256	Блокчейн	141	121	7.9	0.014	3.82	51
PNG	AES-256	Багатовимірна	141	121	7.9	0.014	3.82	43
PNG	RSA	Гібридна (Cloud-Local)	211	191	7.79	0.016	2.49	60
PNG	RSA	Блокчейн	211	191	7.79	0.016	2.49	65
PNG	RSA	Багатовимірна	211	191	7.79	0.016	2.49	57
PNG	XOR	Гібридна (Cloud-Local)	111	99	7.53	0.024	4.76	40
PNG	XOR	Блокчейн	111	99	7.53	0.024	4.76	45
PNG	XOR	Багатовимірна	111	99	7.53	0.024	4.76	37
PNG	DNA	Гібридна (Cloud-Local)	181	161	7.92	0.013	2.92	55
PNG	DNA	Блокчейн	181	161	7.92	0.013	2.92	60
PNG	DNA	Багатовимірна	181	161	7.92	0.013	2.92	52
PNG	Fisher-Yates	Гібридна (Cloud-Local)	126	114	7.63	0.02	4.17	43
PNG	Fisher-Yates	Блокчейн	126	114	7.63	0.02	4.17	48
PNG	Fisher-Yates	Багатовимірна	126	114	7.63	0.02	4.17	40
TIFF	AES-256	Гібридна (Cloud-Local)	155	133	7.91	0.013	3.47	46
TIFF	AES-256	Блокчейн	155	133	7.91	0.013	3.47	51
TIFF	AES-256	Багатовимірна	155	133	7.91	0.013	3.47	43
TIFF	RSA	Гібридна (Cloud-Local)	225	203	7.8	0.015	2.34	60
TIFF	RSA	Блокчейн	225	203	7.8	0.015	2.34	65
TIFF	RSA	Багатовимірна	225	203	7.8	0.015	2.34	57
TIFF	XOR	Гібридна (Cloud-Local)	125	111	7.54	0.023	4.24	40
TIFF	XOR	Блокчейн	125	111	7.54	0.023	4.24	45
TIFF	XOR	Багатовимірна	125	111	7.54	0.023	4.24	37

Продовження таблиці Б.1

TIFF	DNA	Гібридна (Cloud-Local)	195	173	7.93	0.012	2.72	55
TIFF	DNA	Блокчейн	195	173	7.93	0.012	2.72	60
TIFF	DNA	Багатовимірна	195	173	7.93	0.012	2.72	52
TIFF	Fisher-Yates	Гібридна (Cloud-Local)	140	126	7.64	0.019	3.76	43
TIFF	Fisher-Yates	Блокчейн	140	126	7.64	0.019	3.76	48
TIFF	Fisher-Yates	Багатовимірна	140	126	7.64	0.019	3.76	40
BMP	AES-256	Гібридна (Cloud-Local)	152	130	7.9	0.014	3.55	46
BMP	AES-256	Блокчейн	152	130	7.9	0.014	3.55	51
BMP	AES-256	Багатовимірна	152	130	7.9	0.014	3.55	43
BMP	RSA	Гібридна (Cloud-Local)	222	200	7.79	0.016	2.37	60
BMP	RSA	Блокчейн	222	200	7.79	0.016	2.37	65
BMP	RSA	Багатовимірна	222	200	7.79	0.016	2.37	57
BMP	XOR	Гібридна (Cloud-Local)	122	108	7.53	0.024	4.35	40
BMP	XOR	Блокчейн	122	108	7.53	0.024	4.35	45
BMP	XOR	Багатовимірна	122	108	7.53	0.024	4.35	37
BMP	DNA	Гібридна (Cloud-Local)	192	170	7.92	0.013	2.76	55
BMP	DNA	Блокчейн	192	170	7.92	0.013	2.76	60
BMP	DNA	Багатовимірна	192	170	7.92	0.013	2.76	52
BMP	Fisher-Yates	Гібридна (Cloud-Local)	137	123	7.63	0.02	3.85	43
BMP	Fisher-Yates	Блокчейн	137	123	7.63	0.02	3.85	48
BMP	Fisher-Yates	Багатовимірна	137	123	7.63	0.02	3.85	40
GIF	AES-256	Гібридна (Cloud-Local)	135	115	7.86	0.02	4	46
GIF	AES-256	Блокчейн	135	115	7.86	0.02	4	51

Продовження таблиці Б.1

GIF	AES-256	Багатовимірна	135	115	7.86	0.02	4	43
GIF	RSA	Гібридна (Cloud-Local)	205	185	7.75	0.022	2.56	60
GIF	RSA	Блокчейн	205	185	7.75	0.022	2.56	65
GIF	RSA	Багатовимірна	205	185	7.75	0.022	2.56	57
GIF	XOR	Гібридна (Cloud-Local)	105	93	7.49	0.03	5.05	40
GIF	XOR	Блокчейн	105	93	7.49	0.03	5.05	45
GIF	XOR	Багатовимірна	105	93	7.49	0.03	5.05	37
GIF	DNA	Гібридна (Cloud-Local)	175	155	7.88	0.019	3.03	55
GIF	DNA	Блокчейн	175	155	7.88	0.019	3.03	60
GIF	DNA	Багатовимірна	175	155	7.88	0.019	3.03	52
GIF	Fisher-Yates	Гібридна (Cloud-Local)	120	108	7.59	0.026	4.39	43
GIF	Fisher-Yates	Блокчейн	120	108	7.59	0.026	4.39	48
GIF	Fisher-Yates	Багатовимірна	120	108	7.59	0.026	4.39	40
WEBP	AES-256	Гібридна (Cloud-Local)	137	118	7.89	0.015	3.92	46
WEBP	AES-256	Блокчейн	137	118	7.89	0.015	3.92	51
WEBP	AES-256	Багатовимірна	137	118	7.89	0.015	3.92	43
WEBP	RSA	Гібридна (Cloud-Local)	207	188	7.78	0.017	2.53	60
WEBP	RSA	Блокчейн	207	188	7.78	0.017	2.53	65
WEBP	RSA	Багатовимірна	207	188	7.78	0.017	2.53	57
WEBP	XOR	Гібридна (Cloud-Local)	107	96	7.52	0.025	4.93	40
WEBP	XOR	Блокчейн	107	96	7.52	0.025	4.93	45
WEBP	XOR	Багатовимірна	107	96	7.52	0.025	4.93	37
WEBP	DNA	Гібридна (Cloud-Local)	177	158	7.91	0.014	2.99	55
WEBP	DNA	Блокчейн	177	158	7.91	0.014	2.99	60

Кінець таблиці Б.1

WEBP	DNA	Багатовимірна	177	158	7.91	0.014	2.99	52
WEBP	Fisher-Yates	Гібридна (Cloud-Local)	122	111	7.62	0.021	4.29	43
WEBP	Fisher-Yates	Блокчейн	122	111	7.62	0.021	4.29	48
WEBP	Fisher-Yates	Багатовимірна	122	111	7.62	0.021	4.29	40
DICOM	AES-256	Гібридна (Cloud-Local)	160	138	7.9	0.013	3.36	46
DICOM	AES-256	Блокчейн	160	138	7.9	0.013	3.36	51
DICOM	AES-256	Багатовимірна	160	138	7.9	0.013	3.36	43
DICOM	RSA	Гібридна (Cloud-Local)	230	208	7.79	0.015	2.28	60
DICOM	RSA	Блокчейн	230	208	7.79	0.015	2.28	65
DICOM	RSA	Багатовимірна	230	208	7.79	0.015	2.28	57
DICOM	XOR	Гібридна (Cloud-Local)	130	116	7.53	0.023	4.07	40
DICOM	XOR	Блокчейн	130	116	7.53	0.023	4.07	45
DICOM	XOR	Багатовимірна	130	116	7.53	0.023	4.07	37
DICOM	DNA	Гібридна (Cloud-Local)	200	178	7.92	0.012	2.65	55
DICOM	DNA	Блокчейн	200	178	7.92	0.012	2.65	60
DICOM	DNA	Багатовимірна	200	178	7.92	0.012	2.65	52
DICOM	Fisher-Yates	Гібридна (Cloud-Local)	145	131	7.63	0.019	3.62	43
DICOM	Fisher-Yates	Блокчейн	145	131	7.63	0.019	3.62	48
DICOM	Fisher-Yates	Багатовимірна	145	131	7.63	0.019	3.62	40

Додаток В

СЛАЙДИ ПРЕЗЕНТАЦІЇ

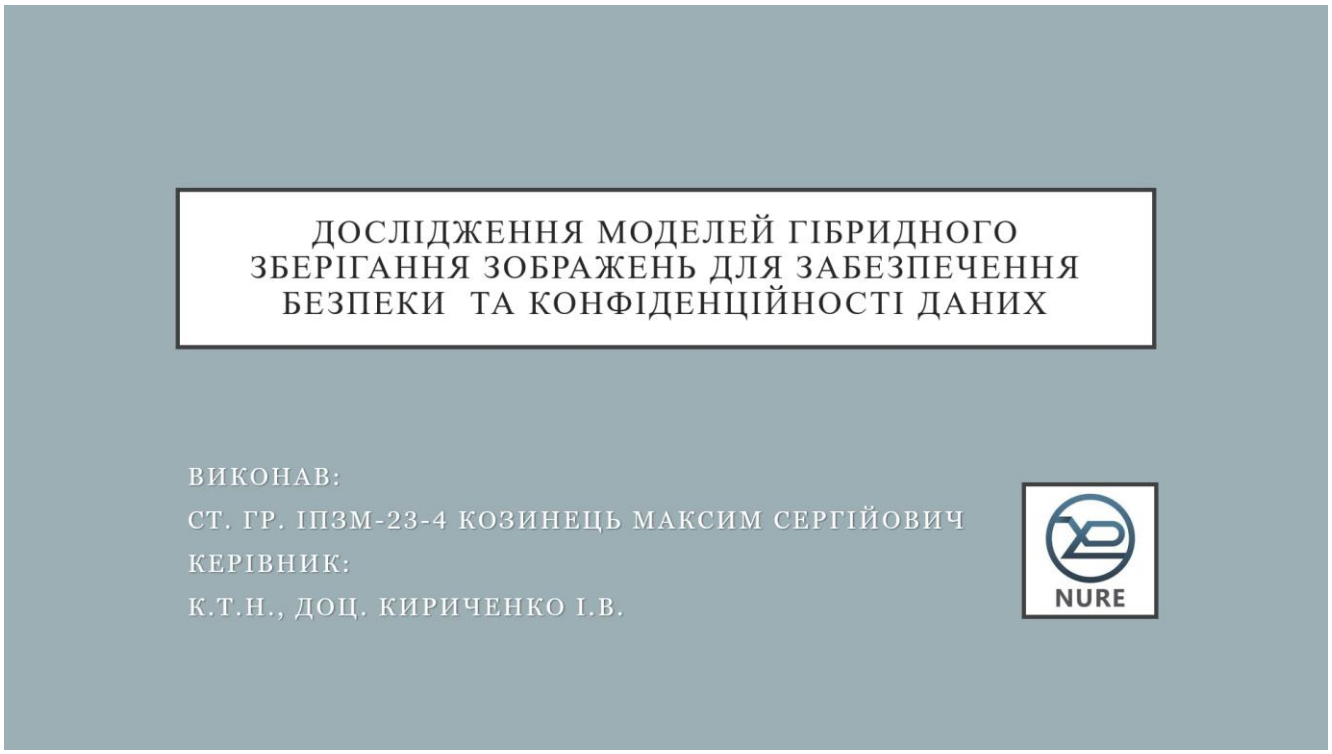

Рисунок В.1 – Презентація дипломної роботи (слайд 1)

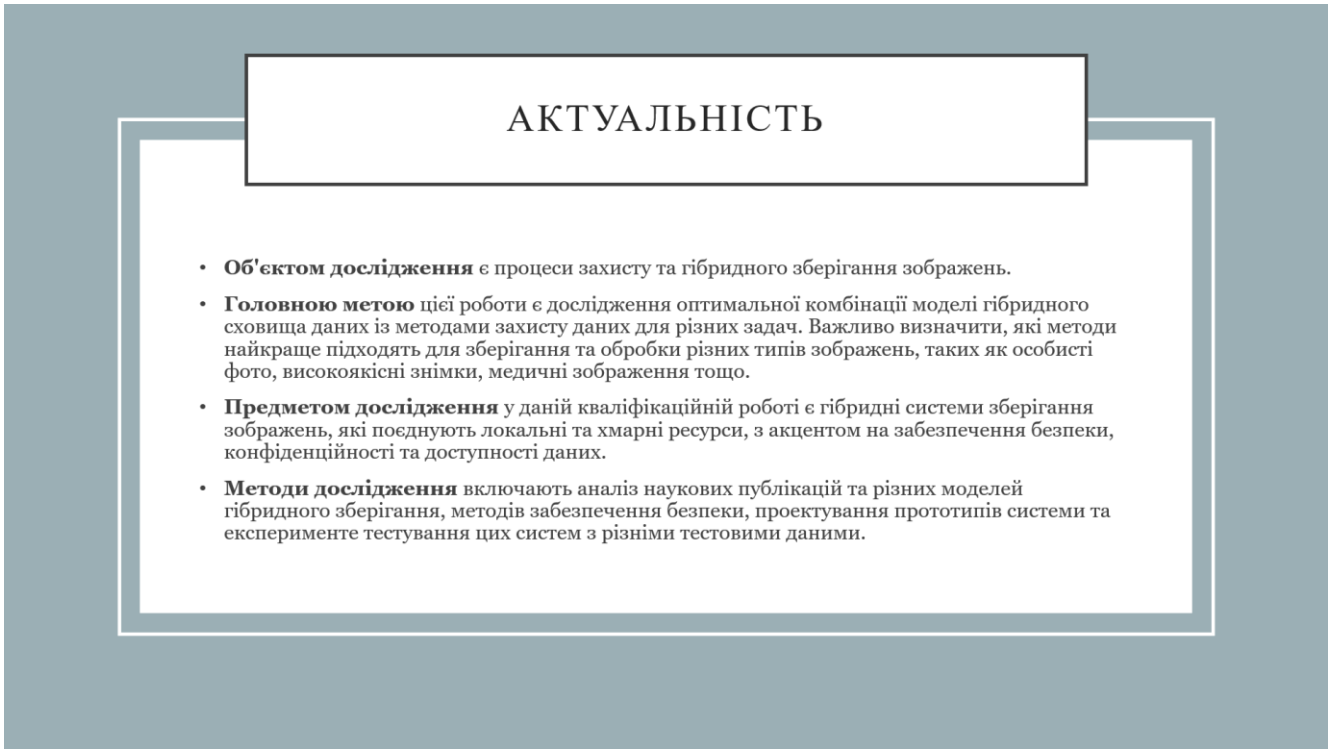

Рисунок В.2 – Презентація дипломної роботи (слайд 2)

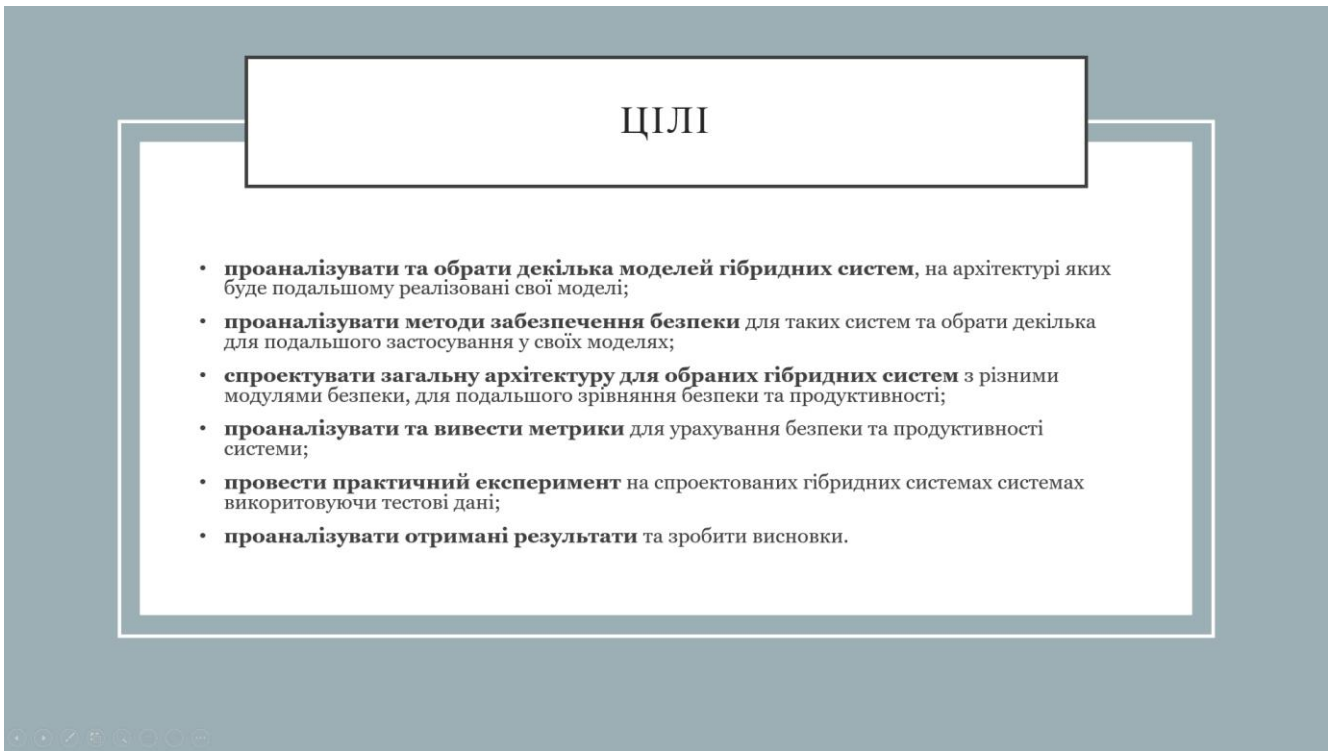

Рисунок В.3 – Презентація дипломної роботи (слайд 3)

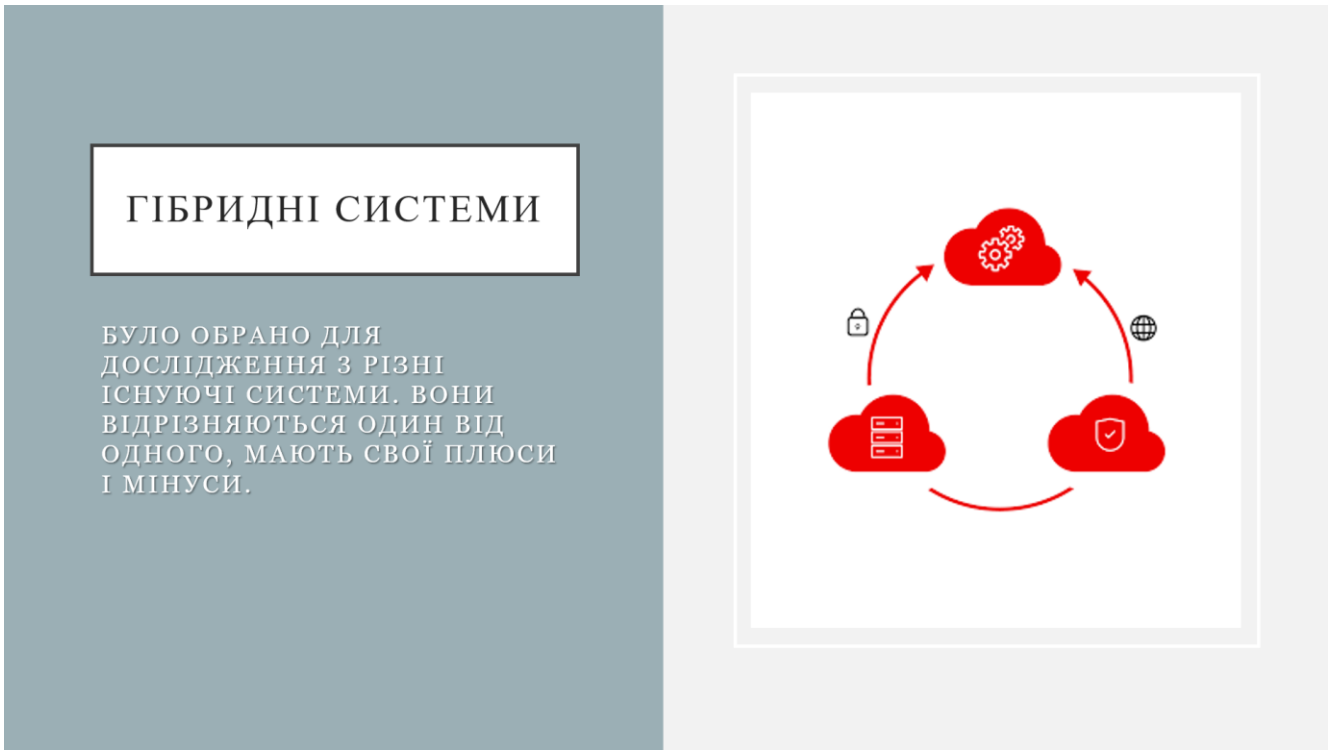

Рисунок В.4 – Презентація дипломної роботи (слайд 4)

ТЕХНОЛОГІЇ БЛОКЧЕЙН З ТРАДИЦІЙНОЮ СИСТЕМОЮ БАЗ ДАНИХ

ПЕРЕВАГИ:

- АУДИТ, ЗАХИСТ ВІД НЕСАНКЦІОНОВАНИХ ЗМІН І МОЖЛИВІСТЬ ВІДСТЕЖЕННЯ ДОСТУПУ ДО ФАЙЛІВ;
- ЗБЕРІГАННЯ ВЕЛИКОЇ КІЛЬКОСТІ ЗОБРАЖЕНЬ;
- СИНХРОНІЗАЦІЯ ЗАПИСІВ, ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ДАНИХ В СИСТЕМІ.

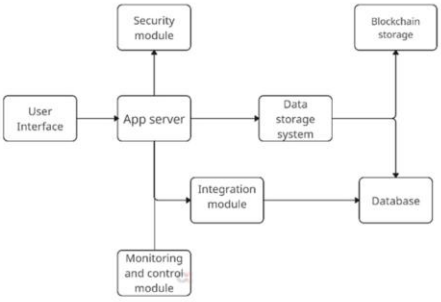

Рисунок В.5 – Презентація дипломної роботи (слайд 5)

АРХІТЕКТУРА БАГАТОВИМІРНОГО СХОВИЩА ДАНИХ

ПЕРЕВАГИ:

- КЕШУВАННЯ;
- МОЖЛИВІСТЬ ОТРИМУВАТИ АГРЕГОВАНІ ДАНІ, ЯКІ КОРИСНІ ДЛЯ АНАЛІТИКИ ТА ПРИЙНЯТТЯ БІЗНЕС-РІШЕНЬ.

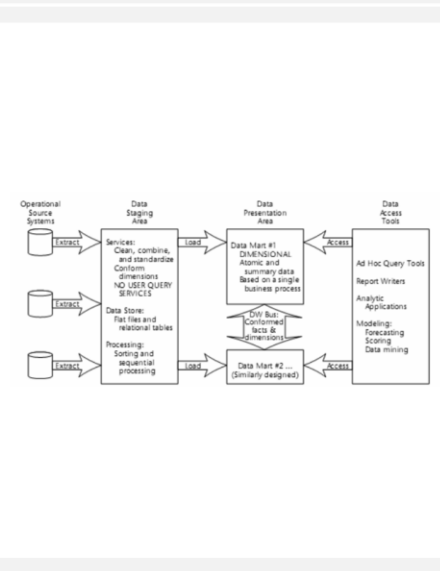

Рисунок В.6 – Презентація дипломної роботи (слайд 6)

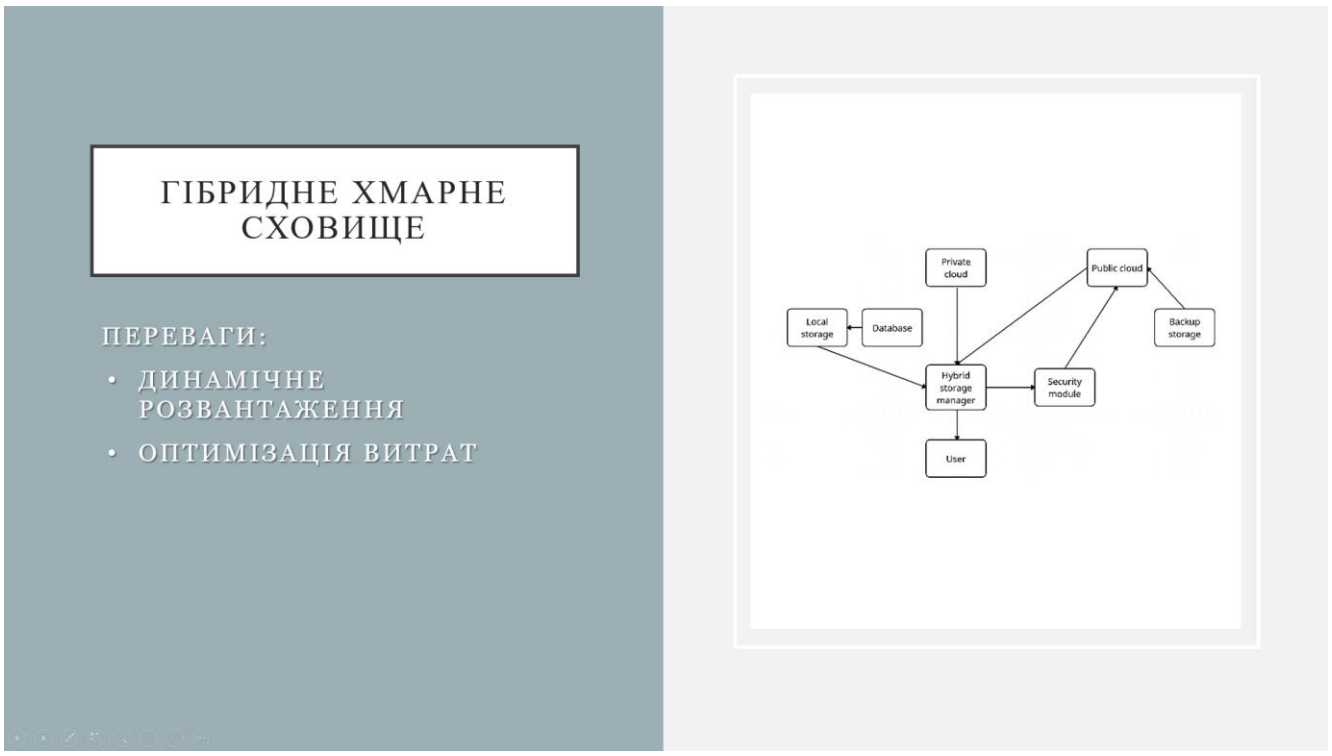

Рисунок В.7 – Презентація дипломної роботи (слайд 7)

Алгоритм	Тип	Ключ	Сильні сторони	Обмеження
AES-256	Симетричний	256-bit	Безпечний, швидкий	—
RSA	Асиметричний	2048+	Дуже безпечний	Повільний
XOR	Побітовий	Довільний	Дуже швидкий	Слабкий захист
Fisher-Yates	Перестановка	—	Простий	Нестабільна кореляція
DNA	Біоінспірований	Залежить від кодування ДНК	Стійкий до атак	Складність реалізації

Рисунок В.8 – Презентація дипломної роботи (слайд 8)

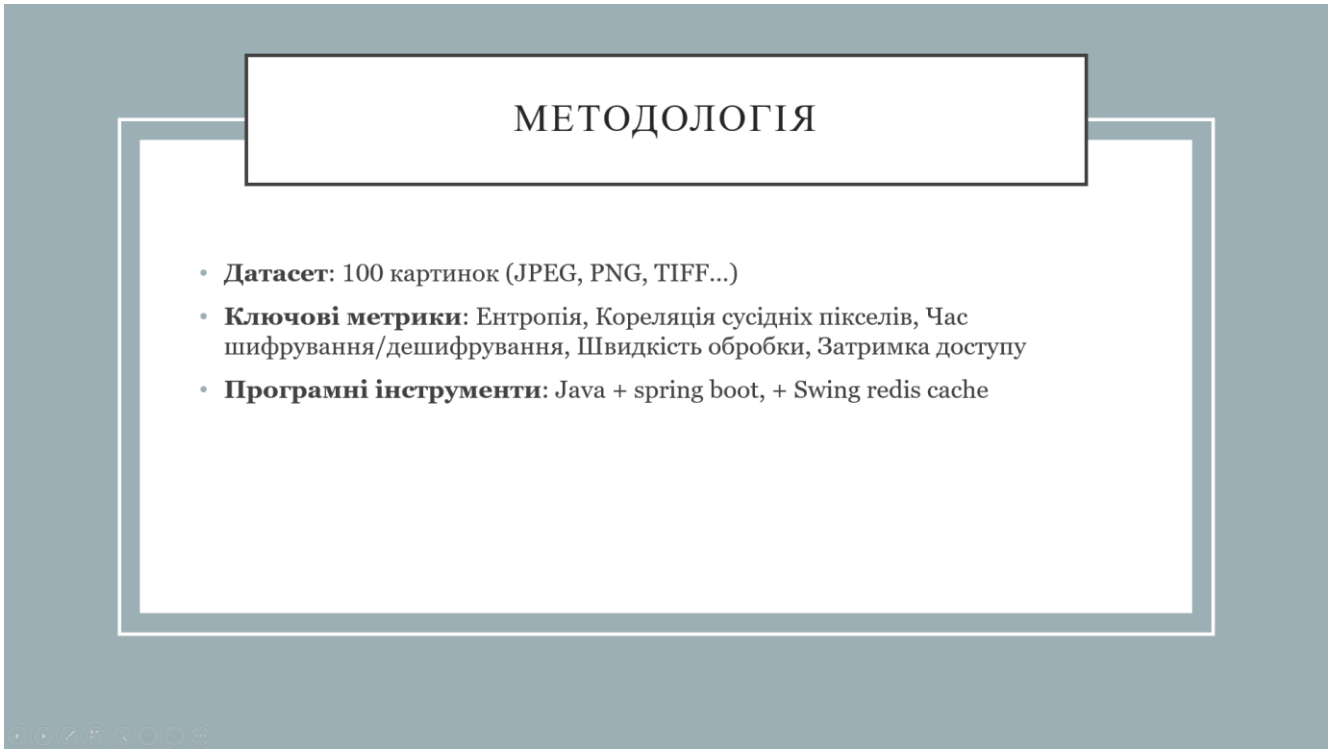

Рисунок В.9 – Презентація дипломної роботи (слайд 9)

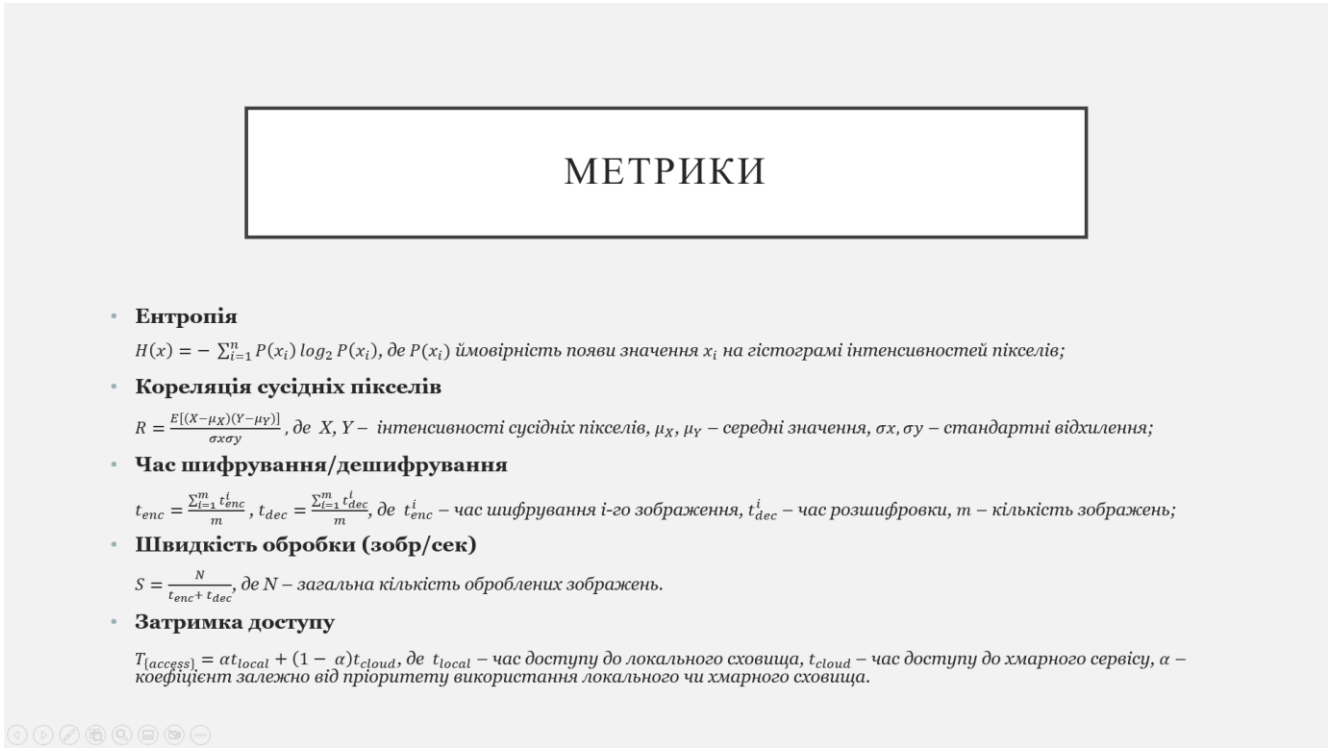

Рисунок В.10 – Презентація дипломної роботи (слайд 10)

Рисунок В.11 – Презентація дипломної роботи (слайд 11)

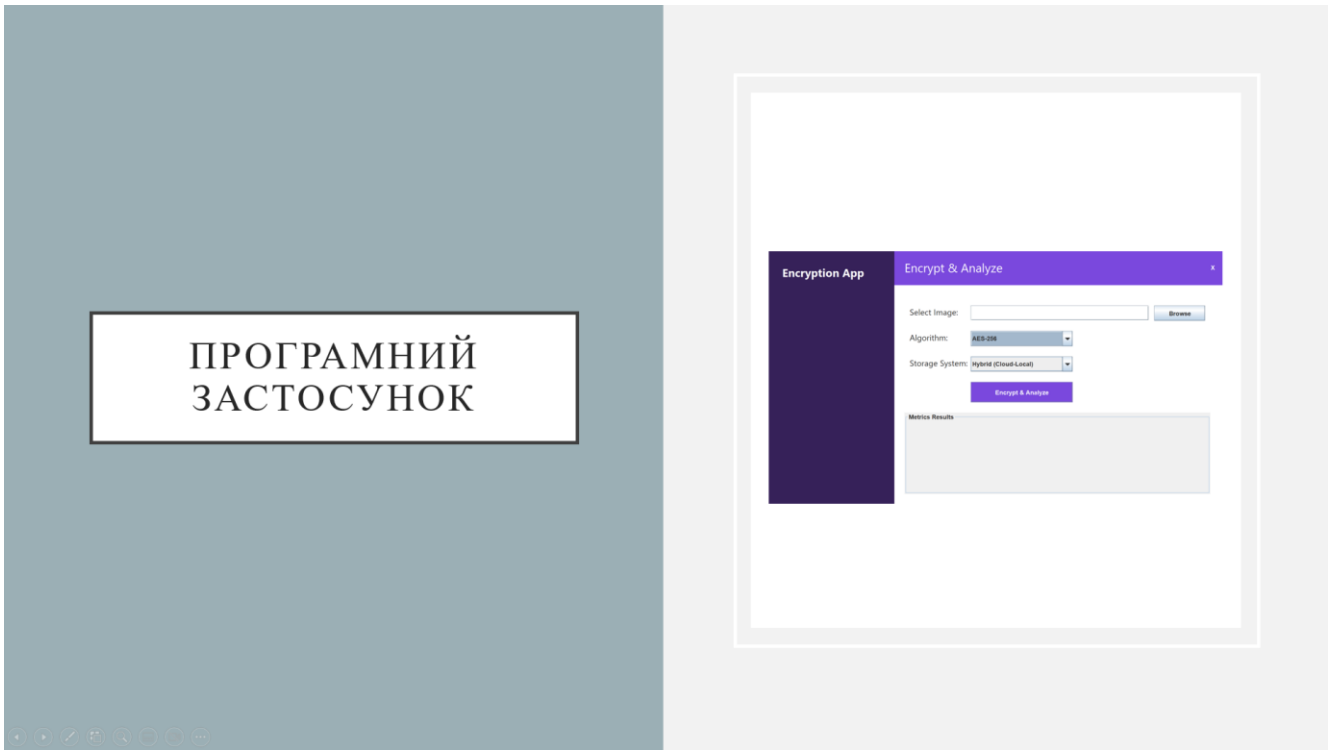

Рисунок В.12 – Презентація дипломної роботи (слайд 12)

СИСТЕМА	АЛГОРИТМ	ЕНТРОПІЯ	ЧАС ШИФРУВАННЯ, МС	ШВИДКІСТЬ ОБРОБКИ, ЗОБР/СЕК	ВИСНОВОК
Blockchain+DB	AES	7.983	162	3.19	Безпечно але повільно
DWH	XOR	7.503	102	3.07	Найшвидший
Router + Cloud	AES	7.892	132	3.52	Оптимальний баланс

Рисунок В.13 – Презентація дипломної роботи (слайд 13)

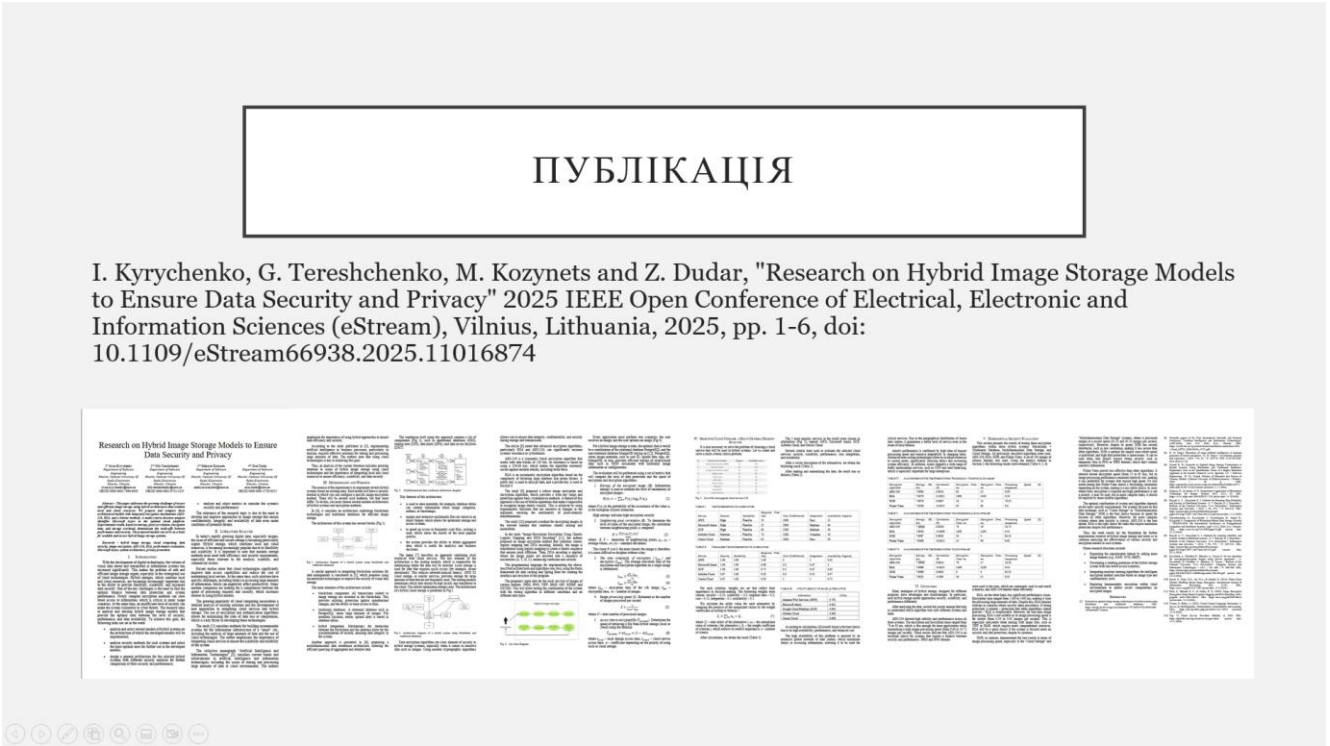

Рисунок В.14 – Презентація дипломної роботи (слайд 14)

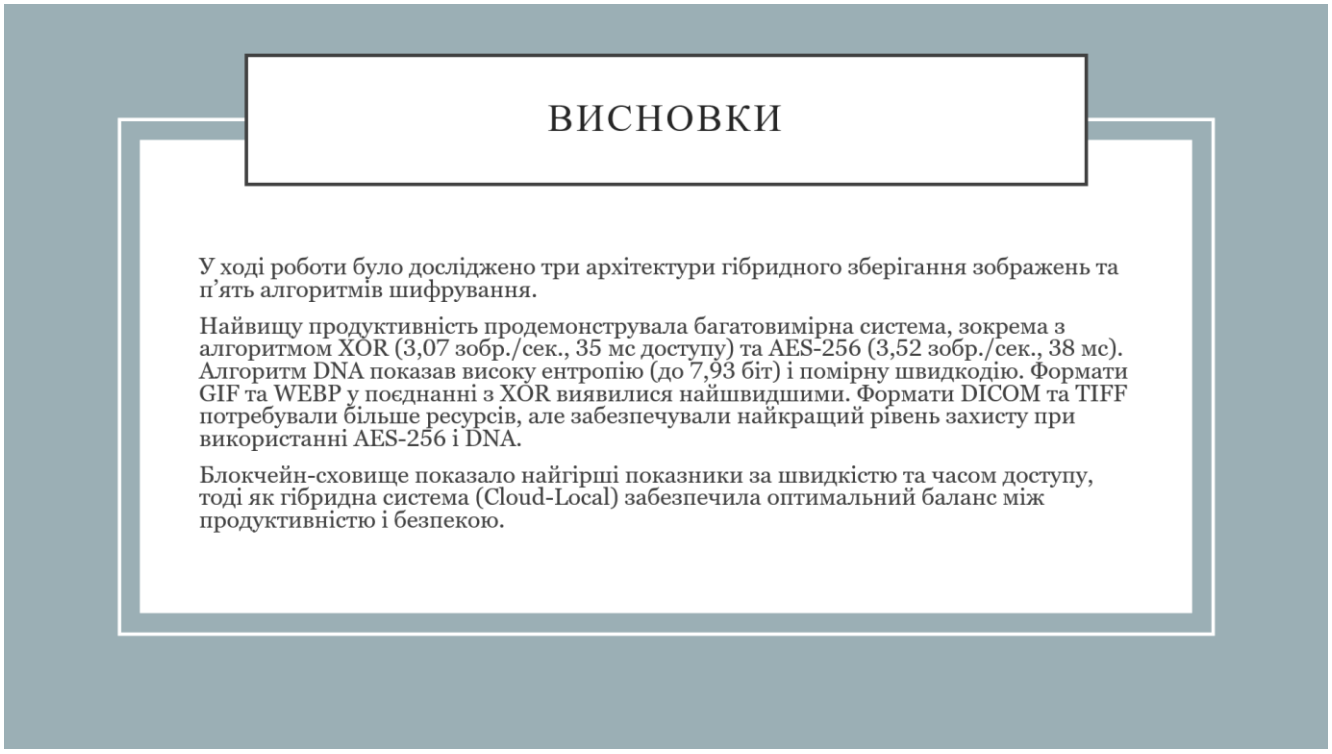

Рисунок В.15 – Презентація дипломної роботи (слайд 15)

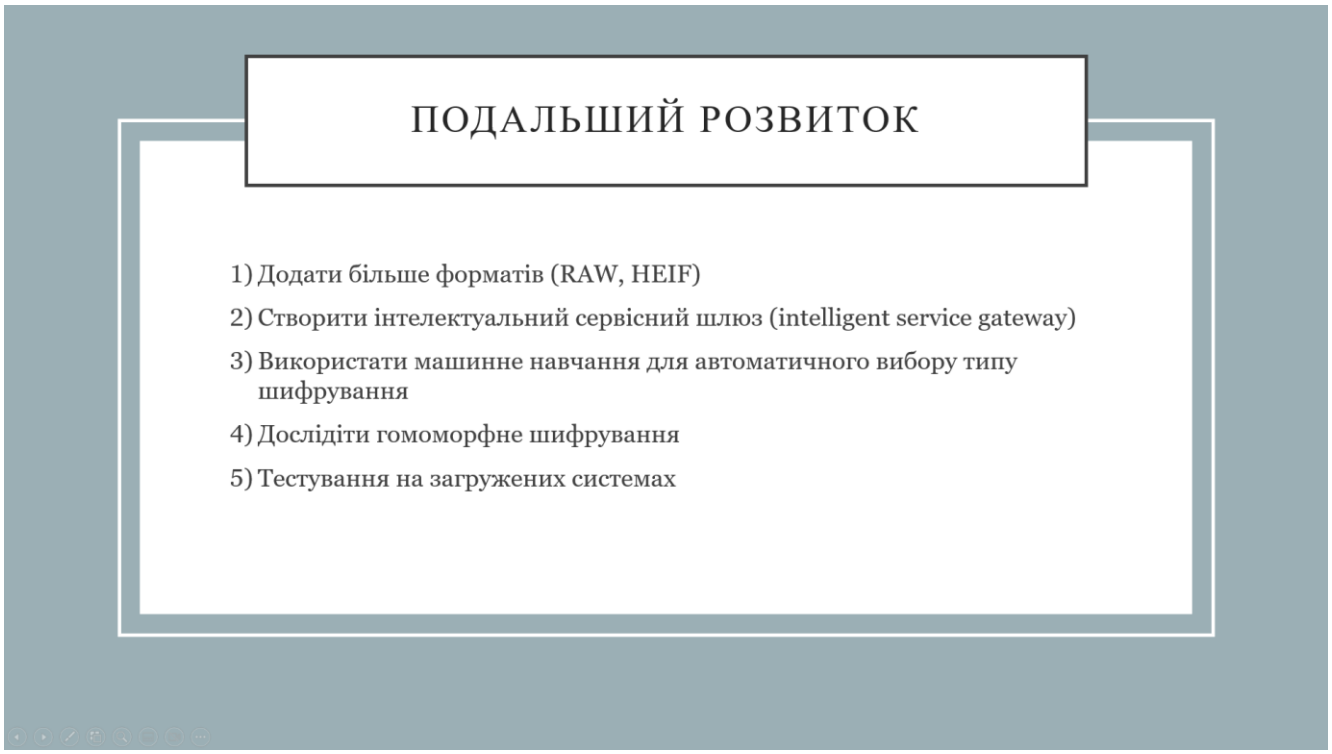

Рисунок В.16 – Презентація дипломної роботи (слайд 16)

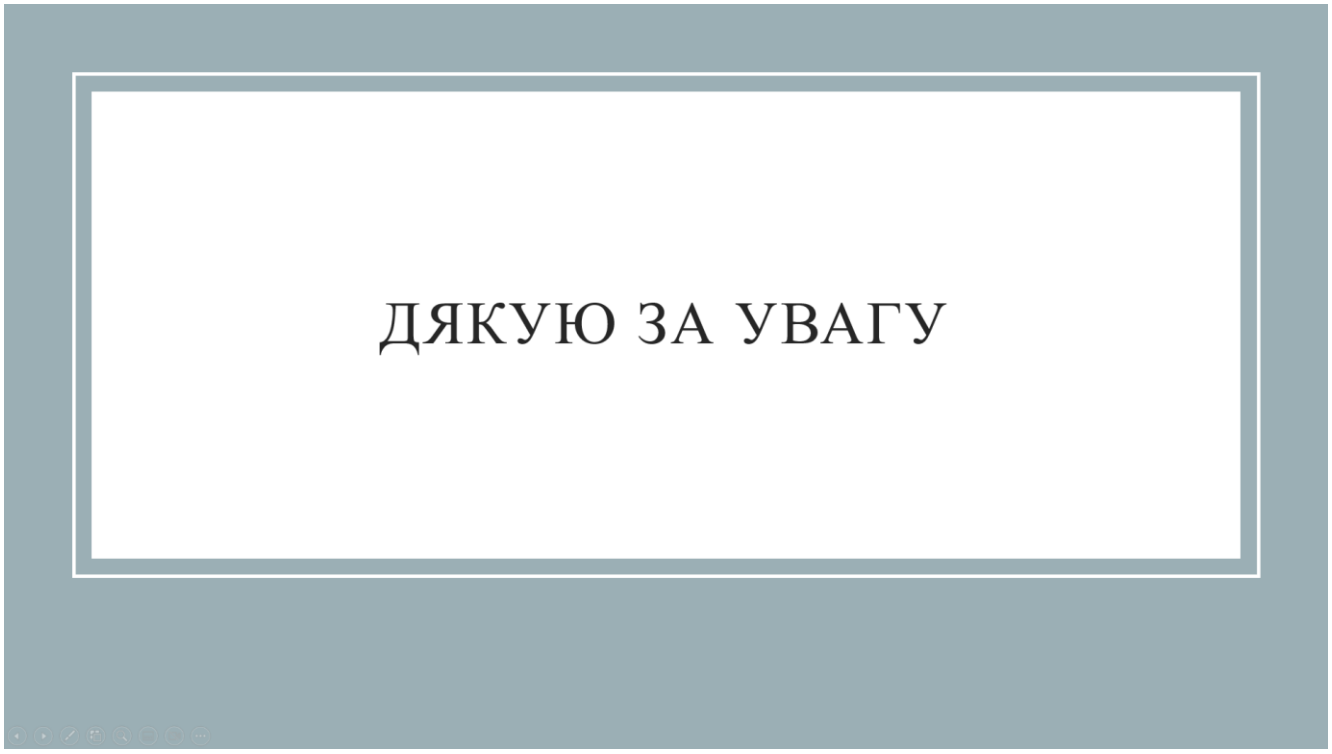

Рисунок В.17 – Презентація дипломної роботи (слайд 17)

Додаток Г

АПРОБАЦІЯ РЕЗУЛЬТАТІВ РОБОТИ

Рисунок Г.1 – Головна сторінка статті

Research on Hybrid Image Storage Models to Ensure Data Security and Privacy

1st Iryna Kyrychenko
Department of Software Engineering
Kharkiv National University Of Radio Electronics
Kharkiv, Ukraine
iryna.kyrychenko@nure.ua
ORCID 0000-0002-7686-6439

2nd Glib Tereshchenko
Department of Software Engineering
Kharkiv National University Of Radio Electronics
Kharkiv, Ukraine
hlib.tereshchenko@nure.ua
ORCID 0000-0001-8731-2135

3rd Maksym Kozynets
Department of Software Engineering
Kharkiv National University Of Radio Electronics
Kharkiv, Ukraine
maksym.kozynets@nure.ua

4th Zoia Dudar
Department of Software Engineering
Kharkiv National University Of Radio Electronics
Kharkiv, Ukraine
zoia.dudar@nure.ua
ORCID 0000-0001-5728-9253

***Abstract* – This paper addresses the growing challenge of secure and efficient image storage using hybrid architectures that combine local and cloud resources. We propose and compare three architectural models with integrated encryption mechanisms (AES-256, RSA, and a bitwise method). A multi-criteria decision analysis identifies Microsoft Azure as the optimal cloud platform. Experimental results, based on entropy, pixel correlation, encryption time, and storage overhead, demonstrate the trade-offs between performance and security. The proposed models can serve as a basis for scalable and secure hybrid image storage systems.**

***Keywords* – hybrid image storage, cloud computing, data security, image encryption, AES-256, RSA, performance evaluation, Microsoft Azure, system architecture, privacy protection.**

I. Introduction

With the development of digital technologies, the volume of visual data stored and transmitted in information systems has increased significantly. This makes the problem of safe and efficient image storage urgent, especially in the widespread use of cloud technologies. Hybrid storages, which combine local and cloud resources, are becoming increasingly important due to the ability to provide flexibility, scalability, and increased data security. One of the key challenges is the need to find the optimal balance between data protection and system performance. Overly complex encryption methods can slow down access to information, which is critical in many usage scenarios. At the same time, an insufficient level of security can make the system vulnerable to cyber threats. The research aims to analyze and develop hybrid image storage models that provide the optimal ratio between the level of security, performance, and data availability. To achieve this goal, the following tasks are set in the work:

- analyze and select several models of hybrid systems on the architecture of which the developed models will be implemented;
- analyze security methods for such systems and select the most optimal ones for further use in the developed models;
- design a general architecture for the selected hybrid systems with different security modules for further comparison of their security and performance;
- analyze and select metrics to consider the system's security and performance.

The relevance of the research topic is due to the need to develop and improve approaches to image storage that ensure confidentiality, integrity, and availability of data even under conditions of potential threats.

II. Literature Analysis

In today's rapidly growing digital data, especially images, the issue of efficient and secure storage is becoming particularly urgent. Hybrid storage, which combines local and cloud resources, is becoming increasingly popular due to its flexibility and scalability. It is important to note that modern storage methods must meet both efficiency and security requirements, especially those relevant to the medical, scientific, and commercial sectors.

Recent studies show that cloud technologies significantly improve data access capabilities and reduce the cost of maintaining local servers. At the same time, such solutions have specific challenges, including delays in accessing large amounts of information, which can negatively affect productivity. Many modern companies are looking for a compromise between the speed of processing requests and security, which increases interest in using hybrid models.

The growing popularity of cloud computing necessitates a detailed analysis of existing solutions and the development of new approaches to integrating cloud services into hybrid storage. The use of encryption and authentication algorithms allows for minimizing the risks of data loss or compromise, which is a key factor in developing these technologies.

The study [1] considers methods for building recommender systems for the information infrastructure of a "smart" city, including the analysis of large amounts of data and the use of cloud technologies. The author emphasizes the importance of integrating cloud services to ensure the scalability and reliability of the system.

The collective monograph "Artificial Intelligence and Information Technologies" [2] considers current trends and achievements in artificial intelligence and information technologies, including the issues of storing and processing large amounts of data in cloud environments. The authors

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE

Рисунок Г.2 – Стаття «Research on Hybrid Image Storage Models to Ensure Data Security and Privacy» (сторінка 1)

emphasize the importance of using hybrid approaches to ensure data efficiency and security.

According to the study published in [3], implementing artificial intelligence in business processes, particularly in tourism, requires effective solutions for storing and processing large amounts of data. The authors note that using cloud technologies is key to achieving this goal.

Thus, an analysis of the current literature indicates growing attention to issues of hybrid image storage using cloud technologies and the importance of integrating local and cloud resources to ensure efficiency, scalability, and data security.

III. Methodology and Working

The essence of the experiment is to implement several hybrid systems based on existing ones. Each model will have a security module in which you can configure a specific image encryption method. There will be several such methods, but they must differ. To do this, you must choose several modern architectures of hybrid systems and encryption methods.

In [4], it considers an architecture combining blockchain technologies and traditional databases for efficient image storage.

The architecture of this system has several blocks (Fig 1).

Fig. 1. Architecture diagram of a hybrid system using blockchain and traditional databases

A similar approach to integrating blockchain solutions for data management is considered in [5], which proposes using decentralized technologies to improve the security of visual data storage.

The main elements of this architecture include:

- blockchain component. All transactions related to image storage are recorded in the blockchain. This provides auditing, protection against unauthorized changes, and the ability to track access to files;
- traditional databases. A relational database such as PostgreSQL stores large amounts of images. File metadata (location, owner, upload date) is stored in database tables;
- hybrid integration. Mechanisms for interaction between the blockchain and the database allow for the synchronization of records, ensuring data integrity in the system.

Another approach is presented in [6], proposing a multidimensional data warehouse architecture, allowing for efficient querying of aggregated and detailed data.

The warehouse built using this approach contains a list of components (Fig 2), such as operational databases (OSS), staging area (DSS), data marts (DPA), and data access facilities (DAT).

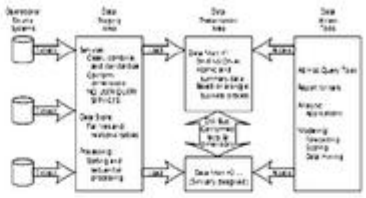

Fig. 2. Multidimensional data warehouse architecture diagram

Key features of this architecture:

- is used to store metadata; for example, database tables can contain information about image categories, authors, or timestamps;
- images and extensive multimedia files are stored in an object format, which allows for optimized storage and access to them;
- to speed up access to frequently used files, caching is used, which stores the results of the most popular queries;
- the system provides the ability to obtain aggregated data, which is useful for analytics and business decisions.

The paper [7] describes an approach combining local resources with cloud services. The key element of the architecture is the routing module, which is responsible for determining where the data will be directed. Local storage is used for data that requires quick access (for example, recent downloads). This reduces network-induced latency. AWS S3 cloud storage, or similar services, provides storage for large amounts of data that are not frequently used. The routing module determines which data should be kept locally and transferred to the cloud. This allows optimizing storage costs. The architecture of a hybrid cloud storage is presented in Fig 3.

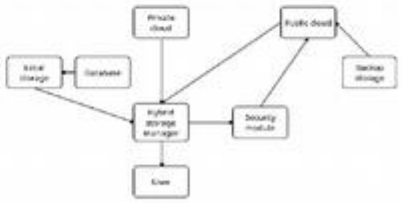

Fig. 3. Architecture diagram of a hybrid system using blockchain and traditional databases

Data encryption algorithms are a key element of security in hybrid storage systems, especially when it comes to sensitive data such as images. Using modern cryptographic algorithms

Рисунок Г.3 – Стаття «Research on Hybrid Image Storage Models to Ensure Data Security and Privacy» (сторінка 2)

allows you to ensure data integrity, confidentiality, and security during storage and transmission.

The article [8] noted that advanced encryption algorithms, particularly RSA and AES-256, can significantly increase systems' resistance to cyberattacks.

AES-256 is a symmetric block encryption algorithm that works with data blocks of 128 bits. Its resistance is based on using a 256-bit key, which makes the algorithm extremely secure against modern attacks, including brute force.

RSA is an asymmetric encryption algorithm based on the complexity of factoring large numbers into prime factors. A public key is used to encrypt data, and a private key is used to decrypt it.

The study [9] proposed a robust image encryption and decryption algorithm, which provides a wide key range and protection against basic cryptanalysis methods. A feature of this approach is the use of bitwise operations that make it impossible to recognize image details visually. This is achieved by using trigonometric functions that are sensitive to changes in the argument, ensuring the nonlinearity of pixel-intensity transformations.

The study [10] proposed a method for encrypting images in the wavelet domain that combines chaotic mixing and modulation.

In the study "Image Encryption Decryption Using Chaotic Logistic Mapping and DNA Encoding" [11], the authors proposed an image encryption method that combines chaotic logistic mapping and DNA encoding. Initially, the image is transformed using logistic mapping to create a chaotic sequence that ensures pixel diffusion. Then, DNA encoding is applied, where the image pixels are encoded into a sequence of nucleotides (A, T, G, C), enhancing confusion and security.

The programming language for implementing the above-described architectures and algorithms was Java, using the Redis framework for data caching and Spring Boot for creating the interface and structure of the program.

The program's input data for the study are lists of images of various formats: JPEG, PNG, TIFF, BMP, GIF, WEBP, and DICOM. This will allow testing the combination of the system with the testing algorithm in different conditions and on different data types.

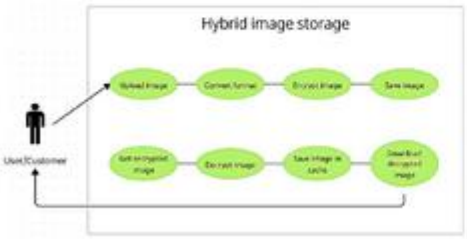

Fig. 4. Use Case Diagram

Every application must perform two scenarios: the user receives an image, and the user uploads an image (Fig 4).

For a hybrid image storage system, the optimal choice would be a combination of the relational database PostgreSQL and the non-relational database MongoDB relying on [12]. PostgreSQL stores image metadata, such as user ID, upload date, tags, etc. MongoDB, in turn, provides efficient storage of unstructured data, such as JSON documents with additional image information or configurations.

The evaluation will be performed using a set of metrics that will compare the level of data protection and the speed of encryption and decryption algorithms.

1. *Entropy of the encrypted image (H).* Information entropy is used to estimate the level of randomness of encrypted images.:

$$H(x) = -\sum_{i=1}^{n} P(x_i)\log_2 P(x_i), \quad (1)$$

where $P(x_i)$is the probability of the occurrence of the value x_i in the histogram of pixel intensities.

High entropy indicates high encryption security.

2. *Neighboring pixel correlation (R).* To determine the level of chaos of the encrypted image, the correlation between neighbouring pixels is compared:

$$R = \frac{E[(X-\mu_X)(Y-\mu_Y)]}{\sigma x \sigma y} \quad (2)$$

where X, Y – intensities of neighbouring pixels, μ_X, μ_Y – average values, σx, σy – standard deviations.

The closer R is to 0, the more chaotic the image is; therefore, it is more difficult to decipher without a key.

3. *The time complexity of encryption (t_{enc}) and decryption (t_{dec}).* The average execution time of the encryption and decryption algorithm on a single image is determined:

$$t_{enc} = \frac{\sum_{i=1}^{m} t_{enc}^{i}}{m}, \quad (3)$$

$$t_{dec} = \frac{\sum_{i=1}^{m} t_{dec}^{i}}{m} \quad (4)$$

where t_{enc}^{i} – encryption time of the i-th image, t_{dec}^{i} – decryption time, m – number of images.

4. *Image processing speed (S).* Estimated as the number of images processed per second:

$$S = \frac{N}{t_{enc} + t_{dec}} \quad (5)$$

where N – total number of processed images.

5. *Access time to encrypted file ($T_{[access]}$).* Determines the speed of retrieving a file from hybrid storage (local or cloud) using the formula:

$$T_{[access]} = \alpha t_{local} + (1-\alpha)t_{cloud} \quad (6)$$

where t_{local} – local storage access time, t_{cloud} – cloud service access time, α – coefficient depending on the priority of using local or cloud storage.

Рисунок Г.4 – Стаття «Research on Hybrid Image Storage Models to Ensure Data Security and Privacy» (сторінка 3)

IV. Selecting Cloud Storage: A Multi-Criteria Decision Analysis

It is also necessary to solve the problem of choosing a cloud service that will be used in hybrid systems. Let us create and solve a multi-criteria choice problem.

#	Cloud Service Provider	Regions	Availability Zones
1	Amazon Web Services (AWS)	33	105
2	Microsoft Azure	64	126
3	Google Cloud Platform (GCP)	40	121
4	Alibaba Cloud	30	89
5	Oracle Cloud	48	58
6	IBM Cloud	10	30
7	Tencent Cloud	21	65
8	OVHcloud	17	37
9	DigitalOcean	9	13
10	Linode (Akamai)	20	20

Fig. 5. List of the most popular cloud services [15]

The 5 most popular services in the world were chosen as alternatives (Fig. 5), namely AWS, Microsoft Azure, GCP, Alibaba Cloud, and Oracle Cloud.

Several criteria were used to evaluate the selected cloud services: security, scalability, performance, cost, integration, and availability.

After a vector description of the alternatives, we obtain the following result (Table 1).

After ranking and normalizing the data, the result was as follows (Table 2).

TABLE I VECTOR DESCRIPTION OF ALTERNATIVES

Service	*Security*	*Scalability*	*Response Time (ms)*	*Cost (UAH/month)*	*Integration*	*Availability (regions)*
AWS	High	Flexible	50	3000	Easy	33
Microsoft Azure	High	Flexible	55	2800	Medium	64
GCP	High	Flexible	60	2500	Medium	40
Alibaba Cloud	Medium	Flexible	70	2200	Complex	30
Oracle Cloud	Medium	Flexible	65	2000	Easy	48

TABLE II NORMALIZED VECTOR DESCRIPTION OF ALTERNATIVES

Service	*Security*	*Scalability*	*Response Time (ms)*	*Cost (UAH/month)*	*Integration*	*Availability (regions)*
AWS	1.00	1.00	1.00	0	1	0.41
Microsoft Azure	1.00	1.00	0.89	0.2	0.67	1
GCP	1.00	1.00	0.75	0.5	0.67	0.63
Alibaba Cloud	0.67	1.00	0.50	0.8	0.33	0.47
Oracle Cloud	0.67	1.00	0.58	1	1	0.75

For each criterion, weights are set that reflect their importance in decision-making. The following weights were chosen: security – 0.25; scalability – 0.2; response time – 0.2; cost – 0.15; integration – 0.1; availability – 0.1.

We calculate the utility value for each alternative by summing the products of the normalized values by the weight coefficients according to formula 7:

$$Z_i = \sum_{j=1}^{n} \alpha_{ij} * \beta_j, \quad (7)$$

where Zi – total utility of the alternative i; α_{ij} – the normalized value of criterion j for alternative i; β_j – the weight coefficient of criterion j, which reflects its relative importance; n – number of criteria.

After calculations, we obtain the result (Table 3).

TABLE III. UTILITY RESULT OF EACH ALTERNATIVE

Alternative	*Utility*
Amazon Web Services (AWS)	0.791
Microsoft Azure	0.825
Google Cloud Platform (GCP)	0.805
Alibaba Cloud	0.668
Oracle Cloud	0.809

According to calculations, Microsoft Azure is the best choice due to its high availability, performance, and balanced cost.

The high availability of this platform is ensured by an extensive global network of data centers, which minimizes delays in accessing information, allowing it to be used for

Рисунок Г.5 – Стаття «Research on Hybrid Image Storage Models to Ensure Data Security and Privacy» (сторінка 4)

critical services. Due to the geographical distribution of Azure data centres, it guarantees a stable level of service even in the event of local failures.

Azure's performance is confirmed by high rates of request processing speed and resource adaptability to changing loads. Advanced auto-scaling technologies allow us to adjust resources to current needs, significantly reducing delays and increasing system efficiency. In addition, Azure supports a wide range of traffic optimization services, such as CDN and load balancing, which is especially important for large enterprises.

V. Experimental Security Evaluation

This section presents the results of testing three encryption algorithms within three hybrid systems: Blockchain + Traditional Database, Multidimensional Data Storage, and Cloud Storage. All previously described algorithms were used: AES-256, RSA, XOR, and Fisher-Yates. A set of 100 images of various formats was used. Using the metrics defined in Section 3, the following results were obtained (Table 4, 5, 6).

TABLE IV. ANALYSIS RESULTS FOR THE HYBRID SYSTEM "BLOCKCHAIN + TRADITIONAL DATABASE"

Encryption Algorithm	*Entropy (H), bits*	*Correlation (R)*	*Encryption Time, ms*	*Decryption Time, ms*	*Processing Speed (S), images/sec*
AES-256	7.9982	0.0015	92	25	9.80
RSA	7.9870	-0.0012	1400	1450	0.34
XOR	7.9970	0.0007	18	11	70.52
Fisher-Yates	7.9500	-0.0015	65	60	8.8

TABLE V. ANALYSIS RESULTS FOR THE HYBRID SYSTEM "MULTIDIMENSIONAL DATA STORAGE"

Encryption Algorithm	*Entropy (H), bits*	*Correlation (R)*	*Encryption Time, ms*	*Decryption Time, ms*	*Processing Speed (S), images/sec*
AES-256	7.9996	0.0020	78	16	10.75
RSA	7.9918	-0.0009	1189	1240	0.41
XOR	7.9987	0.0005	10	4	83.33
Fisher-Yates	7.9608	-0.0011	55	48	9.62

TABLE VI. ANALYSIS RESULTS FOR THE HYBRID SYSTEM "CLOUD STORAGE"

Encryption Algorithm	*Entropy (H), bits*	*Correlation (R)*	*Encryption Time, ms*	*Decryption Time, ms*	*Processing Speed (S), images/sec*
AES-256	7.9998	0.0022	79	17	10.42
RSA	7.9896	-0.0012	1168	1229	0.42
XOR	7.9989	0.0003	8	4	83.33
Fisher-Yates	7.9621	-0.009	56	51	9.35

VI. Conclusion

Many analogues of hybrid storage, designed for different purposes, have advantages and disadvantages. In particular, each hybrid storage model approaches security, scalability, and performance differently.

After analyzing the data, several key points emerge that help us understand which algorithm best suits different systems and tasks.

AES-256 showed high stability and performance across all three systems. The encryption and decryption times ranged from 78 to 92 ms, which is fast enough for most applications while maintaining a high image processing speed (from 9.80 to 10.75 images per second). These results indicate that AES-256 is an excellent choice for systems that require a balance between security and performance. JPEG and PNG formats were used in the tests, which are commonly used in real-world scenarios, and AES-256 handles them efficiently.

RSA, on the other hand, has significant performance issues. Encryption time ranged from 1168 to 1400 ms, making it slow for processing large amounts of data. Despite this, RSA remains relevant in scenarios where security takes precedence. If strong protection is needed – protection that other algorithms cannot provide – RSA is irreplaceable. However, for real-time image processing, RSA is not suitable as its image processing speed is far slower (from 0.34 to 0.42 images per second). This is especially noticeable when dealing with larger files, such as TIFF or BMP, which require more computational resources. RSA will be a good choice if the system is focused more on security and data protection, despite its slowness.

XOR, in contrast, demonstrated the best results in terms of image processing speed, especially in the "Cloud Storage" and

Рисунок Г.6 – Стаття «Research on Hybrid Image Storage Models to Ensure Data Security and Privacy» (сторінка 5)

"Multidimensional Data Storage" systems, where it processed images at a record speed (83.33 and 83.33 images per second, respectively). However, despite its speed, XOR has several drawbacks, such as low correlation, making it less secure than other algorithms. XOR is optimal for simple cases where speed is prioritised, and high data protection is unnecessary. It can be used when data doesn't require strong security, such as temporary files in PNG or JPEG formats, which don't contain sensitive information.

Fisher-Yates proved less effective than other algorithms. It showed decent encryption speed (from 55 to 65 ms), but its image processing performance remained relatively low, making it less preferable for systems that require high speed. It's also worth noting that Fisher-Yates shows a fluctuating correlation depending on the system, making it a less stable choice. In cases where basic encryption is required and high performance is not a priority, it may be used, but in more complex tasks, it should be replaced by more reliable algorithms.

The optimal combination of system and algorithm depends on the task's specific requirements. For systems focused on fast data exchange, such as "Cloud Storage" or "Multidimensional Data Storage," XOR is the best choice because its speed far exceeds all other algorithms. However, for more complex systems where data security is critical, AES-256 is the best option. RSA is the right choice for tasks that require maximum protection despite low performance.

Thus, the work results lay the foundation for further experimental research of hybrid image storage and allow us to continue analysing the effectiveness of various security and encryption models in such systems.

Future research directions include:

- Expanding the experimental dataset by adding more image formats (e.g., RAW, SVG, HEIF);
- Developing a working prototype of the hybrid storage system with real-world access scenarios;
- Integrating machine learning algorithms for intelligent encryption method selection based on image type and confidentiality level;
- Exploring homomorphic encryption within cloud environments to enable secure computations on encrypted images.

References

[1] Research on optimal image storage technologies in hybrid systems using blockchain and traditional databases. URL: https://ela.kpi.ua/server/api/core/bitstreams/797e4592-478e-4034-b8fe-1463a4c4a427/content

[2] Scientific papers of the First International Scientific and Practical Conference "Artificial Intelligence and Information Technologies" (AIIT-2024), June 3–4, 2024, Kyiv, Ukraine. URL: https://it.nuft.edu.ua/wp-content/themes/itaiu/theme/assets/docs/2024-1-Conf_AIIT01_2024-06-04_v0721.pdf

[3] K. M. Mugyl. Directions of using artificial intelligence in business processes of tourist enterprises / K. M. Mugyl // Investments: practice and experience. – 2024. – No. 23. – P. 136–141. DOI: 10.32702/2306-6814.2024.23.136

[4] Myand D. Yu. Research on Optimal Image Storage Technologies in Hybrid Systems Using Blockchain and Traditional Databases: Explanatory Note to the Qualification Thesis of a Higher Education Applicant at the Second (Master's) Level, Specialty 121 – Software Engineering / D. Yu. Myand; Ministry of Education and Science of Ukraine, Kharkiv National University of Radioelectronics. – Kharkiv, 2024. – 65 p. URL: https://openarchive.nure.ua/server/api/core/bitstreams/01d00bee-8571-48da-aadc-5e1fe77e1252/content (accessed: 11.11.2024).

[5] Koptyra, K., & Ogiela, M. R. Imagechain—Application of Blockchain Technology for Images. Sensors, 2021, 21(1), 82. URL: https://www.mdpi.com/1424-8220/21/1/82 (access date: 11/18/2024)

[6] Buryak A. V., Muzychuk O. I. Methods for Ensuring Data Reliability and Security in Distributed Systems / A. V. Buryak, O. I. Muzychuk // Bulletin of the National University "Lviv Polytechnic". Information Systems and Networks. – 2019. – No. 673. – P. 205–213. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2019/apr/15997/vis673ism-205-213.pdf (access date: 11/11/2024)

[7] Cherednichenko O., Kyrychenko I., Tereshchenko H., Miand D., Pylypenko S. Comparison of Blockchain-Based Data Storage Systems // COLINS-2024: 8th International Conference on Computational Linguistics and Intelligent Systems, April 12–13, 2024, Lviv, Ukraine. URL: https://ceur-ws.org/Vol-3688/paper10.pdf (access date: 15.12.2024).

[8] Buryak A. V., Muzychuk O. I. Methods for ensuring reliability and security of data in distributed systems / A. V. Buryak, O. I. Muzychuk // Bulletin of the National University "Lviv Polytechnic". Information systems and networks. – 2019. – No. 673. – P. 205–213. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2019/apr/15997/vis673ism-205-213.pdf (access date: 22.11.2024).

[9] Kovalchuk A., Peleshko D., Shkodyn A., Troyan O. On one algorithm for encrypting-decrypting images using bitwise operations / A. Kovalchuk, D. Peleshko, A. Shkodyn, O. Troyan // Bulletin of the National University "Lviv Polytechnic". Computer Science and Information Technologies. – 2011. – No. 694. – P. 389–394. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2024/feb/33655/vis694komp-nauky-389-394.pdf (access date: 12/15/2024).

[10] Saeed, S., Umar, M.S., Ali, M.A., & Ahmad, M. (2014). Fisher-Yates Chaotic Shuffling Based Image Encryption. International Journal of Information Processing, 8(3), 31–41. URL: https://arxiv.org/pdf/1410.7540 (access date: 12/15/2024.)

[11] Patel, S., Bharath K. P., & Muthu, R. K. (2020). Image Encryption Decryption Using Chaotic Logistic Mapping and DNA Encoding. arXiv preprint arXiv:2003.06616. URL: https://arxiv.org/pdf/2003.06616 (access date: 12/15/2024.)

[12] Turuta, O., Babiy, A. (2022). Machine Learning Algorithms for Image Classification and Sorting. Journal of Artificial Intelligence Research, 75, Article 12918. URL: https://jair.org/index.php/jair/article/view/12918 (accessed 12/15/2024).

[13] Top 10 Cloud Service Providers Globally in 2024. URL: https://dgtlinfra.com/top-cloud-service-providers/ (access date: 15.11.2024).

Рисунок Г.7 – Стаття «Research on Hybrid Image Storage Models to Ensure Data Security and Privacy» (сторінка 6)

Додаток Д

ЕКСПЕРНИЙ ВИСНОВОК РЕЗУЛЬТАТІВ ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ НА ВІДПОВІДНІСТЬ ОФОРМЛЕННЯ ВИМОГАМ ДСТУ 3008:2015

Експертний висновок результатів перевірки кваліфікаційної роботи

студент (посада) | програмної інженерії (кафедра) | ІПЗм-23-4 (група)

Максим КОЗИНЕЦЬ

(прізвище, ім'я, по батькові)

Зауваження

Пункт ДСТУ 3008-2015	Зміст пункту	Сторінка кваліфікаційної роботи
1	2	3
	7.1 Загальні положення	
	7.3 Нумерація сторінок звіту	
	7.5 Рисунки	
	7.6 Таблиці	
	7.7 Переліки	
	7.8 Примітки	
	7.9 Виноски	
	7.10 Формули та рівняння	
	7.11 Посилання	
	7.13 Список авторів	
	7.14 Скорочення та умовні позначки	
	7.15 Додатки	

Експерт _____ (підпис) Вадим НЕЧВОЛОД (прізвище, ініціали)

Робота оформлена згідно з ДСТУ 3008:2015. Зауважень немає.
13.06.2025

Рисунок Д.1 – Експерний висновок результатів перевірки кваліфікаційної роботи на відповідність оформлення вимогам ДСТУ 3008:2015