

**Секція 4. GN (Глобальні мережі, grid та cloud системи).  
Section 4. GN (Global networks, grid and cloud systems).**

UDC 004.8

Ярич Андрій

**ПИТАННЯ ВИБОРУ CLOUD-ДОДАТКУ  
НА ОСНОВІ АНАЛІЗУ GOOGLE, AMAZON ТА APPLE РІШЕНЬ**

**QUESTION OF CLOUD APP CHOOSING  
ON GOOGLE, AMAZON AND APPLE ANALYSIS**

У статті розглядається питання вибору програмного додатку хмарної технології. Для початку використовується набір даних про основні характеристики Google, Apple та Amazon рішень. Вибір базується на основі аналізу ключових параметрів. Розглядаються рішення AmazonAWS (S3), GoogleDrive та Apple iCloud.

**Ключові слова:** iCloud, Amazon, GoogleDrive, шифрування, AES.

Рис.: 3. Табл.: 0. Бібл.: 4.

The article deals with the choice of a software application for cloud technology. To begin with, it “uses” a set of data on the key features of Google, Apple and Amazon solutions. The choice is based on the analysis of key parameters. Amazon AWS (S3), Google Drive and Apple iCloud samples were considered.

**Key words:** iCloud, Amazon, Google Drive, encryption, AES.

Fig.: 3. Tabl.: 0. Bibl.: 4.

**Target setting.** Cloud technologies become more and more demand in the world; people use storage services for documents, photo and another files so it's important to have a file protection and fast downloading. Due to these facts cloud services are actual topic for discussion.

**Actual scientific researches and issues analysis.** In connection to the invention of new methods and approaches in the field of cloud technologies, the topic of cloud choosing has become more studied in recent years.

**Uninvestigated parts of general matters defining.** There are a lot of uninvestigated moments that should be opened. I am mostly going to focus on the 1TB to 2TB range for ease of comparison, and because that should address the needs of most users. I am also sticking with the big names.

**The research objective.** The purpose of this paper is to investigate the applications of the iCloud, AMAZON AWS (S3) and Google Drive. As a solution, the article will focus on data protection and price comparison, on choosing the best application.

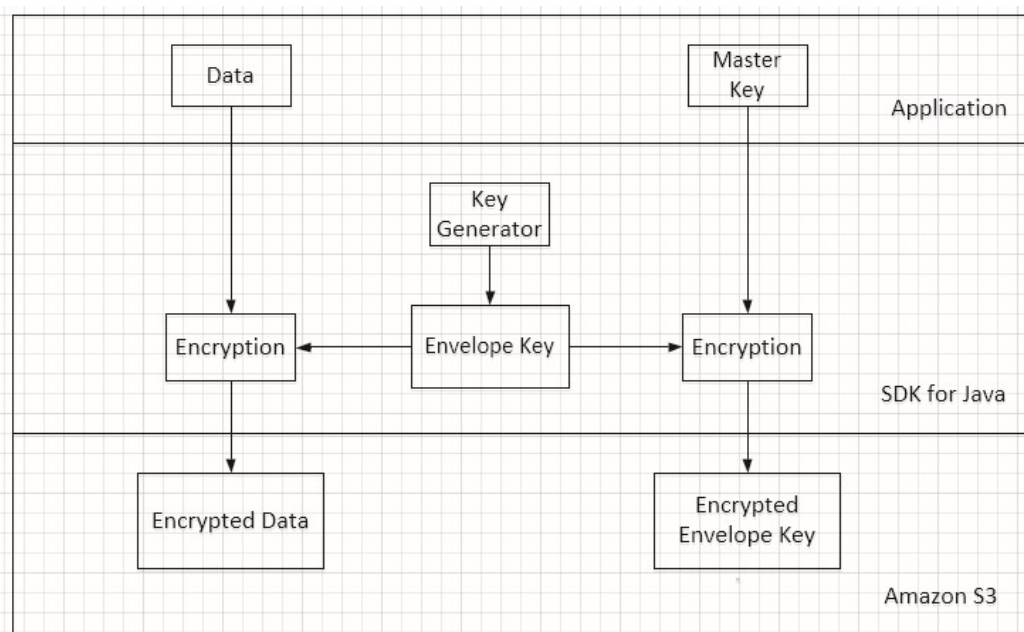
**The statement of basic materials.** After your data reaches Google, it gets unencrypted then re-encrypted using 128-bit AES. While not the 256-bit algorithm that most other services use, this is still normal. This is done on-the-fly before the data is actually stored, which prevents the possible leakage of unencrypted data on their hard drives. The AES encryption keys that were used to encrypt data are then, themselves,

encrypted with a rotating set of master keys. This adds another layer of security by requiring a *second* set of encryption keys.

Amazon offers what is called ‘Server Side Encryption’ for S3, or if user is looking at S3 bucket in the AWS console, it will be called ‘Default encryption’ under the properties sheet. Consumer can enable encryption simply by toggling a button in the UI and telling AWS how he/she would like the key to be managed. One option is AES-256 keys managed per bucket, and the other option is allow KMS — the AWS Key Management Service — handle key management.

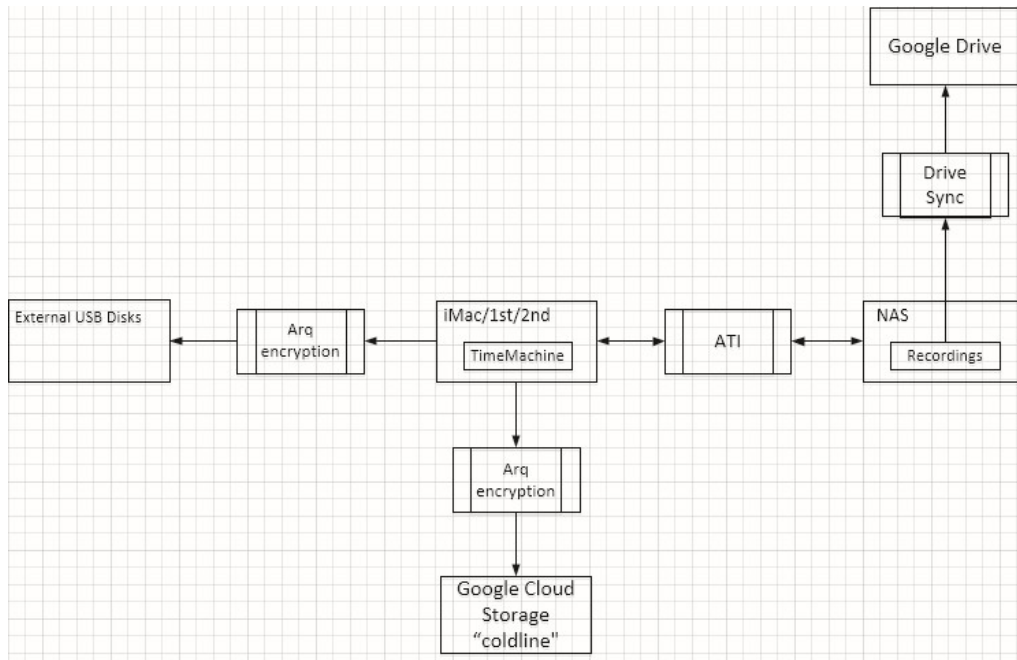
iCloud secures information by encrypting it when it's in transit, storing it in iCloud in an encrypted format, and using secure tokens for authentication. For certain sensitive information, Apple uses end-to-end encryption that provides high level of data security. Information is protected with a key derived from information unique to device, combined with device passcode.

**General model structure.** The structure of the model was chosen to compare the level of security models. First is AMAZON:



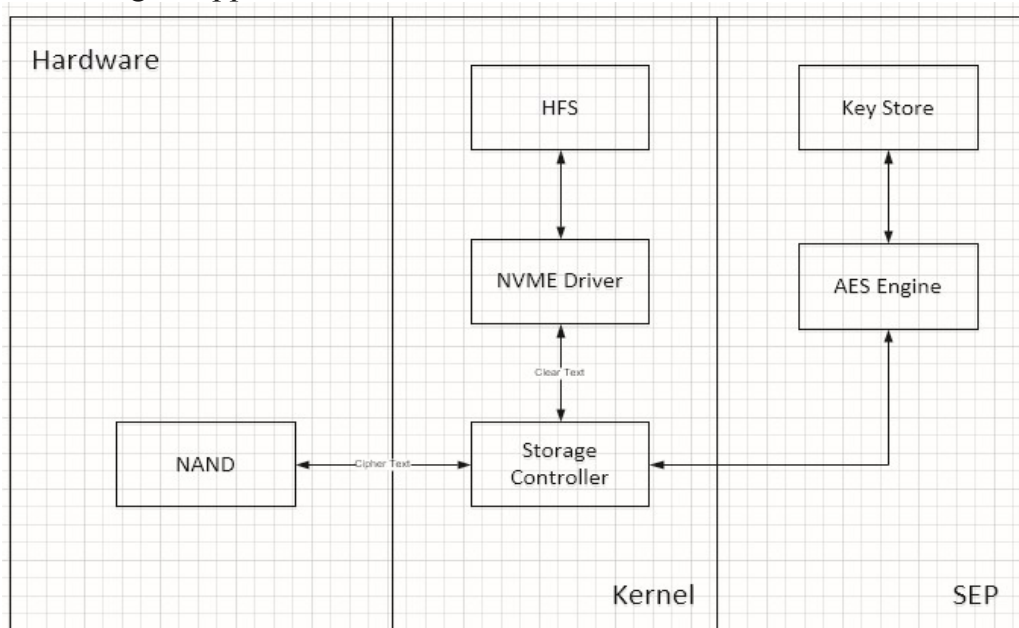
**Fig. 1.** Client-Side Data Encryption for Amazon S3

Second thing is Google's variant:



**Fig. 2.** Google Data Protection strategy

Third thing is Apple’s variant:



**Fig. 3.** iCloud Filesystem Data Protection

**Conclusions.** The paper has demonstrated the ability of iCloud to be the best cloud based storage. It can be seen that the use of such service produces qualitative results. iCloud has enough data protection level and price is cheaper than competitors have.

There are several directions for future work. One is to change the test protection’s model for all services, increasing the number of hidden units and adding more productive parts. Another is to create a completely new cloud scheme. These changes will definitely improve the results. It also would be interesting to test the hybrid model that consists of 3 templates.

### References

1. Google Cloud Platform Documentation. – Link:<https://cloud.google.com/docs/>. – Date: 22.04.2018.
2. How Do I Enable Default Encryption for an S3 Bucket? – Link:<https://docs.aws.amazon.com/AmazonS3/latest/user-guide/default-bucket-encryption.html>. – Date: 22.04.2018.
3. How the Apple iCloud Works. – Link: <https://computer.howstuffworks.com/cloud-computing/icloud4.htm>. – Date: 25.04.2018.
4. Price comparison. – Link:<https://www.wired.com/story/amazon-just-killed-the-best-deal-in-tech/>. – Date: 25.04.2018.

### ДОВІДКА ПРО АВТОРІВ

Ярич Андрій Миколайович – магістрант, кафедра обчислювальної техніки, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського».

Yarych Andriy – magistrate, Department of Computer Engineering, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”.

E-mail: [andriyarych@zoho.com](mailto:andriyarych@zoho.com)

Ярич Андрій

## ПИТАННЯ ВИБОРУ CLOUD-ДОДАТКУ НА ОСНОВІ АНАЛІЗУ GOOGLE, AMAZON ТА APPLE РІШЕНЬ

**Актуальність теми дослідження.** Хмарні технології стають все більш й більш поширеними на світі; люди використовують сервіси зберігання для документів, фото та інших файлів, тому так важливо мати захист даних та їх швидке завантаження.

**Постановка проблеми.** На даний момент існує достатньо широка необізнаність населення щодо потенціалу та репутації різноманітних хмарних додатків, тому слід виділити найкращий, що повністю задовольнятиме потребам користувачів.

**Аналіз останніх досліджень і публікацій.** У зв'язку з появою нових методів та підходів на ниві хмарних технологій тема вибору хмарних додатків стає більш популярною в останні роки.

**Виділення недосліджених частин загальної проблеми.** Існує достатньо невивчених моментів, які повинні бути відкритими. Слід звернути увагу на рішення з об'ємом в 1 та 2 ТБ, оскільки це найбільш релевантно для багатьох юзерів; акцент був поставлений на програмах від відомих компаній.

**Постановка завдання.** Завданням є повністю розкрити особливості усіх рішень; на основі отриманих даних (у більшій мірі – від рівня захисту інформації та ціни послуг) вибирається найбільш актуальне та потрібне програмне рішення.

**Викладення основного матеріалу.** Перш ніж дані залишать пристрій, він зашифровується за стандартом TLS. Це той самий стандарт, який використовується для шифрування веб-переглядачів на веб-сайтах із безпечним HTTPS. Після того, як дані досягають Google, вони шифруються за допомогою 128-бітної AES. Хоча це не 256-бітний алгоритм, який використовують більшість інших служб, однак непогано.

Amazon пропонує те, що називається «Шифрування за замовчуванням» під панеллю властивостей. Можна ввімкнути шифрування, просто перемикаючи кнопку в інтерфейсі користувача та повідомляючи AWS, як хочеться керувати додатком. Одним з варіантів є керування ключами AES-256, а інший варіант - дозволити KMS - службі керування ключами AWS – працювати із ключами.

Про iCloud. Щоб використовувати повне шифрування, то для Apple ID потрібно мати двофакторну автентифікацію. Щоб отримати доступ до даних на новому пристрої, може знадобитися введення паролю для існуючого або колишнього пристрою Apple.

**Висновки.** Дана стаття продемонструвала першість “яблука” серед всіх розглянутих додатків; було чітко видно, що використання даного сервісу дає результати відносно юзера та його сподівань; є декілька напрямів подальшого розкриття питання. Наприклад, можна протестувати гібридну модель хмари або створити якісно нову; також за ідею можна взяти покращення системи захисту інформації iCloud.

**Ключові слова:** iCloud, Amazon, GoogleDrive, шифрування, AES.