Exploration of the Security of Free Data Encryption Applications for Cloud Storage

Eka Hero Ramadhani*, Herman Kabetta, Amiruddin Amiruddin
Cyber Security Engineering Department, Politeknik Siber dan Sandi Negara, Bogor, Indonesia

*eka.hero@student.poltekssn.ac.id

Abstract. Cloud storage has become an urgent need in the digital age, especially for companies with high level of work collaboration and mobile workers. To prevent data in cloud storage from being accessed illegally, the data must first be encrypted before being uploaded. However, encrypting data separately with cloud data storage media is considered to be less efficient and less secure. To that end, several data encryption applications designed specifically for cloud storage appeared in the market. However, which application is suitable for your requirement, needs to be further investigated. For this premise, in this research, an exploratory study of the security of several free applications of data encryption called Boxcryptor, Cryptomator, and nCrypted Cloud was conducted based on security parameters defined in ISO/IEC 25010. The results showed that two of five security parameters, integrity, and authenticity, are not satisfied by all the applications being reviewed, but Cryptomator outperformed the other two applications.

1. Introduction
Cloud storage has become an urgent need in this digital age, especially for companies with high level of work collaboration and mobile workers. Cloud storage allows users to flexibly store and access data in storage that is managed by a cloud storage service provider [1]. The cloud storage service provider is responsible for securing, managing, and maintaining the cloud storage infrastructure, as well as ensuring the availability of cloud storage services can be accessed anytime when needed by users [2]. However, to comfortably use cloud storage services, users need to make subscription and pay a service fee [1]. In addition, data stored in cloud storage is not fully guaranteed secure and consequently, there is a high risk of unauthorized access [3] and is vulnerable to modification and disclosure [4].

Encrypting data before it is stored in cloud storage can protect and preserve data privacy [5]. Therefore, several applications such as Boxcryptor, Cryptomator, and nCrypted Cloud have been developed specifically to encrypt data before it is stored in cloud storage [6]. Some of these types of applications are inexpensive solutions to protect data privacy in cloud storage because they are free to be downloaded from the developer's website. However, it’s worth noting that not all free software products reach maturity, succeed, and are of good quality [7]. Because they are free, these applications often come without adequate security mechanisms.

In this study, we explored the security aspect of several free applications for data encryption for cloud storage namely Boxcryptor, Cryptomator, and nCrypted Cloud. The exploration is guided by referring the security parameters defined in ISO/IEC 25010. The results of this study can be used as a
reference in choosing the best free data encryption application to protect and preserve data privacy. It also can give an insight in conducting similar research related to cloud storage in the future.

2. Method and Materials

2.1. Exploration preparation
To conduct an exploratory study on the security aspect of the applications, the first step to do is selecting the target of exploration. In this study, the applications chosen for analysis were three free data encryption applications, named Boxcryptor, Cryptomator, and nCrypted Cloud. These applications are widely used for data encryption before being stored in cloud storage. The applications can be found on URLs given in Table 1.

| Applications     | URLs                                      |
|------------------|-------------------------------------------|
| Boxcryptor       | https://www.boxcryptor.com/en/download/   |
| Cryptomator      | https://cryptomator.org/downloads/        |
| nCrypted Cloud   | https://www.ncryptedcloud.com/download/   |

In the preparation stage of this research the following activities were carried out:
1. Study the application documentation under study. The purpose of this activity is to obtain information about the workings and application specifications.
2. Conduct interviews with expert in the field of software testing to obtain information related to data collection, processing, and analysis methods.
3. Create a Google account to get the free Google Drive cloud storage service used in this study.
4. Prepare the application installer to be examined. Free data encryption applications for cloud storage examined in this study are Boxcryptor version 2.35.1033, Cryptomator version 1.4.15, and nCrypted Cloud version 1.45.8.
5. Prepare the installer applications such as VirtualBox, 64-bit Windows 10 Education ISO, Google Drive Backup and Sync for Windows, and md5sum.
6. Prepare a laptop used to do this research with specifications: Lenovo ideapad 320, Ubuntu 18.04.4 LTS, AMD A9-9420 RADEON R5, 5 COMPUTE CORES 2C+3G, 7603 MB.
7. Create three virtual machine units that have identical specifications as a work environment for each application studied. This activity is carried out by installing Windows 10 Education 64-bit on one virtual machine which is then cloned as many as three virtual machine units with specifications: Windows 10 Education 64-bit, AMD A9-9420 RADEON R5, 5 COMPUTE CORES 2C+3G (2 CPUs), ~3.0GHz, 4096 MB.
8. Install the Google Drive Backup and Sync application in each virtual machine.
9. Install the Boxcryptor application on virtual machine-1, Cryptomator on virtual machine-2, and nCrypted Cloud on virtual machine-3.
10. Test the use of applications used for research that have been installed on each virtual machine working environment. The purpose of this activity is to ensure that these applications work well so they are ready to be used for research.
11. Prepare sample files that are used as test data for the applications as given in Table 2.

| No. | File Name             | File Size  |
|-----|-----------------------|------------|
| 1   | 2.729.385 bytes.pdf   | 2.729.385 bytes |
| 2   | 5.664.556 bytes.pdf   | 5.664.556 bytes |
| 3   | 10.780.930 bytes.pdf  | 10.780.930 bytes |
| 4   | 15.996.374 bytes.pdf  | 15.996.374 bytes |
| 5   | 24.238.390 bytes.pdf  | 24.238.390 bytes |
2.2. Method
The study of the application security was done by exploring several security parameters of the three applications using several literatures, for example, Boxcryptor [8], Cryptomator [9], and nCrypted Cloud [10] as well as AES algorithm [11]. The security parameters, defined in ISO/IEC 25010, are confidentiality, integrity, non-repudiation, accountability, and authenticity [12] as defined in Table 3 along with the expected results of the measurement.

### Table 3. Security parameters used for exploration study

| Parameters          | How to measure                                                                 | Expected result                                                                 |
|---------------------|-------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| Confidentiality     | Looking for the type of encryption algorithm used in the documentation of the application. | The type of encryption algorithm used.                                         |
| Integrity           | Checks whether the encrypted sample file after decrypted by the application under study holds its integrity. Check whether the application under study is able to detect any modifications to the ciphertext file. | It is known the integrity of the sample file that has been processed using the application under study. It is known the ability of the application under study in detecting any modifications to the ciphertext file. |
| Non-repudiation     | Check whether the application under study is able to prove that an event or action has occurred on the application. | It is known that the ability of the application under study in proving an event or action has occurred in the application. |
| Accountability      | Check whether the application under study is able to trace the actions of an entity uniquely. | It is known that the ability of the application under study in tracing the actions of an entity is unique. |
| Authenticity        | Check whether the identity of a subject or resource can be proven as claimed by the application under study. | The known identity of a subject or resource can be proven as claimed by the application under study. |

Using the results obtained from the encryption/decryption and hashing/verification, the security performance of the applications can be compared and analyzed as described in Section 3.

3. Results and Discussion

3.1. Result
The results of the exploration of the security of the application being reviewed i.e. Boxcryptor, Cryptomator, and nCrypted Cloud, are presented in accordance with the security parameters defined in ISO/IEC 25010. The security parameters consists of confidentiality, integrity, non-repudiation, accountability, and authenticity. Based on the exploration results, we summarized the security performance of the applications being reviewed as given in Table 4. Two of the five parameters, integrity and authenticity, are not satisfied. All the applications do not meet the integrity parameter and only the Cryptomator application does meet the authenticity parameter.

### Table 4. Comparison on security parameters

| Parameters          | Applications          |
|---------------------|-----------------------|
|                     | Boxcryptor | Cryptomator | nCrypted Cloud |
| Confidentiality     | Yes         | Yes         | Yes           |
| Integrity           | No          | No          | No            |
| Non-repudiation     | Yes         | Yes         | Yes           |
| Accountability      | Yes         | Yes         | Yes           |
| Authenticity        | No          | Yes         | No            |
3.2. Discussion

3.2.1. Confidentiality
Based on the study of the application's documentation, it is known that all the applications under study, Boxcryptor, Cryptomator, and nCrypted Cloud, use the 256-bit AES algorithm for encrypting or decrypting user files and that fulfills the NIST recommendation for using AES as an encryption algorithm to secure data. Although the Boxcryptor, Cryptomator, and nCrypted Cloud applications use the AES algorithm, the encrypted user files are not fully secure guaranteed. Based on our observations, the three applications have advantages and disadvantages of each in securing the privacy of user files as described in the following.

Using a local account on Boxcryptor, we found that the generated key file is stored on the local device so that the user has full control over the security of the key file. If the attacker has only one of these two key factors (key file or password), then the attacker will not be able to decrypt the ciphertext file. If the user switches devices and the key file is not present on the new device, the user will not be able to decrypt the ciphertext file, even if the corresponding password is known. If the user loses the key file, then the user will not be able to generate the same key file even with the same initialization password as the lost key file.

Using an online account on Boxcryptor, we found that the user can decrypt the ciphertext file on a different device because the corresponding encryption key is stored on the Boxcryptor server. Simply by authenticating a Boxcryptor account, users can encrypt and decrypt files on different devices that have the Boxcryptor application installed and connected to the internet.

Users can recover lost account passwords with the password recovery feature. If the user forgets the username (registered email account), then the user cannot recover his account and decrypt the ciphertext file. The user's Boxcryptor account identity information and the corresponding encryption key are stored on the Boxcryptor application developer server which is a vulnerability and potential privacy violations that may be committed by the developer.

Using Cryptomator, we found that the password that corresponds to the vault for file encryption and decryption is only known by the user. If the user forgets the password, the ciphertext file can never be decrypted.

Using nCrypted Cloud, we found that users can decrypt the ciphertext file on different devices because the encryption key matches the account that is connected to the nCrypted Cloud server. Simply by authenticating a nCrypted Cloud account, users can encrypt and decrypt files on different devices that have the nCrypted Cloud application installed and connected to the Internet. Users can recover lost account passwords with the password recovery feature. If the user forgets the username (registered email account), then the user cannot recover his account and decrypt the ciphertext file. The nCrypted Cloud account user identity information and the corresponding encryption key are stored on the nCrypted Cloud application developer server. This is a vulnerability and a potential occurrence of privacy violations that may be done by nCrypted Cloud application developers.

3.2.2. Integrity
Based on the data that has been obtained, for the integrity comparison, it can be shown that the encryption and decryption processes of all applications, Boxcryptor, Cryptomator, and nCrypted Cloud, were able to maintain the integrity of the files. This is evidenced by the MD5 hash value of the plaintext sample file which remains the same between the encryption process and the decryption one. However, after testing by conducting modification of the ciphertext sample file in cloud storage, it can be seen that all applications were unable to detect any modification attacks that have occurred in the ciphertext file. This was evidenced by the absence of notification from the three applications to the user that the ciphertext file to be decrypted was modified.
3.2.3. Non-repudiation

Based on data that has been obtained from the previous stage, it can be interpreted that the Boxcryptor, Cryptomator, and nCrypted Cloud applications are able to prove that an action or event has occurred using the system log. By carefully investigating the system log that they have, we can prove what events or actions have occurred, thus, the event or action cannot be denied. Using Boxcryptor application, users can see the data or information about the actions or events that have occurred in the application through the debug log file. The file can be accessed by running the Boxcryptor (Debug) application shortcut program located in the directory C:\Program Files (x86)\Boxcryptor. Meanwhile, using the Cryptomator application, users can see actions or events that have occurred in the application through the log file. By utilizing the nCrypted Cloud application, users can see the actions or events that have occurred in the application through the auditing feature that can be accessed on the Cloud Web Portal. To this end, all the applications have their logging mechanism for proving non-repudiation aspect.

3.2.4. Accountability

Based on the data that has been obtained for accountability comparison variables, it can be interpreted that all applications are able to track the actions of an entity uniquely using their log system. However, to track the actions of an entity uniquely in the Boxcryptor and Cryptomator, users need to have special skills to be able to read and understand the information contained in the log files. Only people who are trained and understand how to read the contents of the system log can read the log files, or those who are expert in the field of systems and software development. Ordinary users or those who do not have the skills cannot easily read and understand the information, making it relatively difficult to track the actions of an entity.

The log systems of Boxcryptor and Cryptomator application are different from the log system owned by the nCrypted Cloud. The nCrypted Cloud application log system is a nCrypted Cloud’s Auditing feature that can only be accessed online via the Cloud Web Portal. It is relatively easy for the user to read to track the actions of an entity uniquely on the application and the data being processed. The Cloud Web Portal of nCrypted Cloud’s Auditing page provides information in the form of the file or directory being accessed, what actions have been taken against the file or directory, the date the action occurred, the identity of the user who took the action, and the device used. Therefore, based on the results of the analysis and interpretation, it can be stated that the nCrypted Cloud application log system can be used with relative ease to trace the actions of an entity uniquely on the application and the data being processed.

3.2.5. Authenticity

Based on the data that has been obtained, for the comparison of authenticity variables, it can be seen in our experiment that the Boxcryptor and nCrypted Cloud applications were able to prove the identity of a subject or resource as claimed, but the Cryptomator application cannot prove it. Thus, the Boxcryptor and nCrypted Cloud can prove the authenticity of the subject or resource whereas Cryptomator cannot. In terms of security, free applications that do not store the user's identity are better because the developer cannot abuse user privacy.

4. Conclusion

In this study, we have explored the security of the three free encryption applications for data to be stored in cloud storage, namely Boxcryptor, Cryptomator, and the desktop version of the Windows platform's nCrypted Cloud, with reference to security parameters defined in ISO/IEC 25010. The results showed that two of five security parameters i.e. integrity and authenticity, are not satisfied by all the applications being reviewed. It also showed that Cryptomator application is better at protecting the privacy of data stored in cloud storage compared to the Boxcryptor and nCrypted Cloud applications.
References

[1] K. Yang and X. Jia, Security for Cloud Storage Systems, Hong Kong: Springer, 2014.

[2] IBM, "Cloud Storage," 2019. [Online]. Available: https://www.ibm.com/cloud/learn/cloud-storage.

[3] T. Galibus, V. V. Krasnoproshin, R. d. O. Albuquerque and E. P. d. Freitas, Elements of Cloud Storage Security: Concepts, Designs and Optimized Practices, Cham: Springer, 2016.

[4] P. S. Deshpande, S. C. Sharma and K. S. Peddoju, Security and Data Storage Aspect in Cloud Computing, Singapore: Springer, 2019.

[5] A. Wheeler and M. Winburn, Cloud Storage Security: A Practical Guide, Amsterdam: Elsevier, 2015.

[6] P. Bischoff, "The best apps to encrypt your files before uploading to the cloud," 2018. [Online]. Available: https://www.comparitech.com/blog/cloud-online-backup/6-apps-to-encrypt-your-files-before-uploading-to-the-cloud/.

[7] M. Michlmayr, F. Hunt and D. Probert, "Quality Practices and Problems in Free Software Projects, in Marco Scotto and Giancarlo Succi (Eds.)," in Proceedings of the First International Conference on Open Source Systems, Genova, 2005.

[8] Secomma GmbH, "Technical Overview," [Online]. Available: https://www.boxcryptor.com/en/technical-overview/.

[9] Skymatic GmbH, "Cryptomator: Free client-side encryption for your cloud files.," 2019. [Online]. Available: https://cryptomator.org/.

[10] e-Share, nCrypted Cloud Windows User Manual: Version 2, e-Share, 2020.

[11] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th Edition, Essex: Pearson Education, 2017.

[12] ISO/IEC, Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models (ISO/IEC 25010:2011(E)), Switzerland: ISO/IEC, 2011.