Acrypt: Minimizing Data Leakage in Cloud Storage with Cryptography Encryption

Ayshwarya Raj
Forensics & Cybersecurity Research Center (FSEC)
Asia Pacific University of Technology and Innovation (APU)
Kuala Lumpur, Malaysia
TP046801@mail.apu.edu.my

Julia Juremi
Forensics & Cybersecurity Research Center (FSEC)
Asia Pacific University of Technology and Innovation (APU)
Kuala Lumpur, Malaysia
julia.juremi@staffemail.apu.edu.my

Salasiah Sulaiman
School of Computing
Asia Pacific University of Technology and Innovation (APU)
Kuala Lumpur, Malaysia
salasiah@staffemail.apu.edu.my

***Abstract*— Organisations today sign up for cloud storage systems from several service providers and rent access from storages spaces to application instead of owning their own computing infrastructure or data centres. However, like any other platform, the cloud infrastructure still remains vulnerable to data leakage. Thus, encryption plays a huge role in ensuring that any data that is uploaded, stored, and retrieved from the cloud remains safe. It is one of security feature that is very essential in cloud security as it locks and secure the data from being retracted by others that are not authorised. The proposed system will demonstrate how to securely encrypt files before sending them to the cloud and how an authorised user decrypts the data and retrieves it back. This proposed system is also meant to create awareness to internet users that data leakage is happening at a daily basis and jeopardises financially as well as personally to the victim.**

Keywords—cloud storage, cryptography, encryption, privacy, confidentiality

I. INTRODUCTION

In this tech savvy world, cloud computing is the most emerging yet widely used data storing technology amongst everyone today. It is known as the delivery of computing services which includes providing servers, storage, databases, networking, software, analytics, and intelligence over the Internet ("the cloud") to offer faster innovation, flexible resources, and economies of scale (Singh & Sharma, 2021). Those were the days that floppy disks, hard disk drives, CD and USB drive were used as means of storing data and to be transmitted to someone easily. Organisations today sign up for cloud computing systems from several service providers and rent access from storages spaces to application instead of owning their own computing infrastructure or data centres. Organisations like Microsoft, Amazon Web Server and Google Cloud are some of the notable cloud service providers to a plethora of organisation (Sasubilli & R, 2021).

However, like any other platform, the cloud infrastructure still remains vulnerable to data leakage as said in lay man terms "it just another person's computer". In addition, according to Open Web Application Security Project (OWASP), user privacy and secondary usage of data is labelled as one of the top ten cloud security risk (Packetlabs, 2020). According to (Boxcryptor, 2021). data leakage results in huge monetary losses to the firm or organization. Data leakage in cloud computing can be traced to as early as 2010 whereby Microsoft Corporation experienced a breach that was traced back to a configuration issue within its Business Productivity Online Suite (Winder, 2020). The problem allowed non-authorized users of the cloud service to access employee contact info in their offline address books. Microsoft claims that customer had access to their data and that they fixed the issue two hours after it occurred. While only a small number of users were affected, this incident is worth noting.

Thus, encryption plays a huge role in ensuring that any data that is uploaded, stored, and retrieved from the cloud remains safe as every file/application has its own unique encryption and decryption key. By implementing encryption on the files before sending them to the cloud storage, users of this application would gain essential benefits and extra layer of security.

II. SIMILAR SYSTEMS

A. Cryptomator

Cryptomator is one such tool that offers its clients a platform to securely encrypt and decrypt their data stored in the cloud. It is a free, open-source German encryption solution that was launched in 2016 by a start-up organisation called Skymatic GmbH. It offers a multi-platform transparent client-side encryption using the AES encryption algorithm of 256-bits key length. This tool functions by having "vaults" for users to store distinctively secret data in it (CRYPTOMATOR, 2021). These vaults acts a compartment of encryption of these secret data using the AES 256 algorithm after which a decryption key is assigned to the responding user that is associated with the secret data encrypted. Fig. 1 shows the desktop interface of the Cryptomator.

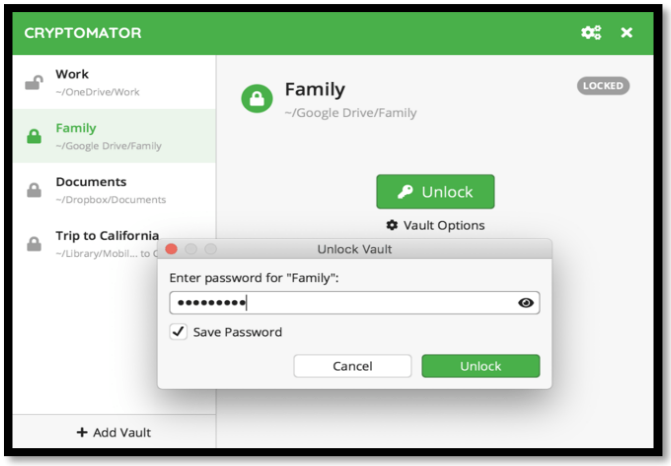

Fig. 1. Cryptomator desktop interface

The responding user will then need to use the decryption key that has been emailed to them to decrypt the file to a readable message. The user can set rules and restricts as to the controls of the responding user towards the data associated with them.

B. Boxcryptor

Another similar tool that is also available in the market today is called the Boxcryptor. This tool is a free encryption application that enables users to easily synchronize encrypted files with more than 30 cloud storage. Boxcryptor is mostly focused on cloud storage, allowing easy encryption, editing and decryption of files with more than 30 cloud storage providers as well as can encrypt local files. The Boxcryptor as shown in Fig. 2. uses both the RSA-4096 algorithm as well as the AES-256 algorithm for both encryption and decryption of the data. A public and private RSA-4096 key is associated together from which a key generated from the user's master password is used to encrypt their private key, which is needed to decrypt the files. Once the password is entered, the private key unlocks, which pairs with the public key [1]. Since the RSA key pair is used to encrypt the AES keys, it can then decrypt the files as well. This tool is made available for both desktop and mobile version on all operating systems.

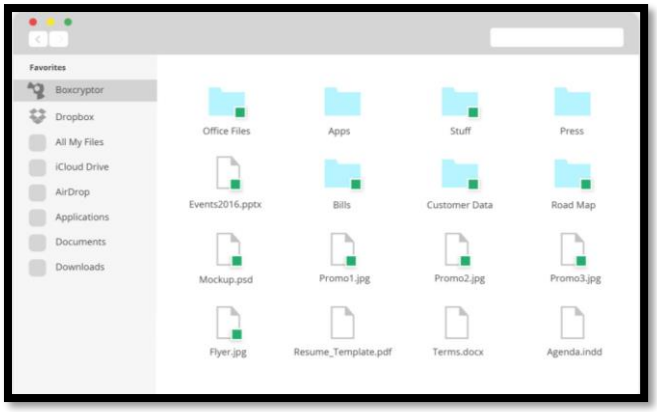

Fig. 2. Boxcryptor's User Interface

TABLE I. COMPARISON BETWEEN SIMILAR AND PROPOSED SYSTEMS

Name of Application/ Criteria of comparison	**BoxCryptor**	**Cryptomator**	**AcRypt**
Encryption Algorithm Used	Combination of RSA and AES encryption	AES-SIV encryption	AES encryption
Pricing	Free on desktop version and paid for mobile versions	Free	Free
Cloud Platforms Supported	Dropbox, OneDrive, Google Drive, in addition to over 30 more cloud providers in total, such as iCloud and SharePoint	Dropbox, OneDrive, Google Drive and WebDAV based cloud storages.	Google Drive and Dropbox
Supporting Operating Systems	Windows, macOS, iOS, Android, (Linux with limited functionality)	Windows, macOS, iOS, Android, Linux	Windows OS
User-Friendliness	Very user-friendly	Very user-friendly	Very user-friendly
Security	Secured	Very Secured	Secured

Fig. 3. displays a comparison of the two systems with the proposed system named as Acrypt. Fig 3. figure also summarises the different features and suggests the features that are to be implemented in the proposed system in the development phase. The algorithms proposed by these researchers are of the latest in technology such as the AES and RSA. A proposed combination of both the algorithm goes to show how effective data encryption will be in the future. Hence, as the developer of this project, it is important to take note and consideration of all the proposed solutions to the current issues faced in today's cloud computing advance as this will help provide a consensus and effective proposal to the project.

III. PROPOSED SYSTEM

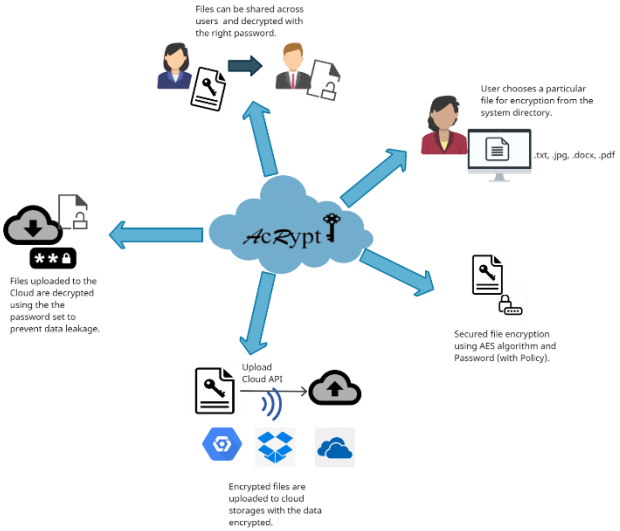

Fig. 3. System design of acrypt tool

Fig. 4. shows the system design of the proposed encryption tool, AcRypt. This proposed tool has very simple functionalities for non-computer literate users to benefit out of the file security tool. The main core functionalities of the system includes encryption of various files with different formats, using password (with password policy) to encrypt the files, upload the encrypted files to cloud storages (in this project, Google Drive) and decryption files using the set password after downloading from the cloud storage.

For the development of prototype, developer chooses to develop the system using the Eclipse IDE. Developer will be using Java programming language which is very well associated with the Eclipse IDE to develop and program the cryptographic system as this language is very well supported in this IDE. Besides that, developer would also implement the AES algorithm using 128 bits that is able to function simultaneously in providing secure encryption to the data uploaded in the system. To add on, the developer will be using the Windows 10 operating system as the main operating system to develop the project, as it is more user-friendly and easier to troubleshoot issues. Lastly, the developer would also be using the Google Drive API application as the main API to demonstrate the uploading of encrypted files to the cloud as well as it enables proper synchronizing of data to the develop project with the Eclipse IDE.

Acrypt consists of a main welcome page with a "Start" button to open to the main interface page as shown in Fig. 5.

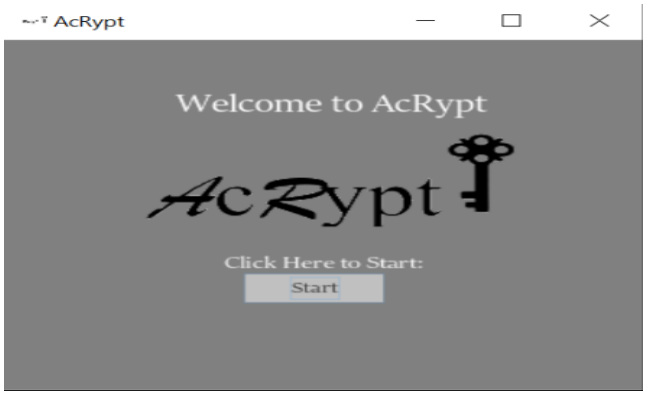

Fig. 4. Acrypt main page

The main page will then be split into three different sections, one is for encryption of files and password setting. Second part is uploading a file to Google Drive and lastly, the decryption section of the files uploaded to Google Drive when downloaded from the site which can be seen in Fig. 6, 7 and 8 below.

Fig. 5. Acrypt File encryption

The user will need to choose a file from the system directory upon clicking the "Choose" button. After selecting the file for encryption, then the user is able to set a password of 8 characters. The user is then needed to retype the password onto the system before clicking on the "Encrypt" button. Once, the "Encrypt" button is clicked, then the file is encrypted with a password set for it.

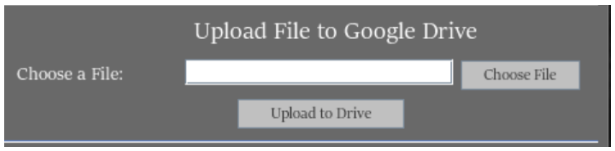

Fig. 6. Acrypt Upload File to Google Drive

User can also upload their file to Google Drive Section of the AcRypt application. The user can choose the encrypted file that is saved in the system directory when the "Choose File" button is clicked. Once the file is selected, the user can simply click the "Upload to Drive" button on the system interface and the file will be immediately uploaded to the Google Drive Account synced in the application.

Fig. 7. Acrypt File Decryption

In the case of if the user need to decrypt back their file, they can choose to download their file from the Google Drive. After downloading the encrypted file from Google Drive, the user just need to choose the file from the system directory by clicking the "Choose" button. After choosing the file, the user will need to insert the correct password to decrypt the file. After typing the correct password for the file chosen, then the user needs to click the "Decrypt" button in order to decrypt the file.

IV. UNIT TESTING & USER ACCEPTANCE TESTING

In the face of all testing the researcher has good test output evaluation results. Several results from the unit testing has been shown in Table.II. Acrypt has passed all the crucial unit testing without any issue with the proposed functionalities which is to encrypt, decrypt and upload the encrypted files to the cloud storage.

TABLE II. UNIT TESTING FOR ACRYPT

Test ID	Description	Expected Output	Actual Output	Result
C001	Select file Input	To display all the file directories in the system.	Displayed all the file directories in the system.	Pass
C002	Encryption of different file formats.	The encrypted file should be e.g.: Hello_encrypt.txt	The encrypted file releases the output as e.g.: Hello_encrypt.txt	Pass
C003	Implementing a password to encrypt the file and be used for decryption later	After setting the password, the pop-up message should prompt a message "This file is encrypted"	After setting the password, the pop-up message prompted was "This file is encrypted"	Pass
C004	Decryption of different file formats and read the original context.	The file output should be e.g.: Hello_encrypted_decrypted.txt	The file output is e.g.: Hello_encrypted_decrypted.txt	Pass
C005	Uploading a file to Google Drive on a test account.	The encrypted file should be uploaded to the test Google Drive Account with the details encrypted. A pop-up message "Uploaded to Drive" should be prompted	The encrypted file is successfully uploaded to cloud with the pop-up message prompted as "Uploaded to Drive"	Pass
C006	When the wrong password is keyed in for file decryption.	The pop-up message "Insert Correct Password" should be prompted when the wrong password is keyed in for decryption.	The pop-up message "Insert Correct Password" is prompted when the wrong password is keyed in for decryption.	Pass

Acrypt has also go through User Acceptance Test and the results can be seen in Fig. 9, 10 and 11 below.

Name:	Jeyamalar Sivapatham		**Occupation:**	Banker	
Date:	19/02/2021		**Location/Platform:**	Petaling Jaya	
Criteria:	**Strongly Agree**	**Agree**	**Neither**	**Disagree**	**Strongly Disagree**
Ease of Use		✔			
GUI	✔				
Functionality	✔				
Feedback from Tester:	Well-developed cryptography system with password strength. To include more cloud storage features in the future.				
Feedback from Developer:	Feedback is regarded and taken into consideration by the developer.				

Fig. 8. User Acceptance Test by User 1

Name:	Fazrina bt Mohd Anif		**Occupation:**	Secretary	
Date:	19/02/2021		**Location/Platform:**	Microsoft Teams	
Criteria:	**Strongly Agree**	**Agree**	**Neither**	**Disagree**	**Strongly Disagree**
Ease of Use	✔				
GUI		✔			
Functionality		✔			
Feedback from Tester:	Very good and simple system on file cryptography.				
Feedback from Developer:	Feedback is regarded and taken into consideration by the developer.				

Fig. 9. User Acceptance Test by User 2

Name:	Keevashiny A/P Chandrasegeran		**Occupation:**	Student	
Date:	19/02/2021		**Location/Platform:**	Microsoft Teams	
Criteria:	**Strongly Agree**	**Agree**	**Neither**	**Disagree**	**Strongly Disagree**
Ease of Use	✔				
GUI	✔				
Functionality		✔			
Feedback from Tester:	Very good alternative cryptographic tool that uses password-based encryption. Should include more cloud storage application access for future.				
Feedback from Developer:	Feedback is regarded and taken into consideration by the developer.				

Fig. 10. User Acceptance Test by User 3

IV. CONCLUSION

As an emerging technology, cloud computing still remains vulnerable to the cyber world as some activities cannot be controlled in the cloud platform which includes tracing out the data breach that often happens in this environment. As an alternative security step, users of these cloud platforms must be aware that these cloud storages are not as safe as it seems to be, therefore they should incorporate tools such as AcRpt to secure their confidential files prior to storing them in the virtual environment. One of the limitation that can be found in this application is the limitation of encryption algorithms available to secure the confidential files that are intended to be stored in the cloud. Implementation of RSA algorithm as a decryption method as implemented in the Boxcryptor with having a very large key size with 1024 and 2014 bit long will prove to provide an extremely secure encryption and decryption process for this application. The application also can be further improved to include different cloud applications such as Dropbox and AWS. Due to the fact that this is a cryptographic tool that secures files by means of encryption to be uploaded to the cloud, hence, in the future, for commercial purposes this tool should include the following features so that users can have a myriad of options to choose from as an alternative file securing application for cloud synchronizing so that regular user of the internet will be aware of data security in cloud computing.

REFERENCES

Boxcryptor. (2021). *Boxcryptor | Security for your Cloud*. https://www.boxcryptor.com/en/.

CRYPTOMATOR. (2021). *Put a lock on your cloud*. https://cryptomator.org/.

Packetlabs. (2020). *OWASP Cloud Top 10 Risks*. https://www.packetlabs.net/cloud-security/

Sasubilli, M. K., & R, V. (2021). Cloud Computing Security Challenges, Threats and Vulnerabilities. *2021 6th International Conference on Inventive Computation Technologies (ICICT)*, 476–480. https://doi.org/10.1109/ICICT50816.2021.9358709

Singh, U. K., & Sharma, A. (2021). Cloud Computing Security Framework Based on Shared Responsibility Models . In *Cyber-Physical, IoT, and Autonomous Systems in Industry 4.0* (1st Edition, pp. 39–55).

Winder, D. (2020). *Microsoft Security Shocker As 250 Million Customer Records Exposed Online*. https://www.forbes.com/sites/daveywinder/2020/01/22/microsoft-security-shocker-as-250-million-customer-records-exposed-online/?sh=1f2236584d1b