Desktop Application for Data Encryption on Google Drive

RGC Upeksha[1#] and PPNV Kumara[2]

[1,2] *Faculty of Computing, General Sir John Kotelawala Defence University Ratmalana, Sri Lanka*
[#] For correspondence; 33-se-003@kdu.ac.lk

Abstract— *Storage as Service (STaaS) is the main feature that gives the popularity for cloud storage, which provides the use of the maximum capacity with minimum hardware requirements. Data security has become the major aspect that limits the spread of this service due to the cyber-attacks. Google drive is the trending and widely used cloud-based storage service with millions of active users where they can store and access data without charges. The project presented from this paper is a desktop application that can encrypt data, before storing on Google drive. The main focus of the project is to facilitate the users by converting data to a ciphertext format using encryption algorithms. Therefore, the issues in Privacy of data, Confidentiality of data, Data Permanence, Data Integrity, and Malicious insiders can be solved by using this application for storing data on Google drive. The interfaces of the system are designed adding simplicity and user-friendliness, targeting the public users with different levels of computer knowledge.*

Keywords— **Encryption, Data Privacy, Cyber security**

I. INTRODUCTION

A. Cloud Computing

The emergence of cloud computing technology provides shared computing resources over the internet or in an internal network that are dynamically scalable. Since cloud services are always being developed, still there are many vulnerabilities that can be exploited by cybercriminals easily. Their main goals are to access user data and prevent accesses to cloud services which will a cause serious damage to cloud users. By exploiting vulnerabilities in clouds, unauthorized access by stealing user credentials or cracking passwords and act as a malicious intruder are the ways used by cybercriminals to intrude between cloud users and service vendors (User, n.d.). Cloud computing service models such as SaaS, PaaS, IaaS, STaaS, etc. should be interleaved with the security principles of Confidentiality, Integrity, and Availability (CIA) (Hanna, 2009).

B. Cryptography

Cryptography is the technique that can be used to transform understandable and readable data into a form called ciphertext which will not be readable or accessible. Data encryption is the process that converts data into ciphertext format and decryption is the process that

converts data back into original form. Goals we can achieve using cryptography ("3630-Article Text-6635-1- 10-20180104 (1).pdf," n.d.).

- Confidentiality
- Authentication
- Data Integrity
- Non-Repudiation
- Access Control

DES, AES are symmetric key ciphers and RSA, Diffie- Hellman key exchange, ElGamal cryptographic system, Elliptic curve cryptography are asymmetric key ciphers that we can use to encrypt and decrypt our data ("Cryptography and Network Security_ Principles and Practice 7th Global Edition.pdf," n.d.).

Boxcryptor is the latest desktop application that encrypts data for cloud storages. The project this paper presents, is carrying out the similar functionalities, enhanced security and features. Cryptomator, Tresorit, pCloud Crypto, SpiderOak, IDrive (techsegun, 2019), nCrypted Cloud, Odrive are the other similar systems which are desktop based or web-based and using different encryption techniques ("Best Free Apps to Encrypt Files & Data before Uploading to the Cloud," 2018).

Even though cloud vendors provide security mechanisms on user data, still accounts are being attacked with the newest technologies. The recent incident called Gooligan was the largest malicious attack on Google Accounts including Google Drive ("More Than 1 Million Google Accounts Breached by Gooligan," 2016). Data Encryption is the best method we can use to secure our sensitive and confidential data stored on Google Drive.

This paper will present a system that is going to provide solutions to the discussed problem. The rest of the paper is organized as follows: In related works, different encryption algorithms and similar systems are reviewed. Methodology section describes the design of the system. The conclusion presents the summary of the system and the future work describes the intentions on further developments of the system.

II. LITERATURE REVIEW

The main concern of this project is to develop a desktop application to encrypt our confidential and sensitive data by ourselves and directly upload in the Google drive. To achieve this output most secured and efficient encryption algorithm should be identified, and usability of the system should be high. These facts give the motivation to build a better software solution that would provide increased data security and high quality of usability and understandability as main expected outputs.

Manisha R. Shinde and Rahul D. Taur stated that problems associated cloud computing as data privacy, security, anonymity, and reliability, etc (Shinde and Taur, n.d.). They also signify the most important facts as security and how to assure it. Using cloud computing users can access, manipulate and configure applications online and not need any specific software installation. Clients can access cloud resources, platform independently. No required interactions with the cloud service provider to use resources and cloud computing is a highly cost-effective service with greater efficiencies. Issues in the cloud can be defined as less trustworthy data and service management since cloud moves data to large software and database centers. In this research, the proposed technique used is to convert a plain text to ASCII code value of each alphabet.

This research of Zaid Kartit, Ali Azougahe, H.Kamal Idrissi, M.El Marraki, M.Hedabou, M.Belkasmi, and A.Karitit is on applying encryption algorithm for data security in cloud storage(Kartit et al., 2016). These cloud storages are known as Storage as a Service (STaaS) where service providers rent out storage spaces for individuals or companies. However, still, there are problems regarding data privacy, security, and reliability. Authors have stated that AES symmetric encryption algorithm has been used in this project for its robustness and speed. RSA algorithm has been used to encrypt AES key. Cloud models have five essential characteristics of On-demand self-service, broad network access, resource pooling, elasticity measures service. Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (Sass) are the layers of cloud computing. There are also several types of cloud deployment models like private, public, hybrid and community.

Research by Abdel-Karim A Tamimi addresses the performance analysis of data encryption algorithm (Tamimi, n.d.). Algorithms can be compared by using two characteristics of,

- Ability to protect secured data against attacks

- Speed and efficiency in protecting those data

The author has compared performance among four encryption algorithms: DES, 3DES, Blowfish and AES. Five main cryptography goals are authentication, secrecy or confidentiality, integrity, non-repudiation and service reliability, and availability. The research has concluded stating that Blowfish has a better performance than other common encryption algorithms considered. Blowfish has become the best algorithm since no security weaknesses identified so far.

Nasarul Islam.K.V, Mohammed Rigas.K.V have done a research on analysis of various encryption algorithms in cloud computing("V6I7201729.pdf," n.d.). According to their survey, they have found that more than 70% of Chief Technical Officers State the reason for not using cloud storages as data security and privacy concerns. Stated benefits of cloud computing are reduced cost, scalability and flexibility, backup and recovery, collaboration and deliver new services.

Muhammed Faheem Mushataq, Sapiee Jamel, Abdulladir Hassan Disinia, Zahraddeen A.Pindar, Nur Shafinaz, Ahamad Sakir, and Mustafa Mat Deris are the authors who have done a survey on the cryptographic encryption algorithms(Faheem et al., 2017). They have examined the security aspects and processes in Data Encryption Standard (DES), 3DES, AES, Hybrid Cubes Encryption Algorithm (HiSea) and Blowfish. Based on the performance they have concluded that Blowfish, AES, and HiSea will provide more security from available resources. This survey also concludes that the Blowfish algorithm is the best for applications where memory and cryptographic operations are mainly concerned with the software. They also state that AES and HiSea are suitable for applications that give priority for integrity and confidentiality.

A research study on Encryption Algorithms AES, DES, and RSA for security have completed by Dr.Prerna Mahajan and Abhishek Sachdeva(Mahajan and Sachdeva, 2013), in order to focus on the area of Cryptography to secure the data while transmitting through networks. Authors have compared the algorithms AES, DES, and RSA by performance and simulated time. They conclude that the AES algorithm consumes least time compared to RSA which has consumed the longest encryption time. For AES simulation and Decryption are better than the other two algorithms.

Research on Encryption Algorithms RSA, DES, BDES, and AES for Information security is done by the author

Gurpreet Singh (Singh and Supriya, 2013). He states that Asymmetric encryption is slower than symmetric encryption technology and it is quite hard to use on a large amount of data.

Speed up Ratio = Mean processing time on single processor/ Mean processing time of cloud

Speed up ratio is used for implementing security algorithms using cloud resources. Avalanche effect is measured by the change in the ciphertext according to the small change in the key or plain text. For AES avalanche effect is higher than for DES. According to the comparison, AES is the fastest most secured symmetric block cipher which has a block size of 128 bits.

Ranjeet D.Masram has done research on an efficient selection of the compression-Encryption algorithm for securing data("121222010-Masram.pdf," n.d.). He considered the file formats such as H17, DICOM images and other audio, images, text data formats regarding health data that must be remitted confidentially. For that security, performance and implementation cost of cryptography algorithms are discarded. He suggests if compression of data added with the encrypting process would provide higher security and faster transfer rate. For different algorithms, performance will vary on parameters like data type, data size, density, key sizes, and block cipher modes. Analysis of this project states that encryption rate of AES was the highest from all selected block ciphers and encryption time is directly proportional to the data size.

Ekta Agrawal, Dr. Parshu Ram Pal has done research on a secure and fast approaching for encryption and decryption of message communication (Agrawal and Pal, 2017). They stated encryption as the most effective method for achieving data security and privacy. The security parameters can be identified as architecture, performance, security, flexibility, scalability, and limitations. The research concludes that short messages can be sent securely with the use of encryption.

According to the searches and observations carried out, there are only a few desktop-based applications that encrypt data for google drive with a simple mechanism of select data, encrypt data and upload encrypted data. Researching and identifying the best encryption algorithm adds the innovativeness to the proposed system. Developing a user-friendly interface without user guides will be a new feature compared to the existing similar systems.

Boxcryptor is a similar existing system found, that is a desktop-based application for data encryption on cloud drives. It provides private, end-to-end encryption for both cloud and local storage (Feb'19 2018-03-20T05:31:54- 08:00, 2018). Boxcryptor can be used for personal and business purposes and users can share files securely. The issues can be encountered are the inability to reset the password and user-friendliness. It provides user guidance through a tutorial that would be difficult for some users, having basic computer knowledge.

III. METHODOLOGY

Table 1. Comparison of Similar Systems

System	Features			
	Encryption Algorithm used	**Compatibility**	**Platform**	**Weaknesses**
Boxcryptor	RSA and AES	Windows and MacOS	Desktop based	No password reset
Cryptomator	AES-256	Windows, Linux and MacOS	Desktop based	File and folder names are encrypted
Tresorit	AES-256	Windows, Android, iOS, Mac, and Linux	Web based	Expensive, Lacks integration
pCloud Crypto	AES-256 and RSA-409bit	Provides a separate cloud storage	Web based	Limited support channels, Limited support available in other languages
IDrive	AES-256	Windows, iOS, Mac or Android and provides separate cloud storage	Web based	No unlimited backup plans, Versioning limited to 30 versions
Sookasa	AES-256	Windows, Mac, Android, and iOS	Desktop based	Mostly used for audit activities, free only for individual users

Above issues motivate to develop a system that can provide data security to the cloud storages. This system suggests a mechanism that encrypts data before uploading to the cloud. Since the proposed application is a desktop-based system, it provides another facility to encrypt data in local drives. Direct login mechanism is performed through a system window by providing email and password of the cloud drive, creates the similarity to the usual log in mechanism done through a web browser. It would make the user understand and use the system easily. By making the decryption process only through the system, provides data integrity and confidentiality after a successful authentication. The file selected from the PC will be encrypted using the AES algorithm. In order to increase the security, the keys generated by AES encryption will be encrypted again by using RSA algorithm. Encrypted keys then will be stored in an embedded database for future use on decryption.

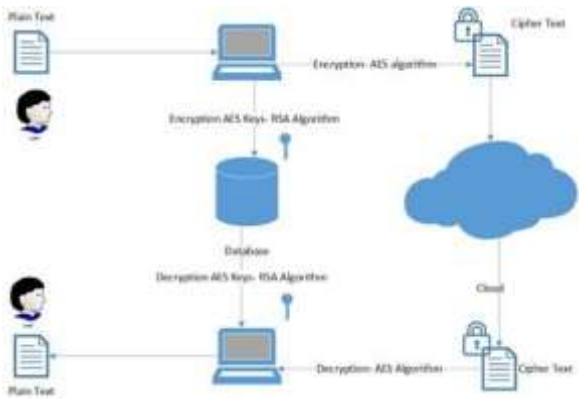

Figure 1. System model on cloud data encryption and decryption

A. File Uploading Process

This is the main mechanism of the system that consists of two processes. The main function is the encryption of the selected file using AES algorithm. The second function is the encryption of AES-keys generated by the first encryption process, using the RSA algorithm. Then store the encrypted AES-keys in a database.

Functions for the file upload process:

No_Of_Blocks(File): Returns the number of blocks in the file.

Encrypt_AES(Block,Key): Encrypts 'Block' using AES algorithm generating ' Key'

Upload_to_Cloud(E_File): Uploads the encrypted File 'E_File' to Cloud (Google Drive)

Encrypt_RSA(Key): Encrypt the 'Key' generated from first encryption using RSA algorithm

Key_size(Key): Size of the generated key

Store_In_Database(E_Key): Store encrypted key 'E_Key' in the database

Algorithm 01: File_Upload

```
1.  EncryptFile(File){
2.
3.  /*process 1: File encryption using AES */
4.  for Block <- No_Of_Blocks(File){
5.  do {
6.    E_File=Encrypt_AES(Block,Key); 7.}
8.  return (E_File);
9.  }
10. Upload_to_Cloud(E_File);
11.
12.  /* process 2: Key encryption using RSA*/
13. for Key <- Key_size(Key) {
14. do {
15.           E_Key=Encrypt_RSA(Key);
16. }
17. return (E_Key);
18. }
19. Store_In_Dayabase(E_Key);
20. }
```

B. File Downloading Process

The file download process is the next important task need to be done by the system. It also consists of two phases of decrypting the file and decrypting the key, retrieved from database.

Following are the functions for the download file download process:

No_Of_Blocks(E_File): Returns the number of blocks in the file.

Decrypt_RSA(E_Key): Decrypt the key using RSA algorithm.

Decrypt_AES(E_Block,Key): Decrypt the file using AES key by decrypting each encrypted block

Algorithm 02: File_Download

```
1.  DecryptFile(E_File){
2.
3.  /*process 1: AES Key Decryption using RSA*/
```

4. for E_Key <- Key_Size(E_Key){

```
5.    do {
6.      Key=Decrypt_RSA(E_Key); 7.
        }
8.    return (Key);
9.    }
10.
11.    /* process 2: File Decryption using AES*/
12.   for E_Block <- No_Of_Blocks(E_File) {
13.   do {
14.             File= Decrypt_AES(E_Block,Key)
15.   }
16.   return (File);
17.   }
18.   }
```

C. File Encryption in local drives

An additional facility is the file encryption on local drives. User can get the encrypted form of the files in the computer for applying enhanced security. This process also uses the AES algorithm for file encryption and RSA algorithm for key encryption. When a user selects this option, he is provided with a user login interface that enables new users to create a new account and others to login to their account by providing username and password. For each account, a separate table will be created in the database to store encryption keys that will be generated by the file encryptions.

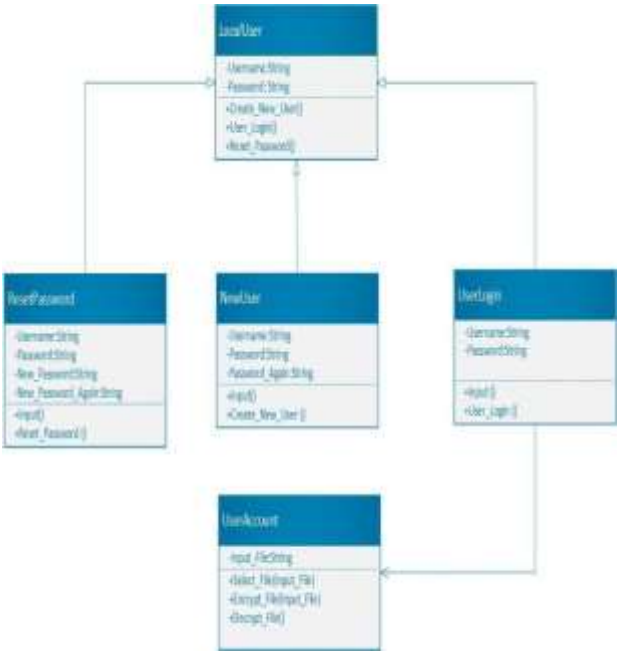

Figure 2. UML class diagram for local file encryption

D. Implement results and analysis

The system is developed using Java 8. Implementations are done using an ASUS laptop with the following

specifications: Intel CORE i7-6700HQ, up to 3.5 GHz and 8 GB RAM.

The system has following advantages and strengths:

- Reduce the damage can be caused by cyber- attacks in Sri Lanka.
- Increase the security of personal data.
- Reduce the financial loss that can be happened by cyber-attacks.
- Develop the data integrity in government and private sectors providing a secure way to use public cloud storages.
- Encourage more developments regarding Cyber security.
- Provides enhanced security to the encrypted files not by storing decryption keys in the cloud.
- Use of AES encryption algorithm gives the fastest performance in file uploading and downloading processes.
- AES algorithm adds more integrity and confidentiality compared to other block ciphers.
- Symmetric keys can be changed to improve security.
- Since the key generated by AES encryption, is again encrypted using the RSA algorithm, the integrity can never be broken.

IV. CONCLUSION AND FUTURE WORK

Most of everything depends on data now in the society, and the presented project will mainly help to protect the safety of the people by securing the important and sensitive data that may bring harm to them if get vulnerable. Even though cloud storage provides some security within the services, there are cyber-attacks being carried out to exploit the information. If we can provide solutions to the issues encountered from these exploitations, cloud storage services will benefit small and large business developments. This system will encrypt data on Google Drive and even if an intruder accesses the data, he cannot decrypt the files without the keys that are encrypted and securely stored in the local database, not within the cloud. As perspectives, use of the system can be extended for different cloud services and improve the security with enhanced encryption algorithms.

V. REFERENCES

3630-Article Text-6635-1-10-20180104 (1).pdf, n.d.

121222010-Masram.pdf, n.d.

Agrawal, E., Pal, D.P.R., 2017. A Secure and Fast Approach for Encryption and Decryption of Message Communication 6.

Best Free Apps to Encrypt Files & Data before Uploading to the Cloud, 2018. . Comparitech. URL https://www.comparitech.com/blog/cloud-online-backup/6-apps-to-encrypt-your-files-before-uploading-to-the-cloud/ (accessed 5.25.19).

Cryptography and Network Security_ Principles and Practice 7th Global Edition.pdf, n.d.

Faheem, M., Jamel, S., Hassan, A., A., Z., Shafinaz, N., Mat, M., 2017. A Survey on the Cryptographic Encryption Algorithms. Int. J. Adv. Comput. Sci. Appl. 8. https://doi.org/10.14569/IJACSA.2017.081141

Feb'19 2018-03-20T05:31:54-08:00, J.G.-L.U. 11, 2018. Boxcryptor Review [WWW Document]. Cloudwards. URL https://www.cloudwards.net/boxcryptor/ (accessed 5.25.19).

Hanna, S., 2009. Cloud Computing: Finding the Silver Lining 41.

Kartit, Z., Azougaghe, A., Kamal Idrissi, H., El Marraki, M., Hedabou, M., Belkasmi, M., Kartit, A., 2016. Applying Encryption Algorithm for Data Security in Cloud Storage, in: Sabir, E., Medromi, H., Sadik, M. (Eds.), Advances in Ubiquitous Networking. Springer Singapore, Singapore, pp. 141–154. https://doi.org/10.1007/978-981-287-990-5_12

Mahajan, D.P., Sachdeva, A., 2013. A Study of Encryption Algorithms AES, DES and RSA for Security 9.

More Than 1 Million Google Accounts Breached by Gooligan [WWW Document], 2016. . Check Point Softw. Blog. URL https://blog.checkpoint.com/2016/11/30/1-million-google-accounts-breached-gooligan/ (accessed 5.25.19).

Shinde, M.R., Taur, R.D., n.d. Encryption Algorithm for Data Security and Privacy in Cloud Storage 6.

Singh, G., Supriya, S., 2013. A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security. Int. J. Comput. Appl. 67, 33–38. https://doi.org/10.5120/11507-7224

Tamimi, A.R.A., n.d. Performance Analysis of Data Encryption Algorithms 14.

techsegun, 2019. What are the best cloud encryption tools in 2019? [Updated List] [WWW Document]. Window Rep. - Window 10 Microsoft News - Tips. URL https://windowsreport.com/cloud-encryption-tools/ (accessed 5.25.19).

User, S., n.d. Cloud Computing: A New Vector for Cyber Attacks [WWW Document]. Apriorit. URL https://www.apriorit.com/dev-blog/523-cloud-computing-cyber-attacks?jve=1558711458 (accessed 5.24.19).

V6I7201729.pdf, n.d.