European Proceedings of
Multidisciplinary Sciences
EpMS

www.europeanproceedings.com

e-ISSN: 2421-826X

DOI: 10.15405/epms.2022.10.26

ICONSPADU 2021
International Conference on Sustainable Practices, Development and Urbanisation

SECURING ACADEMIC STUDENT FILE USING AES ALGORITHM FOR CLOUD STORAGE WEB-BASED SYSTEM

Juanita Zainudin (a)*, Fatin Puteri (b), Faizah Miserom (c), Nurshafinas Roslan (d)
*Corresponding author

(a) Kolej University Poly-Tech MARA, 56100 Cheras, Kuala Lumpur, Malaysia, anis_juanita@kuptm.edu.my
(b) Kolej University Poly-Tech MARA, 56100 Cheras, Kuala Lumpur, Malaysia, fatinputeri.fnhp@gmail.com
(c) Kolej University Poly-Tech MARA, 56100 Cheras, Kuala Lumpur, Malaysia, faizah@kuptm.edu.my
(d) Kolej University Poly-Tech MARA, 56100 Cheras, Kuala Lumpur, Malaysia, shafinas@kuptm.edu.my

Abstract

Cloud storage is an innovative technology that provides storage services to users. Many universities or companies have recently started using cloud storage services and realised their importance. However, preserving data security control in cloud storage is an issue and a very challenging task to solve. To safeguard data stored in the cloud, this study presents a web-based system using encryption techniques to handle the security and privacy issue in cloud storage. File Encryption Cloud Storage (FECS) system is a web-based system that secures students' academic files in cloud storage using encryption techniques. The system can encrypt students' academic files in cloud storage to avoid unauthorised access and misused risk. The targeted users are students of Kolej University Poly-Tech MARA (KUPTM). Moreover, the JavaScript and PHP programming languages are employed to create this system in the Microsoft Visual Studio Code Integrated Development Environment (IDE). The MySQL database is used as the backend of the system. The Advanced Encryption Standard (AES) technique is employed in the system. Furthermore, the AES approach yielded a positive outcome in the system's development. The survey's results indicate that the system is valuable and helpful to KUPTM students.

Keywords: Academic, cloud storage, cryptography, encryption, security

https://doi.org/10.15405/epms.2022.10.26
Corresponding Author: Juanita Zainudin
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

1. Introduction

The continuous advancement of technology has introduced cloud storage as a space to backup and save private files or documents in the cloud. Cloud storage has massive benefits, including reducing costs by creating a shared ecosystem for cloud users. They may access and keep their data in the cloud from anywhere. Users can avoid the burden of maintaining the physical or standalone data storage by outsourcing the data to the cloud. However, ensuring data security in the cloud is a complicated matter.

This research studies the cryptography technique to secure private files or documents in cloud storage. A cloud storage application known as File Encryption Cloud Storage (FECS) system was developed to implement the encryption technique to all uploaded files in the cloud. The development of the system aims to assist users in backup and to save their files in the cloud in secure ways. Recently, users preferred to backup and save files in cloud storage such as Google Drive, iCloud, and Dropbox (Chen et al., 2020). However, the current application has been exposed to certain unauthorised access and misused risk from external threats (Chen et al., 2020). This occurred when private files in the cloud storage were accessed by unauthorised users by mistake or intentionally after successfully breaching the entry password (Goel & Hofstede, 2021).

Various methods are available in the cryptography technology used to protect data privacy, authentication, and integrity. This study uses encryption to secure private files or documents in the cloud storage application. According to (Pansotra and Singh (2015), encryption is a process to protect the data by changing it into a secure format. The Advanced Encryption Standard (AES) encryption method is used as the algorithm to encrypt files and documents saved in the cloud storage application. This algorithm is suitable for securing data because they need keys to decrypt the files (Bhardwaj et al., 2016). According to (Harba, 2018), the AES encryption method will keep data safe against any Men-in-the-Middle Attack. The same key is used to decrypt and encrypt data in AES encryption. The public key is used to secure files or data sent by the sender. At the same time, the recipient who holds the correct private key can decrypt the files. In this work, we have postulated a File Encryption Cloud Storage (FECS) system that uses the AES encryption method on the client-side of the application before uploading data to a cloud storage service.

According to (TECHOPEDIA, 2020), a cloud drive is a web-based service that provides storage that can be accessed through the internet using client-side server software that enables the users to save their files in the cloud-based storage and not in their hardware devices. It can be accessed at anytime and anywhere. The target users of this study are students. Problems and issues are analysed to identify the requirements of the system. Using cloud storage to save files and documents can save the student hassle of carrying a pen drive everywhere. FECS system will benefit users by providing a secured cloud drive storage with 24/7 accessibility. The application will allow students to manage their files and documents securely. Therefore, developing the application is a prominent initiative because it will be effective and efficient for users in the long run.

https://doi.org/10.15405/epms.2022.10.26
Corresponding Author: Juanita Zainudin
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

1.1. System Framework

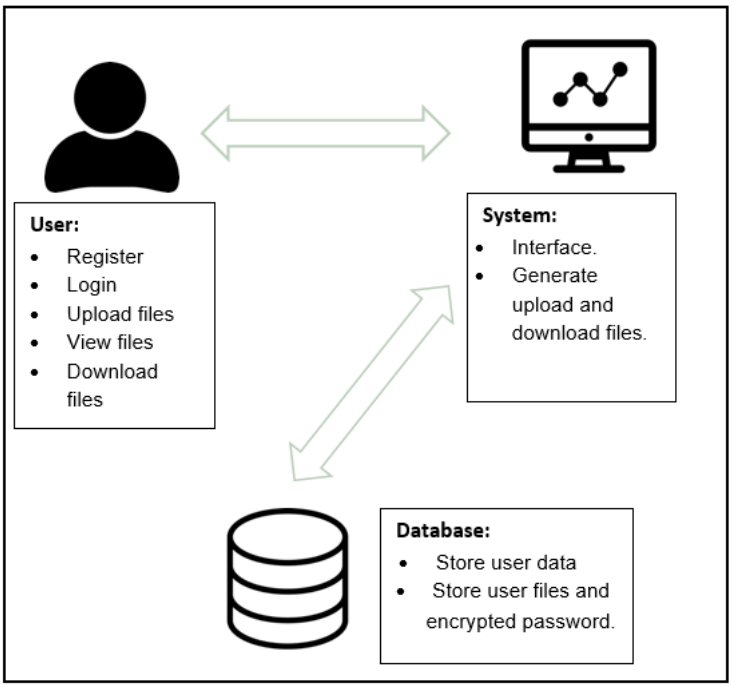

Figure 1. File encryption cloud storage framework

Figure 1 shows the framework of the File Encryption Cloud Storage (FECS) system. Users must register and log in before being able to access the system. Furthermore, users can manage the upload and download of files or documents themselves. Uploaded files or documents will be encrypted and saved in cloud storage. The role of a cloud database is to store user data, encrypted files, and passwords.

1.2. Previous Study

According to (Shrivastava et al., 2020), encryption is mixed-up data that only an authorised person can understand. The process of encryption is converting plain text into ciphertext (Sahi et al., 2021). The process is changing the legible data into an output that consists of random words. This method requires using an encryption key value that only the sender and receiver would know the encrypted message. Symmetric encryption is the type of encryption with only one key called a secret key (Sun & Mu, 2020). The information is decrypted and encrypted using this key. Therefore, the procedure communicates using symmetric encryption and must exchange the key applied in the decryption process in this encryption (Hariss et al., 2020).

Information exchange activities continue to increase, especially in the age of digital communication. All data transferred or received is susceptible to various active and passive assaults. As a result, the most pressing worry is data security during communication. Cryptography is crucial for securing network communication, and it offers a fantastic method for providing the required security (Bokhari & Shallal, 2016). There are numerous pairs of keys in a wide network that must be properly monitored. As a result, the administration of the effective key necessitates using a TTP that can be trusted entirely.

https://doi.org/10.15405/epms.2022.10.26
Corresponding Author: Juanita Zainudin
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

Typically, the cloud drive provides a limited amount of free online storage space, with more storage space to be purchased monthly or annually. Access to the same data can be synchronised via a cloud drive. It also handles reading and writing requests for a variety of data. In addition, the cloud drive indirectly creates a system that enhances the existing system where the user does not have to do it manually. Besides that, it can also create a secure place and provide a security element in the system where the users do not have to worry about the safety of the files they save in the cloud drive.

Hossein (2021) mentions that a sophisticated cryptography technique is pointless as computational speed is critical. As a result, this method employs a combination of an elliptic curve-based and improved Blowfish algorithms. The data will be encrypted with Blowfish, and the key will be encrypted with the elliptic curve technique, increasing security and performance. Although cloud computing makes our life easier, it also creates a serious risk and exposes us to cyberattacks such as authentication exploitation, sniffer, spoofing, and resource manipulation (Tabrizchi & Rafsanjani, 2020).

The AES technique is widely used for data encryption. This method was chosen because it is more secure than IDES or 3DES. Symmetrical block encryption is how AES is described. The algorithm's operations are 8-bit or higher (Hidayat & Mahardiko, 2020). Moreover, AES is used to safeguard data transmission and storage in cloud computing to prevent an attack by an unauthorised individual.

2. Problem Statement

Almost every company has incorporated cloud computing into its operations to some degree. Nevertheless, cloud adoption necessitates a review of the company's cloud security plan. This is to see if cloud adoption can fend off the most frequent cloud security threats. In addition, given the ease with which cloud infrastructure may be used and shared, it can be difficult for businesses to make sure the data is only available to those who require it. Data loss, multi-tenancy, leakage, identity management, cloud accessibility, unsafe APIs, internal threats, patch management, service level agreement, and inconsistencies are all examples of cloud computing security challenges (Sachdev, 2013).

The current cloud drive application does not apply any file encryption technique. No file encryption technique is used in the present cloud drive application. The users would simply save their files to the cloud. Users need to encrypt the files in another application before uploading them to the cloud drive. However, a cybercriminal can easily access the cloud by breaking the password and guessing the security question. This occurs when the unauthorised person accesses the user's cloud drive and can lead to data leakage. The unauthorised person can transmit personal files to an external destination without the encryption element.

According to Mather et al. (2009), users' data can be protected in the cloud by utilising encryption. However, the issue of whether or not a user's data is encrypted when stored in the cloud emerges. EMC's MozyEnterprise, for instance, encrypts user data, while AWS S3 does not. In addition, as companies become more dependent on cloud-based infrastructure and applications for critical business operations, account hijacking is among the most critical cloud security issues. Moreover, an attacker capable of accessing an employee's accounts can acquire access to sensitive information or activity, whereas a stolen customer's credentials grant them total power over their online account.

https://doi.org/10.15405/epms.2022.10.26
Corresponding Author: Juanita Zainudin
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

The process of encryption and the uploading process in the cloud is not synchronised, which means users need to go through many procedures before they can save the encrypted files in the cloud drive. Some of it requires the cost to encrypt the files in the cloud drive. Existing security solutions only use one or two features simultaneously, resulting in reduced security and increased time spent encrypting and decrypting data. As a result, the process takes longer, resulting in increased network usage, energy consumption, and network delay (Abikoye et al., 2019). Because cloud computing is a platform that successfully exchanges data and resources, users must be given security, as security is a vital part of cloud computing. As a result, the cloud service provider's job is to offer security with all features, including decreased power use, network delay, and time consumption (Essa & Ashoor, 2019).

To provide excellent services without losing any data, cloud storage requires diagnosing security mechanisms such as integrity, confidentiality, and availability. Encryption is a method of concealing information by transforming it into random data. Therefore, encryption is essential for Internet protection (CLOUDFLARE, n.d.). With this system, users can upload their files to the cloud system with the automatic encryption process. However, encrypting the files is essential to secure them from potential harm.

3. Research Questions

i. What is the cryptography technique used to secure cloud storage from unauthorised access?
ii. What is the user satisfaction level toward the system?

4. Purpose of the Study

The study aims to offer better solutions for KUPTM students in securely managing their files. The files are now saved and secured in cloud storage. In addition, cloud storage can avoid the hassle of bringing a pen drive everywhere. Students can access their saved works in cloud drive regardless of place and time. The system uses the AES method to encrypt the uploaded files. As the cloud storage exposes files to data breaches and unauthorised access, the AES method provides a solution by encrypting the files in the cloud. Hence, files in the cloud are not easily stolen by unauthorised parties. The AES method is successfully implemented in the system. The system benefits users in terms of accessibility and safety. Findings from the users' experience survey show that the system is functioning well and is beneficial to KUPTM students.

5. Research Methods

The waterfall model is employed in developing the encryption system. The waterfall model (Figure 2) is controlled by seven non-overlapping stages: requirements, analysis, design, coding/implementation, testing, implementation, and maintenance. A software project is a highlight of the logical progression of steps. This method is linear and flows function like a waterfall that starts from high to low level. Each phase has its own goals and cannot turn back after completing the phases. Waterfall methodology depends on the sequential approach that every phase should complete before starting the next phase. It allows for departmentalisation as well as administrative authority. It is effortless to

https://doi.org/10.15405/epms.2022.10.26
Corresponding Author: Juanita Zainudin
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

understand and put into practice. The model's rigidity may be easily controlled since each phase has its deliverables and review procedures. Subsequently, each matter is reviewed and finalised. As a result, this system is appropriate for its primary development model for the encryption system's maintenance, planning, design, and programming.

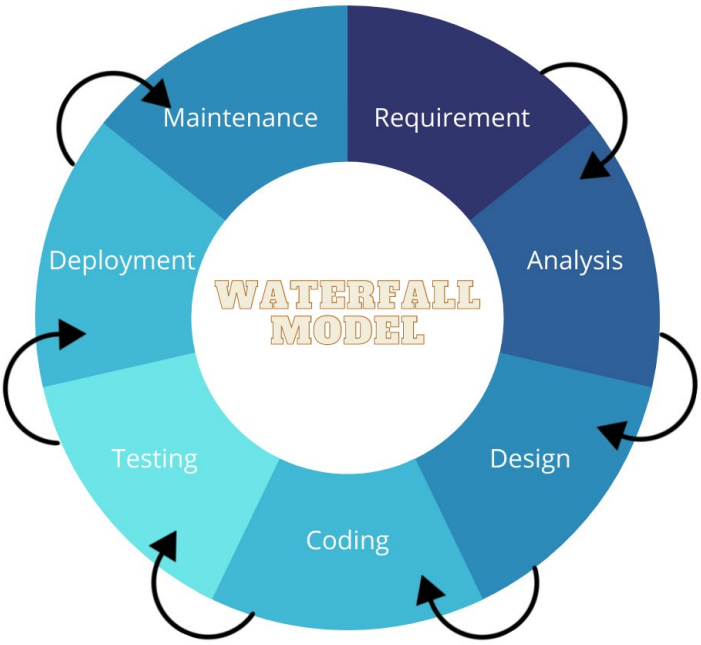

Figure 2. Waterfall model

The users' application was developed using PHP programming, used as the programming language for the implementation. At the development stage, Apache, XAMPP, and PHP were employed as server backends, while Atom was used as a code editor. The actions completed at each phase are listed in Table 1. Each phase comprises important tasks starting from the requirement to the maintenance phase. All the tasks in each phase flow to each other, where progress is seen as flowing steadily downwards through the phases.

Table 1. List of tasks

Phase	Task
Requirement	Define and plan the project without mentioning the specific process through a questionnaire.
Analysis	Investigate the function software to check the chance and consequence.
Design	Identify and describe the software system.
Coding	Source code is developed using the logic, models, and requirement design in the earlier stage.
Testing	Integrated and tested as a complete system to ensure the system meets the requirement.
Deployment	System is ready for launch.
Maintenance	Improving the system and enhancing the system serves as a new requirement are discovered.

https://doi.org/10.15405/epms.2022.10.26
Corresponding Author: Juanita Zainudin
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

5.1. System Design

The use case diagram shows the process and activities involved in this system. Figure 3 and Figure 4 portrays the use case diagram and entity relationship for the FECS system. Here, the main actor is the user. The system's target user is KUPTM students. The system's main activities are register/login, uploading files, downloading files, changing passwords, and logout. Next, the system will encrypt the uploaded file before being saved in cloud storage. Finally, the system will decrypt the downloaded file for the user's access and view.

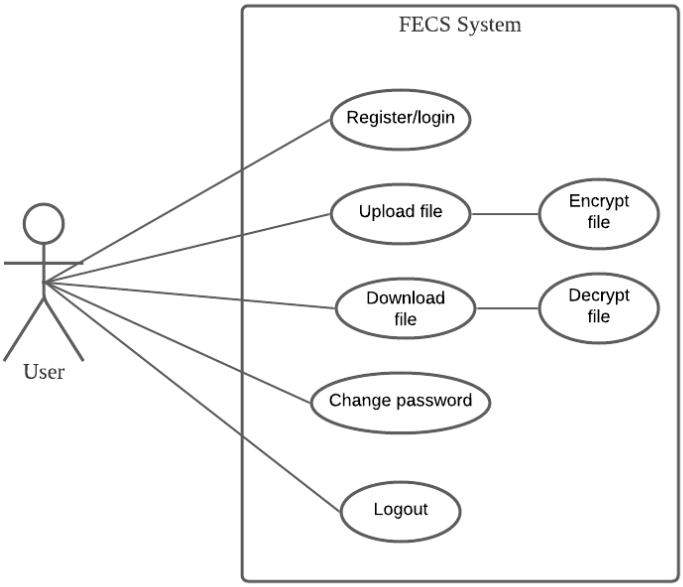

Figure 3. FECS use case diagram

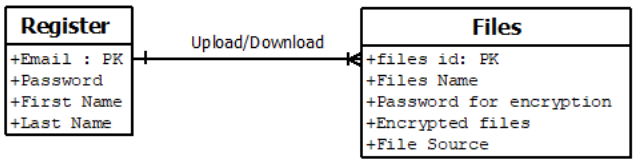

Figure 4. FECS entity relationship diagram

The Business Process Modeling Notation (BPMN) diagram in Figure 5 shows the process and flow of the system in detail. The process starts with a user who needs to log in before proceeding to the default page. The new user needs to register first. The system will validate the newly registered username. If the username already exists, the system will notify the user to use another name. The main page contains upload and download file functions. The uploaded file is encrypted by the system and saved to the database. The user can access or review the encrypted file using the download function. The system decrypted the downloaded file for the user to view or access.

https://doi.org/10.15405/epms.2022.10.26
Corresponding Author: Juanita Zainudin
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

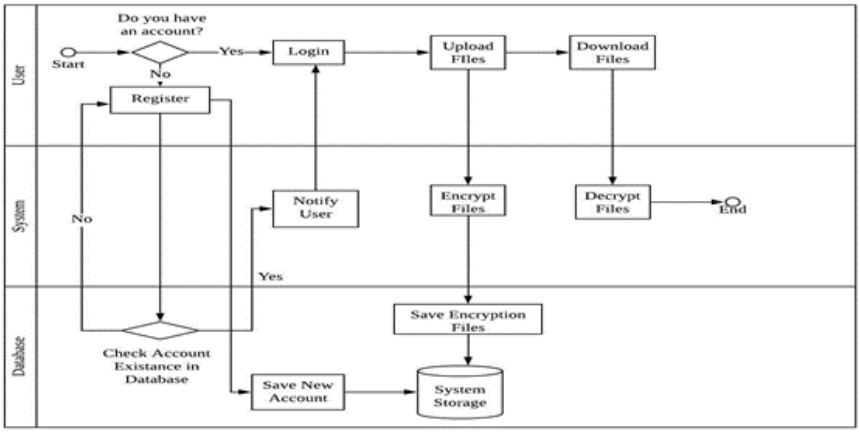

Figure 5. FECS BPMN diagram

6. Findings

6.1. Interface System

6.1.1. Login & Sign Up Interface

Figure 6. Login interface

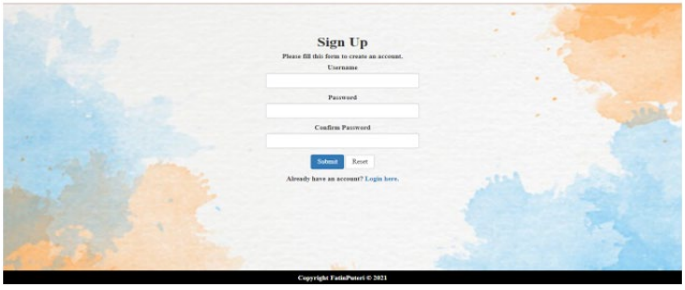

Figure 7. Sign up interface

The Encrypted Cloud Storage System login's main interface is shown in Figure 6. The user needs to have an account, and only authorised users are able to enter the system. The username and password are formed on the Sign-Up page, in which the user could use the username and password to establish his or her own account. The sign-up screen for a new system user is shown in Figure 7. Users will create an account by providing the necessary login information, for instance, their username and password. The

https://doi.org/10.15405/epms.2022.10.26
Corresponding Author: Juanita Zainudin
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

user must complete all fields, and after the submit button is pushed, the information will be submitted. Users can also reset their data after completing the form if they enter inaccurate information. Moreover, the username must be distinct, have never been registered, and cannot be similar to another username that has been previously registered. The user can log in if they have a registered account by clicking the login icon.

6.1.2. Home & File Uploaded Interface

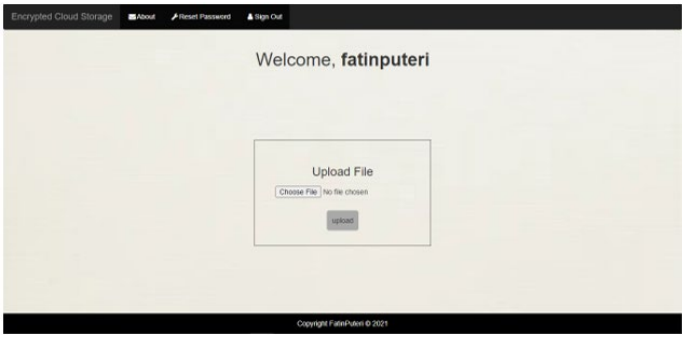

Figure 8. Home interface

Figure 9. Files uploaded interface

The home interface is portrayed in Figure 8. It welcomes the user by their first and last name. “About,” “Reset Password,” and “Sign Out” are the three navigation tabs on the menu bar. Users can add their papers to be encrypted in the space in the middle of the main page. After the user chooses files and hits the upload button, the encryption procedure will begin. Only .pdf, .docx, and.txt files are allowed to be uploaded by the user. The files will be kept in a database after being encrypted. A list of files uploaded to the home interface is shown in Figure 9. It also shows how many times the file has been downloaded, as well as the tasks that must be completed. By clicking the link, the user can obtain the necessary files.

6.2. Respondent Survey

Twenty-five students from diverse degree programmes were randomly assigned a survey questionnaire. They are between the ages of 21 and 25, and the majority are in the seventh to ninth grade/semester. The survey includes a system overview. The questionnaire for students consisted of 15 questions that assessed and focused on students’ perceptions of the proposed system. Each question was assessed using an ordinal scaling technique ranging from (1) strongly disagree to (5) strongly agree. Here,

https://doi.org/10.15405/epms.2022.10.26
Corresponding Author: Juanita Zainudin
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

respondents are selected using purposive sampling. Table 2 shows the result of the survey. It summarises the users' opinions and responses to the system.

Table 2. Users' opinion and response towards the system

Question	System Overview
Q1	58.8% of the respondents strongly agree that this system is user-friendly and not confusing.
Q2	94.1% of the respondents strongly agree that the button on the Login page is functioning.
Q3	82.4% of the respondents strongly agree that they can fill up the Signup page and the button is working perfectly fine.
Q4	82.4% of the respondents strongly agree that users can register and login into this system.
Q5	52.9% of the respondents agree that users cannot register with the same username. This reflects that users need a unique username to register in order to have a security element in the login phase.
Q6	64.7% of the respondents agree that users can access the Frequently Asked Questions (FAQ) page without logging in. FAQ provides information regarding the system if users have enquiries.
Q7	82.4% of the respondents strongly agree users can upload files once they have chosen and selected the file to be uploaded. It indicates that users may search and upload their file.
Q8	82.4% of the respondents strongly agree that the upload button can be clicked. It indicates that the upload button is works well.
Q9	70.6% of the respondents strongly agree the files are encrypted when users click the upload button. It indicates the upload button and the functionality of the upload button with the encryption process work well.
Q10	82.4% of the respondents strongly agree they can view their uploaded files on the home page.
Q11	70.6% of the respondents strongly agreed that each of the buttons on the navigation bar function well.
Q12	82.4% of the respondents strongly agree that users may download the selected files.
Q13	82.4% of the respondents strongly agree that users may observe an error after downloading the files since the files are encrypted.
Q14	82.4% of the respondents strongly agree that users may not go back to the homepage once they sign out Unless they have to re-login.
Q15	76.5% of the respondents strongly agree this system may facilitate the users to secure their uploaded files.

6.3. Encryption Process

Because it integrates speed and security, AES is now one of the greatest encryption methods on the market. AES has 128, 192, or 256 key lengths, providing billions of potential combinations. Traditional algorithms like RSA (Rivest–Shamir–Adleman) are substantially slower than this (Zhang et al., 2020). As a result, it is a fantastic way to secure data on the cloud. This approach is best for those who have a steady internet connection.

https://doi.org/10.15405/epms.2022.10.26
Corresponding Author: Juanita Zainudin
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

The AES algorithm is used to encrypt and decode the file in this suggested system. Users can both upload and download files to the system. The system will then encrypt the uploaded file for security purposes. Hence, the unauthorised user who successfully breaches the system cannot view the encrypted files. The download file is decrypted and can be viewed as the original version. Figure 10 shows a schematic representation of the complete process. The steps for downloading and uploading files are outlined in this section

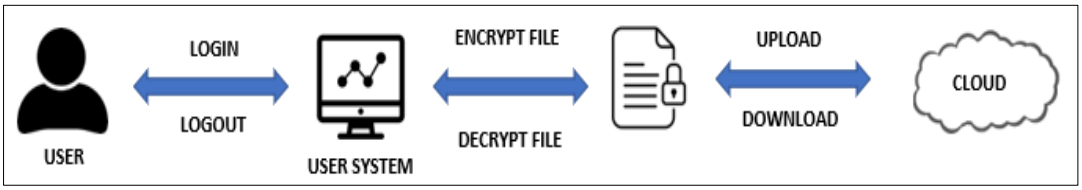

Figure 10. Process upload and download file

The process begins with user authentication. Username and password will be accepted and verified by the system. Only authentic login credentials are used to establish a cloud connection. The system will show an error message, in which the authentication process will be refused if the username or password entered is incorrect. Next, users are allowed to upload files when they have been verified. Any text file on the user's computer can be selected. Only three file types are supported by the system at the moment: plain text, Microsoft Word, and PDF. The plain text is encrypted using the AES technique when a user clicks the Upload Button. For the encryption method, a key is created. The AES algorithm is a symmetric key algorithm. It employs a similar key to encrypt and decode data. The keys of the AES algorithm are impervious to any known attack. A Brute-force assault on the password is, however, doable. Therefore, the user is highly urged to create the key using long passwords. The data will be uploaded to the cloud after the encryption procedure is completed. Users can also save the encrypted files to their computers by downloading them. The download process is secured by a key code password. Authorised user needs to enter a key code password before able download and decrypt the file. The downloaded file with the correct key code password will be decrypted, and the user can view back the original file format. Finally, if a user chooses to stop using the service, the user will then log out of the account and get disconnected from the cloud.

7. Conclusion

A mechanism for encrypting files prior to uploading them to the cloud was proposed in this study. AES is among the most secure encryption algorithms available, as even when data encrypted with AES is subjected to a limited number of attacks, the files are secured. Users should also use a login id and password to verify that their information is accessible in a legitimate and permitted manner. As a result, when cloud computing is used safely, it offers extraordinary value to users and eliminates its only drawback: security issues. Extra security authentication, such as One Time Password (OTP) passwords and the ability to share files, will be proposed in future work.

https://doi.org/10.15405/epms.2022.10.26
Corresponding Author: Juanita Zainudin
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

References

Abikoye, O. C., Haruna, A. D., Abubakar, A., Akande, N. O., & Asani, E. O. (2019). Modified Advanced Encryption Standard Algorithm for Information Security. *Symmetry, 11*(12), 1484. https://doi.org/10.3390/sym11121484

Bhardwaj, A., Subrahmanyam, G. V., Avasthi, V., & Sastry, H. G. (2016). Security Algorithms for Cloud Computing. *Procedia Computer Science, 85*, 535-542. https://doi.org/10.1016/j.procs.2016.05.215

Bokhari, M. U., & Shallal, Q. M. (2016). A Review on Symmetric Key Encryption Techniques in Cryptography. *International Journal of Computer Applications, 147*, 43-48. https://doi.org/10.5120/ijca2016911203

Chen, S. J., Qin, Z., Wilson, Z., Calaci, B., Rose, M., Evans, R., Abraham, S., Metzler, D., Tata, S., & Colagrosso, M. (2020). Improving recommendation quality in google drive. In Proceedings of the 26th ACM SIGKDD *International Conference on Knowledge Discovery & Data Mining* (pp. 2900-2908). https://doi.org/10.1145/3394486.3403341

Essa, H. A., & Ashoor, A. S. (2019). Enhancing Performance Of AES Algorithm Using Concurrency and Multithreading. *ARPN Journal of Engineering and Applied Sciences, 14*(11).

Goel, K., & Hofstede, A. H. (2021). Privacy-Breaching Patterns in NoSQL Databases. *IEEE Access, 9*, 35229-35239. https://doi.org/10.1109/ACCESS.2021.3062034

Harba, E. S. (2018). Secure Data Encryption by Combination AES, RSA and HMAC. *Al-Kut Univ. College Journal, 2*(2).

Hariss, K., Noura, H. N., & Samhat, A. E. (2020). An efficient fully homomorphic symmetric encryption algorithm. *Multimedia Tools and Applications, 79*, 12139-12164. https://doi.org/10.1007/s11042-019-08511-2

Hidayat, T., & Mahardiko, R. (2020). A Systematic Literature Review Method on AES Algorithm for Data Sharing Encryption on Cloud Computing. *International Journal of Artificial Intelligence Research, 4*(1), 49-57. https://doi.org/10.29099/ijair.v4i1.154

Hossein, A. (2021). A Hybrid Encryption Solution to Improve Cloud Computing Security using Symmetric and Asymmetric Cryptography Algorithms. *International Journal of Advanced Computer Science and Applications (IJACSA), 12*(6). https://doi.org/10.14569/IJACSA.2021.0120604

Mather, T., Kumaraswamy, S., & Latif, S. (2009). *Cloud security and privacy*. O'Reilly Media, Inc

Pansotra, E. A., & Singh, E. S. (2015). Cloud Security Algorithms. *International Journal of Security and its Applications, 9*, 353-360. https://doi.org/10.14257/ijsia.2015.9.10.32

Sachdev, A. (2013). Addressing the Cloud Computing Security Menace. *International Journal of Research in Engineering and Technology, 02*, 126-130. https://doi.org/10.15623/ijret.2013.0202007

Sahi, A., Lai, D., & Li, Y. (2021). A Review of the State of the Arts in Privacy and Security in the eHealth Cloud. *IEEE Access, 9*, 104127-104141. https://doi.org/10.1109/ACCESS.2021.3098708

Shrivastava, S., Palnitkar, S., Pathak, S., & Shinde, M. (2020). Secure Encryption of data using Symmetric and Asymmetric Cryptographic Algorithm. *Mukt Shabd Journal, 9*(6), 1100-1109.

Sun, D., & Mu, Y. (2020). On the Security of Symmetric Encryption Against Mass Surveillance. *IEEE Access, 8*, 175625-175636. https://doi.org/10.1109/ACCESS.2020.3025848

Tabrizchi, H., & Rafsanjani, M. K. (2020). A Survey on Security Challenges in Cloud Computing: Issues, Threats, and Solutions. *The Journal of Supercomputing, 76*(12), 9493-9532. https://doi.org/10.1007/s11227-020-03213-1

What is Cloud Drive? TECHOPEDIA. Retrieved on August 1, 2020, from https://www.techopedia.com/definition/26524/cloud-drive

What is encryption? | types of encryption. CLOUDFLARE. (n.d.). Retrieved on April 11, 2021, from https://www.cloudflare.com/en-gb/learning/ssl/what-is-encryption/

Zhang, L., Su, J., & Mu, Y. (2020). Outsourcing Attributed-based Ranked Searchable Encryption with Revocation for Cloud Storage. *IEEE Access, 8*, 104344-104356. https://doi.org/10.1109/ACCESS.2020.3000049