CHAPTER 5
CONCLUSION

Introduction

In this chapter, there is a comprehensive description of the topics of the project, its success and the general effect of the secured cloud storage unit that has been installed and has been using Advanced Encryption Standard (AES) encryption and a malware analyzer. It describes the purpose of the undertaken project, the benefit it is supposed to provide, the obstacles it faced, and/or how the same can be done in the next project. The chapter ends its discussion with summary of principal points and the reason as to why the project is important.

5.1 Purpose of The Project

The most important objective in this project was to design a secure cloud storage system not only scanned of malwares, but also encrypted using AES algorithm to ensure documents carrying very sensitive information were safe. This program is meant to make sure that vital data was accessed only by persons authorized and hence remained safe, precise and reliable. The project had the effects of enhancing safety of file storage system, introducing the kind of powerful encryption and active malware detecting that would help avoid data theft and unlawful access.

The initial goal that entailed having a safe cloud storage system comprising malware analysis and encryption was achieved through the development of an effective web-based storage entity. This system will help the users to save their files in their own personal cloud. The platform is well encrypted and contains malware scans so no one can unauthorized get to your files and viruses can get to them. This system was developed in a secure design which assists in the files being stored and accessed within a short period of time.

The second goal was elicited by the introduction of malware analyzer and AES encryption with QR key authentication to make cloud storage doubly secured. The files uploaded are scanned against malware and only healthy files are stored. When it is stored or transferred, the data will remain confidential as AES is reputed to be effective and strong. The user on his part has an encrypted file which is sent by him, and therefore the file remains secure end to end. QR key authentication provides an additional measure to the keys management.

The final objective which was to check that the cloud storage was secure and could be reached after establishing encryption and file uploads, was fulfilled through the basis of testing the system effectively. Various testing methods have been applied to test the effectiveness of the system, its security and operation. The speed of the encryption as well as decryption was measured, and tests were conducted to ensure that data was not wiped, the effectiveness of the malware analyzer was tested and how hard it was to use the system interface. According to the results, it was concluded that the system secured files using AES, identified uploaded malware and prevented their downloads and ensured data integrity during encryption and decryption.

5.2 Benefits

The benefits of AES encryption plus malware analyzer in secure file storage system are very high. To begin with, the level of protection offered by AES is satisfactory, one that ensures that even the unsuspected can hardly break down the encrypted data, hence safeguarding secrets of sensitive documents. Second, it incorporates the malware analyzer which identifies and blocks any attempts to upload a malicious file, which becomes a useful element of security and preventive measure against a threat. The two-fold mechanism improves the security system. In addition, the user interface is user-friendly giving the user ease to encrypt, upload, and decrypt information and upload keys using QR codes.

5.3 Limitations

It must be noted however that the project has limitations. Another disk cost that is likely to be too high is the computational overhead of large files when malware runs in a file. The larger the file grows, the longer the malware analysis, encryption, and decryption could take, which will affect the performance. According to the second limiting factor, AES is focused on as the main encryption method. Although AES is quite safe and very efficient in large data files, the ability to apply other encryption algorithms such as RSA or Elliptic Curve Cryptography (ECC) may make the system more versatile and attractive to each individual user. In addition, the system uses a stable internet connection to access the cloud and measure malware in real-time, which can be a weakness in areas with poor connectivity.

5.4 Future Recommendation

These challenges present numerous ideas of how this system can be developed in the future. First of all, the opportunity to provide the users with RSA and ECC encryption may result in the increased security and more choice. In addition, the system might be made simpler and more effective in the QR key authentication process with the help of frequent updates of the user interface using the users reactions. The security levels of the system such as the used of malware analyzer and AES encryption should be regularly checked and upgraded as a means of ensuring that the system is secure against any emerging threats and risks. Second, the endless adjustments to user interface using the feedback may make the system more friendly and operative, in particular, the process of QR key authentication. Lastly but not least, security systems of the system like the malware analyser and the AES encryption should be frequently updated and monitored to sustain the security of the system in the face of emerging threats and vulnerabilities in the system.

5.5 Conclusion

Lastly, the project has been able to come up with a secure cloud storage system that adds AES encryption with a malware analyzer to enhance the security of data by a substantial margin. QR key authentication is also done as an added layer of security that is coupled with other security mechanisms which is a double layer of protection. Intuitive user experience is also created and secured by the whole system and the sensitive information is secured under the backbone of confidentiality, integrity and availability. It is a proactive solution that ensures the protection against unwanted users access as well as malicious data and content. Regardless of some of the identified restrictions, the project has provided a sturdy base on which it should be built in the future. The suggested enhancements will also enhance the system to make it even stronger and flexible in storing files securely in the cloud storage system.