**User Driven Data Security Ensuring Henchman**

***R. Praveen Kumar\*1, Kalyan Chatteerji\*, B. Raju\*, M. Sravani\*, V. M. Ajay\*, P. S. Raj\*, P. Srividya\****

***\*Nalla Malla Reddy Engineering College, Department of Computer Science and Engineering, Divyanagar, Narapally, Hyderabad. 1Corresponding Author: praveenkumar.cse@nmrec.edu.in***

***Abstract***

This project's primary goal is to increase user data security by giving all users access to cutting-edge crypto-data secured methods and models, regardless of their level of technological proficiency. Crypto algorithms and models succeeded providing data security in the cloud, data storage, and digitized world. However, those are inaccessible to a technically limited individual. A Graphical User Interface (GUI) has been harnessed on the JAVA platform with the opportunity to select a key as a passcode to add another layer of protection for the user data. The Interface has been implemented on the 128-bit Advanced Encryption Standard (AES) method. Additionally, 192-bit and 256-bit versions are expected.

***Keywords: AES, GUI, JAVA, Cryptography, Algorithms and Models.***

***Introduction***

Data protection is an essential component. By using a variety of algorithms and models, cryptography protects the data. Advanced Encryption Standard Algorithm (AES) is the most practical and an open-source encryption method, is one of them. This algorithm is crucial for securing the data, even in public and private industries. This algorithm is widely used in the defense industry and in numerous storage systems, including SSDs, to store data in an encrypted format. The utilization of cryptographic algorithms is limited to administrators or other authorized individuals. The problem is that a regular person can’t use this AES algorithm for securing files due to a technical trench. A user harnessed with an additional data security benefit through implementing a Graphical User Interface which is implemented based on crpto-secured algorithms and that serves as a bridge between a regular user and advanced technology. On the other hand, as cloud computing systems advance, more people are using cloud services daily. Models and algorithms are available to complete the job, but they generate security keys automatically. Cryptography serves data security, but if a user is permitted to have their password to secure their data, which doubles the data security. As a result, data security improved.

***Problem statement***

The existing systems, such as cryptool2 and ARICA, are in the form of algorithms and models, which are difficult to be used by the technically wretched user. How expertly we design the algorithms and models to secure data may not assure a user unless we supply them with a tool to choose their security code that increases trust**.**Moreover, the existing system is unable to help all kinds of people rather than one who is aware of the technology. Harnessing a GUI overcomes the issue. The GUI also fetches the greater user community who are unaware of cryptography and its algorithms.

***Proposed system***

Implementation of GUI allows employing cryptographic techniques independent of user’s knowledge. Hence a GUI is implemented as a henchman. A user can adopt this henchman for encrypting or decrypting multifarious files. It is developed on JAVA that attains platform-independent. Unlike cryptool2, the GUI implemented works independently of any other crypto algorithm. The workflow of a process is shown below as an example.

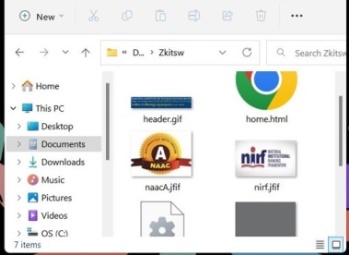
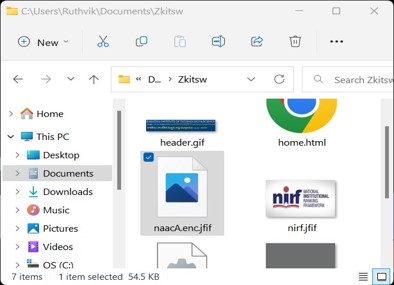
   

Figure: (Left most) actual file (in circle), (second from left) encrypting the file (user defined security key, circled), (third from left) highlighted the encrypted file, (right most) decrypting the file through providing same user defined key.

***Github link:***

***References:***

1. *(preprint)*Ahmad Loay-sousi Dalia Yehya Mohmad Joudi “AES Encryption: Study & Evaluation”, Presented to: Dr. Jad Nasreddine , November 2020.
2. Othman Saeed, Riaz Ahmed Shaikh, A User-Based Trust Model for Cloud Computing Environment, *(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 9, No. 3, 2018.*
3. Singh, G., A study of encryption algorithms (RSA, DES, 3DES and AES) for information security, *International Journal of Computer Applications, 67(19), 2013*.
4. M. Pitchaiah, Philemon Daniel, Praveen, “Implementation of Advanced Encryption Standard Algorithm”, *International Journal of Scientific & Engineering Research Volume 3, Issue 3, March -2012.*