# *MAJOR PROJECT VIVA VOCE - EXTERNAL*

***SECURING CONFIDENTIAL DATA USING FUSION OF TWO CRYPTOGRAPHIC ALGORITHMS AND STEGANOGRAPHIC TECHNIQUE***

***1***



**NAME :**

VISALINI S

**Supervisor:**

DR.SUMATHI N



***TABLE OF CONTENTS***

* Introduction
* Objective of the project
* Challenges in Existing System
* Contribution(s)
* Proposed System
* System Design (Hardware and Software Description)
* Results and Discussion
* Conclusion and Future Work
* References
  + Sending and receiving data through the internet is being a vital part in day to day life. But among those, people don't encrypt their data though they know that data contains personal information and the chances of data loss or hacking is very high.
  + Cryptography provides a layer of security in cases, where the medium of transmission is susceptible to interception, by translating a message into a form that cannot be read by an unauthorised third party.
  + It is of two types, symmetric and asymmetric key cryptography. In symmetric key cryptography identical key is used for both encryption and decryption while in public key or asymmetric key cryptography dissimilar keys are used for both encryption and decryption i.e. the public key for encryption and private key for decryption or vice versa
  + The main purpose of this project is to provide an efficient way to the user to send and receive the message over a secured channel and ensures the principles of security.

Cryptography is the study of different techniques to secure data from an unauthorized entity. In computer science, we try to develop strategies and practices for protecting sensitive data. Most of the cryptography involves very advanced Mathematical functions used for securing data. The sole purpose of the algorithms developed for cryptography is to hide data from the attacker or middleman.



***OBJECTIVE (S) OF THE PROJECT***

* Secure communication is vital to facilitate confidential exchange of information between any sender and receiver.
* The security of information passed over an open channel has become a fundamental issue and therefore confidentiality, authentication and data integrity are required.
* Multiple cryptographic techniques are used for the purpose of making the exchange of information secure.
* Almost all cryptosystems are vulnerable to different types of cryptographic attacks. Hence there is a need to protect the system by using fusion of cryptographic algorithms.



***CHALLENGE(S) IN EXISTING SYSTEM***

* + Cryptography does not guard against the vulnerabilities and **threats that emerge from the poor design of systems,** protocols, and procedures. These need to be fixed through proper design and setting up of a defensive infrastructure.
  + The security of cryptographic technique is based on the computational difficulty of mathematical problems. Any breakthrough in solving such mathematical problems or increasing the computing power can render a cryptographic technique vulnerable.



***CONTRIBUTION(S)***

* Sorting which algorithm to use was not an easy task
* Analysing the disadvantages of existing system, a lot of research was done on different types of algorithm and best secured way of transferring data from sender to the receiver.
* Understanding that AES is difficult to crack and is safe against most brute force attacks. However, the key size used for encryption should always be large enough that it could not be cracked by modern computers despite considering advancements in processor speeds.
* The main web page has the registration button for new users and login button for pre existing users.
* It is mandatory to specify during the registration that whether the user is the sender or the receiver.
* To send the data, the user should login with the appropriate credentials as a sender.The user page has a side bar menu with the buttons consisting of share data ,send items and logout.
* Proceeding into the share data section, the username of the current user will be the sender and the registered receiver name should be given.
* As similar as sending an email, subject should be given and the data file should be attached.
* The main and key factor is a 16-digit key consisting of only numbers should be given on own which should be noted down by the userAnd should be send to the receiver.Once the upload is clicked after this, The data file will be encrypted using AES algorithm.

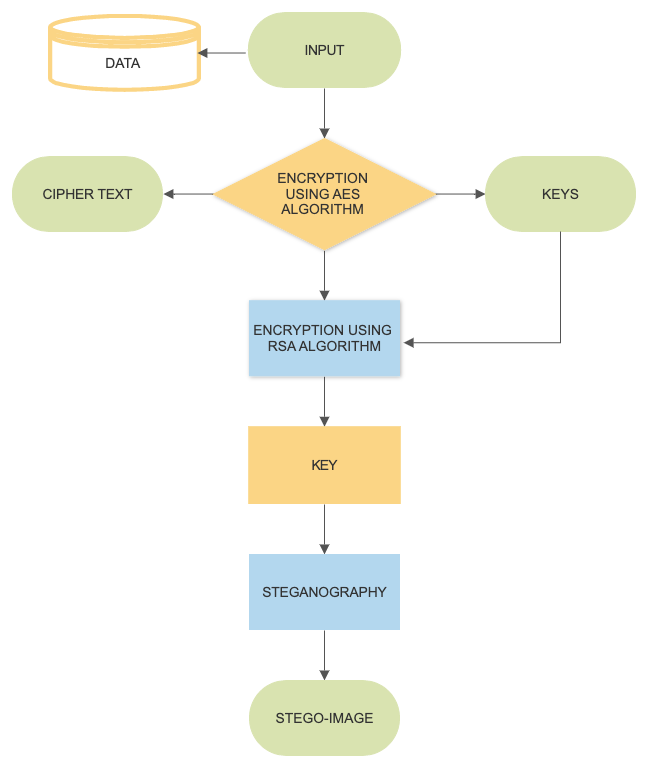


* Instead of encrypting the data file once again with another encryption method which is usually made by typical hybrid cryptography methods,
* Here the keys that are obtained by the AES algorithm is encrypted using RSA algorithm and a new set of keys are obtained which make this encryption method unique.
* The encrypted key obtained from the RSA algorithm is hidden into the new image uploaded, that is by stegnography method.Then the receivable is logged in using the appropriate credentials and under the shared data section, the stegnography image is downloaded.
* The downloaded stegnography image is once again uploaded and the unique 16 digit key which was created by the sender is required only by which the RSA key can be obtained.
* The RSA key is now copied and pasted in the next tab and once everything matches the data file is decrypted and downloaded



***PROPOSED SYSTEM – FLOW CHART***

*2/1/44 11*



*Major Project Viva Voce - External*

* + Processor
  + Ram
  + Storage

: i3 or above

: 2 GB or above

2 GB minimum



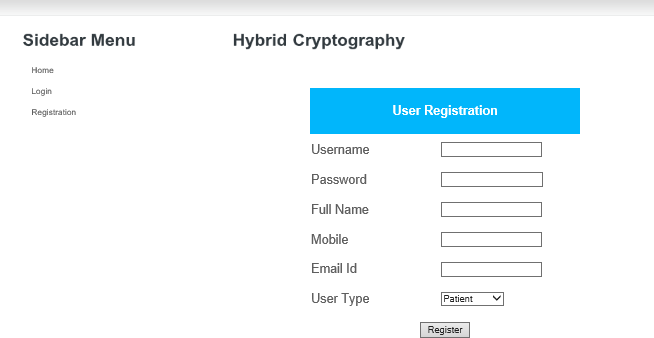
Operating System : Windows 7 / 8 / 10 Language : Java

Database : MySql Server

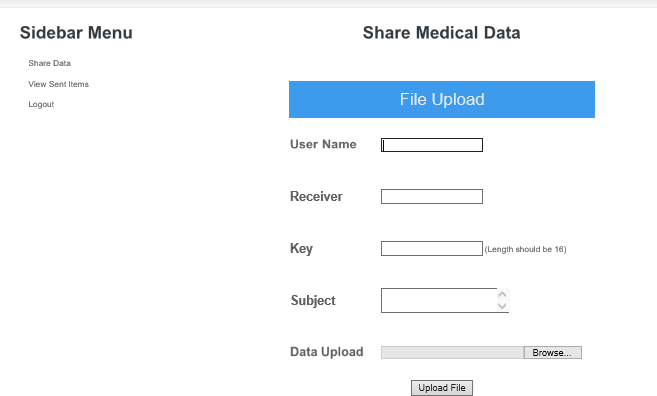
IDE : Netbeans 8.1

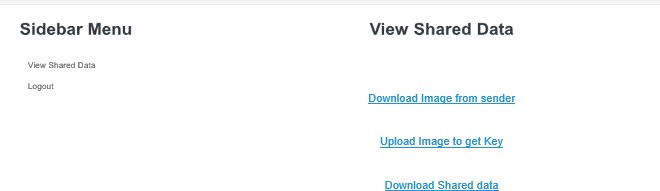
Front End : JSP

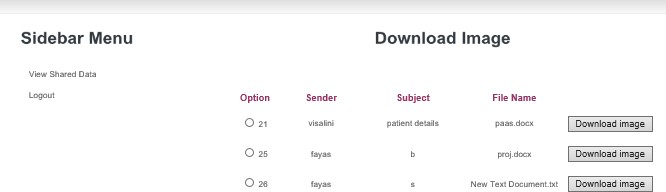
Back End : Java Servlet

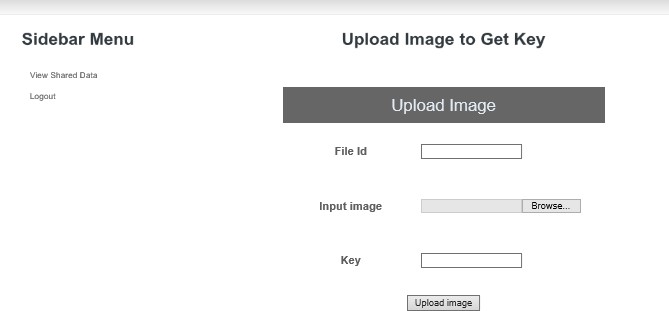
 

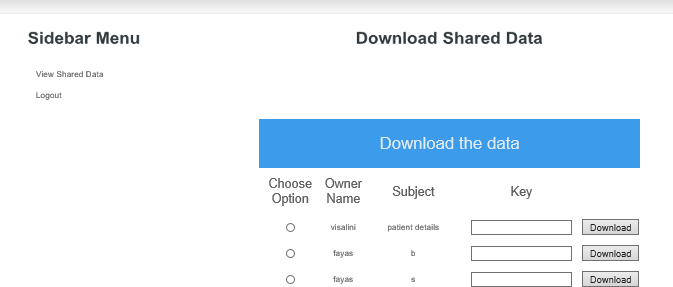


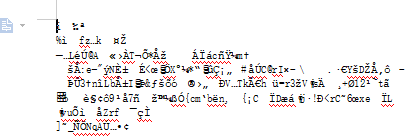












* Increasing the volume of data has resulted in users saving the data on remote access storage media, such as cloud computing storage infrastructures.
* Outsourcing the data makes it beyond the user’s control and vulnerable to untrusted, anonymous operations.
* In this study, we have developed an automated hybrid cryptographic system that works without interference from cloud third parties to maintain data confidentiality and reduce the burden on users to secure their data by themselves.
* Privacy is one of the key issues addressed by information Security
  + Currently this system works flawlessly by both encrypting and decrypting for plain texts which are in editable formats.
  + While the encryption of any format is possible but the decryption is not precise, we are working to also make the PDF or other text files which are in non editable formats.
* As a big step, the encryption and decryption of photos and video files will also be made possible in further works.
* It's now limited that only one file could be send by the sender to the receiver in one session.Option of selection of multiple files and sending in bulk will be added in further refurbishment of the project.

1. UIC, (2017).Why Data Security is The Biggest Concern of Health Care. Re-trieved [from: http://healthinformatics.uic.edu/resources/articles/why-datasecurity-is-the-biggest-](http://healthinformatics.uic.edu/resources/articles/why-datasecurity-is-the-biggest-) concern-of-health-care/ Retrieved date: 17th July, 2017.
2. P. Bharathi, G. Annam, J. B. Kandi, V. K. Duggana and A. T., "Secure File Storage using Hybrid Cryptography," 2021 6th International Conference on Communication and Electronics Systems (ICCES), 2021, pp. 1-6, doi: 10.1109/ICCES51350.2021.9489026.

*2/1/44*

1. Zodape Megha Mrs. Pragya Shulka. (2012, june). Analysis of triple DES and RSA

Algorithm in securing Image Steganography. International Journal of Computer Archictecture and Mobility, 1(8), 4-6.

*24*

* 1. Chhabra, A., & Mathur, S. (2011, October). Modified RSA Algorithm: A Secure Approach. In Computational Intelligence and Communication Networks (CICN), 2011 International Conference on (pp. 545-548). IEEE.
  2. Sun, Hung-Min, Mu-En Wu, Wei-Chi Ting, and M. Jason Hinek. ‘Dual RSA and its security analysis.’ Information Theory, IEEE Transactions on 53, no. 8 (2007): 2922-2933.
  3. Pugila, Dhananjay, Harsh Chitrala, Salpesh Lunawat, and PM Durai Raj Vincent. ‘AN EFFICEIENT ENCRPYTION ALGORITHM BASED ON PUBLIC KEY CRYPTOGRAPHY.’ International Journal of Engineering and Technology
  4. A Hybrid Cryptography Scheme for NILM Data Security by Ruijue Feng ,Zhidong Wang ,Zhifeng Li ,Haixia Ma ,Ruiyuan Chen ,Zhengbin Pu ,Ziqiu Chen and Xianyu Zeng, 11 June 2020 / Revised: 29 June 2020 / Accepted: 8 July 2020 / Published: 10 July 2020
  5. Kaur, S. Bansal and R. K. Bansal, "Steganography and classification of image steganography techniques," 2014 International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2014, pp. 870-875.

*2/1/44 Major Project Viva Voce - External 25*