TIME AND SPACE BOUND ENCRYPTION CLOAK

[1]Urmila Biradar, [2]Harshada Makhamale, [3]Nainisha Mahindrakar, [4]Rangoli Agarwal, [5]Saurabh Pachauli

Dept. of computer science engineering, Savitribai Phule Pune University.
G.H.R.C.E.M, Wagholi, Pune, Maharashtra, India

***Abstract*— The system aims at strengthening the AES algorithm further, by using another dimension for enhancing the encryption technique. A inclusion of time and location, which shall work as an additional level of security. Since the exact time and location will only be known to the user, the encryption becomes safer. The AES algorithm is only used for the encryption purpose. There will a sender, receiver and a server. The sender will encrypt the message and will send it to the server along with the location of the receiver and time at which the message will be decrypted. Hence, server will generate the key and will send it to the receiver at that particular time along with the key. The key will keep on generating itself at the particular time interval. The receiver should be present at the location specified by the sender while encryption.**

***Index Terms*— Encryption, Decryption, AES, Location**

I. INTRODUCTION

The rapid change in technologies and increase in data intrusion has led to the development of different encryption algorithms. A new text based encryption technique that uses the advanced encryption algorithm that provides high level security against any intrusion in the transmission of emails or any other message is proposed in this paper. Any data that is to be transmitted in the form of texts can be secured from intrusion. Proposed method uses the AES algorithm for the encryption and decryption purpose. AES is a symmetric key algorithm i.e. the public and the private keys are same. In the system proposed in the paper, there will be a sender, receiver and a server. The sender will encrypt the message using the AES algorithm and will transmit it to the server along with the location of the receiver and the time at which the message will be decrypted by the receiver. The server will keep on re-generating the key at a particular time interval and the final key generated at the time of decryption will be sent to the receiver. The receiver will then decrypt the message using the key only if the receiver is present in the location specified by the sender. An added feature of snoozing will be added to the system. In this, the receiver can even snooze the reminder for decryption if he is busy or out of reach. During the snoozing period also the key will be re-generated. The proposed idea will reduce the file size leading to the faster transmission of data within seconds without compromising the information and security. The security provided to the system is very high in nature.

II. SYSTEM ARCHITECTURE

Here the architecture shows who the system is going to work:

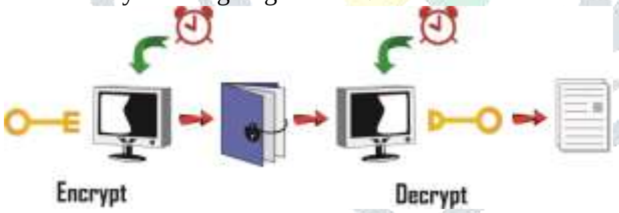


Fig1: Architecture of the system

Clock: Represents the time stamp.
'E' Key: Public key.
'D' Key: Private key.
Locked file: Encrypted text.
Open file: Decrypted text.

III. ALGORITHMS

Algorithm: At the sender end

- Begin.
- For encryption:
- Call AES module.
- Specify the location of the receiver.
- Specify the time at which the data will be decrypted.

- Transmit the file to the server.
- End.

Algorithm: At the server end

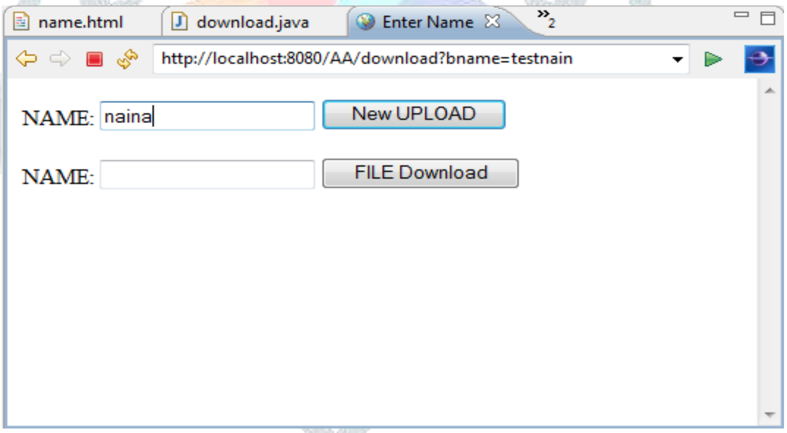
- Begin.
- Re-generate the key at the particular time interval.
- The last key generated will be transmitted to the receiver at the time specifiedd by the sender for the decrytion of the data.
- End.

Algorithm: At the receiver end

- Begin.
- The receiver can decrypt the message only if he is present at the location specified by the sender during the particular time interval.
- The receiver can even snooze the reminder for the decryption of the data
- During the snoozing period, the key will keep on re-generating itself.
- The last key generated will be considered.
- End.

IV. SYSTEM IMPLEMENTATION / USER INTERFACE

To upload a file:



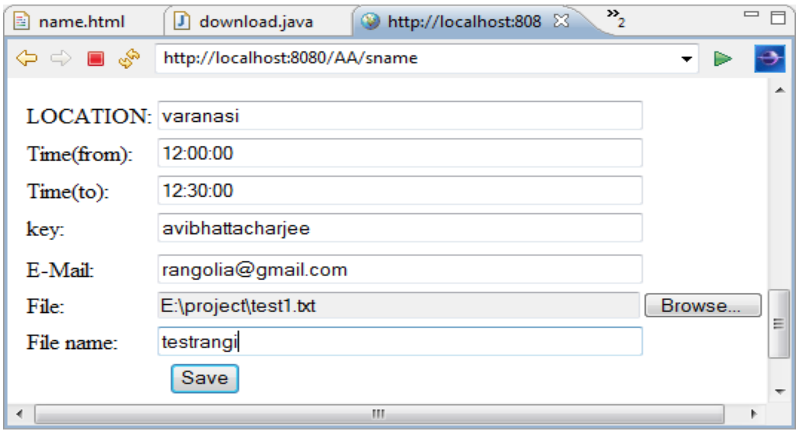
http://localhost:8080/AA/download?bname=testnain

NAME: naina

NAME:

Fig 1:Uploading a file

Enter file info.



http://localhost:8080/AA/sname

LOCATION: varanasi

Time(from): 12:00:00

Time(to): 12:30:00

key: avibhattacharjee

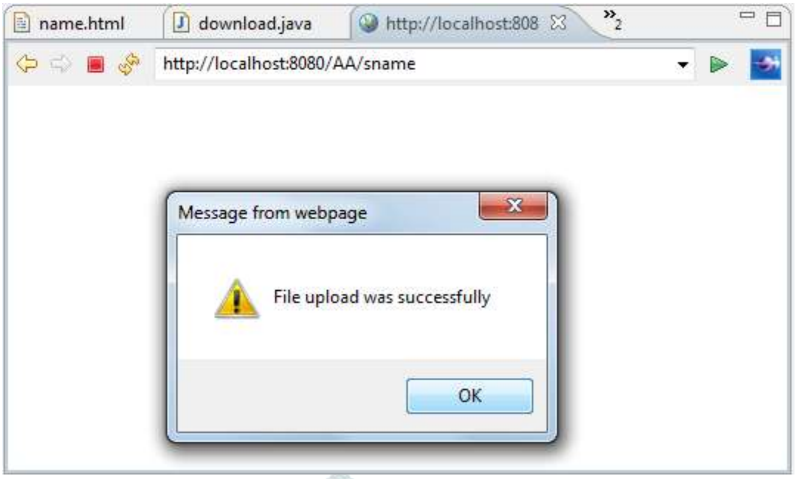
E-Mail: rangolia@gmail.com

File: E:\project\test1.txt

File name: testrangi

Fig 2:Entering information

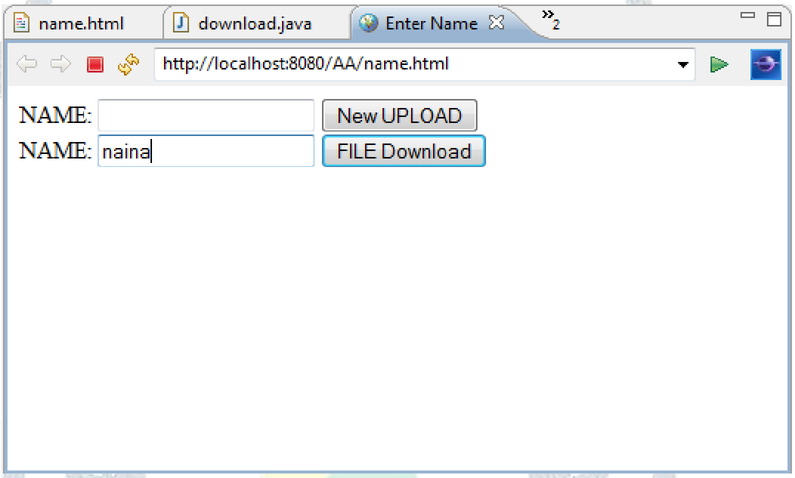
Upload successful:



File upload was successfully

Fig 3:successful upload

Enter name to download file:

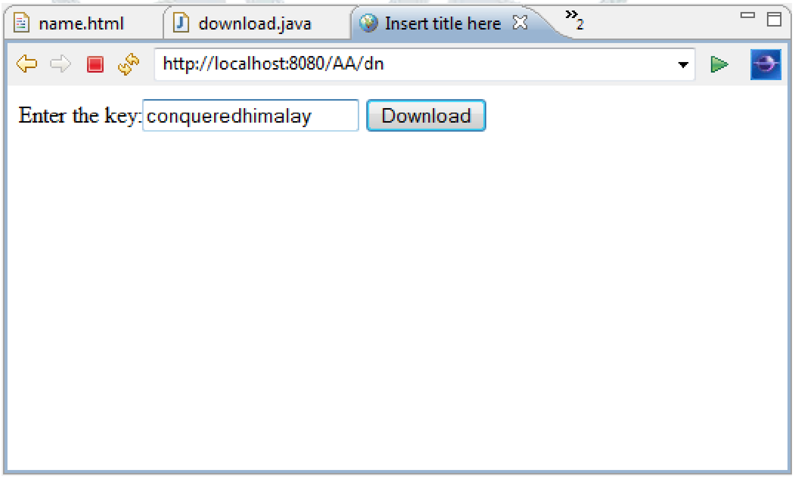


NAME:

NAME: naina

Fig 4:downloading a file

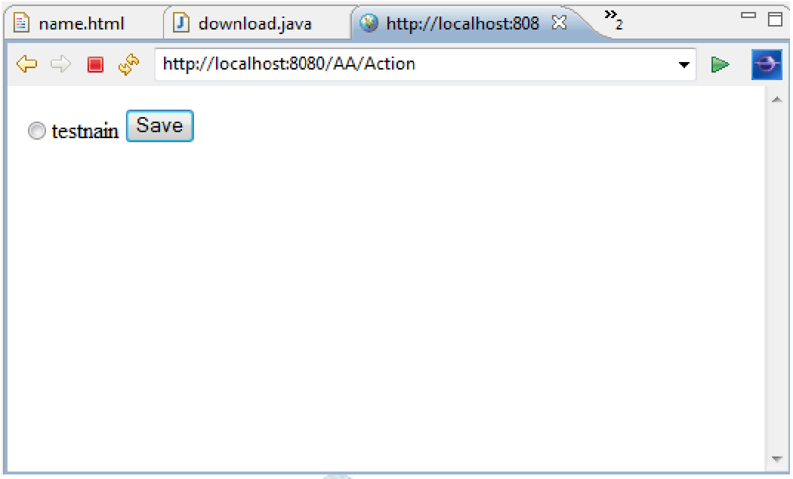
Enter the key:



Enter the key: conqueredhimalay

Fig 5:entering a key

Select the file to download:

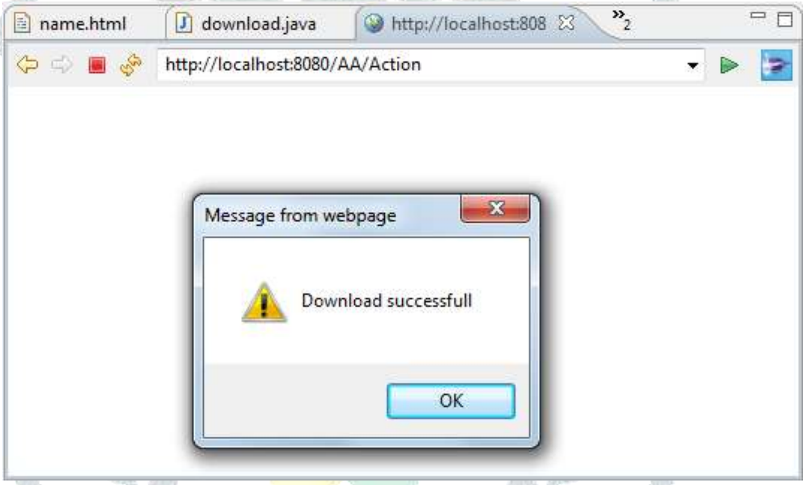


http://localhost:8080/AA/Action

○ testnain

Fig 6: Select the file to download

Download successful:



http://localhost:8080/AA/Action

Message from webpage

Download successfull

Fig 7: successful downloading

V. CONCLUSION

The main aim is to create a new encryption technique which uses a small cipher key and provides a higher level of security and to decrease the size of the ciphered text, for faster transmission. To prevent interception and deny message content to th e interceptor and to create an asymmetric encryption algorithm.

The proposed idea provides us with high security. Any data that is to be transmitted in the form of texts can be secured from intrusion .The proposed idea will reduce the file size leading to the faster transmission of data within seconds. The use of time and location makes the encryption more complicated that makes it almost difficult for the intruders to crack it. The proposed idea can be used in various fields such as the personal data security, corporate data security, military and defense data security and many more. There are various advantages of the proposed idea such as as small size of encrypted file, intrusion detection and many more.

The proposed method is a new method using time and location based strategy for text encryption. The conventional techniques is extended to using both location and time for encryption. A inclusion of time and location is introduced for every transaction, which shall work as an additional level of security. Since the exact time will only be known to the user, the encryption becomes safer. The method is effective and feasible. The proposed method can enhance the security of conventional cryptosystems.

Thus this method using both time and location as an important attributes increases the security of transmission of any text data.

VI. ACKNOWLEDGMENT

We here by wish to take this opportunity to express our gratitude to our teachers and friends and all who have helped towards the completion of our system. We take a great honour in presenting this System Report to our Principal Prof. D.D.Shah. We also like to give thanks to our H.O.D. Mrs. Poonam Gupta for helping us and guiding us throughout our endeavor.We are very grateful to our Guide Mrs. Urmila Biradar for her guidance through the system. We are very grateful to our teaching staff for guiding us all over the duration of the degree. They were very helpful to us, as and when we required their help. We are also very grateful to non-teaching staff to help us in the laboratory in various ways.

REFERENCES

[1] improvements-of-rijndael--algorithm -through-key-multiplication.html]www.ijser.org/paper/
[2] AES Implementation and Performance Evaluation on 8-bit Microcontrollers, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6 No. 1, 2009.
[3] Hyubgun Lee, Kyounghwa Lee, Yongtae Shin, [7] Ritu Pahal, Vikas kumar, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2013
[4] Enhancing Advanced Encryption Standard S-Box Generation Based on Round Key , International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(3): 183-188 The Society of Digital Information and Wireless Communications (SDIWC) 2012 (ISSN: 2305-0012)
Julia Juremi Ramlan Mahmod, Salasiah Sulaiman Jazrin Ramli,