ISSN No:-2456-2165

Automatic System Lock and File Encryption using Bluetooth Device

Lokesh M
Dept. of ISE
NIE Institute of Technology
Mysuru, India

Manjunath D P
Dept. of ISE
NIE Institute of Technology
Mysuru, India

Manoj Kumar M S
Dept. of ISE
NIE Institute of Technology
Mysuru, India

Shashank M R
Dept. of ISE
NIE Institute of Technology
Mysuru, India

Chitra R
Associate Professor
Dept. of ISE
NIE Institute of Technology
Mysuru, India

Abstract:- Now a days, we are relying more and more on digital data. These data may include sensitive information. These information should be stored securely. Only authorized user should be able to access these information. Securing the sensitive information has become the major issue in the current technology. Traditional authentication mechanism which uses username and password is not sufficient to secure the data. Therefore, new technologies are being invented every day. Two-Factor authentication is one of those mechanisms which improves the security of the system.

Keywords:- *security, encryption, two factor authentication, Bluetooth device.*

I. INTRODUCTION

We propose a system which uses Bluetooth as a token of authentication. Here, Users register a Bluetooth device and selects files and folders to be encrypted. The MAC (Media Access Control) address of the Bluetooth device is stored in the system. The system constantly keeps checking for the registered Bluetooth device and as soon as the Bluetooth device goes out of the system's vicinity, the workstation will be locked and specified files and folders will be encrypted.

Our system performs the MAC address validation of the Bluetooth device. The Bluetooth device need not be connected with the computer. Our system uses Service Discovery Protocol implemented in data link layer to obtain the handshaking information of the Bluetooth device. The handshaking information contains the basic information of the Bluetooth device such as device name, MAC address and services provided by the Bluetooth device. This information is used validate the MAC address of the Bluetooth device.

Our System also automatically unlocks the workstation when the specified Bluetooth device is validated. When the system is locked, any unlocked sensitive files will be automatically locked.

Our system enables the use of Bluetooth device as two-factor authentication which requires both Bluetooth device and password to unlock files. This makes it nearly impossible for the intruders to access the secured files and folders.

II. LITERATURE SURVEY

Traditional authentication mechanism which uses username and password are widely used, it has many disadvantages and can be easily broken [1]. Thus, two factor authentication are used to enforce the security of the system. There are many two factor authentication mechanism e.g. Biometrics. Mobile phones can also be used as token for two factor authentication [2]. We use Bluetooth device as a token of authentication.

Many cryptographic algorithms are available to encrypt files. AES (Advanced Encryption Standard) algorithm turns out to be the most efficient algorithm in terms of space, time and security [3]. We use AES algorithm to encrypt files and folders.

III. SYSTEM OVERVIEW

In our proposed system, the key feature is the use of Bluetooth device as the token of authentication. First, the user will specify the Bluetooth device, the MAC address of the Bluetooth device will be stored in the computer.

Our Proposed system uses AES – 128 bit algorithm to encrypt files. When our system encrypts file for the first time, a random key of length 128 bit is generated using Random Key Generator. The generated key will be stored in the System using Java Key Store file. In which, each key is encrypted using the password provided by the user.

IV. SYSTEM DESIGN

A. *Software architecture*

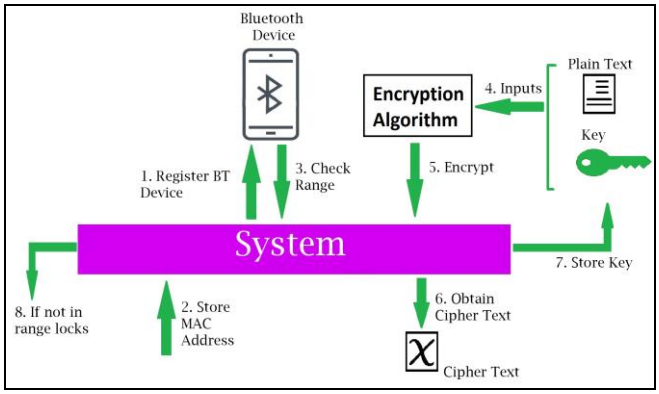

Fig 1:- Software Architecture

B. *Operations of our proposed system*

- User will register the Bluetooth device with our system.
- Our system stores the MAC address of the specified device.
- Our system constantly keeps checking the range of the specified Bluetooth device.
- Once the Bluetooth device leaves the vacinity of the system, Encryption algorithm takes Plain text and secret key as input.
- Encrypts the file(s) using the secret key
- The encrypted file(s) are stored in the system.
- If the secret key is generated, it will be stored in our system
- Our system also locks the workstation when the specified Bluetooth device leaves the vacinity of the system.

C. *AES Algorithm*

After research, AES algorithm found to be the best and feasible algorithm for our project implementation. AES algorithm found to be more secure than DES and 3DES algorithm. Different key size of AES algorithm are 128 bit, 192 bit, and 256 bit. Our proposed system uses key of size 128 bit. Major steps of AES algorithm are:

- Sub Byte: In this operation provides non linearity in cipher. Here boxes are derived from multiplicative inverse and then are used to substitute them in place of the original text.
- Shift Rows: This step operates on the rows of the state; it cyclically shifts the bytes in each row by a certain offset. In AES first row is shifted by 0 bits, second by 1 bit and so on.
- Mix Column: In this step, the four bytes of each column of the state are combined using an invertible linear transformation.
- Add Round Key: In this step, the sub-key is combined with the state.

The way these steps are executed in order to complete the encryption is shown later using a diagram.

Similarly as encryption, decryption is carried out by reversing the order of the steps involved in encryption.

The diagram shows the steps in AES algorithm

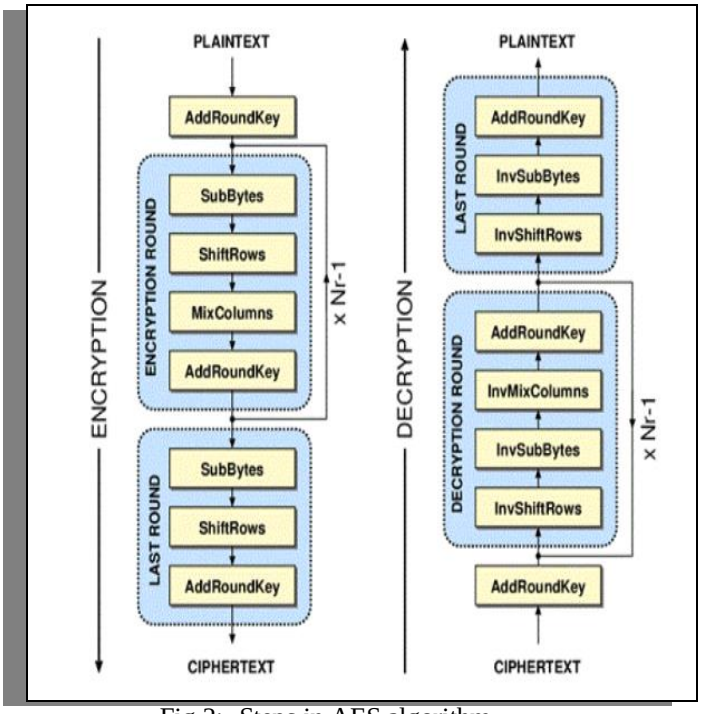

Fig 2:- Steps in AES algorithm

V. CONCLUSION

This paper proposes a windows application that uses Bluetooth device to authenticate user and store sensitive files securely by encrypting them. By using our application, user will be able to secure files which contains sensitive information. In future, this system can be enhance to make it more automated, user friendly and advanced.

REFERENCES

[1] Philip Inglesant and M. Angela Sasse, “The True Cost of Unusable Passwords” at Association for Computing Machinery, New York, 2010.

[2] Steffen Hallsteinsen and Ivar Jorstad , “Using Mobile phones as a security token for Unified authentication”, IEEE, 2007.

[3] Gurpreet Singh and Supriya, “A Study of Different Encryption algorithms for Information Securit”, International Journal for Computer Application, 2013.

[4] P M Nagendra and Chandra Sekhar, “Performance Improvement of AES Algorithm using Parallel Computation”, International Journal of Software Engineering and Its Applications, 2014.

[5] Brijender Kahanwal and Girish Pal Singh, “Java File Secure System”, Global Journal of Computer Science and Technology, 2011.