MORADABAD INSTITUTE OF TECHNOLOGY

CERTIFICATE

Certified that the project report entitled "**Securing Computer Folders with Rijndael Security Extension and Your Bluetooth Enabled Mobile Phone**" submitted by "**Krishna kumar Singh**" Roll No:- **1508210062**, "**Aanchal Gupta**" Roll No:- **1508210003,** "**Firoj Khan**" Roll No:- **1508210047 ,**"**Aman Singh**" Roll No:- **1508210018** is their own work and has been carried out under my supervision. It is recommended that the candidates may now be evaluated for their project work by the university.

Ms. Kanchan

Assistant Professor

\

ABSTRACT

In cryptography, Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor. In an encryption scheme, the intended communication information or message, referred to as plaintext, is encrypted using an encryption algorithm, generating cipher text that can only be read if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, large computational resources and skill are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients, but not to unauthorized interceptors. Encryption/Decryption is the art of hiding the fact that communication is taking place, by hiding information in other information. For hiding secret information in images, there exists a large variety of Encryption/Decryption techniques some are more complex than others and all of them have respective strong and weak points.

Security of the computer files and folders have been a core issue ever since the advent of the windows. Passwords were then introduced to solve this issue but they themselves lend a host of disadvantages. In this paper, we shall study what disadvantages the passwords bring and how we can tackle them. Also we shall propose a Two Factor Authentication (T-FA) system utilizing Bluetooth as a factor coupled with the powerful Rijndael Encryption Algorithm. Bluetooth is the most commonly used technology for Point to Point short range of communication of devices.

Besides from being commonly used, it also offers multi connection. Rijndael algorithm is an Advanced Encryption standard, believed to be the most effective encryption and decryption cryptographic algorithm. Its minimum 10 rounds of encryption and variable key size with a minimum of 128 bits makes it difficult to crack. Coupling the widespread accessibility of Bluetooth and powerful encryption of Rijndael, a Two Factor Authentication System [T-FA] can be created which will not only efface the disadvantages of passwords, but also create a user friendly security system.

In present day, the increasing reliance on computer systems has led to the dependence on confidential security measures. Various methods used to identify a user are Digital signature, Challenge-Response, Biometrics, IPSec (Internet Protocol Security), Single- Sign On and Password. Password has become one of the most ubiquitous modern day security tool and is very commonly used for authentication. These passwords are string of characters used for authentication or user access. Unfortunately users set passwords that can be easily memorized, in turn increasing threats. Password meters indicating password strength are used to increase effectiveness of passwords and make them less predictable. Biometrics on the other hand requires the assumption of unrealistic preconditions for performance gain. Access control systems require time-trusted and reliable personal recognition. To overcome the problems faced by these processes individually, we can use a combination of two or more security processes. Two-factor authentication has ameliorated security in authentication systems. Sensitive files can be provided double protection using Rijndael security extension and Mobile Bluetooth tokens.

This paper will mainly compare various authentication methods and present the improvement in windows password policies using a combination of mobile Bluetooth and Rijndael encryption.

File Security is a feature of your file system which controls which users can access which files, and places limitations on what users can do to files. The file system considers the user's identity, and what kind of action the user is performing, and consults the file's permissions.

Advanced Encryption Standard(AES) is based on a design principle known as a substitution-permutation network, and is fast in both software and hardware. Unlike its predecessor Data Encryption Standard(DES), AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specification is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.

In order to protect the file against unauthorized reading and undetected mutilation, a user encrypts it with a secret cryptographic key of a symmetric cryptosystem. This symmetric key is needed to encrypt or decrypt data with it.

The cryptographic keys are used in data encryption to make the file more secure. The same key must be used to decrypt the data. This means that we have to either memorize the key or store it somewhere. Memorizing it isn't practical, so we must store it so that we can recall it when we want to decrypt the data back into its meaningful form, but no one else can.

For storage we use windows registry. There are many useful adjustments to the windows configuration or behavior that can be made by simple editing of the registry. Unless you are the administrator, registry cannot be edited.

The three most popular standards that can be used for transferring the keys are IrDA, Bluetooth, and Wi-Fi. Each allows battery-powered devices to communicate wirelessly and each one of them has its own benefits and limitations. After presenting the benefits and limitations of each technology, it is found that Bluetooth is the most appropriate technology for the proposed system.

ACKNOWLEDGEMENT

I express my deepest sense of gratitude towards my guide Ms. Kanchan Assistant Professor, department of Computer Science Engineering, Moradabad Institute of Technology, Moradabad for his/her patience, inspiration, guidance, constant encouragement, moral support, keen interest and valuable suggestion during preparation of this project report.

My heartfelt gratitude goes to all my faculty members of computer science engineering department. Who with their encouraging and caring words and most valuable suggestions have contributed, directly and indirectly, in a significant way towards completion of this project report.

I am indebted to all my classmates for taking interest in discussing my problem and encouraging me.

I owe a debt of gratitude to my father and mother for their consistent support, sacrifice, candid views, and meaningful suggestion given to me at different stages of this work.

Last but not the least I am thankful to the almighty who gave me the strength and heath for completing my report.

KRISHNA KR SINGH (1508210062)

AANCHAL GUPTA (1508210003)

FIROJ KHAN (1508210047)

AMAN SINGH (1508210018)

LIST OF CONTENT

LIST OF FIGURES