SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348 – 8549 /doi:10.14445/23488549/IJECE-V6I12P101
Volume 6 Issue 12, 1-2, December 2019

Security of data using encrypted Graphical password

Virajesh
Student, Dept. Electronics & Communication Engg., Institute of Technology & Management, Aligarh, India

Abstract: *The purpose of this paper is to provide an overview of data security. Nowadays, data security is very important in every field of life. In this system, the security of data is done by using an encrypted graphical password. Since conventional password schemes are vulnerable as the password are entered either by a physical keyboard or the on-screen keyboard, so encrypted graphical password is used to secure data. The system provides user identity security such as name, date of birth by registering them and secure them with an encrypted graphical password. An encrypted password is unreadable to a person or entity accessing without permission. In this paper, we have used textual and graphical passwords both in an encrypted form.*

Keywords - *Graphical password, Data Security, Encryption, Textual password, Programming languages.*

I. Introduction

Data security is a process of protecting data from unauthorized access without permission. Security of data is very important in all organizations. In every organization, data is an important freehold, so it is essential to save from criminals or hackers. In graphical passwords, we have taken images by clicking them, we can set a password, and we have taken one text password also, by clicking one image, we have to input any text password, so it becomes complicated for others to guess the password. By both text and graphical passwords, it becomes difficult to hack passwords by the hacker. The main intention of this project is to secure personal identity by using text and graphical password in an encrypted form which is unreadable to a person. There are fewer chances for hackers to steal the graphical password because hackers will not access image sequences uploaded by the user as a password.

II. Literature Review

A. Existing System

G.E blender proposed a graphical password technique first time. In this user can select some image in the registration phase to choose a password. The images are predefined. In the login, a user selects those images which were selected in the registration phase; if these points are matched, then the user is identified as an authorized user.

There are many other proposals given by different men based on graphical passwords, including some different techniques.

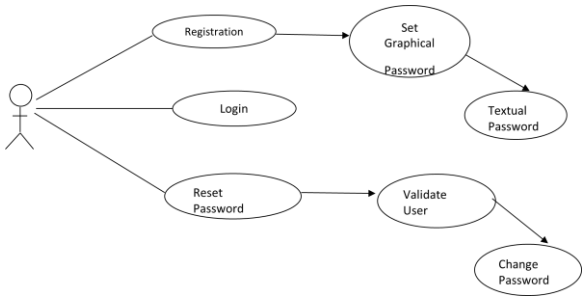
B. Proposed system

In this section, we have described graphical password in encrypted form, and it also includes one text password as the user wants to enter. This includes three phases-

a) Registration phase - In this, the user has to enter their identity like name, DOB, and he or she is a male or female. A graphical password then secures it by clicking images as the user wants to select from predefined images. If the user wants to enter a text message, then the user has to select one image that is a laptop, then both text and graphical passwords are used for securing data.

b) Login phase - In this user have to enter the correct password as he has entered in the registration, then the user will be logged in, and the identity of the user is displayed on the screen which the user has entered in the registration, if the password is wrong then it will display invalid.

c) Reset password- By entering the existing password correctly, we can reset the password of our own choice. We can select any image from predefined images for the password. We can skip text passwords by our choice. Password can be text or graphical based on the user.



3D BLOCK DIAGRAM

III. Some popular languages used in the project

A. AES (Advanced Encryption Standard)

It is used for encryption of the password. An encrypted password is unreadable to a person, so it becomes more secure.

B. Netbeans- IDE

It is an open-source integrated development environment. It supports the development of all Java application types, all the functions of the ide are provided by modules. Each module provides a well-defined function, such as support for Java language, editing or support for the CVS versioning system, and SVN. NetBeans contains all the modules needed for Java development in a single download, allowing the user to start working immediately.

C. JDBC (Java DataBase Connectivity)

Java database connectivity is a Java-based data access technology. This technology is an API for the Java programming language that defines how a client may access a database. It provides methods for querying and updating data in a database.

D. MYSQL

It is the world's most used relational database management system (RDBMS) that runs as a server providing multi-user access to many
databases. It is written in C and C++.

IV. Features

1. Pictures are easy to remember than text.
2. Keylogging or key listening spyware cannot be used to break a graphical password.
3. A graphical password is less vulnerable than a text-based password.
4. It is more secure because less research has been done to study the difficulties of cracking graphical passwords. After all, it is not widely used in practice.

V. Conclusion

Graphical password is that people are better at memorizing graphical passwords than the text-based password. Graphical password is difficult to break because it is in encrypted form, unreadable to a person. This system prevents identity theft and security from using confidential data. It follows images that were uploaded during registration. The uploaded images are not visible to others. The person who registers can only log in by uploading the images from predefined images.

References

[1] http://en.wikipedia.org/wiki/data_ security

[2] http://www.researchgate.net/graphical password

[3] http://www.google.co.in/encryption

[4] http://www.java.net

[5] http://www.future.wikia.com/data_ security

[6] Partha Pratim Ray. "Ray's Scheme: Graphical Password Based Hybrid Authentication System for Smart Hand Held Devices"International Journal of Computer Trends and Technology (IJCTT),V3(2):230-236 Issue 2012 .ISSN 2231-2803.www.ijcttjournal.org. Published by Seventh Sense Research Group.

[7] K. L. R. S. Himaja, Mrs.T. Sri Lakshmi"Prevention Of Attacks And Mitigates The Packet Drop In Wireless Adhoc Networks", International Journal of Computer & organization Trends (IJCOT), V6(6):17-19 Nov - Dec 2016, ISSN:2249-2593, www.ijcotjournal.org. Published by Seventh Sense Research Group.

[8] Venkadesh .S , K.Palanivel "A Survey on Password Stealing Attacks and Its Protecting Mechanism", International Journal of Engineering Trends and Technology (IJETT), V19(4), 223-226 Jan 2015. ISSN:2231-5381. www.ijettjournal.org. published by seventh sense research group.

[9] Omkar Ghaisas, Prof. Yogita Borse"Survey of Data Protection Mechanisms to Protect Data at Rest on Cloud", International Journal of Engineering Trends and Technology (IJETT), V59(2),105-107 May 2018. ISSN:2231-5381. www.ijettjournal.org. published by seventh sense research group.

[10] Sonia Rathi , Raunak Chitnis , Ramakant Yadav , Mrs. M.V.Bhosle. "Securing ATM Using Graphical Password Authentication Scheme". International Journal of Computer Trends and Technology (IJCTT) V8(3):133-137, February 2014. ISSN:2231-2803. www.ijcttjournal.org. Published by Seventh Sense Research Group.