A GRAPHICAL PASSWORD AUTHENTICATION IN STORAGE SYSTEM

JAYALAKSHMI S
2019202018
MCA REGULAR(3 year)

GUIDE:MR.H.RIASUDHEEN

ABSTRACT:

In this era, technology has become an important aspect of human needs especially communication technology. Now a days communication technology are some of the security drawbacks.One of the most important primitive security mechanisms is the authentication system. Authentication through the use of alpha numerical password is a commonly utilized mechanism for authentication of users. If the passwords are too simple and predictable, then there is the danger of being susceptible to threats. In order to overcome the problems with authentication an alternative and new approach has been introduced utilizing images for passwords. The idea gains support from the knowledge that the human's brain is highly capable of remembering many detailed images, however remembering texts are more difficult. Users who utilize the graphic authentication carry out certain functions on the images such as to click, drag, and movement of the mouse. Meanwhile million of images and text files are transferred everyday across the network. These images are confidential and we want these images to be transferred securely.To achieve the security cryptography plays a significant role in transferring images and text files securely. It is hard to solve an Elliptic Curve Discrete Logarithm Problem with respect to key size of Elliptic Curve Cryptography helps in providing a high level of security with smaller key size compared to other cryptographic technique.

INTRODUCTION

Human factors are often considered the weakest link in a computer security system. If we point out that there are three major areas where human-computer interaction is important: authentication, security operations, and developing secure systems. Here I'm focusing on the developing a secure system. To achieve a secure system development we need to implement some of data encryption and decryption methodologies.Data encryption is used to protect digital data stored on computer systems, and transmitted through the internet to servers and other computer networks. It's one of the first lines of defense when it comes to securing IT systems and communications.This is because, even if it's accessed without authorization, the encryption will protect the information contained in your data – it will not be readable without the proper key.Unfortunately data breaches are a scary reality in the world today. In 2019, there were more data breaches than ever before, with more than 4.1 billion breaches in the first half of 2019 alone.Encryption is not a "magic bullet" to make your systems fully secure. However, it does add another layer of protection to your identity, privacy and data. It protects your data even if it's lost, and encryption systems allow you to hide data if you are ever being watched by a threat or a hacker.Along with the data encryption the system uses a graphical authentication method for secure authentication.

PROBLEM STATEMENT:

- The most widely and commonly used authentication is traditional "Username" and"Password". For such authentication generally text (alphanumeric) is used

- It is well-known, however that passwords are susceptible to attack: users tend to choose passwords that are easy to remember, and often this means that they are also easy for an attacker to obtain by searching for candidate passwords.

- A lot of information is perceived when we transfer files .Personal files have become an inevitable source of information. When files are not confidential when we transfer the system will be infeasible.

OBJECTIVE

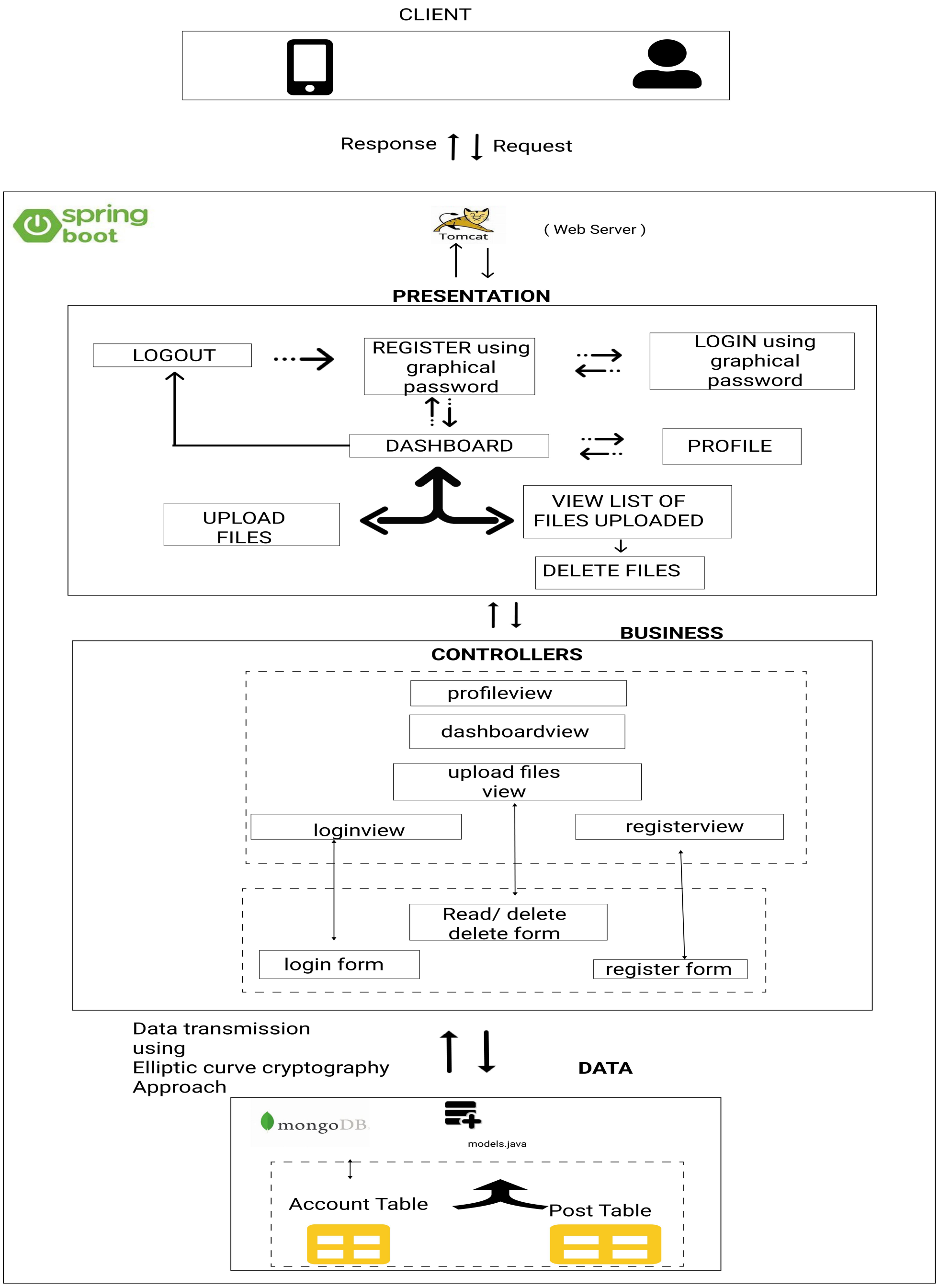
The project are to create a system that can protect a data which Consist of encryption and decryption process and to fully design an system in a secure way. The objectives of this project are

- To implement the graphical password authentication instead of alphanumerical passwords.
- To understand the SHA3 Algorithm and apply it in grid values of the image
- To understand how the Encryption and Decryption process.
- To store the data into the database in a encrypted form.Encryption is achieved by applying elliptic curve cryptography.

ARCHITECTURE EXPLANATION:

The secure storage system starts with the user authentication phase,in which the user has to select an image which is stored locally in a system.Once the user select the image then he/she need to select the point of interest in that image Once the password is set.The selected image is stored into database for automatic image loading at login phase.Concentrating on the secure developing even the password image also encrypted by a SHA3-224 Algorithm.Next comes the login phase the user needs to select the same point of interest which he/she select at the time of registration phase .Once the system is login successfully next comes the storage phase. Here my system store only image and text document.For storing the text and image document in a encrypted way.I'm using the Elliptic curve cryptography approach.The files are encrypted while storing and decrypted while retrieving automatically.User allows to do Create, update ,delete operation on the files. For securing the data in the file the architecture contains approach called Elliptic curve cryptography at the model phase. Elliptic curve cryptography applied only for text and image document.

ARCHITECTURE DIAGRAM:



LIST OF MODULES

(I) Image selection and applying grid on the image

(II) Store and fetch the image:

(III) Dashboard

a) Profile

b) Upload file

c) Read and delete file

BRIEF DESCRIPTION OF MODULES

Image selection and applying grid on the image:

The system uses the graphical image as a password,So in this modules I'm developing code which select the local image in a system.Once the selection process is completed,the transparent grid view is applied on the image,which is used to pick the pixel detail of the image when the user clicks the point of interest to set password

Store and fetch the image:

In this module the image is encrypted using a SHA-3 Algorithm and stored into a database.Once the image is stored it should be retrieved at login phase,In this modules the code supports to retrieve the data from the database automatically when the user enters his user id.

Dashboard:

In the dashboard module we have three sub-modules

(I) Profile

(II) Upload files

(III) Read and delete files

Profile:

This modules is used to keep tract of the personal details of the user. This modules contains the code for storing the user details.It also contains the feature of auto age calculation based on their birth date. This module contains code for updation of the user details

Upload file:

As I already mentioned that this secure storage system support only the text and image format document.The module contains the code for uploading the files from the local storage to a database in a encrypted form,By applying the Elliptic curve encryption cryptography algorithm.Once the encryption is done successfully the file are stored into a database securely

Read and delete file:

In this module contains code for when the user request to read the stored file,the request go to the server fetch the particular file and decrypt a file in a human readable format.This module also used to make operations on the file which the user is loaded into a system previously. Its also used to delete a file.

REFERENCES

[1] P. C. Golar and B. Khandelwal, "Study of Usability Parameter for Graphical Based Authentication System," 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART), 2020, pp. 23-26, doi: 10.1109/SMART50582.2020.9337116.

[2] H. Arora, G. K. Soni, R. K. Kushwaha and P. Prasoon, "Digital Image Security Based on the Hybrid Model of Image Hiding and Encryption," 2021 6th International Conference on Communication and Electronics Systems (ICCES), 2021, pp. 1153-1157, doi: 10.1109/IC

[3] http://www.iosrjen.org/Papers/Conf.ICIATE-2018/Volume-6/12-58-60.pdf
https://www.irjet.net/archives/V4/i11/IRJET-V4I11330.pdf

[4] C. A. S. Murty, H. Rana, R. Verma, R. Pathak and P. H. Rughani, "A Review of Web Application Security Risks: Auditing and Assessment of the Dark Web," 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICEC)