Second National Conference on Internet of Things : Solution for Societal Needs
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Enhanced Password Processing Scheme Based On Visual Cryptography and OCR

Dr. P. Mangayarkarasi[1], Rakesh H P [2]

[1]Associate Professor, ISE Department, New Horizon College of Engineering, Bengaluru, Karnataka, India
[2]M. Tech. Scholar, Cyber Forensics and Information Security, ISE Department, New Horizon College of Engineering, Bengaluru, Karnataka, India

ABSTRACT

Customary secret phrase change conspires for client verification is to change the passwords into hash esteems. These hash-based secret phrase plans are similarly straightforward and quick on the grounds that those depend on text and celebrated cryptography. Notwithstanding, those can be presented to digital assaults using secret word by breaking instrument or hash- breaking on the web locales. Aggressors can altogether sort out a unique secret word from hash esteem when that is generally straightforward and plain. Thus, many hacking mishaps have been happened prevalently in frameworks embracing those hash- based plans. In this work, we recommend upgraded secret key preparing plan dependent on picture utilizing visual cryptogra- phy (VC). Not quite the same as the customary plan dependent on hash and text, our plan changes a client ID of text type to two pictures scrambled by VC. The client should make two pictures comprised of subpixels by irregular capacity with SEED which incorporates individual data. The worker just has client's ID and one of the pictures rather than secret word. At the point when the client signs in and sends another picture, the worker can extricate ID by using OCR (Optical Character Recognition). Therefore, it can validate client by contrasting removed ID and the saved one. Our proposition has lower calculation, forestalls digital assault pointed toward hash cracking, and supports confirmation not to uncover individual data like ID to assailants.

I. INTRODUCTION

Client validation overall frameworks has continued essen- tially through check of the ID and secret key. To send and check secret word, the framework utilizes a hash-based secret key plan that changes unique secret word to hash esteem by acclaimed work. The benefits are that it can be adapted in framework without trouble, and computational speed of cycle is quick on the grounds that a sort of hash-put together plan is generally based with respect to message using famous hash capacity like MD5, SHA256. Be that as it may, it is helpless against assaults, for example, beast power assault or word reference based assault clearly by secret key breaking device or hash-breaking on the web destinations. Accept that somebody characterizes secret word "1qaz2wsx" in a framework. On the off chance that an assailant knows about the hash esteem " 1c63129ae9db9c60c3e8aa94d3e00495", the worth can be adequately broken essentially by free break site . Despite the fact that the aggressor doesn't have a clue about any data about hash capacity, the individual can without much of a stretch supposition which sort

of hash work is adjusted in the framework. As the outcome, the aggressor can make optional harm the framework.

Problem Statement

Despite the fact that the aggressor doesn't have the foggiest idea about any data about hash capacity, the person can without much of a stretch theory which sort of hash work is adjusted in the framework. As the outcome, the assailant can make auxiliary harm the framework. Members have the obligation on this sort of assaults. At the point when an analyst asked to numerous individuals about secret word the executives practices.

II. SYSTEM ANALYSIS

INTRODUCTION TO SYSTEM ANALYSIS

System

A framework is an efficient gathering of associated parts connected together as indicated by an arrangement to accom- plish a particular goal. Its principle qualities are association, communication, reliance, coordination and a focal target.

System Analysis

Framework examination and configuration are the utilization of the framework way to deal with critical thinking for the most part utilizing PCs. To recreate a framework the expert should consider its components yield and data sources, processors, controls, criticism and climate.

Analysis

Examination is an itemized investigation of the different activities performed by a framework and their connections inside and outside of the framework. One part of examination is characterizing the limits of the framework and deciding if an up-and-comer framework ought to think about other related frameworks. During investigation information are gathered on the accessible documents choice focuses and exchanges took care of by the current framework. This includes gathering data and utilizing organized instruments for investigation.

III. EXISTING SYSTEM

Examination is an itemized investigation of the different activities performed by a framework and their connections inside and outside of the framework. One part of examination is characterizing the limits of the framework and deciding if an up-and-comer framework ought to think about other related frameworks. During investigation information are gathered on the accessible documents choice focuses and exchanges took care of by the current framework. This includes gathering data and utilizing organized instruments for investigation.

IV. PROPOSED SYSTEM

1) The user inputs the ID and password.
2) The device of user creates an original image composed of black characters and white background. If the saved original image exists on user's device, it dose not have to create the original image again.
3) Although the device does not possess the first shared im- age, it can thoroughly construct second shared image referred to the original image and first shared image because the device already knows the SEED to make up the first shared image.
4) The user sends the second shared image only to the server.
5) The server overlaps the first shared image saved and the second shared image received.
6) The server should remove the background of the over- lapped image as in Figure 3 (d), to gain original image.

7) ID is retrieved from the background-removed image by OCR .
8) The server confirms whether the extracted ID corresponds with saved ID, and determines success or fail.
9) The result is sent to the user.

Advantages of the Proposed System

The goal of our proposal is to prevent cyber attack and support privacy of personal information.

Project Module Description Modules

Visual Cryptography Technique:

In this module showed a visual secret sharing scheme, where a picture was separated into n shares so just somebody with all n shares could unscramble the picture, while any n– 1 shares uncovered no data about the first picture. Each offer was imprinted on a different straightforwardness, and decoding was performed by overlaying the offers. When all n shares were overlaid, the first picture would show up. There are a few speculations of the fundamental plan including k-out-of-n visual cryptography.

Region Growing Algorithm:

It is likewise delegated a pixel-based picture division strat- egy since it includes the choice of initial seed focuses. This way to deal with division analyzes adjoining pixels of intro- ductory seed focuses and decides if the pixel neighbors ought to be added to the area. The cycle is iterated on, in a similar way as general data clustering algorithms.

OCR (optical character recognition)

OCR (optical character acknowledgment) is the acknowl- edgment of printed or composed content characters by a PC. This includes photograph checking of the content character-by- character, examination of the filtered in picture, and afterward interpretation of the character picture into character codes, like ASCII, regularly utilized in data processing.

V. SYSTEM REQUIREMENTS

Functional Requirements

This System must be created in MVC Architecture on java innovation. There ought to be two entertainers Admin, User.

- Admin ought to have separate login meeting where she/he can ready to login with Username and secret word and ready to keep up User Creation subtleties.
- At the hour of client creation itself client accepting offer picture to client register email and offer (II) administrator putting away in Server.
- User needs to login by utilizing username and he needs to get the verify picture in worker application as offer (II).
- Already client got share (I) picture from their email and offer (II) worker App now following stage he needs to blend the share(I) and share(II) picture then, at that point removing the userid utilizing OCR method we are doing userid confirmation measure.

Non Functional Requirements

- **Usability**

Basic is the key here. The framework should be basic that individuals like to utilize it, however not so intricate that individuals try not to utilize it. The client should be acquainted with the UIs and ought not have issues in relocating to another framework with another climate. The menus, catches and exchange boxes ought to be named in a way that they give clear comprehension of the usefulness. A few clients will utilize the framework all the while, so the convenience of the framework ought not get influenced concerning singular clients.

- **Reliability**

The framework ought to be dependable and solid in giving the functionalities. When a client has rolled out certain improvements, the progressions should be made apparent by the framework. The progressions made by the Programmer ought to be noticeable both to the Project chief just as the Test engineer.

- **Performance**

The framework will be utilized by numerous workers all the while. Since the framework will be facilitated on a solitary web worker with a solitary data set worker behind the scenes, execution turns into a significant concern. The framework ought not surrender when numerous clients would utilize it at the same time. It ought to permit quick availability to the entirety of its clients. For instance, if two test engineers are at the same time attempting to report the presence of a bug, then, at that point there ought not be any irregularity at the same time.

- **Scalability**

The framework ought to be adequately adaptable to add new functionalities at a later stage. There ought to be a typical channel, which can oblige the new functionalities.

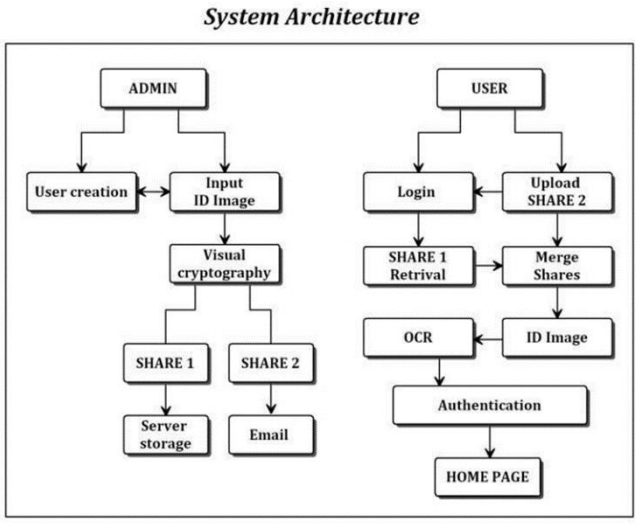
- **Maintainability**

The framework observing and support ought to be basic and objective in its methodology. There ought not be an excessive number of occupations running on various machines to such an extent that it gets hard to screen whether the positions are running without blunders.

- **Portability**

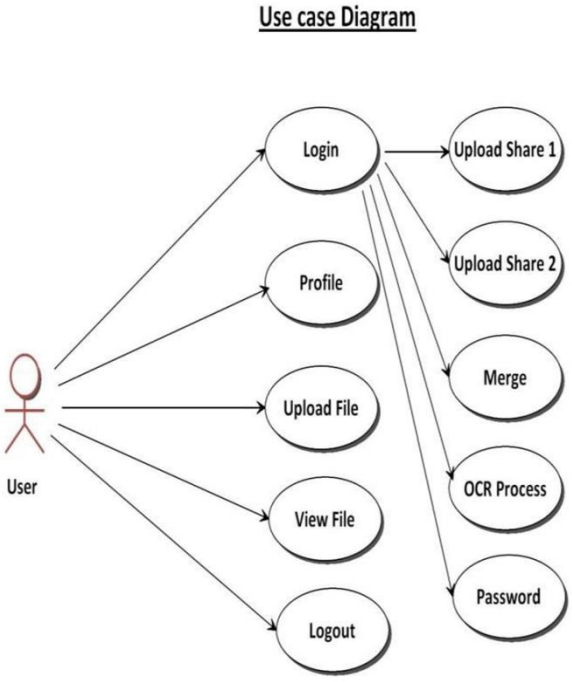
The framework ought to be effectively compact to another framework. This is required when the web worker, which s facilitating the framework stalls out because of certain issues, which requires the framework to be taken to another framework.

VI. SYSTEM ARCHITECTURE

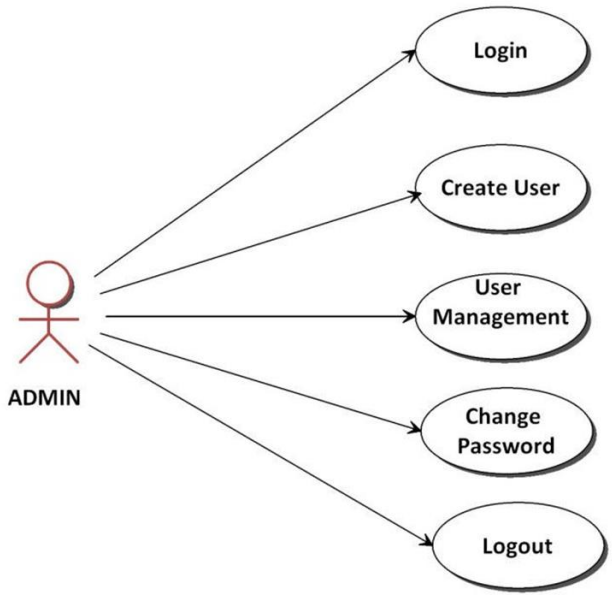


USE CASE DIAGRAM

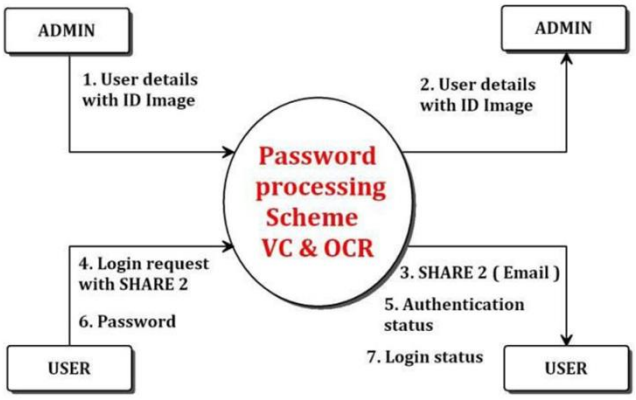
Admin:



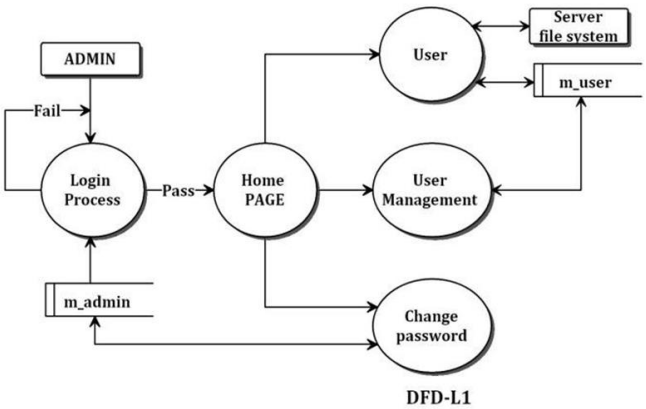
Use case Diagram



Contaxt Analysis Diagram



DFD - Admin Session



DFD-L1

IMPLEMENTATION TECHNOLOGIES

The execution stage includes something beyond composing code. Code additionally should be tried and fixed just as arranged and incorporated into a total executable item. We normally need to use design the executives to monitor diverse form of code. This is the phase of the undertaking where the hypothetical plan is transformed into a functioning framework. On the off chance that the execution isn't painstakingly arranged and controlled, it can cause bedlam and disarrays. It is consistently a smart thought to remember that a few qualities that ought to be found in a decent execution like Readability- our code is written in MVC Architecture ,JAVA to accomplish the target of the undertaking that is to present a novel plan of component plan for adjusting the asset utilizations .

Our execution stage requires the accompanying undertakings:

- Careful arranging
- Investigation of framework and limitations
- Design of techniques to accomplish the changeover
- Evaluation of the changeover technique
- Correct choices in regards to determination of the stage
- Appropriate determination of the language for application improvement Java Technology Java innovation is both a programming language and a stage.

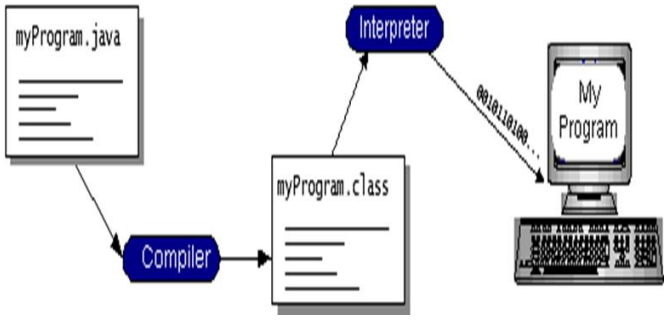
THE JAVA PROGRAMMING LANGUAGE

The Java programming language is a significant level language that can be portrayed by the entirety of the accompanying popular expressions:

- Simple
- Architecture nonpartisan
- Object arranged
- Portable

- Distributed
- High execution
- Interpreted
- Multithreaded
- Robust
- Dynamic
- Secure

With most programming dialects, you either accumulate or decipher a program so you can run it on your PC. The Java programming language is surprising in that a program is both accumulated and deciphered. With the compiler, first you make an interpretation of a program into a transitional language called Java byte codes — the stage free codes deciphered by the translator on the Java stage. The translator parses and runs every Java byte code guidance on the PC. Aggregation happens only a single time; understanding happens each time the program is executed. The accompanying figure outlines how this functions.



You can consider Java byte codes as the machine code directions for the Java Virtual Machine (Java VM). Each Java mediator, regardless of whether it's an improvement apparatus or a Web program that can run applets, is an execution of the Java VM. Java byte codes help make "compose once, run anyplace" conceivable. You can assemble your program into byte codes on any stage that has a Java compiler. The byte codes would then be able to be run on any execution of the Java VM. That implies that up to a PC has a Java VM, a similar program written in the Java programming language can run on Windows 2000, a Solaris workstation, or on an iMac.

VII. REFERENCES

[1]. Brian Cluster analysis. , West Sussex, U.: Wiley. ISBN 9780470749913, 2011.

[2]. Silva, , "Practical Eclipse Rich Client Platform Projects (1st ed.)". . p. 352. ISBN 1-4302-1827-4, March 2009.

[3]. Riedl, C.; Zanibbi, R.; Hearst, M. A.; Zhu, S.; Menietti, M.; Crusan, J.; Metelsky, I.; Lakhani, K. (February 20, 2016). "Detecting Figures and Part Labels in Patents: Competition-Based Development of Image Processing Algorithms". International Journal on Document Analysis andRecognition. 19 (2):155.

[4]. Gaw, Shirley, and Edward W. Felten, "Password management strategies for online accounts," Proceedings of the second symposiumon Usable privacy and security. ACM, 2006.

[5]. Nguyen, Thi Thu Trang, and Quang Uy Nguyen, "An analysis of Persuasive Text Passwords, "Information and Computer Science (NICS), 2015 2nd National Foundation for Science and Technology Development Conference on. IEEE,2015.

[6]. Tam, Leona, Myron Glassman, and Mark Vandenwauver, "The psychology of password management: a tradeoff between security and convenience, "Behaviour & Information Technology 29.3 (2010): 233- 244.

[7]. Wang, Luren, Yue Li, and Kun Sun, "Amnesia: A Bilateral Generative Password Manager," 2016 IEEE 36th International Conference on Distributed Computing Systems.