

# Cloud-Based Criminal Record Management with Graphical Authentication

DR. K. N. Honwadkar<sup>1</sup> Mauli Jadhav<sup>2</sup> Harish Sabale<sup>3</sup> Ashvini Patil<sup>4</sup> Shubham Morgoankar<sup>5</sup>  
<sup>1,2,3,4,5</sup>SKNCOE, SPPU University

**Abstract**— Here we have one of the algorithms which are based on selection of username and images as a password. From this paper we are trying to give bunch of images on basis of alphabet series position of characters in username. Hence cloud is provided with graphical password authentication. Other advantages of this system are it is a Shoulder-Surfing Resistant Graphical Password Scheme. We applied this way to create the persuasive click-based graphical password scheme, Persuasive Cued Click-Points (PCCP) check usability and security. Steganography is hidden communication which means to hide the very reality of a message from a third party. Due to growing use for security of data, image Steganography is popular. The ancient image Steganography algorithm is Least powerful Bit embedding, but it can be easily detected by the attackers as it fix data sequentially in all pixels. Instead of constantly embedding data, data can be inserting in random pixels, but it causes speckles in the image. A superior approach is to hide the data in the sectors like fringes. Essentially above system help graphical password, cued click points and edge-LSB Steganography for cloud security (i.e. secure criminal cloud).

**Key words:** Graphical Authentication, Cloud-Based Criminal Record Management

## I. INTRODUCTION

A graphical password is a second option to text passwords and alphanumeric passwords in which users click on images to authenticate themselves rather than type alphanumeric text strings. We have advanced one such system, called Pass Points, and created it with human end users. The results of the evaluation were more auspicious with respect to graphical password. In this research we increase our human factors testing by studying these issues: the effect of tolerance or margin of fault, in clicking on the password points and the outcome of the image used in the password system. In our study, results show that exact memory for the password is strongly decrease when using a small tolerance as per 10 x 10 pixels around the user's password points. This may occur because user fails to encode the password points in memory in the accurate manner that is necessary to recall the password over a lapse of time.

## II. PROPOSED SYSTEM

The aim of study is to increase the security of criminal database cloud by using graphical password authentication process. Text password, graphical password and persuasive cued click point password authentication process. Therefore the extension of the study will be to make dataset online and make it more secure for end user. Cloud will provide the access to every authenticated user and make the database easily available

### A. Objectives

- Creation of criminal database
- Put of criminal database on cloud

- Providing graphical authentication
- Additional security using edge LSB Steganography

## III. PROPOSED SOLUTION

Graphical password authentication with cued click points & Edge- LSB Steganography for data hiding:

In this approach when any user wants to access cloud services they will be hand over with two options sign in and sign up. At server side calculation in sign up registration process is made for user. User has to enter the username based on that particular image which will be provided to them on the support of algorithm. In this algorithm first username is checked. After set of images will be supply to user. User has to select two images as client side selection and other two will be from server side as server side selection. In sign in the user have to give username which he has given during sign in process and select the password from given set of images. Authentication of user is done then cloud access is given to particular user. They access their accounts with uploading and downloading facility. Graphical password provides more security than alphanumeric password. Most of the system provides image linked password i.e. graphical password. In this method selectable images are used, user can have more number of images on every page and among this entire password is selected. Images are different for each case, so if hackers try to each combination to find the correct password it will take millions of years. In the Least Significant Bit embedding algorithm (LSB) and Random Least Significant Bit embedding algorithm (RLSB) an attacker can easily detect the presence of hidden image.

To overcome these problems anew algorithm is proposed based on least significant bit embedding algorithm (LSB) for covering secret data in the edges of the image. The algorithm of Edge LSB hides data in edge pixel. The proposed algorithm is applicable to all sort of images and can be used in covert communication, hiding secret information like copyrights, trade secrets and chemical formulae.

### A. Architectures Design

Notation

A=secure authentication mechanism using graphical password

B=standalone data encryption system (offline)

C= web application that will interact with cloud

D=secure cloud for storage

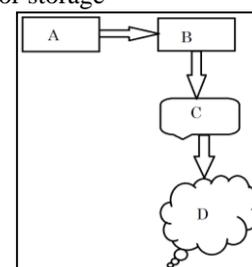


Fig. 1: Architecture

#### B. Hardware Resources Required

- 1) Hardware: Pentium based systems
- 2) RAM: 256MB (minimum)

#### C. Software Resources Required

- 1) Operating System: Windows 7 & above
- 2) Technology: Java/J2ee (JDBC, JSP)
- 3) Web Technologies: Html, JavaScript, CSS
- 4) Web Server: Tomcat 5.5
- 5) Database: Oracle 4 and above
- 6) Software's: J2SDK1.5

#### D. Technical Keywords

- 1) Persuasive cued click point (PCCP)
- 2) Graphical password
- 3) Pass-Points, password security
- 4) Human factors, usable security.
- 5) Shoulder surfing
- 6) Image based scheme
- 7) Steganography

Implementation, and Evaluation of a Knowledge-Based Authentication system," Technical Report TR-11-03, School of Computer Science, Carleton Univ., Feb. 2011.[2]

- [6] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "The Memorability and Security of Passwords," Security and Usability: Designing Systems That People Can Use, L. Cranor and S. Garfinkel, eds., ch. 7, pp. 129-142, O'Reilly Media, 2005.[2]
- [7] L.Jones, A.Anton, and J.Earp, "Towards Understanding User Perceptions of Authentication Technologies,"
- [8] E. Stobert, A. Forget, S. Chiasson, P. van Oorschot, and R. Biddle, "Exploring Usability Effects of Increasing Security in Click-Based Graphical Passwords," Proc. Ann. Computer Security Applications Conf. (ACSAC), 2010. [2]

#### IV. CONCLUSION

Thus we have successfully expanded the safety of criminal database cloud by using graphical password authentication process. Text password, graphical password and persuasive cued click point password authentication process.

Also by including the Edge-LSB Steganography we tried our best to make it unbreakable.

#### ACKNOWLEDGMENT

It gives us great pleasure in presenting the paper on 'Cloud based criminal record with graphical authentication'

We would like to take this opportunity to thank our internal guide Dr. K. N. Honwadkar for offering us all the help and guidance we needed. We are really grateful to them for their gentle support. Their beneficial suggestions were very helpful.

We are also grateful to Dr. P. N. Mahalle, Head of Computer Engineering Department of SKNCOE for his indispensable support, suggestions.

In the end our special thanks to computer department of SKNCOE for providing various resources as laboratory with all needed software platforms, continuous Internet connection, for our study.

#### REFERENCES

- [1] Wang, Ran-Zan, Chi-Fang Lin, and Ja-Chen Lin. "Image hiding by optimal LSB substitution and genetic algorithm."
- [2] Zayed, Hala H. "A High-Hiding Capacity Technique for Hiding Data in images Based on K-Bit LSB Substitution."
- [3] Nadeem Akhtar, Pragati Johri, Shabbaaz Khan, "Enhancing the Security and Quality of LSB based Image Steganography", [IEEE International Conference on Computational Intelligence and Computer Networks (CICN), 27-29 September, 2013, Mathura, India [3]
- [4] Diggle, Statistical Analysis of Spatial Point Patterns. Academic Press, 1983.[2]
- [5] R. Biddle, P. Van, S. Chiasson, E. Stobert, A. Forget, Oorschot, "Persuasive Cued Click-Points: Design,