iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** III **Month of publication:** March 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Sound Signature in Graphical Password

Monali D. Supare[1], Swati V. Badone[2], Prof. R.P. Bijwe[3]
Final Year, CSE, H.V.P.M's COET, Amravati

Abstract: Mostly user select password that is predictable. This happens with both graphical and text based passwords. Users tend to choose memorable password, unfortunately it means that the passwords tend to follow predictable patterns that are easier for attackers to guess. While the predictability problem can be solved by disallowing user choice and assigning passwords to users, this usually leads to usability issues since users cannot easily remember such random passwords. Numbers of graphical password systems have been developed. Study shows that text-based passwords suffer with both security and usability problems. According to a recent news article, a security team at a company ran a network password cracker and within 30 seconds and they identified about 80% of the passwords. It is well know that the human brain is better at recognizing and recalling images than text, graphical passwords exploit this human characteristic. We proposed a sound signature graphical password consists of user-chosen click points in a displayed image.
Keywords: - Sound signature, Authentication, CCP(Cued Click Points).

I. INTRODUCTION

Various graphical password schemes have been proposed as alternatives to text-based passwords. Psychology research has proved that the human brain is better at recognizing and Recalling images compare to text. Graphical passwords are intended to capitalize on this human characteristic in hopes that by reducing the memory burden on users, coupled with a larger full password space offered by images, more secure passwords can be produced and users will not resort to unsafe practices in order to Scope .Mostly user select password that is predictable. This happens with both graphical and text based passwords. Users tend to choose memorable password, unfortunately it means that the passwords tend to follow predictable patterns that are easier for attackers to guess. While the predictability problem can be solved by prohibiting user choice and assigning passwords to Users using some standards, this usually leads to usability issues since users cannot easily remember random passwords. Number of graphical password systems has been developed. Study shows that text-based passwords suffer with both security and usability problems. Integration of sound signature in graphical password authentication system is designing and developing new model of graphical password which works on click based graphic method, in this method random images are used where user need to select one click per image after selecting image user is requested to select sound signature corresponding to each click Point .

II. BACKGROUND

The Cued Click Points scheme shows promise as a usable and memorable authentication mechanism. By taking advantage of user's ability to recognize images and the memory trigger associated with seeing a new image, CCP has advantages over Pass Points in terms of usability. The existing system is Pass Points proposed passwords which could be composed of several points anywhere on an Image.

A. Graphical Password:

Access to computer systems is most often based on the use of alphanumeric passwords. However, users have difficulty remembering a password that is long and random appearing. Instead, they create short, simple, and insecure passwords. Graphical passwords have been designed to try to make passwords more memorable and easier for people to use and, therefore, more secure .The password problem arises largely from Limitations of human's long-term memory (LTM).

B. System Implementation

The implementation has mainly three modules:

1) Create Password Module: PCCP encourages users to select less predictable passwords, and makes it difficult to select

Volume 3 Issue III, March 2015
ISSN: 2321-9653

passwords where all five click-points are hotspots. Specifically, when user creates a password, user selects a click-point within each selected image. User is also asked to select the tolerance dimension during password creation. In addition user is asked to select a sound signature or music which helps the user in order to remember the click-points during login phase even if the user tries to login after a long time.

2) *Login Module:* In login module, the user can give their username and password. In addition, a sound signature is integrated to help in recalling the password. Hacking of username and password can be done. But if the pixels are pointed out correctly, then only one can login in to user page. During login phase, username is taken from the user and is stored in corresponding variable. If the entered value matches the data in the database which is stored earlier, it will display corresponding user's first image which is selected previously during registration session. And the user can select their previously chosen images by clicking on the specific region or point chosen earlier. After repeating the same steps for all the images, comparisons are made. Even if the point chosen in the image was wrong, the user will not be informed about the wrong path which reduces the ability of hacker to guess the password. Else the user is directed to the home page where they can lock or unlock the folders and can also able to change their password as well as the music. During login, if the pixels are clicked correctly, then the selected sound is started to play. Else any other sound will be played. Here number of login attempts is limited to three since an extra protection is essential to our password protected system. Security is the main reason to restrict access. Login attempt-limit blocks a user from making further attempts after a specified limit on retries is reached.
3) *Verification Module:* During verification phase, the details that the user enters during registration phase and login phase are verified.
4) *Folder Lock/Unlock Module:* Protecting your data and information from certain unwanted and prying eyes may become a dilemma if you end up with enough personal and private data on your computer.

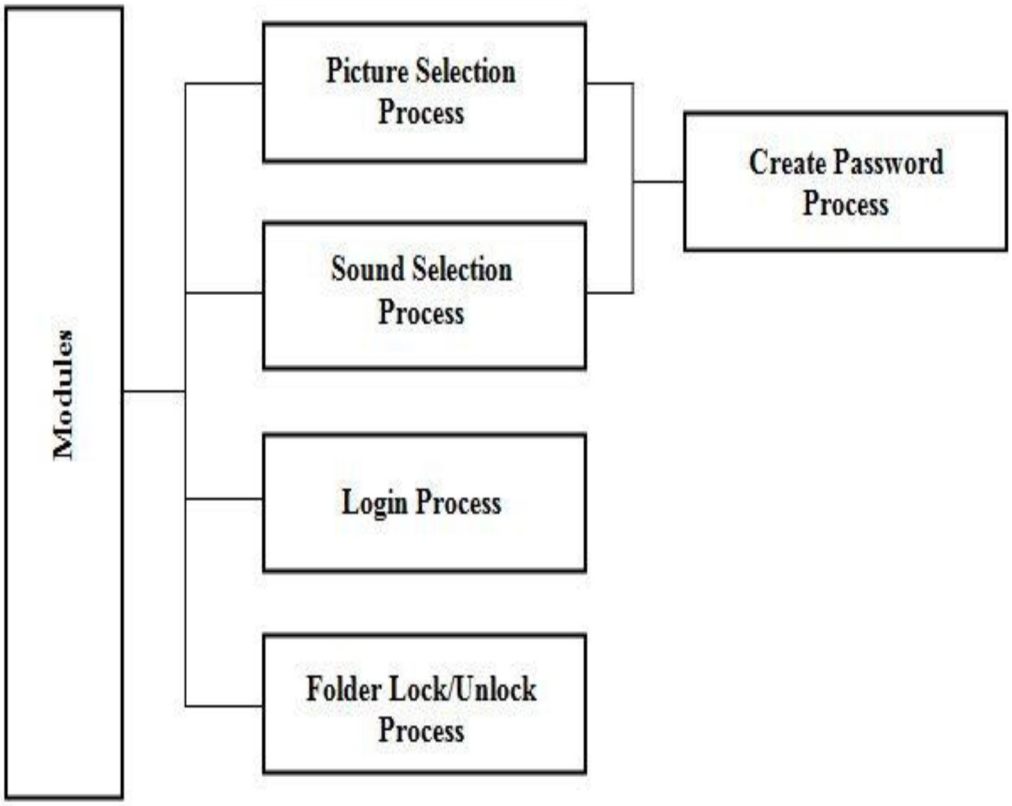


Fig 1.Modules Description

Volume 3 Issue III, March 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

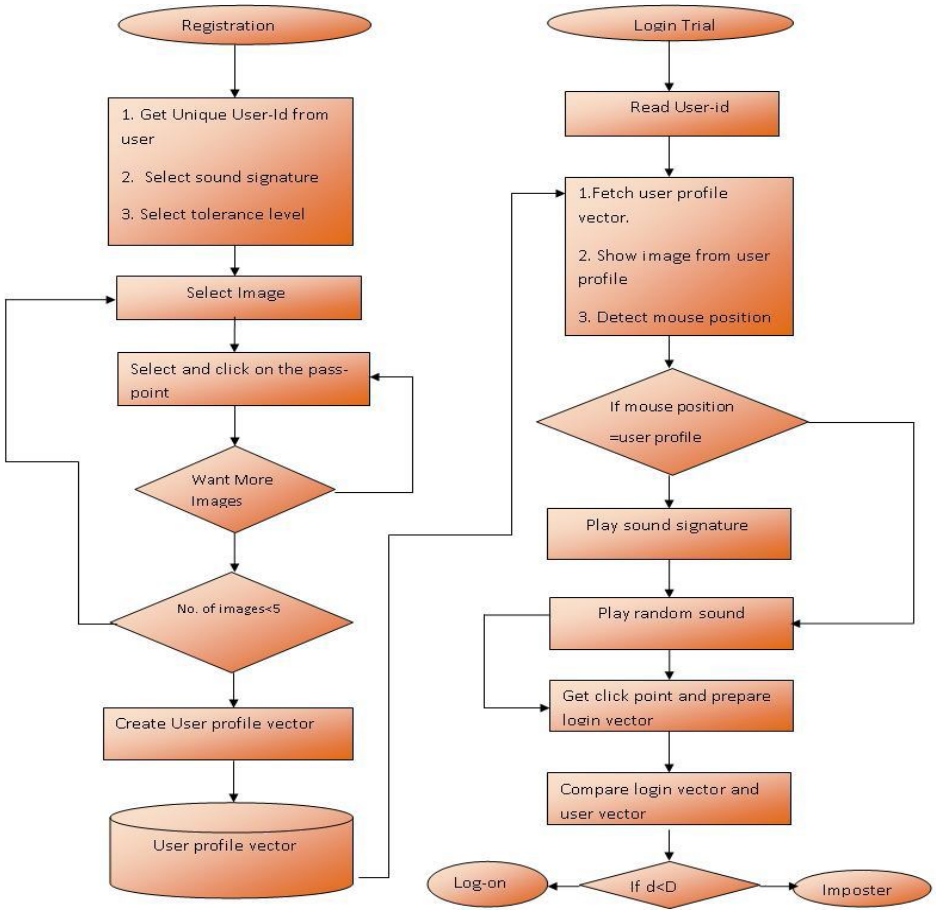


Fig 2.Block Diagram of Proposed System

III. IMPLEMENTATIONS DETAILS

We have proposed system and implementing an application for the security and recovery of the graphical password .Till now the systems are developed for the security of the password but by this application we are trying to provide the security as well as recovery also. This application will use sound signature to help the user to recover the password. Hence to store the password, we need to discrete the point by calculating its offset d and its images will be shown to the user corresponding segment identifier i. Offset d will get stored in clear while I store in protected form. Hence when the re-entry of the password will occur the System should aware of the tolerance segment identifier i which is the acceptable inaccuracy calculated by

$i = [x-r/2r]$ …… (i)

At the time of sign-up user has to select a sequence of points on images with required tolerance and the corresponding sound signature and at the time of login if user clicks on pixel that lies within a tolerance area his/her login will be successful. Otherwise any random images will be shown to the user To store the images and account details (eg.User id ,email id). We have used a mechanism called object serialization which will act as a database of our system. We have also used serialization instead of any other database system as it is less complex as well as it requires less time than any others. The main goal of our system is to integrate the sound with graphical password being use .Thus whatever textual signature you will give will be converted into sound signature. You may assign a sound of your own choice to your graphical password. User can select sound to each image or selected set of images depending on your wish. In case if user forgot the password and clicked on any wrong pixel then as a result user's selected sound signature at the time of registration will be play. This will definitely help the user to recover the password. This system will work same as that of real world accounts, you can send mail, receive mail, send image files etc

Volume 3 Issue III, March 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

IV. EXPERIMENTAL RESULTS & ANALYSIS

In the proposed work we have integrated sound signature to help in recalling the password. No system has been developed so far which uses sound signature in graphical password authentication.

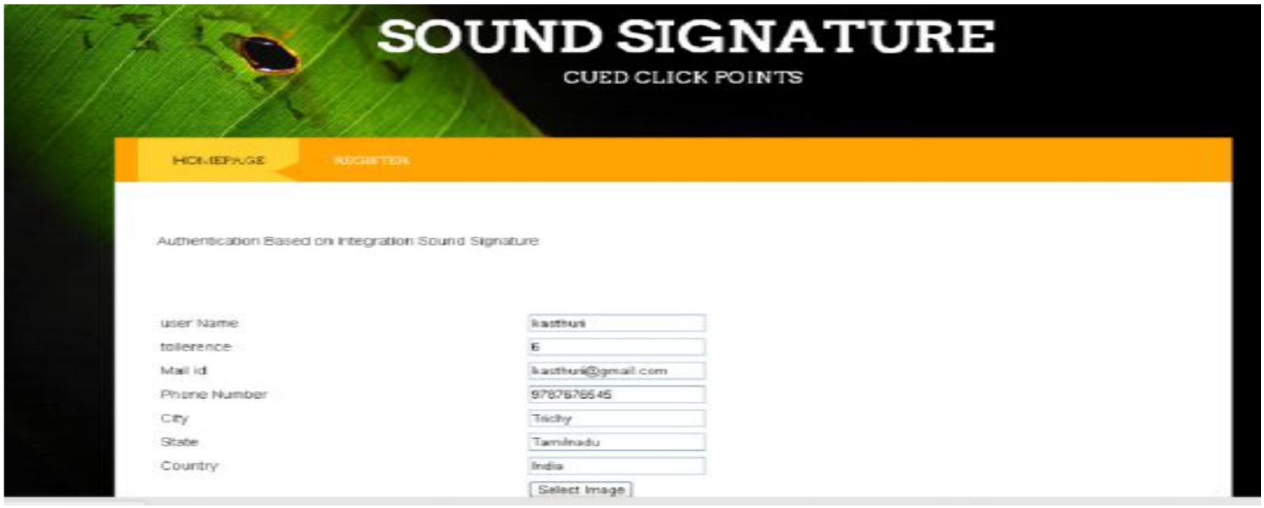


Figure 3. Registered Tolerance Sound Sign Login Process

Study says that sound signature or tone can be used to recall facts like images, text etc. In daily life we see various examples of recalling an object by the sound related to that object enters User ID and select one sound frequency which he want to be played at login time, a tolerance value is also selected with will decide that the user is legitimate or an imposter. To create detailed vector user has to select sequence of images and clicks on each image at click points of his choice . Profile vector is created. Enters User ID and select one sound frequency which he wants to be played at login time, a tolerance value is also selected with will decide that the user is legitimate or an imposter.

Fig 4. User uploading the images for Sound verification

Volume 3 Issue III, March 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

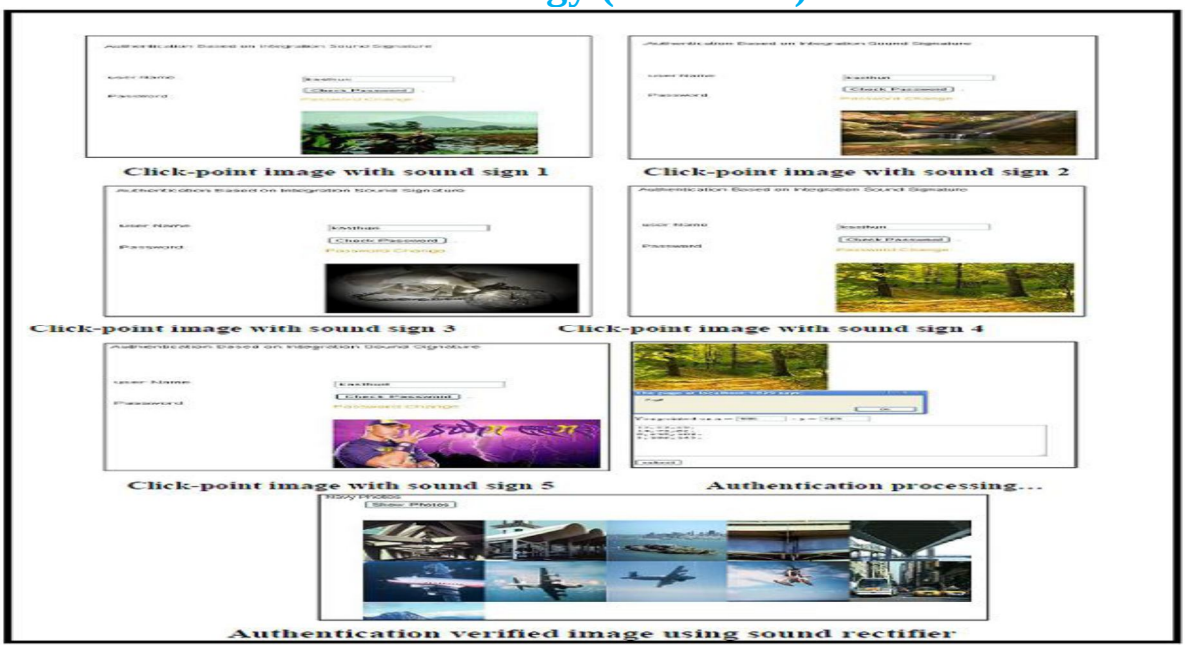


Figure 5. Recognition of Sound by Clicking the Image

V. CONCLUSION AND FUTURE ENHANCEMENT

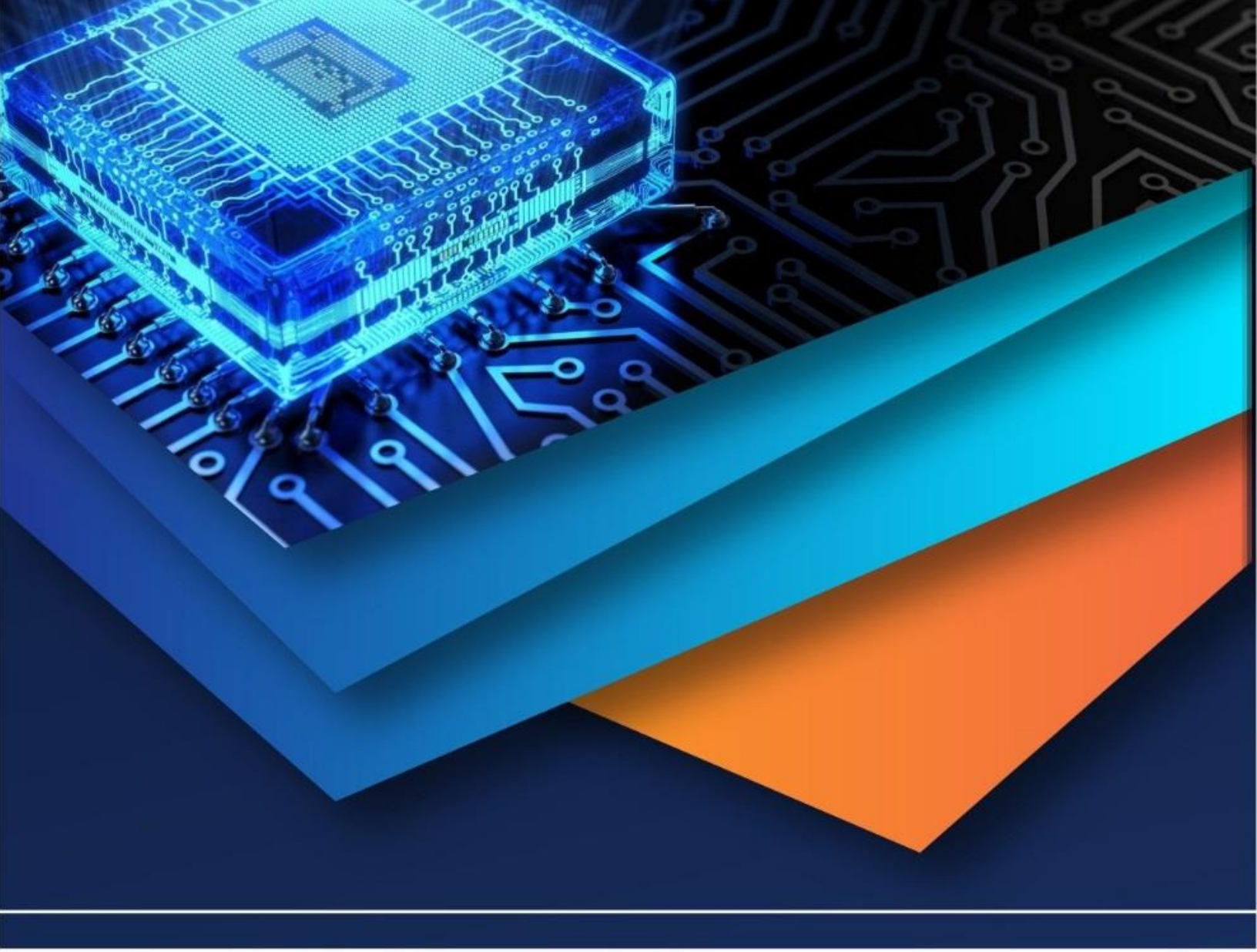
We have proposed a novel approach which uses sound signature to recall graphical password click points .No previously developed system used this approach this system is helpful when user is logging after a long time. In future systems other patterns may be used for recalling purpose like touch of smells, study shows that these patterns are very useful in recalling the associated objects like images or text, . In future systems other patterns may be used for recalling purpose like touch of smells, study shows that these patterns are very useful in recalling the associated objects like images or text. The general goal is to make the password easy to remember and to increase the security of knowledge-based authentication schemes. Here the focus is on click based graphical passwords. The existing schemes are investigated for designing a new graphical password authentication scheme. It is possible to increase both simultaneously through careful design that considers usability and security in combination. The need for thorough usability and security evaluations is emphasized, because system design can significantly impact user behavior, sometimes in ways, which in turn can significantly impact the security of a system.

VI. ACKNOWLEDGEMENT

First of all we would especially like to express sincere gratitude to our parents. It gives us great pleasure and satisfaction in presenting the paper on **"**Sound Signature in Graphical Password" Before we get into the depth of the things, we show our sincere gratitude towards respected teachers, guide, colleagues and all who have directly or indirectly helped us in the completion of this paper successfully

REFERENCES

[1] Integration of Sound Signature in Gr Graphical Password Authentication System by Saurabh Singh Agarwal .
[2] Integration of Sound Signature in 3D Password Authentication System (by Mr .Jaywant N. Khedkar1,Ms.Pragati P. Katalkar2, Ms. Shalini V. Pathak3)
[3] Integration of Sound Signature and Graphical Password Authentication System Suyog S. Nischal1, Sachin Gaikwad, Kunal Singh3 Prof. A. Devare.
[4] Davis, F. Monrose, and M. Reiter. "On user choice in graphical password schemes", 13th USENIX Security Symposium, August 2010.
[5] D. Weinshall and S. Kirkpatrick. "Passwords You'll Never Forget, but Can't Recall", Proceedings of Conference on Human Factors in Computing Systems (CHI) ACM, Vienna, Austria, pp. 1399-1402., 2011.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY