International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

Image Map: Alternative for Password Based Authentication

Padmaja.Pulicherla, Shiva Reddy Baddam

Abstract*:In the world today there are millions of websites and other web applications which operate with customizations to the user using the user account registration. This naturally requires a user name or a unique ID like email address and a password. This kind of authentication is being employed from days past to invention of authentication systems. But today with many such websites it has become a herculean task to remember the passwords of each and every sites. There are solutions like writing down or noting on any electronic device but these has equal physical chances of being revealed. So there is a need for a brand new authentication techniques which are better than existing ones and are easy to implement. Image map is one such an alternative that can replace traditional systems. This technique makes use of images taken from users during registration and certain number of points on one exclusive image from taken set of images.

Keywords*:Image map, Alternative for password, other login techniques, Alternate authentication.

I. INTRODUCTION

In the world today there are millions of websites and other web applications which operate with customizations to the user using the user account registration. This naturally requires a user name or a unique ID like email address and a password. This kind of authentication is being employed from days past to invention of authentication systems. But today with many such websites it has become a herculean task to remember the passwords of each and every sites. There are solutions like writing down or noting on any electronic device but these has equal physical chances of being revealed. So there is a need for a brand new authentication techniques which are better than existing ones and are easy to implement. Image map is one such an alternative that can replace traditional systems. This technique makes use of images taken from users during registration and certain number of points on one exclusive image from taken set of images.

II. LITERATURE REVIEW

A. Two step verification

Two-step verification is considered an alternative but true is not. Two step verification need the first authentication on platform and second on users phone or any other device. Google implements one such verification process. The main problem with this is, it can be applied only if you have your phone and an extending application of each site installed on it.

B. Finger print

Finger print based authentication is a secured way but this can be applied only if the user carries or possesses a bio-metric device or finger print scanner which is a tuff task and 99% of people today don't do. So this can be a secured way but cannot be an alternative.

C. Face recognition

Face recognition is even a better way to authenticate which can be applied using concepts of computer vision and machine learning. This requires an additional camera to capture the face. Cameras are now a days available on every phone but the problem shows up while dealing with desktops. Not all desktops may have camera which reduces the scope of the applicability.

D. One time passwords to the registered mobile numbers

OTP (One-time password) have proven them efficient in the fields of banking and other high security demanding departments but coming to a average website such security is secondary and the primary factor is easy accessibility. There may be cases where the phone is dead or lost and the owner is trying to find his phone using FindMyDevice, in this case the OTP cannot be received This leads to a obstacle again.

III. PROPOSED SYSTEM

Using image map as alternative the websites during the registration of a user can ask him/her to upload certain number of images of his choice. These images can be stored in the database as BLOB (Binary large object). Then these should be displayed to him and should ask to pick any one of them all.

After picking the image the image should be showed individually with the dimensions of 300px × 300px. Then user should be asked to plot certain points on image. Consider three points. Now record these points and the image offsets and can be sent to the server for the storage in database for future authentication.

The points plotted are of size 1px × 1px, so user may not be able to plot them exactly every time. So we consider a radius of 50px (Maximum size of finger point of touch devices and maximum error negotiation for desktops) around the valid point. If the points plotted during the login are in the valid range, then we call the authentication legitimate else illegitimate.

Manuscript published on 30 September 2019
* Correspondence Author
Prof. Dr. Padmaja.Pulicherla, Professor CSE Dept., TKREC(R9), JNTU Hyderabad, India.
Shiva Reddy Baddam, Student-CSE, TKREC(R9), JNTU Hyderabad, India.

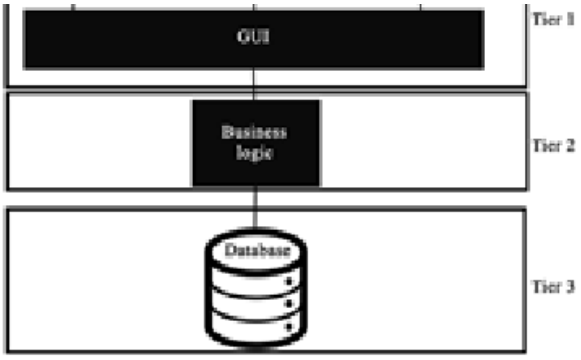

Fig (I) Architecture Diagram

IV. ALGORITHM

1. Start
2. upload images
i.Pick one image
ii. Map points
iii. Store in database
3. Check email id and repeat step 2
4. Compare values and check if the points are in the valid range
5. Display result
END

V. METHODOLOGY

A. Registration

During registration collection and display of the images is easy. After plotting the points the points can be recorded using event invocation and reading the **pageX** and **pageY** values of the point by the means of any client side scripting language. The obtained points are with respect to the webpage or window but not the element. So to get the coordinates of points with respect to the element we read the **offset().left()** and **offset().top() (Here considered scripting language is JQuery).** Now the difference between the pageX and offset().left() gives the x-coordinate with respect to image element and similarly y-coordinate can be obtained. These pairs are to be inserted into the database and can be used to authenticate.

B. Authentication

During authentication a check box or radio input can be implemented to select a image out of displayed list. Once an image is checked then it must be first checked if it is the same image that is selected during the registration. If it is then proceed forward else report the user.

In the next step ask the user to plot the points and calculate the points with respect to the element same as we have done during registration.

Now the valid range is considered as 50px radius. So we need to first generate an inequation of the circle with points in database as centre. The equation looks like below

(x-a)^2+(y-b)^2 <=2500

Here, x=recorded x-coordinate,
Y= recorded y coordinate,
a= x-coordinate in database,
b= y-coordinate in database

The above is the standard equation that satisfies if the point is on the circumference or inside the circumference. So the above standard equation can be applied to check the validity of the points.

Repeat the same for all three points and if found valid then the login is legal. Else report the user.

The accuracy of the authentication can be obtained by finding the probability of the valid region in the whole region.

It can be calculated as,

No. of valid regions=3

Valid area=No. of valid regions × 3.1428×50×50= 3×3.1428×50×50=23571.4285

Total area= 300×300=90000

Accuracy= (90000-23571.4285)×100/90000

= 73.809%

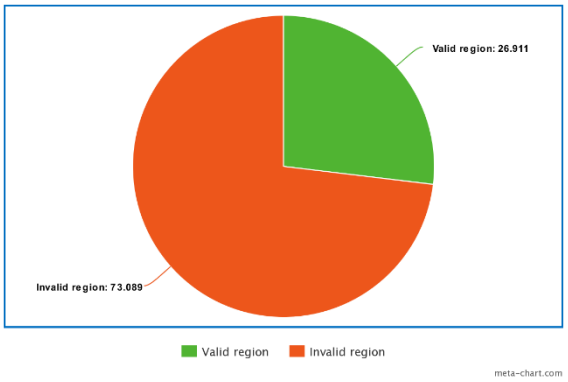

Fig (II) Graph

VI. CONCLUSION

A. Figures and Tables

Hereby, using image map an efficient and highly applicable user authentication system can be built. This can be built using a simple client side script like JavaScript, JQuery, VBScript etc. and server side script like PHP, ASP, JSP etc. Using this technique, the authentication system with the accuracy of 73.809% can be achieved.

VII. FUTUREENHANCEMENTS

Using this as base the applications which can take the lines or curves or patterns as elements for authentication can be build. Several encryption and decryption techniques can also be applied on the coordinates and images to maintain high standards of information security.

VIII. CONCLUSION

A conclusion section is not required. Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions.

REFERENCES

1. Digital Security: 5 Alternatives to Passwords - https://www.bbvaopenmind.com/en/digital-security-5-alternatives-to-passwords/.
2. Top 3 password alternatives for better website security - https://swoopnow.com/password-alternatives/.
3. Passwords Are Scarily Insecure.- https://www.entrepreneur.com/article/309054
4. Job Shifting Prediction and Analysis Using Machine Learning

https://iopscience.iop.org/article/10.1088/1742-6596/1228/1/012056/meta
5. Two Step Approach for Software Reliability : Rayleigh http://www.jmest.org/wp-content/uploads/JMESTN42350891.pdf

AUTHORS PROFILE

Dr.Padmaja.Pulicherla,, Ph.D, CSE-TKREC(R9), Padmaja.j2ee@gmail.com

Shiva Reddy Baddam,B.Tech(Computer Science and Engineering), Teegala Krishna Reddy Engineering College. Email: bshivareddy00@gmail.com