IJSEAT
International Journal of
Science Engineering and Advance Technology

A Newfangled Authentication Protocol Based On Audio Produced Principles

[1]P.Suneetha,[2].B.Sujatha
[1]M.Tech(pursuing),[2]Professor &HOD in Department of Computer Science and Engineering
Godavari Institute of Engineering & Technology (GIET),Rajahmundry, AP, India
Email:[1]suneetha.69@gmail.com,[2]birudusujatha@gmail.com

Abstract-
Graphical authentication is more proficient and more securable. An imperative convenience objective for information based authentication frameworks is to bolster client in selecting passwords for higher security in the feeling of being from an extended viable security space. Here we are utilizing x and y directions to pick a photo secret word. Also the photos in x and y directions are changing haphazardly and subsequently it is hard to locate the first picture. In our base paper the methodologies utilized are "Convincing signaled snap focuses"," Cued snap focuses" and "Pass focuses". Primary apparatuses utilized here are pccp, viewport and that is utilized for secret word creation. Viewport methodologies are utilized to significant client picked secret word and secure framework created arbitrary watchword that are hard to recollect. The pccp making a less guessable secret key is the least demanding game-plan. With a specific end goal to dodge "Shoulder surfing" calculation we are going for AES (Advanced encryption standard). In a contemporary mastery, the customary Authentication methodologies like "alphanumeric - usernames and passwords" can't be a versatile secured technique as it make out a critical downsides. It can't be protected and sound from programmers. Graphical passwords are a different option for existing alphanumeric passwords. In Graphical passwords clients click on pictures than sort a long, complex secret key. Exhaustive examination is finished by different analysts proposes that the photo's majority based authentication plans are essentially delicate as client tends to tap on hotspots in the pictures. A hotspot is the picture's territory which is effectively perceived against every single other picture, accordingly making such strategies defenseless. To make greater from the available confirmation, another convention "in light of the sound time stamps" making it hard for the shams to perform mystery. Here is a novel one of a kind answer for graphical validation defining so as

To take into account sound time stamps another method for model called "A NEWFANGLED AUTHENTICATION PROTOCOL BASED ON AUDIO PRODUCED PRINCIPLES ". This model calls a sound time stamps and in addition the number of sound timestamps and scramble the secret word with message digest adaptation 5 and making it hard for the gatecrasher to break the watchword there by forcing the more elevated amounts of security to the framework. The gatecrasher can't get the time stamps and additionally check of time stamps and making this strategy more secure, dependable and difficult to figure.

Index Terms—Authentication, Security, Graphical Passwords, Knowledge-based, PCCP with dynamic user blocks, Persuasive technology, Password registration, User login process.

I. Introduction

Sending Audio and video data is a typical interest in the present days. Data validness alludes to a surety over the wellspring of data; this suggests that data was not changed amid transmission. In any case, guaranteeing the legitimacy of media data by cryptographic systems is frequently ignored. Thusly the level of trust in sound feature data sent over open systems is constrained since there is no evidence that the got data was not adjusted by pernicious enemies amid transmission. In this setting guaranteeing the legitimacy of sound and feature data is a subject of awesome interest and for this reason cryptographic strategies are the main option, since cryptography is the main security ensure when we are working with data. This paper is worried with the advancement of a Java application that can be utilized to catch sound and feature data and after that send it to some remote PCs from an open system. More concrete, the application catches pictures from a web-cam joined with a PC and sends the sound feature data through RTP to different PCs. A cryptographic authentication convention is actualized with a specific end goal to keep data from being modified amid transmission. The Java environment gives great backing to both overseeing media streams and actualizing cryptography. This paper is composed as takes after. We survey some cryptographic primitives that can be utilized to ensure the legitimacy of data and some cryptographic conventions that can be based upon them.

PC security depends to a great extent on passwords to verify human clients. One of the key territories in security [1] research and practice is validation, the determination of whether a client ought to be permitted access to a given framework or asset. Then again, clients experience issues to recalling take a break in the event that they pick a safe secret word, i.e. a secret word that is long and arbitrary. In this way, they have a tendency to pick short and shaky pass-words. The proceeded with mastery of passwords over every single other strategy for end-client validation is a noteworthy humiliation to security analysts. As web innovation pushes forward quickly in different territories,

Passwords obstinately survive and imitate with each new site. Broad examinations of option confirmation plans have created no complete answers. A secret word confirmation framework ought to empower solid passwords while looking after memorability. We suggest that validation plans permit client decision while affecting clients toward more grounded passwords. In our sys-tem, the undertaking of selecting feeble passwords (which are simple for assailants to foresee) is drearier, debilitating clients from settling on such decisions. As a result, this methodology makes picking a more secure secret word the easy way out. Instead of expanding the weight on clients, it is less demanding to take after the frameworks proposals for a protected passwords highlight ailing in many plans swap content passwords for universally useful client validation on the web utilizing a wide arrangement of a quarter century, send capacity and security advantages that a perfect plan may give. To approve the end client for confirmation we normally like to receive the learning based authentication, which includes content based passwords. The content based passwords are helpless against be hacked. The aggressors can without much of a stretch figure the content passwords with different subtle elements of the framework. In the event that we need to maintain a strategic distance from this, the framework can allocate an in number secret word, which the aggressor can't figure. In any case, the framework doled out passwords are extremely di clique to retain and recalled by the client. The study on the graphical passwords expresses that the snap direct passwords are hard toward supposition by the aggressor and simple to recollect for the clients. So the secret word authentication framework ought to support the solid watchword choice while keeping up the client's memorability. This paper proposes the thought of powerful prompted snap point confirmation with the strategy of scrambling. This plan impact the client to set various snaps from a photo and size of passwords required. The client can likewise change his passwords amid a week oe regular with adjusted pictures. This plan completely relied on upon the client's memorability about his chose pictures. When he couldn't recollect which divide of the picture he chose for the snap, the client won't validate despite the fact that he is a real client. To beat this sort of issue the framework ought to keep a few approaches to hold the passwords.

II. BACKGROUND

Text passwords are the most popular user authentication method but have some security and usability problems. Security problem is nothing but causing various attacks like shoulder surfing (looking over one’s shoulder to get information) etc. and usability problem refers to limited password space. So to overcome from these drawbacks, graphical passwords had been introduced by Greg Blonder in 1996 which offers another alternative and are the focus of this paper. The passwords which we are focusing are cued-recall click based graphical passwords (also known as loci metric).In such systems, users identify and target previously selected locations within one or more images. The images act as memory cues to aid recall. Examples of these systems include Pass Points (PP) and Cued Click-Points (CCP) which are the present or existing systems.

A. Pass Points (PP):

User selects N random points in an image presented to user:

In this system an image is picked from set of images present in a gallery and user is shown the image. Task of user is to click N points as shown in Fig 1. As user clicks on the points, features from points are stored and not the point itself. Because storing points directly reduces the security of the technique. As it is very difficult to remember the random points, user chooses to select points on images that can be easily recognized in the image. It is called Hot Spot. Advantage of this system is simplicity of implementation and drawback is low security. In another variant of this system, user himself picks the image which increases the security. However user has to always enter the same image and within some system-defined tolerance region for each click point during authentication which means that image must be physically present in the client system.

Those object(s). For example, if a user decides that people with dark hair are of interest for some reason, the user’s attention would shift between objects with features that might indicate a dark-haired person. In the Pass Points graphical password scheme a password consists of a sequence of click points (say 5 to 8) that the user chooses in an image. The image is displayed on the screen by the system. The image is not secret and has no role other than helping the user remember the click points. Any pixel in the image is a candidate for a click point.

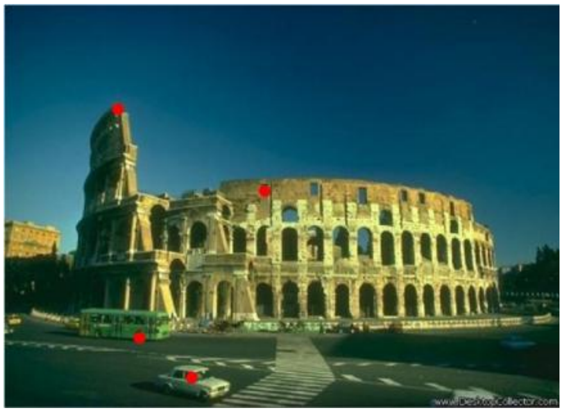

Fig.1. Pass Points (PP)

Cued Click-Point (CCP):

User selects one point in each of N images presented to user randomly:

In order to increase the security loopholes mentioned in pass points system, password distribution scheme is developed. Here user is presented with N random different images and user has to click one point at every image. Based on selected click point of current image next image is displayed randomly by the system as shown in Fig 2.The complexity of this technique is high as user not only has to remember the images in proper order but also has to remember points in every image. This method therefore presents great challenge for the user to remember the password.

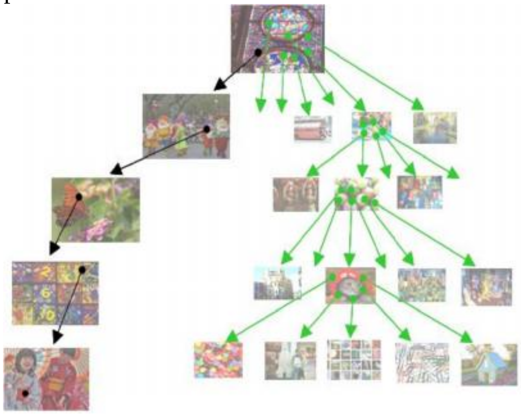

Fig.2. Cued Click-Points (CCP).Each click determines the next image.

To log in, the user has to click again closely to the chosen points, in the chosen sequence. Since it is almost impossible for human users to click repeatedly on exactly the same point, the system allows for an error tolerance r in the click locations (e.g., a disk with radius r = 10 or 15 pixels). This is done by quantizing (discretizing) the click locations, using three different square grids, as described in [3]. Each grid has width 6r between grid lines (horizontal or vertical). Each one of the three grids is staggered with respect to the previous grid by a distance 2r vertically and a distance 2r horizontally. If there were only one quantization grid then a selected click point could be close to a grid line and small variations in the user's clicking could lead to a click in a different grid square, thus leading to the wrong password. On the other hand, one can prove that with the three staggered grids every point in a two dimensional image is at distance at least r from the grid lines of at least one of the three grids; we say that the point is safe in that grid. We pursue heuristic-based strategies for purely automated dictionary generation (e.g., based on click-order patterns), and strategies to prioritize these dictionaries using image processing methods to identify points that users are more likely to choose. Are more likely to choose.

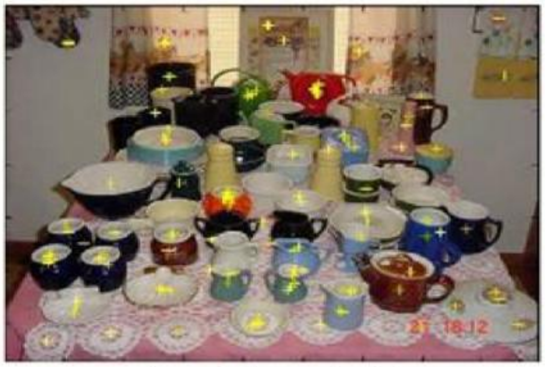

Figure 3(a)Actual click

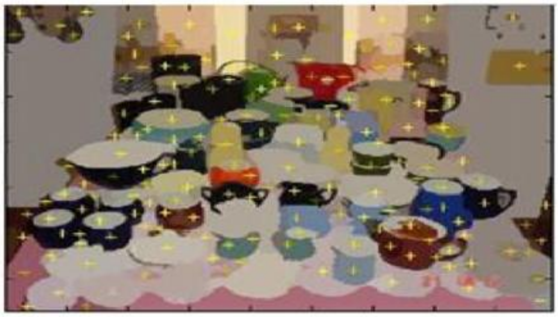

Figure 3(b) Predicted Click in Passpoints

III. PCCP with Dynamic User Blocks

In PCCP approach the image of size 451x331 pixels is segmented in to approximately 400 blocks of size 19x19 pixels. This block is called the tolerance block or the threshold range. Since the threshold area is fixed in PCCP method, the security level provided by it is rigid and concrete in nature. There may be some situations where the security levels need to be decreased. In those situations this PCCP method will not be feasible. To address these requirements, a new system is proposed, where the user can decide how strong the security of the system should be. The tolerance area or the threshold area determines the level of security of the target system. For each click point, it is enough for the user to click in the threshold area of that click point during login. If the threshold area is larger, then the security level is smaller and vice versa.

Password Registration

In this approach, the user provides the threshold range say n (in pixels), where 18<n<101. This user defined threshold value is saved for future login. The view port remains the same as that of the PCCP method. But the threshold area is made variable in this proposal. For each threshold area the system assigns a sound tone. Now, the image is ready to be displayed. When the image is displayed, only the view port portion of the image is visible which is random. Thus the system influences the user to select the click points to avoid the attacker guessing of the hot spots. When the user clicks on the view port, the assigned sound tone is played. The click points and the relevant sound tones are stored for future usage.

IV. P-Fibonacci and P-Lucas Transform

Fibonacci p-code [9] and a new Lucas p-code are introduced in this section. A new 1-D transform and a new 2-D transform are generated for both Fibonacci p-code and Lucas p-co de. The inverse 2-D transform used for recovering the original image is also presented

Definition: The Fibonacci p-code is a sequence defined by,

$$F_p(n) \begin{cases} 0 & n < 1 \\ 1 & n = 1 \\ F(n-1)+F(n-p-1) & n > 1 \end{cases}$$

where p is a nonnegative integer. From the definition above, Fibonacci p-code sequences will di er based on the p value. Specially,

(1) Binary sequence: p=0, the sequence is powers of two, 1, 2, 4, 8, 16…………etc

(2) Classical Fibonacci sequence: p=1, the sequence is 1, 1, 2, 3, 5, 8, 13, 21………etc

(3) For the large values of p the sequence starts with consecutive 1?s and immediately after that 1, 2, 3, 4 ...p Sample sequences are shown in Table

p \ n	1	2	3	4	5	6	7	8	9	10	11	...
0	1	2	4	8	16	32	64	128	256	512	1024	...
1	1	1	2	3	5	8	13	21	34	55	89	...
2	1	1	1	2	3	4	6	9	13	19	28	...
3	1	1	1	1	2	3	4	5	7	10	14	...
4	1	1	1	1	1	2	3	4	5	6	8	...
...												
∞	1	1	1	1	1	1	1	1	1	1	1	...

Table 1 Fibnacci p-code sequence with different p value

V. Image Scrambling Algorithm In The Spatial Domain

The presented image scrambling algorithm in the spatial domain (shown in Figure 4.2) is designed to change the image pixel position using the 2-D P-Fibonacci Transform. Color images have three color components and the scrambling algorithm is applied to each color component individually. Grayscale images are treated as color images with one component. The presented algorithm is a lossless image scrambling method The Detailed description of the algorithm explained below for scrambling and unscrambling of images.

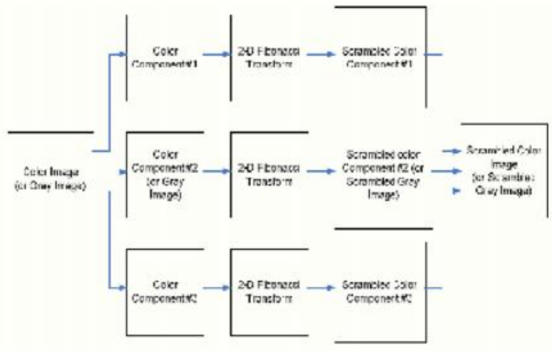
Color Image
(or Gray Image)
Color Component#1
2-D Fibonacci Transform
Scrambled Color Component#1
Color Component#2 (or Grey Image)
2-D Fibonacci Transform
Scrambled color Component #2 (or Scrambled Grey Image)
Scrambled Color Image (or Scrambled Gray Image)
Color Component#3
2-D Fibonacci Transform
Scrambled Color Component#3

Figure 4 Block diagram of spatial domain scrambling Algorithm for image scrambling

Step1:Choose the key parameter p, Calculate the row and column coefficient matrices of 2D p-Fibnaacci Transform

Step2:separate the 2D color image to three color component .Each component is a 2D matrix.

Step3: Apply 2D P-Fibnaacci transform to each color component to set the scrambled color component.

Step4 Recombine the three scrambled components to get the scrambled Image for password selection The above algorithm says how to scramble the given digital images in spatial domain.

VI. KEY BASED RANDOM PERMUTATION (KBRP)

A permutation, also called an "arrangement number" or "order," is a rearrangement of the elements of an ordered list ***S*** into a one-to-one correspondence with *S* itself. The number of permutations on a set of *n* elements is given by ***n!*** (***n*** factorial) A random permutation is a permutation containing a fixed number ***n*** of a random selection from a given set of elements. There are two main algorithms for constructing random permutations. The first constructs a vector of random real numbers and uses them as keys to records containing the integers 1 to ***n***. The second starts with an arbitrary permutation and then exchanges the *i*th element with a randomly selected one from the first *i* elements for *i* = 1, ..., ***n.***

Key Based Random Permutation (**KBRP**) is a method that can generate one permutation of size n out of ***n!*** Permutations. This permutation is generated from certain key (alphanumeric string) by considering all the elements of this given key in the generation process. The permutation is stored in one-dimensional array of size equal to the permutation size (***N***). This technique is used to generate the row and column coefficient matrices of each image components.

VII. IMPLEMENTATION ASPECTS

Image based mutual authentication has become now more reliable, when the scrambling technique applied. Users will me users should keep the click points to enter into the system, because the image get scrambled and it will be rearranged according to the scrambling algorithm discussed above. User have the provision to select his favorite areas according to his interest.

For any password authentication scheme, the prime task is to become a valid user of that system. For performing this each user have to provide the user id and password for creating the account just like in the conventional (textual) login system by specifying the username and password. This is for keeping an entry in the administrative level for further use for checking the intended user is authenticated or not. When a new user is intended to become a valid user, the user have to select the new user and proceed. On the way to registration it will ask the use rid and password, and the user should provide it through textual passwords. Now the user is entering to the PCCP System, here the textual password is replaced by the graphical password via click points (cued). Hence the user have to select the decide how many click points needed to create the password and it will affect the strength of the password security. In order to improve the total security strength of the target system the number of click points used can also be increased while creating the graphical passwords. This can be achieved by setting the number of click point to be received from the user as a predefined value, say v. A number of view ports, which is equal to v are made visible on the image, for the user to click on it.

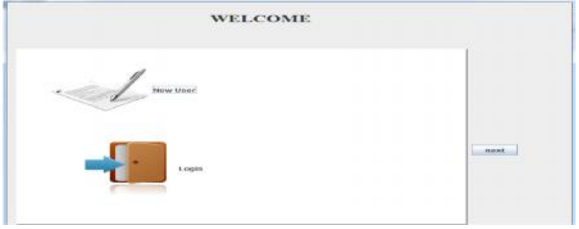

Fig 5. New User SignUp : GUI

View port size

The effective password space is determined by the area of the view port of all images displayed for the password creation. The password strength is increased with the password space. So to create a strong graphical password, which cannot be guessed easily, the area of the view port should be higher. It can be done by deciding how many times the we can select the shuffle button which is directly proportional to the maximum number of viewports possible for an image. Then the number of click points also effecting as a predominant factor for ensuring the security. This idea may increase the strength of the password but this will decrease the user memorability of the password.

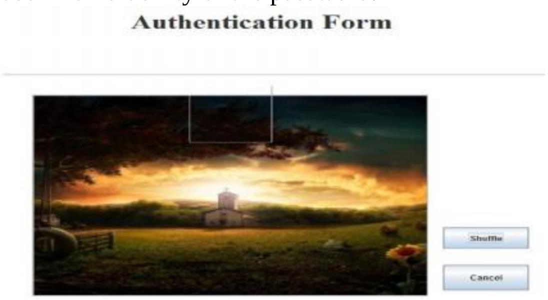

Fig 6 .Actual image for password Creation

Discretization of view port

In some occasions the user may accidentally click the point which is very near to the viewport, while logging in. If the user is genuine then he/she must be correctly logged in. Since we follow a very strict validation method, which requires the user to click on the view port, the genuine user cannot be allowed to use the application. To avoid this situation, we can compute the discretization are for the view port displayed on each image. The user clicks are tolerated up to the discretization area. But this may reduce the robustness of the system.

Authentication of a valid user

The user after registration process have to memories the click points what he selected to make the password.

The basis of PCCP starts from here. If he is a genuine user and he could not memories the cues for click points, he cannot enter into the system. The system will treat him as an unauthorized user. This is the strength of PCCP.

It is fully exploiting the memory and thus protecting your devices like PDA's from unauthorized access and other different kinds of attacks. Thus it termed as a knowledge based password authentication scheme in which the cues leads to the validating/invalidating session .Until the user selecting his last click points the system will not remind the user whether he given the right click or not even if he is a genuine user. This will help to protect the system from shoulder surfing attack and dictionary attack.

For login process the user have to enter the textual username and then he is entering to the PCCP system. System will allow only the valid username will enter into the PCCP system. There he starts accessing the images and starts clicking the click points according to the order what he have received for password creation phase. Since the order is an essential property of PCCP the user have to ensure he is accessing the right images for password selection.

Here the scrambling is applied .While in the login session the user is receiving the scrambled images of the actual image what he selected for password creation.

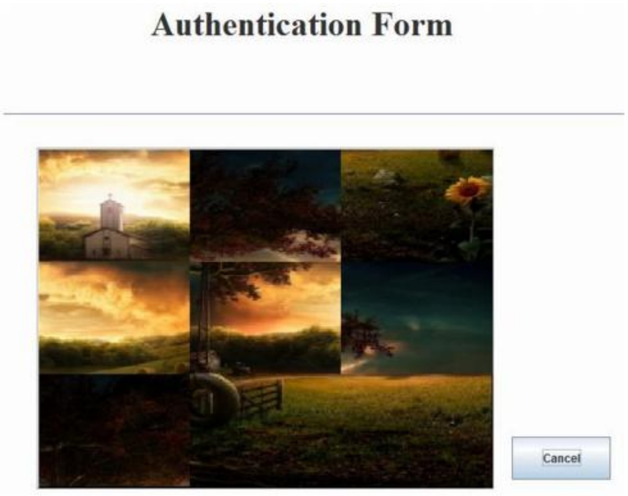

Fig. 7 Scrambled Image for password selection in Login Phase

Here the cues are very important factor, because this will help the users to remember easily. The scrambling process is done by the algorithm shown above and the row and column coefficients are determined by the Key Based random Permutation (KBPR) explained in section 4.3. There is a small comparison of alphanumeric password and graphical password is shown in the figure below with different parameters.

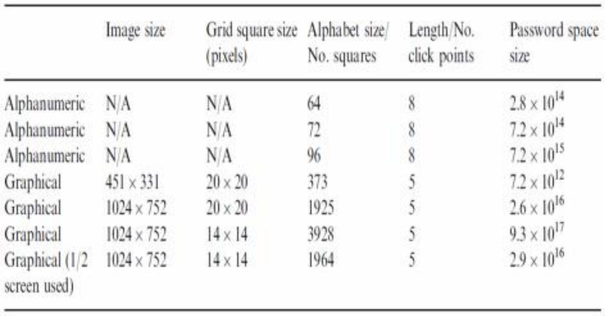

	Image size	Grid square size (pixels)	Alphabet size/ No. squares	Length/No. click points	Password space size
Alphanumeric	N/A	N/A	64	8	2.8×10^{14}
Alphanumeric	N/A	N/A	72	8	7.2×10^{14}
Alphanumeric	N/A	N/A	96	8	7.2×10^{15}
Graphical	451 × 331	20 × 20	373	5	7.2×10^{12}
Graphical	1024 × 752	20 × 20	1925	5	2.6×10^{16}
Graphical	1024 × 752	14 × 14	3928	5	9.3×10^{17}
Graphical (1/2 screen used)	1024 × 752	14 × 14	1964	5	2.9×10^{16}

Fig 8. Comparison of textual and graphical password.

VIII. Proposed System

In this work, unique solution is proposed based on audio time stamps by introducing and implementing a new protocol called "A NEWFANGLED AUTHENTICATION PROTOCOL BASED ON AUDIO PRODUCED PRINCIPLES". This protocol uses Audio, Audio time stamps as well as the count of audio timestamps and encrypt the password with message digest version 5 and making it hard for the intruder to break the password there by imposing the higher levels of security to the system. The intruder can't get the time stamps as well as count of time stamps and making this technique more secure, reliable and hard to guess. In this proposed system an audio is played to the user and the user is allowed to selected words/musical notes in the audio. Whenever user selects a particular word/musical note, time stamp, at which the selection takes place, is collected. User interface is provided in such a way that the user can select any number of time stamps depending on his interest. Once a time stamp is collected at the time of audio time stamp profile registration, it is encrypted using any encryption technique before it is being stored in the database. At the time of login, User has to repeat the same sequence of timestamps, which he selected at the time of audio time stamp registration, to log on to his/her account .The count of audio time stamps and the exact sequence of time stamps at the time registration and at the login time are compared .If the comparison of timestamps is successful, then the user is allowed to log on to account. We can impose restrictions on the number of failed login attempts to provide more security the system. If such restriction is imposed, user is blocked after n number of failed login attempts.

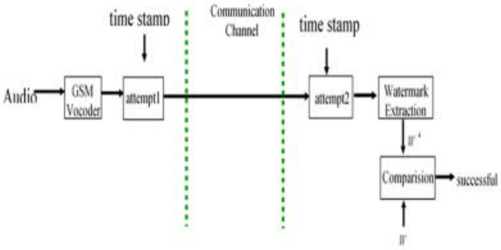

Fig 9. proposed system Architecture

IX. Security Analysis

In this section a discussion on how the proposed system may behave for password guessing attack and capture attack.

Password guessing attack

The most basic guessing attack against PCCP is a brute force attack, with expected success after exploring half of the password space (i.e., with a theoretical password space of 2^{43}, success after 2^{42} guesses). However, skewed password distributions could allow attackers to improve on this attack model. We now consider how these could be leveraged in guessing attacks.

PassPoint system hotspots of small number of users can be collected and an attack dictionary can be formed, with the use of server-side information. Then this dictionary details can be used for the guessing of the click point in an image. But this does not work in PCCP with dynamic user blocks scheme, because the view port does not include the hot spot in almost all cases. If the attackers gain the access to hash table entry of the passwords, they cannot correctly predict the original password, which are kept in a different database.

Capture attacks

Password capture attacks occur when attackers directly obtain passwords (or parts thereof) by intercepting user entered data, or by tricking users into revealing their passwords. For systems like PCCP, CCP, and PassPoints (and many other knowledge-based authentication schemes), capturing one login instance allows fraudulent access by a simple replay attack.

All three security schemes (PP, CCP, PCCP) are vulnerable to shoulder surfing threat. Observing the approximate location of click points may reduce the number of guesses necessary to determine the user’s password. User interface manipulations such as reducing the size of the mouse cursor or dimming the image may offer some protection, but have not been tested.

Malware is a major concern for text and graphical passwords, since key logger, mouse logger, and screen scraper malware could send captured data remotely or otherwise make it available to an attacker.

For social engineering attacks against cued-recall graphical passwords, a frame of reference must be established between parties to convey the password in sufficient detail. One preliminary study suggests that password sharing through verbal description may be possible for PassPoints. For PCCP with dynamic user blocks, more effort may be required to describe each image and the exact location of each click-point. Graphical passwords may also potentially be shared by taking photos, capturing screen shots, or drawing, albeit requiring more effort than for text passwords.

Conclusion

The goal of a good authentication system is to provide a maximized of effective and secure password space. Here in this system the click point on the image have the scope of the view port area and since the view port cannot be exploited, the password created will be robust. Since shuffling of the view port increases the time for registration of new users, it is limited. The graphical click point passwords are more random and strong, so that no hacker can guess it, but easy to remember. The security strength is decided by the user himself, depending upon the requirement. The audio sound accompanied with every click helps the genuine user to identify the wrong clicks. The attacker does not know the difference between right and wrong clicks with the sound. This paper gives an idea of having a effective authentication system, which provides strong and easily remembered graphical passwords with dynamic security level.

References

[1] Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin, The Design And Analysis Of Graphical Passwords, Proceedings of the 8th USENIX Security Symposium Washington, D.C., USA, August 23–26, 1999.

[2] D. Davis, F. Monrose, and M. Reiter. On user choice in graphical password schemes. In 13th USENIX Security Symposium, August 2004.

[3] S. Chiasson, R. Biddle, and P. van Oorschot. A second look at the usability of click-based graphical passwords. In the proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS), July 2007.

[4] Susan Wiedenbeck, Jim Watersa, Jean-Camille Birget, Alex Brodskiy, Nasir Memon, PassPoints: Design and longitudinal evaluation of a graphical password system, Int. J. Human-Computer Studies 63 (2005) 102–127.

[5] Sonia Chiasson1,2, P.C. van Oorschot1, and Robert Biddle , Graphical Password Authentication Using Cued Click Points, April 10, 2007.

[6] Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle and Paul C. van Oorschot, Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism, MARCH/APRIL 2012.

[7] S. Chiasson, J. Srinivasan, R. Biddle, and P. van Oorschot. Centered discretiza-tion with application to graphical passwords. InUSENIX Usability, Psychology, and Security (UPSEC), April 2008.

[8] X. Suo. A design and analysis of graphical password. Georgia State University, August 2006.