International Journal of Research in Advent Technology, Special Issue, March 2019
E-ISSN: 2321-9637
International Conference on Technological Emerging Challenges (ICTEC-2019)
Available online at www.ijrat.org

Four Factor Authentication System Text - Based Graphical Password Scheme

T.Narendrababu[1] , Y.Yasaswini[2], P.Malleswari[3], P.Naga Prasanna[4], P.Ajantha[5].
[1]*Assoc.Prof CSE, Tirumala Engineering College, Narasaraopet,India.*
[2,3,4,5]*B.tech Students CSE,Tirumala Engineering College,Narasaraopet,India.*

Abstract: There are different varieties of authentication schemes that supports various security based applications and most of these authentication schemes have many weaknesses depends upon the behavior of the user. People nowadays faces a lot of security problems such as hacking issues and security breaches. There are huge ways of authentication scheme available presently text-based captcha is in use. These text based captchas are not suitable for highly security applications such as military, banking ,and educational applications. For the people with low eye vision these type of captcha will be annoying. To make banking application more secure image based captcha and puzzle technology are introduced in the banking application. To address various kinds of security attacks such as guessing attacks and relay attacks these image based captcha and puzzle technology will be the most powerful scream. Guessing attack is also known as Brute force attack. Brute force attack is the most used technique for cracking the password by the hackers. Relay attacks is also known as the man-in-the – middle attack and it is a type of hacking technique where a middle man is involved. For a banking application to be more secure another important authentication scheme used is one time password generation to the user's email address. This one time password scheme is very difficult for the attacker to identify. Generally a banking application comprises of one or two authentication schemes which will be easy for the attackers to identify, to overcome this problem a multifactor authentication scheme is used in the banking application.

1. INTRODUCTION

CAPTCHA Completely Automated Public Turing test to tell Computers and Humans Apart. CAPTCHA is a type of justification used to know whether the user is human or not.The CAPTCHA was first invented by two groups working simultaneously. When the CAPTCHA was first invented it is in the form of letters and digits which will appear on the screen. The same series of letters and digits that appears on the screen should be typed by the user.This is all done by a standard turing test and the test is administered by a human.CAPTCHA is also referred as reverse turingtest.CAPTCHA is very easy to solve especially letter and digit based CAPTCHA. For an average person it will not take more than 10seconds to solve typical CAPTCHA.There are different types of CAPTCHA are available such as audio based, video based, image based etc;

Generally CAPTCHA is used to make the particular application more secure. Mostly CAPTCHA is used in banking, educational, military and some social media web sites to user account more secured. CAPTCHA format is produced using java script support.

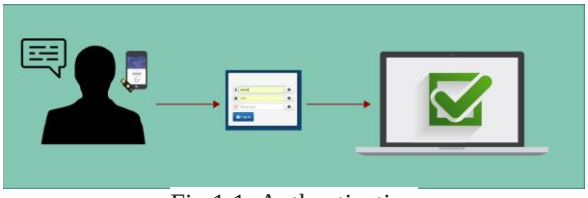

Fig 1.1. Authentication

Usually the captcha refers to the situation where the user will have to enter the certain text or the number into the box through which the authentication will be happened such that it will take the users to move on to the next steps as shown in figure 1.1

In these days these Password guessing attacks also referred to as Brute force attacks are quite common against internet sites and web servers. they're one amongst the foremost common vectors accustomed compromise internet sites. the method is incredibly easy and also the attackers essentially attempt multiple combos of usernames and passwords till they realize one that works.Most attacks rely on the foremost ordinarily used usernames and passwords and take a look at all of them. They additionally permutate entries associated with the website domain and content to extend their success. Humans are bad at selecting passwords and that`s what these attacks try to exploit.

2. LITERATURE VIEW

Haichanget al.,[1] proposed he technology that's used mainly to damspammers and bots that try and mechanically harvest email addresses or try and mechanically register for or build use of websites, blogs or forums. CAPTCHA, whose users embrace Yahoo and Google, blocks machine-controlled systems, that can't scan the distorted letters inside the graphic. A two layer captcha designed by Microsoft for security purpose nonetheless has some limitations. The planned work is intended such to forestall guessing attacks conjointlymentioned as Brute force attacks that square measure quite common against net sitesand internet servers and conjointly addresses varied security problems.

Robert Biddle et al., [2]given a replacement CAPTCHA that relies on characteristic an image's upright orientation. This task needs analysis of the usually advanced contents of a picture, a task that humans sometimes perform well and machines typically don't. Given an outsized repository of pictures, like those from an internet search result, a set of machine-controlled orientation detectors is employed to prune those pictures that may be mechanically set upright simply. A social feedback mechanism is applied to verify that the remaining pictures have a human-recognizable upright orientation

Gabriel Moy et al.,[3] proposed visual based captcha which referred as the best captcha. Now a days this visual based captcha is most widely used. This visual based captcha is the combination of a set of dublicate and original images. According to the given question we have to select all the original images. For example a set of images with a question given like set all the car images. Accordingly the user should select all the car images from the set of images that are given. Suppose a user selects an improper image another question with a relavent image block will be appeared until the user selects the proper image relavent to the question. This type of captcha is used to differentiate between the original user and the automated program. In visual based captcha a set of images a displayed with a question. According to the question the user should select the proper image from the set of images.

Paul c. van oorschot et al., [4] has proposed proposedhistory based login protocol using automated turning test. It is also know as authentication protocol or communication protocol or cryptographic protocol. This protocol is specially designed to transfer secured data between two entities.It allows the receiver side entity to authenticate the client side entity as well as the client side entity to authenticate the receiver side entity.If there occurs a minor variation in login protocol ehich may leads to middle man attack.It is one of the most important protective layer used for secured communication within the system. This protocol is used to transfer the communication between the users in a secured manner. Login protocol will pass the message from client to the server in encrypted form.

Elie Bursztein et al., [5]introduced CAPTCHAs, that area unit machine-controlled tests supposed to differentiate humans from programs, area unit used on several websites to forestall through bot-based account generation. One of the latest authentication scheme used for security is audio based captcha. This is the most trending captcha technology used for security purpose. An audio based captcha is used to differentiatehumans from computers. A audio file will be generated the user has to play and listen the audio file and type in the form of text what the user has listened. If the user has some has problem while hearing the audio due to poor internet connection and if there is a poor quality of speakers then this audio captcha is not suiatable in this case. To overcome this problem a video based captcha has been introduced but still it is in implementation stage

Manuel Egele et al., [6]hasproposed the CAPTCHAs to secure the online resources from spammers. I am not a robot is one of the most common method which is used almost in every application. I am not a robot based captcha is not only commonly used but also it is the simplest form of captcha. I am not a robot is in the check box formate where user has to click on the check box for the verification. The user should selects the check box with in a particular time limit, if suppose the user select the check box multiple times within a tile limit of seven seconds a pop up message will be appear on the screen where the user ip address is considered to be spam. It will also monitor the way the user handles the mouse for clicking the check box.It is very difficult to examine the movement of the mouse handled by the user.There are different varieties of captcha available for securing the online applications

Hung-Min Sun et al.,[7] proposed that when there is weaker authentication of the system the hackers are likely to get the users secured and personal details, this can be performed either by using some devices to record the data or simply by performing some attacks like relay attacks etc. The common way of attacking the passwords is and shoulder surfing attacks. To overcome the shoulder surfing attacks the new authentication scheme called graphical passwords are used, where the Passimages are solved to get into the application. Passmatrix does not leave way to the indication of the passwords to the hackers by providing a strong authentication method. This paradigm can be applied in the real time application to improve the security of the application

Taekyoung Kwon et al.,[8] proposed that there are various types of attacks to get the users credentials. The attack is not only by using recordering devices to record data but also by human

based attacks that is by observing the user and performing shoulder surfing attack. The attackers undergo one of the attacks that usually used to grab the user's credentials like passwords are guessing attacks. To resists this type of internet smuggling and hijacking of the user data, an authentication is provided by PIN number generation ,where a unique PIN number is provided to the each user that is only known to the user. In this way the attacker has the less probability of recording or getting the data manually.

Y. Xu, G. Reynaga, et al.,[9] has explored the advanced way of security primitives called visual based Captchas for moving images ,the user has to view the moving image and should answer according to it. Visual Captcha is the emerging technique used to secure the applications. The user when fails to solve this captcha, then the captcha will be repeated until it is solved correctly this is one of the better way of authentication. This is to find whether the user is an actual user or an automated program. The video captcha has an advantage that unlike the text based captcha it cannot be cracked easily by the attacker. The video based captcha are more secured compared to the traditional captcha forms.

.

Chen-Chiung Hsieh et al.,[10] has proposed that Captcha is generally used to separate and identify the original user and the machine encoded programs. Online dictionary attacks are the major concern in attacking the online applications such as banking applications to steal the users credentials. There are four different forms of captcha such as text based captcha, image based captcha, audio based captcha and video based captcha of moving objects. Here image based captcha is taken into account. The image based captcha using puzzle technology is used ,where the user has to solve the image based captcha that is displayed in the form of puzzle within the allotted time. This method of authentication can be practiced in the different type of applications, that prevent applications from the attacks.

3. EXSTING MODEL

Autentication problem can be overcome by presenting CAPTCHA method. The CAPTCHA will be a combination of text and digit based which is commonly known method and other type of popularly used CAPTCHA is I am not a robot. These are the easy and simple CAPTCHA solving technique. Another commonly used authentication method is math captcha where addition of two numbers or subtraction of two numbers can be solved. CAPTCHA technique is used for making various application more secure. For a banking application to be more secure another important authentication scheme used is one time password generation to the user's email address. This one time password scheme is very difficult for the attacker to identify. Generally a banking application comprises of one or two authentication schemes which will be easy for the attackers to identify, to overcome this problem a multifactor authentication scheme is used in the banking application.

Disadvantages of the Existing system:

- The text based Captcha are sometimes not suitable for visually affected people as it may be hard to read due to the complicated view of the text based Captcha.
- Difficulties in some internet browsers.
- Deciphering may be difficult as it consumes more time.

4. PROPOSED SYSTEM

CaPRP offers security against guessing attacks on passwords, which have been a major security problem for several online services. This threat is widespread and considered as a major risk in cyber security. Defense against online dictionary attacks is a major subtle problem than it might appear. The four-level authentication is a multifactor authentication scheme that combines the features of various authentication schemes. The first level is the account number generation, where the account number is generated to the user's email address. The most secured level is the second level which is the random captcha selection, where the user selects the same images in the same order as selected in the registration phase. The third level is image puzzle solving where the user should solve the image formate puzzle with in the allotted time. The most secure level is the fourth level, which is the generation of one time passwords. By providing the necessary inputs, OTP is generated which is encrypted and appended as a single string . The hidden OTP is generated in the web part is compared with the OTP that is generated in the application side and if they are valid i.e., if both the OTPs generated are similar , then the generated OTP will be sent to the user as an email, with which the user can log in to the system.

A. Advantages of Proposed System:

- This authentication system offers great security for the banking applications, makes online banking safer.
- Resist against the attacks such as guessing attacks, relay attacks etc.
- It reduces spamming and offers considerable web security.

5. ARCHITECTURE

An account number is the primary identifier for ownership of an account, whether a vendor account, a checking or brokerage account, or a loan account. An account number is used whether or not the identifier uses letters or numbers. Each person has unique account number which has been assigned as a primary key.After registration process is completed an account number is generated and sent to the user's registered email address. By using the account number the user can login to the system.

A CAPTCHA is a test that is used to separate humans and machines. CAPTCHA stands for "Completely Automated Turing test to tell Computers and Humans Apart." It is normally an image test or a simple mathematics problem which a human can read or solve, but a computer cannot. It is made to stop computer hackers from using a program to automatically set up hundreds of accounts, such as email accounts. It is named after mathematician.Each individual is chosen randomly and entirely by chance, such that each individual has the same probability of being chosen at any stage during the sampling process, and each subset of n individuals has the same probability of being chosen for the sample as any other subset of n individuals. This process and technique is known as simple random sampling, and should not be confused with systematic random sampling. A simple random sample is an unbiased surveying technique.

To prevent DoS/DDoS attackers from inflating their puzzle-solving capabilities. To this end, a new client puzzle referred to as software puzzle is introduced. Unlike the existing client puzzle schemes, which publish their puzzle algorithms in advance, a puzzle algorithm in the present software puzzle scheme is randomly generated only after a client request is received at the server side and the algorithmis generated such that: 1) an attacker is unable to prepare an implementation to solve the puzzle in advance and 2) the attacker needs considerable effort in translating a central processing unit puzzle software to its functionally equivalent GPU version such that the translation cannot be done in real time. Moreover, it is shown, how to implement software puzzle in the generic server-browser model.

A one-time password (OTP) is a password that is valid for only one login session or transaction, on a computer system or other digital device. Online banking also known as internet banking, e-banking, or virtual banking, is an electronic payment system that enables customers of a bank or other financial institution to conduct a range of financial transactions through the financial institution's website. The online banking system will typically connect to or be part of the core banking system operated by a bank and is in contrast to branch banking that was the traditional way customers access banking services. OTPs avoid a number of shortcomings that are associated with traditional (static) password-based authentication; a number of implementations also incorporate two factor authentication by ensuring that the one-time password requires access to something a person has (such as a small keyring fob device with the OTP calculator built into it, or a smartcard or specific cellphone) as well as something a person knows (such as a PIN).

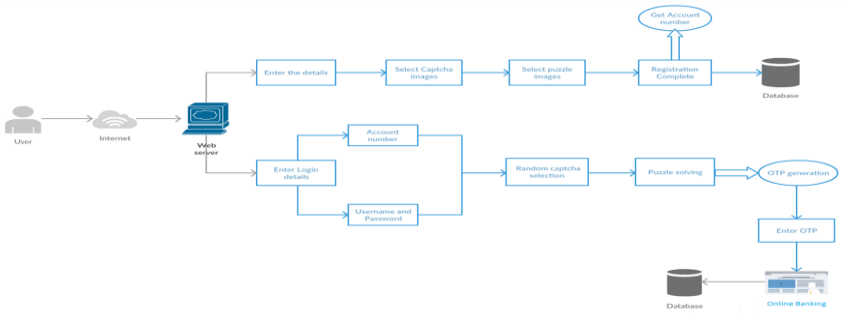

Fig.5.1 Architecture Diagram

With the advent of Java 2, new versions had multiple configurations built for different types of platforms. For example, J2EE was for enterprise applications and the greatly stripped down version J2ME was for mobile applications. J2SE was the designation for the Standard Edition. In 2006, for marketing purposes, new J2 versions were renamed Java EE, Java ME, and Java SE, respectively. In the Java programming language, all source code is first written in plain text files ending with the .java extension. Those source files are then compiled into .class files by the javac compiler. A .class file does not contain code that is native to your processor; it instead contains byte codes — the machine language of the Java Virtual Machine1 (Java VM). The java

launcher tool then runs your application with an instance of the Java Virtual Machine

Fig.5.2 Java Virtual Machine

JavaServer Pages (JSP) is a Java technology that allows software developers to dynamically generate HTML, XML or other types of documents in response to a Web client request as in the fig 5.2. The technology allows Java code and certain pre-defined actions to be embedded into static content. JSPs are compiled into Java Servlet by a JSP compiler. A JSP compiler may generate a servlet in Java code that is then compiled by the Java compiler, or it may generate byte code for the servlet directly. JSPs can also be interpreted on-the-fly reducing the time taken to reload changes

JavaServer Pages (JSP) technology provides a simplified, fast way to create dynamic web content. JSP technology enables rapid development of web-based applications that are server and platform-independent

.

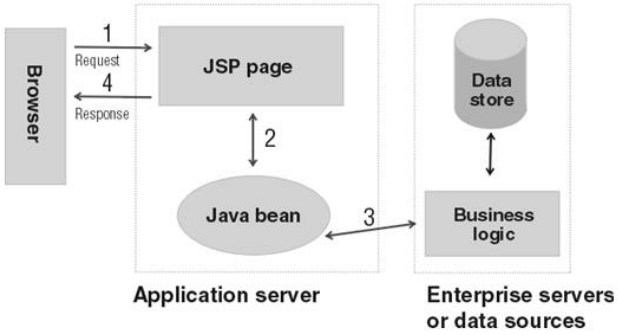

Fig.5.3.Java Server Pages (JSP)

Server-Side Includes (SSI). SSI is a widely-supported technology for including externally-defined pieces into a static Web page. JSP is better because it lets you use Servlet instead of a separate program to generate that dynamic part. Besides, SSI is really only intended for simple inclusions, not for "real" programs that use form data, make database connections, and the like. JavaScript. JavaScript can generate HTML dynamically on the client. This is a useful capability, but only handles situations where the dynamic information is based on the client's environment as shown in fig 5.3.

With the exception of cookies, HTTP and form submission data is not available to JavaScript. And, since it runs on the client, JavaScript can't access server-side resources like databases, catalogs, pricing information, and the like. Static HTML. Regular HTML, of course, cannot contain dynamic information. JSP is so easy and convenient that it is quite feasible to augment HTML pages that only benefit marginally by the insertion of small amounts of dynamic data. Previously, the cost of using dynamic data would preclude its use in all but the most valuable instances.

Cued Click Points (CCP) is a algorithm which is used

In our project to avoid attacks in the day to day life.this will help in such a way that when users selects the one point in authentication then the same point will be selected in the upcoming steps which makes the

system to be more secure. It also makes attacks based on hotspot analysis makes more challenging.

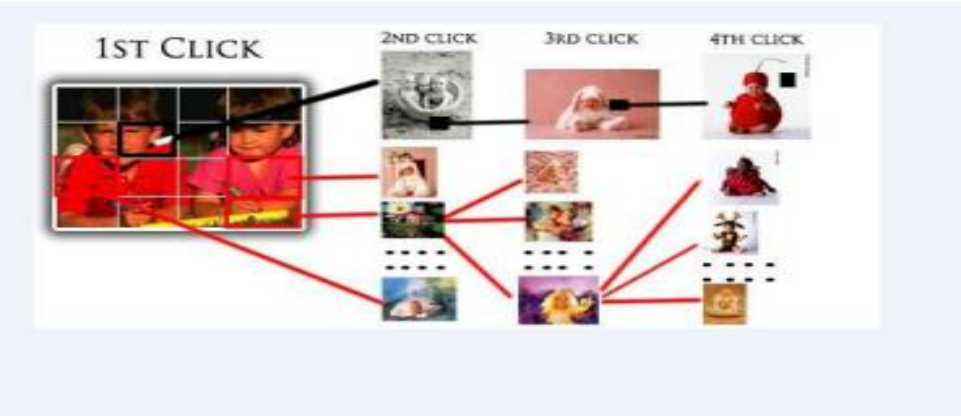

Fig.5.4.Graphical Password Authentication using Cued algorithm

As shown in the figure 5.4.the cued algorithm will be used in such a way to avoid the various incidents of attacks and makes the system more secure.This cued will work on the image based where the user has to selects certains points fro the given or selected image

.

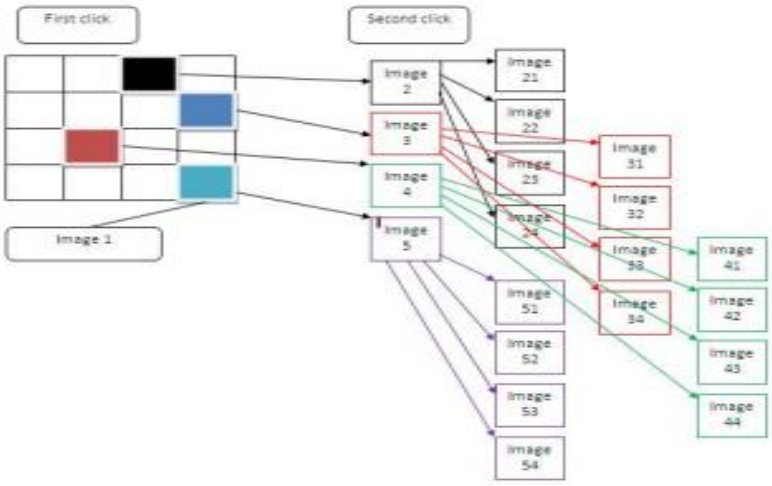

Fig.5.5.Graphical password authentication.

Graphical passoword authentication is mainly user in order to reduce the hacker to much aware of the system.fig.5.5.Illustrates the the basic model of the graphical password authentication which workd on cued algorithm in which the user has to selects certain points from the image,and the selected points will be stored in the repository with their respective image points same as the fig.5.5. and while the user is accessing those steps he will be asked with the selection of the same points in the images when he enters the same points it will make sure that the person is him only,in this way the graphical authentication will happens.

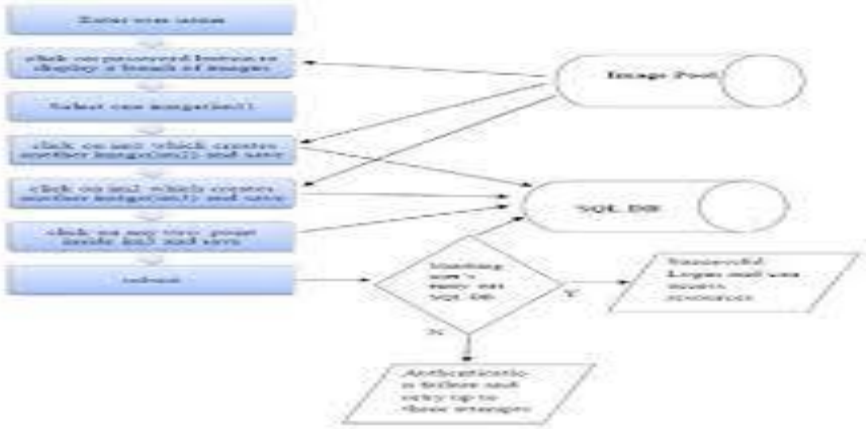

Fig.5.6.Cued click point graphical flow chart.

A major usability improvement over PassPoints is the fact that legitimate users get immediate feedback about an error when trying to log in. When they see an incorrect image, they know that the latest click-point was incorrect and can immediately cancel this attempt and try again from the beginning. The visual cue does not explicitly reveal "right" or "wrong" but is evident using knowledge only the legitimate user should possess. As with text passwords, PassPoints can only safely provide feedback at the end and cannot reveal the cause of error. Providing explicit feedback in PassPoints before the final click-point could allow PassPoints attackers to mount an online attack to prune potential password subspaces, whereas CCP's visual cues should not help attackers in this way. Another usability improvement is that being cued to recall one point on each of five images appears easier than remembering an ordered sequence of five points on one image.

6. CONCLUSION

There are many authentication schemes. Some of the schemes are based on the physical and behavioral properties of the user, and some other authentication schemes are based on the knowledge of the user such as textual and graphical passwords. Also, there are other authentication schemes that are based on tokens such as smart card. Among the various authentication schemes, the most commonly used schemes are textual password and token based schemes, or the combination of both. The four-level authentication is a multifactor authentication scheme that combines the features of various authentication schemes. The first level is the account number generation, where the account number is generated to the user's email address. The most secured level is the second level which is the random captcha selection, where the user selects the same images in the same order as selected in the registration phase. The third level is image puzzle solving where the user should solve the image formate puzzle with in the allotted time. The most secure level is the fourth level, which is the generation of one time passwords. The hidden OTP generated in the web part is compared with the OTP generated in the application side and if they are valid i.e., if both the OTPs generated are same , then the generated OTP will be sent to the user as an email, with which the user logs on to the system. One of the future works will be gathering attackers from different backgrounds to break the system which will lead to system improvement and will prove the complexity of breaking the system. But still the attackers will acquire the knowledge about the system and will try to launch their attacks. Shoulder surfing attacks is a limitation against the 4-factor authentication system. Therefore, a field of research would be a proper solution

REFERENCES

[1] Haichang Gao, Member, Mengyun Tang, Yi Liu, Ping Zhang and Xiyang Liu "Research on the Security of Microsoft's Two-layer Captcha" IEEE Transactions on Information Forensics and Security , Volume: 12, Issue: 7, July 201730

[2] Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng "A Shoulder Surfing Resistant Graphical Authentication System", IEEE Transactions on Dependable and Secure Computing (Volume:PP , Issue: 99),09 March 2016

[3] GabrialMoy,NathanJones,CurtHarkless,Radall Potter "Distortion estimation techniques in solving visual CAPTCHAs" IEEE Computer Society Washington, DC, USA 2014

[4] Paul C. Van Oorschot and Stuart Stubblebine" On Countering Online Dictionary Attacks with Login Histories and Humans-in-the-Loop", ACM Transactions on Information and System Security, Vol. 9, No. 3, August 2006

[5] Elie Bursztein∗ Romain Beauxis† HristoPaskov∗ Daniele Perito‡ Celine Fabry, John Mitchell "The Failure of Noise-Based Non-Continuous Audio Captchas" IEEE Symposium on Security and Privacy,2011

[6] Manuel Egele, Leyla Bilge, EnginKirda and Christopher Kruegel " CAPTCHA Smuggling: Hijacking Web Browsing Sessions to Create CAPTCHA Farms" SAC 2010, 25th ACM Symposium On Applied Computing, March 22-26, 2010

[7] Robert Biddle, Elizabeth Stobert, Alain Forget, Sonia Chiasson, Paul van Oorschot "Exploring Usability Effects of Increasing Security in Click-based Graphical Passwords" Austin, Texas USA ACSAC '10 Dec. 6-10, 2010

[8] Taekyoung Kwon and Sarang Na" Covert Attentional Shoulder Surfing: Human Adversaries Are More Powerful Than Expected", IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 44, no. 6, June 2014

[9] Y. Xu, G. Reynaga, S. Chiasson, J-M. Frahm, F. Monrose, and P. van Oorschot "Security Analysis and Related Usability of Motion-based CAPTCHAs: Decoding Codewords in Motion" IEEE Transactions on depedable and secure computing,2013

[10] Chen-Chiung Hsieh and Zong-Yu Wu "Anti-SIFT Images Based CAPTCHA Using Versatile Characters" IEEE Transactions , 2013