International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 01 | Jan -2017 www.irjet.net p-ISSN: 2395-0072

Image authentication for secure login

Amukthamalyada Chelikani

M. Tech., Department of CSE, Gokul Institute of Technology and Sciences, Piridi, Bobbili, Vizianagaram Dist, AP

Guide: **G. Baghya lakshmi**

Professor, Department of CSE, Gokul Institute of Technology and Sciences, Piridi, Bobbili, Vizianagaram Dist, AP

Abstract: *According to a latest Computerworld news article, the security group at a vast organization ran a system secret key saltine and inside of 30 seconds, they recognized around 80% of the passwords. On alternate hand, passwords that are difficult to figure or break are frequently difficult to recollect. To address the issues with conventional username password validation, elective confirmation methods. However, we will concentrate on another option, utilizing pictures as passwords. Using hard AI (Artificial Intelligence) issues for security primitive at first proposed in is an energizing new paradigm. Under this, the most prominent primitive developed is CAPTCHA, which recognizes human clients from PCs by showing a test i.e. a riddle past the limit of PC yet simple for people.*

CAPTCHA given as "Completely Automated Public Turing test to tell PCs and Humans Apart". It's primarily utilized for clients to getting to their ensured resources. It is a sort of test reaction test utilization to figure particularly whether the client is human or not. The fundamental and basic undertaking in this security based task is to make secured login confirmation towards the end client with help of cryptography strategy named MD5 hash algorithm, security primitives taking into account hard AI numerical issues that are computationally unmanageable with people like existing CAPTCHA.

We present CAPTCHA a novel group of graphical passwords frameworks coordinating CAPTCHA innovation, which we call IASL is snap based graphical passwords, where a succession of snaps on a picture is utilized to infer a password. Not at all like other snap based graphical secret keys, had pictures utilized as a part of IASL is CAPTCHA difficulties and another IASL pictures is produced for each login endeavor.

IASL is based on both content CAPTCHA and picture acknowledgment CAPTCHA. One of them is a content IASL where in a watchword is a grouping of characters like a content secret word, yet entered by tapping the right character arrangement on IASL pictures.

IASL offers assurance against word reference assaults on passwords, which have been for long significant security risk for different online services. IASL obliges explaining a CAPTCHA challenge in every login. This affect on convenience can be alleviated by adjusting the IASL pictures trouble level taking into account the login history of the record and the machine used to sign in.

Key Words: *Artificial Intelligence, passwords, validation, security, endeavour.*

1. INTRODUCTION:

1.1 Application of CAPTCHA:

1) IASL can be connected on touch screen gadgets whereon writing passwords is cumbersome, esp. for secure web applications for e.g., e-banks. Many e-keeping money frameworks have connected CAPTCHA in client login [12]. For illustration ICBC (www.icbc.com.cn), the biggest bank on

the planet, oblige tackling a CAPTCHA challenge for each online login endeavor.

2) IASL builds spammer's working expense and in this manner helps diminish spam emails. For an email administration supplier that sends IASL, a spam bot can't sign into an email record regardless of the possibility that it knows the secret key. Rather, human inclusion is necessary to get to a record. On the off chance that IASL is consolidated with a strategy to throttle the quantity of messages sent to new beneficiaries per login session, a spam however can send just a set number of messages before approaching human help for login, prompting lessened outbound spam movement.

3) Several companies offer free email services. Most of them are suffer from a specific type of attack "bots", so many people are signup for thousands of email accounts for every minute. In these situations can be improved by requiring users to prove they are human or not. So, that yahoo develops a CAPTCHA to prevent this bots register. Here CAPTCHA asks users to read a word and enter for every login.

4) In search engine bots it is sometimes desirable to keep web pages in indexed to prevent others from finding them easily. In html tag to prevent search engine bots from reading web pages. The tag, doesn't guarantee that bots won't read a web page. It only serves to say "no bots please". Since they usually belong to large companies, respect web pages that don't want to allow them in. However that bots won't enter into web pages, CAPTCHA is needed.

5) Preventing dictionary attacks by using this CAPTCHA, pinkas and sander have also suggested using CAPTCHA to prevent dictionary attacks in password systems. This idea is simple to prevent a computer from being able to iterate through the entire space of passwords.

1.2 Security Analysis

Security is most important in our daily life. It is used for protection against different attacks. This framework of graphical passwords, IASL does not rely on specific CAPTCHA scheme. If one CAPTCHA is broken and new one is generated at each login time. In the remaining security analysis, that computer can recognize any objects in any challenge image generated by the underlying CAPTCHA of IASL.

In image based CAPTCHA is click based graphical passwords, where sequence of clicks on an image is used to derive a password. It provides protection against online dictionary attacks on password. For login every time click on images and type password. In early system only text password is used and it is difficult to remember long password and we use smaller password then it can be easily identify and we also used common password for many applications so for that image based CAPTCHA provide more secure during authentication.

1.2.1Online Guessing Attacks:

In automatic online guessing attacks, the trial and error process is executed automatically whereas dictionaries can be constructed manually. If we ignore negligible probabilities, IASL with underlying CPA-secure CAPTCHA has the following properties such as Internal object-points on one IASL image are computationally-independent of internal object-points on another IASL image. Particularly, clickable points on one image are computationally-independent of clickable points on another image.

1.2.2 Shoulder surfing attack:

It is a direct observation technique such as looking over other shoulders to get information. This is used to obtain passwords, pins security code and other confidential data. It is particularly happen in crowded places as it is easy to observe someone who enters their password, a pin, a security code etc. on their smart phone or a computer. This crowded

may commonly referred as public transportation, airport, buses. etc.

1.2.3 Dictionary attack:

It is a technique breaking into a password protected computer or a server by systematically entering all possible passwords beginning with words that have higher possibility of being used, such as names and places. The word dictionary refers to the attacker using all the words in a dictionary to discover the password. These attacks are typically executed with software instead of an individual trying manually each password.

1.2.4 Relay attack:

It is a computer security hacking technique related to a man in the middle and replay attack, in which an attacker relay verbatim a message from the sender to a valid receiver of the message. In classic ma in the middle attack, an attacker intercept on manipulate communication between two parties initiated by one of the party. Generally these type of attacks take place where a smart card or a security device which allows a person to cross a barrier such as entrance at a building or a metro station.

2. LITERATURE SURVEY:

2.1 Graphical Password:

Graphical password [1] [2] have been proposed as a possible alternative to text based, motivated particularly by the fact that humans can remember pictures better than text. Visual objects seem to offer a much larger set of usable passwords. For example we can recognize the people we know from thousands of faces, this fact was used to implement an authentication system. As another example a user could choose a sequence of points in an image as a password, this leads to a vast number of possibilities, if the image is large and complex, and if it has good resolution. An excellent survey of the numerous graphical password schemes [5][17] that has been developed. These graphical passwords can be divided into three types recognition based graphical techniques, recall based graphical techniques, cued recall graphical techniques.

2.2 Recognition Based Graphical Password:

A recognition based plan obliges distinguishing among distractions the visual articles fitting in with a password portfolio. In the time of authentication, faces are the user to select the face having a place with her portfolio. This process is retrograded a few adjusts, round with a panel. A fruitful login requires right determination in every round. The arrangement of images in a panel proceeds as before among logins, yet areas are permuted. Cognitive Authentication [19] Obliges a user to create a way by a panel of takes after beginning of the upper left picture, acting down if the image is in her part, or right generally. The client recognizes among imitations the line or segment name. This operation is hashed over, every time with an alternate panel. An effective login requires that the total likelihood that right answers were not entered by chance surpasses an edge inside of a given number of rounds.

2.3 CAPTCHA:

The CAPTCHA relies on gap of potentiality between humans and bots in settling certain hard AI issues. It contains two sorts of visual CAPTCHA i.e. text CAPTCHA and Image-recognition CAPTCHA (IRC). The retiring depends on character recognition while the last relies on upon recognition of non-character items. Security of text CAPTCHA has been broadly contemplated. The accompanying Machine recognition of non-character items is far less competent than character recognition. IRCs depend on the complexity of object identification or classification. It generally relies on upon object classification, a client is requested that recognize a bird from the panel of 12 pictures of flowers, birds and animals. Security of IRCs has likewise been concentrated on (i.e.) CAPTCHA be equipped for be evaded through relay attacks whereby CAPTCHA difficulties are relayed to solvers, whose answers are criticism to the focused on application.

2.4 CAPTCHA in authentication:

It was introduced to use CAPTCHA and password in a exploiter validation protocol, which we will call as CAPTCHA-based (CbPA) protocol, serves challenge the online dictionary attacks. This protocol is used to solving a CAPTCHA challenge after we are giving a suitable pair of userId and password. For an invalid pair of exploiter ID and password, the exploiter has a certain level of likelihood to solve challenge before being access. An Improved CbPA-protocol is wished for to storing cookies only on the user believed machines and using a CAPTCHA dispute only when the amount of died login tries for the particular account has surpassed a threshold limit. CAPTCHA additionally utilized as a part of recognition based graphical passwords to address spyware and Trojans, wherein a text CAPTCHA is shown beneath every picture a user finds their own pass-pictures from diverted pictures, and enters the right characters of every pass-picture as their password during the season of verification. Those particular areas were chosen for every pass-picture during password initiation. CAPTCHA is an autonomous and individual substance utilized together with a text number as a graphical password.

2.5 METHODOLOGY :

2.5.1 Problem Definition:

A fundamental task in security is to create cryptographic primitives based on artificial intelligence problem. For example, the problem of integer factorization is fundamental to public key cryptosystem. Under this paradigm the most notable primitive invented is CAPTCHA, which differentiate human and bots. This CAPTCHA recognize human users and computers by presenting a challenge i.e a puzzle beyond the capability of computers but easy for humans. It is a now standard internet security technique to protect online email and other services from being abused by bots. It is achieved limited success as compared with cryptographic primitive. In proposed system we develop a IASL is a CAPTCHA as graphical password, it is a click based graphical password, where a sequence of clicks on images is used to derive a password. IASL provides protection against online dictionary attacks on passwords, which has been a major security threat for various online services. It offers a relay attacks and shoulder suffering attack. IASL requires solving a CAPTCHA challenge in every login attempt. IASL can be categorized as.

2.5.2 Recognition Based IASL:

For this kind of IASL, a password is an arrangement of visual objects in the alphabet. Per perspective of conventional recognition-based graphical passwords, recognition- based IASL appears to get admission to a transfinite amount of diverse visual articles. We exhibit two recognition- based IASL plans and a version next. In recognition based system a user chooses images or icons or symbols from a large collection. For authentication at the time of login or upload file and for viewing for any purpose we can create security purpose generate recognition IASL, the user need to recognize their previous choice among a large set of candidate, and enter at the time of login.

2.5.3 Click Text:

Click Text is a credit-based IASL strategy made on top of text CAPTCHA. Its alphabet consists of parts without any parts. For instance, Letter "O" and digit "0" may cause disarray in IASL pictures, and consequently one character should be prohibited from the alphabet.

Fig 2.1: Click Text picture with 33 characters

2.5.4 Recognition Recall IASL:

It is an arrangement of some invariant points of objects. A constant dot of an object (e.g. letter "A") will be a point that has a frozen relative proportional in dissimilar incarnations

e.g., textual styles of the object and accordingly can be uniquely distinguished by humans no matter how the object shows up in IASL images.

2.5.4.1 Text Points:

Characters contain constant dots. A dot is read to be an interval point of an item if its distance to the nearest bound of the target passes door. A set of interval invariant purposes of characters is chosen to form an arrangement of clickable points for Text Points. The guarantees that a clickable point is improbable impeded by a neighboring character and that its resistance region of a neighboring character's clickable focuses on the picture produced by the fundamental CAPTCHA engine. In deciding clickable focuses, the separation between any pair of clickable focuses in a character must exceed a threshold. So they are perceptually recognizable and their resilience locales don't cover on IASL pictures.

User registration process is carried out by image CAPTCHA. At time of register user has to select sequence of images as password and server stores the sequence of visual images id and while user login time, he need to recall the same images at register time and enter it. The server checks the same sequence of images user enter, if the sequence of visual object id are same it will allow to login into the system.

2.7 Implementation details & program design:

2.7.1 Implementation Details:

Implementation is the phase of the project when the theoretical plan is curved out into a working system. It is more critical phase that we consider in achieving a successful new system. It gives confidence to the user that the new system will work and will be effective. It involve careful in planning, investigation of the presented system and the constraint on implementation, designing of methods to achieve changeover and evaluation of changeover methods. In this project we proposed a IASL is a click based graphical password, and IASL is a CAPTCHA as graphical password, where a sequence of clicks on images.

2.6 Architecture Diagram:

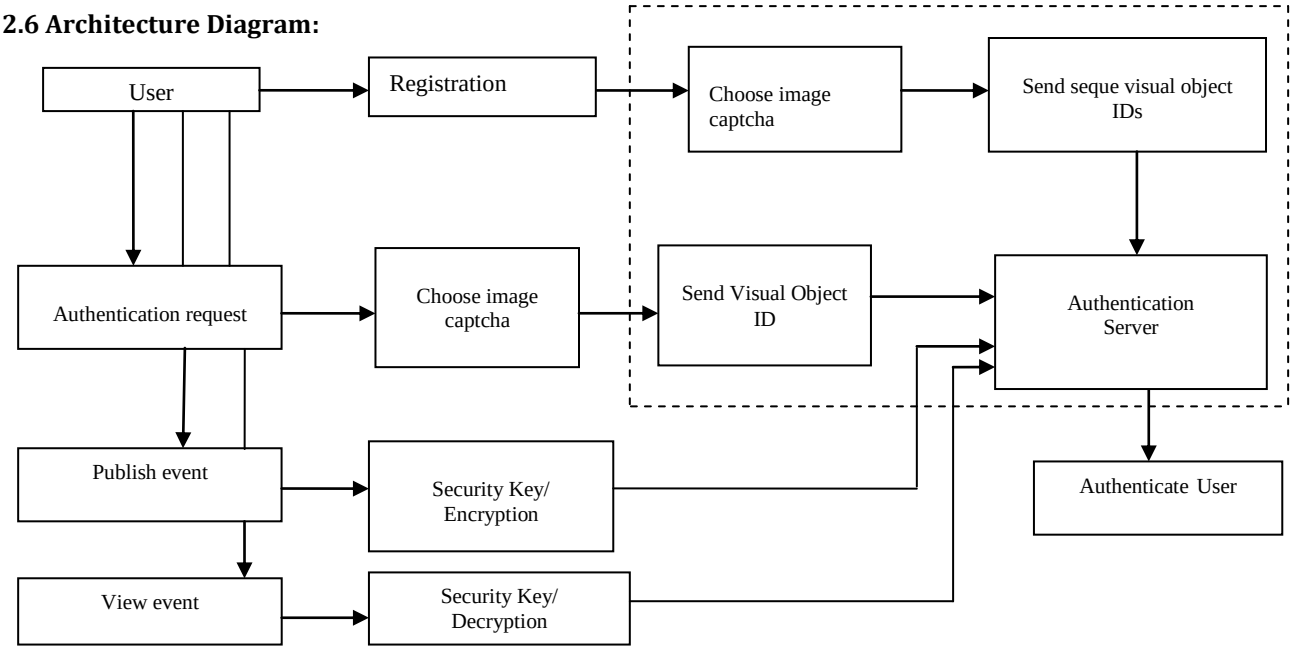

Fig. 2.2: System architecture of IASL

In IASL, new picture is produced for each login assay, even for the same user. IASL uses a alphabet of visual items (e.g., alphanumerical characters, similar animals) to produce a IASL picture, which is additionally CAPTCHA challenge. CAPTCHA pictures is that all the visual object in the alphabet should present in a IASL picture to permit a user to enter any password yet not so much in a CAPTCHA picture. As indicated by the memory undertakings in remembering and entering a password.

3.8 Authentication using IASL scheme:

Here that IASL plans are utilized with extra insurance, for e.g., secure channels in the middle of clients and the verification server .The authentication server (AS) stores a salt (s) and a hash value H (P, S) for every client ID by MD5 algorithm, where the password of the record is are not stored only hash values. A IASL password is a succession of optical target IDs or clickable-points of optical items that the client chooses at the time of registration, (AS) creates a IASL picture and records the areas of the items in the picture. At that point of authentication that the client needs to tapped on the picture. At that point (AS) recovers salt (S) of the record, calculates the hash value of (P) and contrast with the *salt then match the obtained result with the hash value which is already stored for that account. Validation succeeds just if the two hashes matched. This arrangement of procedure is known as the basic IASL level authentication.*

3.8.1 CAPTCHA Generation:

Unlike other click-based graphical passwords, images used in IASL are CAPTCHA challenges, and a new IASL image is generated for every login attempt. Independent images among different login attempts must contain invariant information so that the authentication server can verify claimants. By examining the ecosystem of user authentication, it is noticed that human users enter passwords during authentication, whereas the trial and error process in guessing attacks is executed automatically. The capability gap between humans and machines can be exploited to generate images so that they are computationally independent yet retain invariants that only humans can identify, and thus use as passwords. The invariants among images must be intractable to machines to thwart automatic guessing attacks. This requirement is the same as that of an ideal CAPTCHA, leading to creation of IASL, a new family of graphical passwords robust to online guessing attacks.

3.8.2 User Registration:

User registration process is carried-out with the image CAPTCHA. The user must choose a sequence of images in the registration form. The user must be able to recall the sequence and type of image he has chosen during registration, when he is attempting for login process. In this module, we use different types of animal images for catpcha generation.

3.8.3 IASL Scheme:

IASL [23] schemes are used with additional protection such as secure channels between clients and the authentication server through Transport Layer Security (TLS). The authentication server AS stores a salt s and a hash value H(ρ, s) for each user ID, where ρ is the password of the account and not stored. A IASL password is a sequence of visual object IDs or clickable-points of visual objects that the user selects. Upon receiving a login request, AS generates a IASL image, records the locations of the objects in the image, and sends the image to the user to click her password. The coordinates of the clicked points are recorded and sent to AS along with the user ID. AS maps the received coordinates onto the IASL image, and recovers a sequence of visual object IDs or clickable points of visual objects, ρ', that the user clicked on the image. Then AS retrieves salt s of the account, calculates the hash value of ρ' with the salt, and compares the result with the hash value stored for the account.

3.8.4 User Authentication with IASL Schemes:

Authentication succeeds only if the two hash values match. This process is called the IASL authentication. To recover a

password successfully, each user-clicked point must belong to a single object. The sequence of image clicked during registration process should be recall by the user and given as input for successful authentication.

3.8.5 Event uploads:

After successful login of the application, the user can upload some events.

4 EXPERIMENTAL ANALYSIS AND RESULTS:

4.1 Functionality of the System:

- *IASL is click-based graphical passwords, images used in IASL are CAPTCHA challenges, and a new IASL image is generated for every login attempt.*
- *IASL offers protection against online dictionary attacks on passwords, which have been for long time a major security threat for various online services.*
- *IASL is robust to shoulder-surfing attacks if combined with dual-view technologies.*
- *IASL also offers protection against relay attacks, an increasing threat to bypass CAPTCHA protection, wherein CAPTCHA challenges are relayed to humans to solve.*
- *IASL requires solving a CAPTCHA challenge in every login. This impact on usability can be mitigated by adapting the IASL image's difficulty level based on the login history of the account and the machine used to log in.*

Table 4.1: Test Cases for Functional Testing

Test Cases	Stages	Expected Result	Executed result	Status(Not Exec/Block /Pass/Fail)
1.	*Verify login details*	*User enters a valid user id and password to enter into home page.*	*Enter into home page.*	*Pass*
2.	Allow image as password	Webpage should accept the images given by user.	Server is accepting the images given by user.	Pass
3.	Verify the login images	User should click on images and it should match with register images.	User enter images are match.	Pass
4.	Verify if the images not match	User should enter valid images.	User enter images are not match with register images.	Fail
5.	Upload event	It is allow uploading the file content.	Uploaded the file content	Pass
6.	Event update	It is allow updating a file.	Updated the file	Pass
7.	Verify logout	User click on logout button it should come to login page.	Successfully logout	Pass

4.2 System Configuration:

4.2.1 Minimum Hardware Requirements:

- *Processor : Any Processor above 500 MHz*
- *Ram : 512 Mb.*
- *Hard Disk : 10 GB.*
- *Input device : Standard Keyboard and Mouse.*
- *Output device : High Resolution Monitor.*

4.2.2 Software Requirements:

- *Operating System : Windows Family.*
- *Language :PHP*
- *Database : MySQL Server*
- *PHP : 5.0*

5. Testing:

Testing is the process to verify and validate and ensure the software is working as per the requirement or not. The main objective of testing is to find defects or bugs. The software development is completed. We are conducting the testing with different scenarios.

Testing is a process of executing a program with the aim of finding a fault in the developed system. A good test case is one that has a high probability of finding an undiscovered error. It provides a suitable way to check the functionality of components, sub-modules, modules or a final product it is the process of practicing software with the intent of guaranteeing that the product is error free such that the end user may not feel any difficulty.

5.1Functional testing:

Functional tests are performed to check whether the specified requirement both business and technical is met or not. Testing all the functionality and behavior of software is working as per the requirement specified by user. Functional tests are focused on requirements, key functions, or some special test cases. In addition to that Business process flows, data fields, predefined processes, and successive processes must be considered for testing. Before functional testing is complete, additional tests are identified and the effective value of current tests is determined.

In this application functional testing is performed using some test cases which are mention clearly in the below tables.

5.2 Security Testing:

Security testing is one of the testing techniques which determine whether an information system is protecting data and maintaining functionality as planned. Classic security requirements in security testing may consists of specific elements. They are confidentiality, non-repudiation, availability, integrity, authorization and authentication. Definite security requirements which are tested depend on the security requirements that are implemented by the system. The security can be ensured by not exposing the information to other parties who are unauthorized and making the information to be available to only an intended recipient who are authorized.

Integrity of information refers to protecting information from being modified by unauthorized parties. Authorization is nothing but verifying whether the particular user is authorized one or no by using this CAPTCHA. Availability is defined as the information that should be kept as available to authorized persons whenever they need it.

6.CONCLUSION AND FUTURE ENHANCEMENT:

6.1 Conclusion:

In this project, we investigated the security of the graphical password scheme and the suitability of the images. In proposed a novel way to differentiate humans from machines by an images recognition test. IASL is a new security evolution for unsolved hard AI problems. IASL is a combination of CAPTCHA and a graphical Password scheme, which adopts a new approach to counter online guessing attacks: a new IASL image, which is also a CAPTCHA challenge, is used for every login attempt to make trials of an shoulder suffering attack computationally independent of each other.

6.2 Future enhancement:

In future the scheme may be extended as a web service so that any interconnected user of the network can utilize it to the maximum without the need to implement the code. An interesting property of these protocols is the ability to trade-off authentication time with security, asking many questions only when high security is needed or when an attack is going on. A password of IASL can be found only

probabilistically by automatic online guessing attacks including brute-force attacks, a desired security property that other graphical password schemes lack. IASL forces adversaries to resort to significantly less efficient and much more costly human-based attacks.

7. REFERENCES:

[1] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years," ACM Comput. Surveys, vol. 44, no. 4, 2012.

[2] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in Proc. 8th USENIX Security Symp., 1999, pp. 1–15.

[3] H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability of graphical passwords," Int. J. Netw. Security, vol. 7, no. 2, pp. 273–292, 2008.

[4] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," Int. J. HCI, vol. 63, pp. 102–127, Jul. 2005.

[5] P. C. van Oorschot and J. Thorpe, "On predictive models and userdrawn graphical passwords," ACM Trans. Inf. Syst. Security, vol. 10, no. 4, pp. 1–33, 2008.

[6] K. Golofit, "Click passwords under investigation," in Proc. ESORICS, pp. 343–358, 2007.

[7] A. E. Dirik, N. Memon, and J.-C. Birget, "Modeling user choice in the passpoints graphical password scheme," in Proc. Symp. Usable Privacy Security, pp. 20–28,2007.

[8] J. Thorpe and P. C. van Oorschot, "Human-seeded attacks and exploiting hot spots in graphical passwords," in Proc. USENIX Security, pp. 103–118 ,2007

[9] P. C. van Oorschot, A. Salehi-Abari, and J. Thorpe, "Purely automated attacks on passpoints-style graphical passwords," IEEE Trans. Inf. Forensics Security, vol. 5, no. 3, pp. 393–405, Sep. 2010

[10] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA: Using hard AI problems for security," in Proc. Eurocrypt, pp. 294–311,2003.

[11] S. Li, S. A. H. Shah, M. A. U. Khan, S. A. Khayam, A.-R. Sadeghi, and R. Schmitz, "Breaking e-banking CAPTCHAs," in Proc. ACSAC, pp. 1–10,2010.

[12] S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in Proc. ESORICS, pp. 359–374,2007.

[13] B. Pinkas and T. Sander, "Securing passwords against dictionary attacks," in Proc. ACM CCS, pp. 161–170,2002.

[14] P. C. van Oorschot and J. Thorpe, "Exploiting predictability in click- based graphical passwords," J. Comput. Security, vol. 19, no. 4, pp. 669–702, 2011

[15] T. Wolverton. (2002, Mar. 26). Hackers Attack eBay Accounts [Online]. Available: http://www.zdnet.co.uk/news/networking/2002/03/ 26/hackers-attack-ebay-accounts-2107350/,2002.

[16] D. Davis, F. Monrose, and M. Reiter, "On user choice in graphical password schemes," in Proc. USENIX Security, pp. 1–11,2004.

[17] R. Dhamija and A. Perrig, "Déjà Vu: A user study using images for authentication," in Proc. 9th USENIX Security, pp. 1–4,2000.

[18] D. Weinshall, "Cognitive authentication schemes safe against spyware," in Proc. IEEE Symp. Security Privacy, May pp. 300–306,2006.

[19] P. Dunphy and J. Yan, "Do background images improve 'Draw a Secret' graphical passwords," in Proc. ACM CCS, pp. 1–12,2007.

[20] B. B. Zhu et al., "Attacks and design of image recognition CAPTCHAs," in Proc. ACM CCS, pp. 187–200,2010.

[21] P. Golle, "Machine learning attacks against the Asirra CAPTCHA," in Proc. ACM CCS, pp. 535–542,2008.

[22] The Science behind Passfaces [Online]. Available: Feb,2012.

[23] I.Ravi Shireesh, S. Udayabhanu, "IASL- An Evolution in addressing security problems with CAPTCHA and Graphical Passwords", IJIRCCE, vol. 3, Issue 6, 2015.