

Image Steganography using Pixel Pattern Matching in Cloud Data Storage

K. Usha Nandhini¹, K. Swarna², M.Preetha³, W. Mercy⁴

¹UG Student, Department of CSE, Agni College of Technology, Tamil Nadu, India

⁴Sr. Assistant Professor, Dept of Computer Science and Engineering, Agni College of Technology, Tamil Nadu, India

Abstract - With the event of cloud computing, Information security becomes additional and vital in cloud computing. This paper analyses the fundamental downside of cloud computing information security. Since Cloud Computing share distributed resources via network within the open surroundings, therefore it makes security issues. During this technique, we have a tendency to use Grid choices and Pass Point algorithms. This formula method on the image to urge the component points and therefore the points were used as a secret key for the file uploaded by the user. These techniques were totally different from the standard technique. So here we focus on authentication problem. User authentication is one of the important and fundamental components in most computer security systems. Biometrics is one of the important authentication methods used to tackle the problems associated with traditional username – passwords. But here we will deal with another alternative: using image as password. A graphical password is an authentication system works by having the user interface (GUI).

Key Words: Graphical password, security, protection, CaRP.

1. INTRODUCTION

Computer security (Also called cyber security or IT security) is data security as applied to computers and networks. The sphere covers all the processors and mechanisms by that computer- based instrumentality, data and services square measure protected against unwitting or unauthorized access, modification or destruction. Laptop security additionally includes protection from unplanned events and natural accidents , fig. 1.

Most laptop security measures involve encoding and passwords. Encoding is that the translation of knowledge into a type that's unintelligible while not a deciphering mechanism. A parole may be a secret word or phrase that offers a user to access a selected program or system.



Fig -1: Justify the concerning the secure computing

2. BASIC NEEDS IN THE SECURE COMPUTING

If you don't take basic steps to protect your computer, you put it and all the information on it at risk. You can potentially compromise the operation of the computers on your organizations network, or even the functioning of the network as a whole.

2.1 Physical security:

Technical measures like login passwords, anti-virus is essential. (More about those below) However, a secure physical space is the first and more important line of defense.

Is the place you keep your workplace computer secure enough to prevent theft or access to it while you are away? While the security Department provides coverage the Medical center, it only takes seconds to steal a computer, particularly a portable device like a laptop or a PDA. A computer should be secured like any other valuable possession when you are not present.

Human threats are not the only concern. Computers can be compromised by environment mishaps (e.g., water, coffee) or physical trauma. Make sure the physical location of your computer takes of those risks as well.

2.2 Access passwords:

The University's network and shared information systems are protected in part by login credentials (user-IDs and passwords). Access password is an essential protection for personal computers in our circumstances. Offices are usually

open and shared spaces, so physical access to computers cannot be completely controlled.

2.3 Prying eye protection:

We all deal with all facts of clinical research, educational and administrative data here on the medical campus. This is important to do everything possible to minimize exposure of data to unauthorized individuals.

2.4 Anti-virus software:

Enlightened, properly configured anti-virus software is essential. We have server-side anti-virus software on our network computers, you still need it on the client side (your computer).

2.5 Firewalls:

Anti-virus products inspect files on your computers and in email. Firewall software and hardware monitor communication between your computer and the outside world. That is essential for any networked computer.

2.6 Software updates:

It is critical to keep software up to date, specially the operating system, anti-virus and anti-spyware, email and browser software. The newest versions will contain fixes for discovered vulnerability.

Mass of anti-virus have automatic update features (including SAV). Keeping the "SIGNATURES" (digital patterns) of malicious software detectors enlightened is essential for these products to be effective.

2.7 Keep secure backups:

Even if you take all these security tread, bad things can still happen. Always be prepared for the worst by making backup copies of critical data, and keeping those backup copies in a separate, secure location. For example, use supplemental hard drives, CDs/DVDs, or flash drives to store critical, hard-to-replace data.

2.8 Report problems:

If you believe that your computer or any data on it has been compromised, you should make a information security incident report. It is required by University policy for all data on our systems, and legitimately required for health, education, financial and any other kind of record containing identifiable personal information.

3. BENEFITS OF SECURE COMPUTING

3.1 Protect yourself – Civil liability:

You may be held amenable to compensate a third party should they experience financial damage or distress as a

result of their personal data being stolen from you or leaked by you.

3.2 Protect your credibility - Compliance:

You may require compliancy with the Data Protection Act, the FSA, SOX or other regulatory quality. Each of these bodies demand that certain measures be taken to protect the data on your network.

3.3 Protect your reputation – Spam:

A common usage for infected systems is to join them to a botnet (a collection of infected machines which takes orders from a command server) and use them to send out spam. This spam can be traced back to you, your server will be blacklisted and you will be unable to send email.

3.4 Protect your income – Competitive advantages:

There are a number of "hackers-for-hire" advertising their services on the internet selling their skills in breaking into company's servers to steal client database, proprietary software, merger and acquisition information, personal detail set.

3.5 Protect your business – Blackmail:

A seldom-reported source of income for "hackers" is to break into your server, change all your passwords and secure you out of it. The password is then sold back to you. *Note:* the "hackers" may implant a backdoor program on your server so that can repeat the exercise at will.

3.6 Protect your investment – Free storage:

Your server's hard drive space is used to house the hacker's video clips, music collections, pirated software or worse. Your server or computer then becomes continuously slow and your internet connection speeds deteriorate due to the number of people connecting to your server in order to download the offered wares.

4. RELATED WORK

In this section we have studied few papers which shows about the graphical passwords for security

1. P.C Van Oorschot and J. Thorpe proposed "On predictive models and user drawn graphical passwords" which results quantitatively support suggestions that user-drawn graphical password systems employ measures, such as graphical password rules or guideline and proactive password checking.
2. A. E. Dirik, N. Memon and J.-C. Birget proposed "Modeling user choice in the Pass Point graphical password scheme" which results that the model and experiments are small and limited, but they show that user choice can be modeled and that

expansions of the model and the experiments are promising direction of research.

3. B.Pinkas and T. Sandar proposed "Secure passwords against dictionary attacks" it is easy to implement and overcome some of the difficulties of previously suggested methods of improving the security of user authentication scheme and it provides better protection against denial of service attacks against user accounts.
4. M. Alsaleh, M. Mannan, and P. C. Van Oorschot proposed "Revisiting defenses against large-scale online password guessing attacks" it analyze the performance of PGRP with two real-world data sets and find it more promising than existing proposals.

5. SYSTEM ANALYSIS

5.1 Existing System:

The security of the theme continues to be secure if the outflow of the key secret is up to bound bits such the information of those bits doesn't facilitate to recover the total secret key. However, although victimization outflow resilient primitive will safeguard the outflow of bound bits, there exists another sensible limitation. Suppose we tend to place a part of the key into protection device. The user has to acquire a replacement so he will still decipher his corresponding secret key. This approach are often simply achieved. Still, there exists security risk. If the register may also force to lock the personal computer wherever a part of secret is keep, then it will decipher all cipher text comparable to the victim user. The foremost secure approach is to stop the validity of the taken security.

5.2 Disadvantages of Existing System:

1. If the user has lost his secret key, then his / her corresponding cipher text within the cloud can not be decrypted forever that's, the approach cannot support secret key update / revocability.
2. Processing step are high.
3. Knowledge loss will occur.
4. Computation price is high.

5.3 Proposed System:

In this paper, we present a new security primitive based on AI problems, namely, a NOVEL family of graphical password, which called as Graphical passwords. It addresses a number of security problems, such as online guessing attacks, relay attacks, and if combined with dual-view technologies, shoulder-surfing attacks. The proposed system model is given fig. 2.

5.4 Advantages of Proposed System:

1. Graphical watch word offers protection against online wordbook attacks on passwords, that are for very long time a significant security threat for varied online services.
2. It additionally offers protection against relay threat to bypass encoding protection.

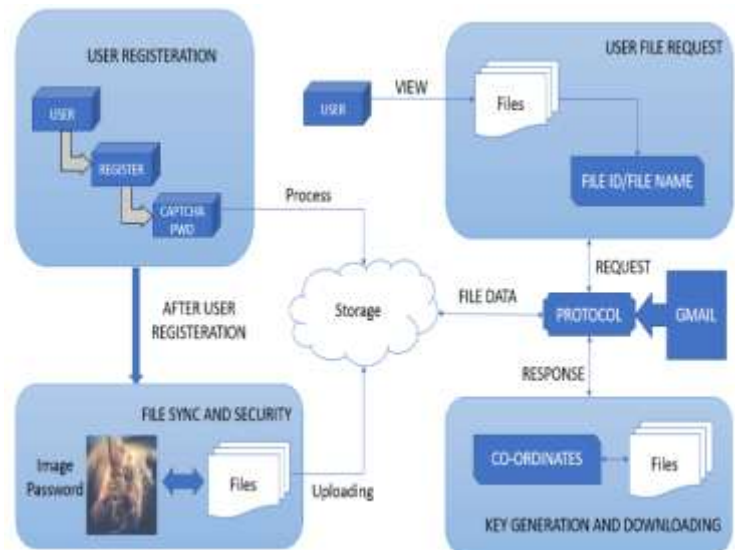


Fig -2: Proposed System Model

6. ALGORITHM

In 2005, Pass Point created in order to cover the limitation of BLONDER ALGORITHM which was limitation of image. The picture will be any natural picture or painting but at the same time should be rich enough in order to have many possible click points. On the contrary, the image is not secret and has no role other than helping the user to remember the click point. Another source of flexibility is that there is no need for artificial predefined click region with well-marked boundaries like BLONDER ALGORITHM.

The user is choosing several points on the picture in a particular order. In order to login, the user has to click close to the chosen click point, within some (adjustable) tolerance distance, for example within 0.25cm from actual click point.

As in BLONDER ALGORITHM, user had to click on the predefined image at predefined region. Passpoint over comes this by selecting any natural image and having as a many click points as possible which make the system more secure.

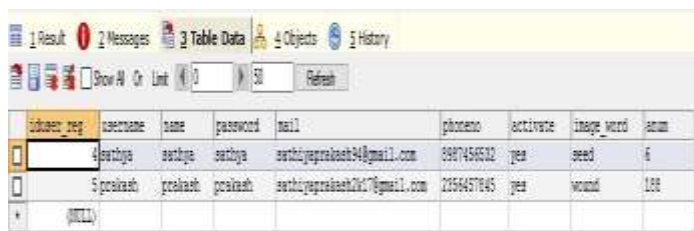
Passpoint system has the potential for extremely high entropy. As any pixel in the image is the candidate for a click point so there are hundreds of possible memorable points in the challenge image. There are number of researching on the characteristics of this model like predicting probabilities of

likely click point which enables the predicting the entropy of the click point in a graphical password for a given image.

7. MODULES

7.1 User Registration:

In this module, users are having authentication and security to access the cloud. For security, captcha technique is implemented to access the detail which is presented in the image system. Each time users have to enter, registered captcha text and password for accessing the account. The registered data can be stored in a table fig. 3.



iduser_reg	username	name	password	mail	phoneno	activate	image_word	acum
4	satbya	satbya	satbya	satbyaprabash24@gmail.com	9987456532	yes	seed	6
5	prakash	prakash	prakash	satbyaprabash24@gmail.com	2356457845	yes	wound	188

Fig -3: Register Data in Table Form

7.2 File Synchronization And Security:

The user can set up the server after system is opened. Then the user can upload the file to the storage with the key to a0access it. The key process is done with grid selection and Pass Point algorithm. By clicking particular point at the given image, the position of the image pixel is taken as X & Y Co-ordinates as key. These co-ordinates were assigns as X1, Y1 and by clicking on different position 2nd coordinates were assigned as X2, Y2, which is referred in fig.4. In this a password guess tested in an unsuccessful trial is determined than traditional approaches.



idfile	filename	files	owner	x1	y1	x2	y2	time
20	file	(Binary Image)	satbya	254	269	256	321	2019/12/12 12:04:10
21	weat	/*5Qjyog Zmzprpse - My6...	satbya	230	269	333	297	2020/02/07 14:34:12
22	hill	(Binary Image)	satbya	144	104	159	164	2020/02/07 14:38:17

Fig -3: Key Generation for Authorized Users

7.3 User File Request:

The request process is done via protocol and key is send to an authorized user through mail. By this process key is shared and the file is viewed/downloaded by the other user with the key given by the data owner.

7.4 Key Generation And Downloading:

The number of undetermined positive identification guesses decreases with a lot of trials, resulting in an improved

likelihood of finding the positive identification. To counter shot attacks, ancient approaches in planning graphical positive identifications aim at increasing the effective password area to form passwords more durable to guess and therefore need a lot of trials, the positive identification will invariably be found by a brute force attack. In this paper, we tend to distinguish key generated through which concept than the normal approaches, and key request method is finished through the protocol with the opposite user to access files.

8. CONCLUSION

We have projected CaRP, a replacement security primitive hoping on unsolved onerous AI issues. CaRP is the combination of a Captcha and a graphical secret theme. The notion of CaRP introduces a replacement family of graphical passwords. Like Captcha CaRp utilizes unsolved AI issues. However a watchword is way a lot of valuable to attackers than a free email account that captcha is usually won't to defend. Thus there square measure a lot of incentives for attackers to hack CaRP than Captcha. That is, a lot of efforts are going to be drawn to the subsequent win-win game by CaRP than normal Captcha: If attackers succeed, they contribute to up AI by providing solutions to open issues like segmenting second texts. Otherwise, our system stays secure, conductive to sensible security. As a framework, CaRP doesn't think about any specific Captcha theme. Once one Captcha theme is broken, a brand new and safer one could seem and be regenerate to CaRP theme. Overall, our work is one break through within the paradigm of mistreatment exhausting AI issues or security. Of cheap security and value and sensible applications, CaRP has smart potential for refinements, that concern helpful future work. A lot of significantly, we have a tendency to expect CaRP to inspire new inventions of such AI based mostly security primitives.

9. REFERENCES:

[1] Mudassar Ali Khan, Ikram Ud Din, Sultan Ullah Jadoon, Muhmmad Khurram Khan, Mohsen Guizani, Kamran Ahmad Awan "g-RAT | A Novel Graphical Randomized Authentication Technique for Consumer Smart Devices", 2019, IEEE Transaction on Consumer Elctronics.

[2] (2012, Eeb) The Science Behind Passfaces [Online] Available: <http://www.realuser.com/published/ScienceBehindPassfaces.pdf>

[3] 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.1-5.

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

[5] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Menon, "Pass Point: Design and longitudinal evaluation of graphical password system" In. J. HCI, vol. 102-127, Jul.2005.

[6] P. C. van Oorschot and J. Thrope, "On predictive models and user drawn graphical passwords" ACM Trans. Inf. Syst. Security, vol. 10, no. 4, pp. 1-33, 2008.

[7] K. Golofit, "Click passwords under investigation," in proc. ESORICS, 2007, pp. 343-358.

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

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

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