International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 06, June-2019

Secure Authentication and Tracking Mechanism with Honeyword

Nayansukh Patil
Department of Computer Engineering,
A. C. Patil College of Engineering, Kharghar,
Navi Mumbai, MS, India

Rachana Patil
Department of Computer Engineering,
A. C. Patil College of Engineering, Kharghar,
Navi Mumbai, MS, India

***Abstract*— The new advancement in the field of IT offered the people enjoyment, comforts and convenience, but there are many security related difficulties. One of them is password file. Password files mechanism has got a lot of security problem that has affected millions of users as well as many companies in the world. Password file is basically stored in encrypted format, if a password file is hacked by hacker by using the password cracking techniques and decryption technique it is easy to find most of the plaintext from encrypts passwords. To solve this here we produce the honey word password, i.e. a false password using a perfectly flat honey word generation method, and try to attract unauthorized user. Hence that time it finds the unauthorized user. Here this system also protects the original data from unauthorized user. If hacker trying to access user account and enter 3 times wrong password then hacker will get decoy file, also for each wrong password notification will go to admin and user. This will provide security. For each wrong password user and admin get notification. Also we maintaining location tracking of the user and proposing a new technique called video click based captcha scheme to authenticate user. Thus, this whole architecture protects and secures the data and application over the online network reducing the threats against the unauthorized users. System send login notification to owner mobile number .At the time of login if password is from honey pot the user and admin will get the mail that someone is trying to access user's account. Video pause time on submit button is performed and that matched at every time of login button. Here location tracking is performed by taking current user latitude and longitude In Web application location of user for failed password will send after when he trying to login that time forensic details send to owner account with system private IP address techniques, public IP address, City name, State, Country name. System shows Google map location of hacker via sending link to mail directly.**

Keywords—Authentication, Forensic details, honeypot, honeyword, login, passwords, password cracking.

I. INTRODUCTION

Generally in many companies and software industries store their data in databases like SQL or some NO-SQL databases. So, the entry point of a system which is required user name and Passwords are stored in encrypted form in database. Once password file is stolen, by using the password cracking technique it is easy to capture most of the plaintext passwords so for avoiding it, there are two issues that should be considered to overcome these security problems: First passwords must be protected and secure by using the appropriate algorithm. And the second point is that a secure system should detect the entry of unauthorized user in the system. Password files have got a lot of security problem that has affected millions of users as well as many companies. The password file is generally stored in an encrypted format, if a password file is hacked or theft by using the password cracking techniques and decryption technique it is easy to capture or find most of the plaintext and encrypt passwords. In the proposed system we focus on the honeywords i.e. fake passwords and accounts. The administrator purposely creates user accounts and detects a password disclosure, if any one of the honey pot passwords get used it is easy to detect the admin. According to the study, for each user incorrect login attempts with some passwords lead to Honey pot accounts, i.e. malicious behavior is recognized. In the proposed system, we create the password in plain text and stored it with the fake password set. We analyze the honeyword approach and give some remarks about the security of the system. When an unauthorized user attempts to enter the system and get access to the database, the alarm is triggered and gets the notification to the administrator, since that time unauthorized user get decoy documents. i.e. fake database, and also propose the Video-based captcha authentication technique to avoid the OCR (Optical character recognition or optical character reader) based authorized access to the system and also focus someone is trying to get access of system both admin and the user are notified by email with the system and location details of the user including private and public IP of system. the main objective to design a system to identify the occurrence of a password database breach. Focus on fake passwords or accounts as a simple and cost-effective solution to detect a compromise of passwords. Design a system that focuses the cracked password files can be detected by the system administrator if a login attempt is done with a honeyword by the adversary. Use this technology to launch disinformation attacks against malicious insiders, preventing them from distinguishing the real sensitive customer data from fake worthless data. Perform forensic details like system and location details sending notification via mail.

II. LITERATURE SURVEY

From the last decade use of computers have increased numerously for carrying out many processes across the world which includes data change, online transactions, Social Networks, etc. Public users want their data to be controlled and harmless over the digital network for avoiding many future problems, Authentication of user can be done to avoid this problem i.e. user verification and identification in such a way that when a user is trying to request to access any data over Network he should be the owner of that data. This can solve the problem of user security and to differentiate every

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 06, June-2019

user over the digital network they are provided with unique Identification called as Password. The Password in Internet world is the secret key of each user to store and access his data over the network without producing any prohibited activities or scams. So password theory is a very important characteristic in the digital world when comes to the security level. There are many third party attackers or hackers which are creating new methods to crash these passwords simply and causing scam to that specific password, hence to overcome the problem of these attackers new system securities are been proposed by many authors and is taken into attention to attain security over the network[20].

A. Password Generation Method

Key logger Attack: It captures the keystrokes of the user for stealing their password. It uses key press and release time, the action of logging the keys hit on a keyboard typically covertly, so that person using the keyboard is unaware that their actions are being observed. Data can then be recovered by the attacker operating the logging program.

Brute Force attack: A computer program or ready-made software is commonly used for implementing brute force attack to crack the passwords. Brute force attack might try commonly-used passwords or combinations of letters and numbers. Suppose an adversary got a password file F and cracked the number user passwords. Then, he/she tries to login with any accounts in the list instead of compromising a specific account. Furthermore, we assume that the adversary has no advantage in guessing the correct password by analyzing corresponding honey words, i.e. Pr(g = pi) = 1=k. Last, if one of the users honey words is entered, the system takes the appropriate action according to one of the example policies as follows: Login proceeds, as usual or Users account is suspended until the user created a new password.

Dictionary attack: In this type of attacks generally, an attacker trying all the possible strings from the pre-arranged list of strings, this attack tries only those possibilities which are supposed most likely to succeed these attacks. This attack repeatedly succeeds because many people have a trend to choose short passwords that are normal words or common passwords, or simple alternatives found.

Dos-attack: To detect DoS (denial of service) resistance, we use two types of parameter in consideration i.e. strong and weak. Strong DoS resistance means that DoS attack is doubtful. Weak DoS resistance means attacker can view with non-negligible possibility to submit the Honeyword based on given knowledge of password. We show that the other model may suffer from a DoS attack, due to predictability of the honeyword. Unlikely, other model provides resistance against such an attack, because honeyword are generated by using a list of passwords such that they may be independent from the correct password. Passwords files are stored on different server so traffic problem on single server will resolve.

TABLE I. explain the Comparative study of honeywords generation method there are five of honeywords generation method.as well as TABLE II. explains different categories of captcha method.

B. Captcha Methods

TABLE I. PASSWORD GENERATION METHODS

METHOD	Dos resistance	Dictionary attack	Brute Force attack	FLATNESS	Key Logger Attack
Chaffing by tweaking[1]	Medium	Medium	High	Low	No
Chaffing with-a-Password Model[1]	Strong	Strong	Medium	Medium	No
Chaffing with Tough nuts[19]	Strong	Medium	High	Medium	No
Take a-Tail[19]	Weak	Weak	High	Low	No
Hybrid[19]	Strong	Medium	Medium	Strong	No

There are many types of CAPTCHA systems. Like

Text based Captcha: Text based CAPTCHAs is a very simple to implement. It is very effective and requires a large question bank. In Text based captcha the Number of classes of characters and digits are very small so the problem occurs for user to identify the correct characters and digits [16]. The text based captcha is possible to identify the character and digit through Optical character recognition (OCR) technique. In Text based CAPTCHAs simple asked questions like as based on arithmetic equation.

Image based Captcha: Image based Captcha: Graphics based

CAPTCHAs are challenge-tests in which the users have to guess those images that have some similarity. The advantage of image based CAPTCHA is that pattern recognition is hard AI problem and therefore it is difficult to break this test using pattern recognition technique [14].

Audio based Captcha: Audio based Captcha: Audio based CAPTCHAs are based on the sound-based systems. These CAPTCHAs are developed for visually disabled users. It contains downloadable audio-clips. In this type of CAPTCHA, first the user listens and after that submits the spoken word [14].

Video based Captcha: Video based Captcha: Video CAPTCHA is a newer and less commonly seen CAPTCHA system. In video-based CAPTCHAs, three words (tags) are provided to the user which describes a video. The users tag must match to a set of automatically generated ground truth tags then only the test is said to be passed dictionary to guess users password. Bot detection will use like Optical character recognition (OCR) technique to guess password

TABLE II. COMPARATIVE TABLE FOR CAPTCHA GENERATION METHODS

Method	Flatness	Brute Force Attack	Dictionary Attack	Bot detection
Text based Captcha[13]	low	High	High	High
Image Based Captcha[14]	low	Medium	Medium	Medium
Audio Based Captcha[14]	Medium	Medium	Medium	high

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 06, June-2019

Video Based Captcha[17]	Medium	Medium	Low	high
Video Click Based captcha	High	Low	Low	Low

III. SYSTEM ARCHITECTURE

Proposed model is still based on use of honey words to detect password-cracking. However, instead of generating the honey words and storing them in the password file, we suggest to benefit from existing passwords to simulate honey words. In order to achieve this, for each account k - 1 existing password indexes, which we call honey indexes, are randomly assigned to a newly created account of ui, where k ¿= 2. Moreover,a random index number is given to this account and hash of the correct password is kept with the correct index in list. On the other hand, in another list ui is stored with an integer set which is consisted of the honey indexes and the correct index. So, when an adversary analyzes the two lists,she recognizes that each username is paired with k numbers as sweet indexes and each of which points to real passwords in the system. The tentative password indexes hamper an adversary to make a correct guess and she cannot be easily sure about which index is the correct one. It is equivalent to say that to create uncertainty about the correct password, we propose to use indexes that map to valid passwords in the system. The contribution of our approach is twofold. First, this method requires less storage compared to the original study.

Second, in the previous sections we argue that effectiveness of the honey word system directly depends on how Gen() flatness is provided and how it is close to human behavior in choosing passwords. Within our approach passwords of other users are used as the fake passwords, so guess of which password is fake and which is correct becomes more complicated for an adversary. Making System secure against Machines/Bots attacks using Video click based CAPTCHA which is used to detect between real user humans and machines which has behavior like machines which can be achieved using OCR algorithm which all hackers or attacker's used to train the machine to act like real user. Using Video based click Captcha we can avoid all these threats to system as we are recording the current time, RBGs and X and y axis to record the points from video where user clicks and is stored in database. The machine is unable to understand the video and cannot move the cursor to the exact points as real human does

Registration Process: At the time of user registration password is taken. Video pause based time is stored in database. Then video pause time is maintained at the time of registration by moving mouse on registration submit video.

Login process: System is developed by considering two approaches Desktop based as well as Application based. While login user enters username and password and simply click pause the video based on the clicking time is maintained at the time of registration by play and pause of video and location tracking is done. All information taken at the time of registration and used at the time of login. Here in desktop application location tracking is performed by taking current user latitude and longitude which is registering to present system. After when he/she trying to login that time system will check present latitude and longitude of that user who is logging to system. If difference is more then he will not access the system. In web application forensic details are sending to owner of account that is Private and public IP address, city, country, hostname. System sends google map location in mail also. In system at time of login shoulder suffering may happen to remove this proposed system will take login time of video pause at the time by moving mouse on login button but who is seeing will see pause time is login button click time(Display time) but it is actual time of mouse moving on login button(Actual time).

Honey checker: In our approach, the auxiliary service honey checker is employed to store correct indexes for each account and we assume that it communicates with the main server through a secure channel in an authenticated manner.

IV. SYSTEM ANALYSIS AND RESULTS

In proposed system video is playing continue after entering a password. To reduce shoulder suffering user has to move the mouse on submit button then the video will play faster and mouse move time will be taken as pause time so back person will see stop time is the actual submit button time but it's not so paused time will be mouse move only on submit button. That overcomes the problem of OCR. In text based and video-based captcha OCR Can read text from video in proposed system OCR Also shoulder suffering will remove it will not happen in the proposed system. also if any unauthorized attempt is happens then we notify the user as

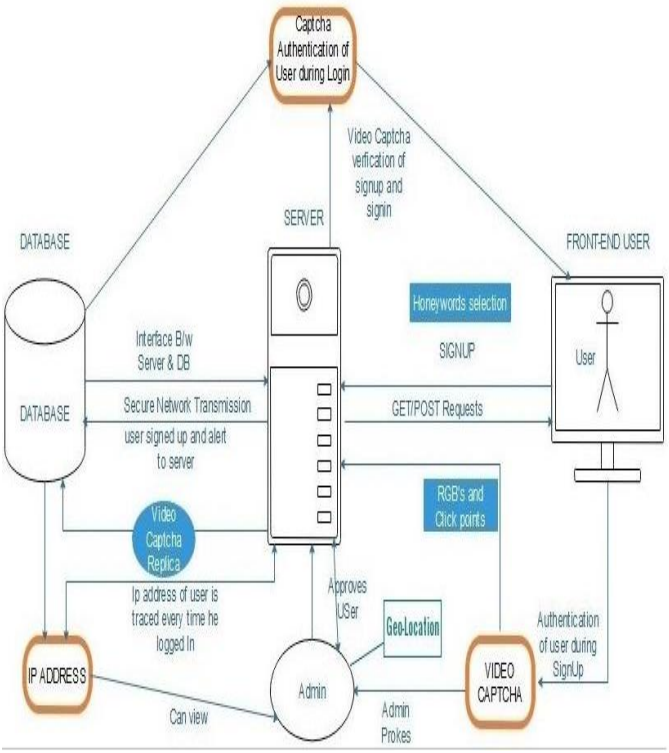

Fig 1 system Architecture.

Well as admin by providing the location machine details of the attackers and change the password of the user as well as

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 06, June-2019

respective honeywords. By using the machine and location details of unauthorized user we can block the unauthorized user. in order to secure the user sensitive data. Video based captcha is use to avoid machine/bot attack and forensic details are use to block the authorized users. so, using honeywords and tracking system it is very difficult for the attacker to break the password and access the system.

TABLE III. DIFFERENCE BETWEEN PROPOSED AND EXISTING SYSTEM.

Attributes	Proposed system	Existing system
DB File stored	Two server	One server
Forensic details	Inform to admin and owner	Not inform
GPS Location tracking view on map	Yes	No

Fig 2 shows the Actual time and Display time of login to avoid the shoulder suffering Attack while click on the video in logon process.

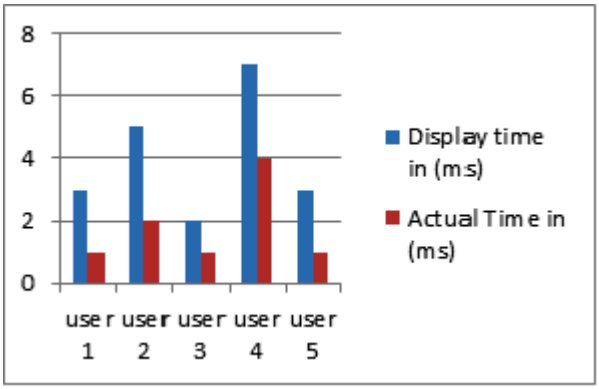

Fig. 2. Actual and Display login time.

CONCLUSIONS

The proposed system have analyzed the security of the honeyword system and addressed a number of flaws that need to be handled before successful realization of the scheme. It successfully worked on video and Location tracking of user. It uses Levenshtein distance algorithm to match latitude and longitude of user current location in desktop application. In web application system working on doing forensic details
Like private, public IP address of system and city, country, pin code and host name. In case of unauthorized user trying to access the system.

REFERENCES

[1] Imran Erguler, Achieving Flatness: Selecting the Honeywords from Existing User Passwords, DOI 10.1109/TDSC.2015.2406707, IEEE Transactions on Dependable and Secure Computing.

[2] Ms. Manisha B. Kale, Prof. D. V. Jadhav, Security Analysis of Honey words Generation Scheme to Evade Unauthorized Access , Department of Computer Engineering, Zeal College of Engineering and Research, Pune, India1, Tech. Rep. Issue 7, July 2016.

[3] A. Pathak, An Analysis of Various Tools, Methods and Systems to Generate Fake Accounts for Social Media, Ph.D. dissertation, Northeastern University Boston, 2014.

[4] L. Zhao and M. Mannan, Explicit Authentication Response Considered Harmful, in Proceedings of the 2013 Workshop on New Security Paradigms WorkshopNSPW 13. New York, NY, USA: ACM, 2013, pp. 7786. [Online].Available: http://doi.acm.org/10.1145/2535813.2535822.

[5] K. Brown, The Dangers of Weak Hashes, SANS Institute InfoSec Reading Room, Tech. Rep., 2013.J. Bonneau, The science of guessing: Analyzing an anonymized corpus of 70 million passwords, in Security and Privacy (SP), 2012 IEEE Symposium on. IEEE, 2012, pp. 538552.

[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[7] MattWeir, Sudhir Aggarwal, Breno de Medeiros, Bill Glodek , Password Cracking Using Probabilistic Context Free Grammars,18 August 2009,IEEE Symposium on Security and Privacy.

[8] P. G. Kelley, S. Komanduri, M. L. Mazurek, R. Shay, T. Vidas, L. Bauer, N. Christin, L.F. Cranor, and J. Lopez, Guess again (and gain and again): Measuring Password Strength by Simulating Passwordcracking

[9] Algorithms, in Security and Privacy (SP), 2012 IEEE Symposium on. IEEE, 2012, pp. 523537.

[10] Manisha Jagannath Bhole Honeywords: A New Approach For Enhancing Security Nov.2015,International Research Journal of Engineering and Technology.

[11] Z. A. Genc, S. Kardas, and K. M. Sabir, Examination of a New Defense Mechanism: Honeywords, Cryptology ePrint Archive, Report 2013/696,2013.

[12] Security and Usability Challenges of Moving-Object CAPTCHAs: Decoding Codewords in Motion. Prof. Anisaara Nadaph, Juwairiya Shaikh2, Nikita Bodhe2, Hemlata Pingale2, Mrunali khunte,4 april 2016.

[13] Anjitha K, Rijin I KCaptcha As Graphical Passwords-Enhanced WithVideo-Based Captcha For Secure Services, 978-1-4673-9223-5/15/2015 IEEE.

[14] Baljit Singh Saini and Anju Bala "A Review of Bot Protection using CAPTCHA for Web Security," IOSR Journal of Computer Engineering, 2013, pp. 36-42, 2013.

[15] S. Karthika, Dr. P. Devaki,An Efficient User Authentication using Captcha and Graphical Passwords-A Survey Volume 3 Issue 11, November 2014, International Journal of Science and Research (IJSR).

[16] Buvanesvari1, V. Prasath,,A New Security Mechanism for Graphical Password Authentication using Combo Captcha in Video Technology, International Journal of Science and Research (IJSR) IVolume 4 Issue 1, January 2015.

[17] Priyanka K.Kukadeet al,International Journal of Computer Science and Mobile Computing, Vol.4 Issue.5, May-2015,International Journal of Computer Science and Mobile Computing CAPTCHA Problems on AI Based For Protection from Automated Hacking Tool.

[18] Prof. Anisaara Nadaph1, Juwairiya Shaikh2, Nikita Bodhe2, Hemlata Pingale2, Mrunali khunte ,International Journal of Innovative Research in Computerand Communication Engineering,Vol. 4, Issue 4, April 2016 Video CAPTCHA Design Based on Moving Object Recognition.

[19] Ari Juels, Ronald L. Rivest, Honeywords:Making Password-Cracking Detectable, May 2, 2013.

[20] Nayansukh Patil, Rachana Patil Achieving Flatness: with Video Captcha, Location Tracking, Selecting the Honeywords DOI: 10.1109/ICSCET.2018.8537339 2018, IEEE International Conference on Smart City and Emerging Technology (ICSCET)