SELECTING HONEYWORDS FROM EXISTING PASSWORD

Prof. S. M. Satre (*Author*), Mamta Donga (*Author*), Abhishek Gaikwad (*Author*), Priyanka Pawar (*Author*)

Assistant Professor, Student, Student, Student
Department of InformationTechnology
Bharati Vidyapeeth College of Engineering
Kharghar, Navi Mumbai, India.

Abstract— Username is useful to find the particular user and the password for the authorization of the user. The username-password checking is more important in the security system, so to protect password from third party we implement for each user account, the valid password is converted new password using honeywords and hash password. New password is the combination of existing user passwords called honeywords. Fake password is nothing but the honeywords, if honeywords will chosen properly, a cyber-attacker who takes a file of hashed passwords, cannot be sure if it is the real password or a honeywords for any account. Moreover, entering with a honeywords to login will trigger an alarm and inform the administrator about a password file so we introduce an easy and capable solution to the detection of password file exposure events. In this study, we examine in detail with careful attention the honeywords system and present System. Also focus on reducing storage size of password and alternate way to choose the new password from existing user passwords

Keywords- **Honeywords, Password, Login, Password Cracking, Authentication, Security, Encryption, Decryption, Notification.**

I.INTRODUCTION

The term "honeywords" is a play on "honeypot," which in the information security really refers to creating fake servers and then learning how attackers attempt to exploit them in effect, using them to help detect more widespread intrusions inside a network [10]. "Honeywords are a simple but clever idea," said Bruce Schneider. "Seed password files with dummy entries that will trigger an alarm when used. That way a site can know when a hacker is trying to decrypt the password file. “The honeywords concept is also elegant because any attacker who's able to steal a copy of a password database won't know if the information it contains is real or fake. An adversary who steals a file of hashed passwords and inverts the hash function cannot tell if he has found the password or a honeywords [7]. The proposed mechanism can distinguish the user password from honeywords for the login routine and will redirect user to decoy data. Real passwords are often weak and easily guessed; either by sharing passwords, using names of loved ones, dictionary words, and brute force attacks. Motivation towards this project is to prevent the attacks and keep the adversaries away from the user accounts. Theft of password hash files are increasing. Therefore, this technique will give a break to hackers. Indeed, once a password file is stolen, by using the password cracking techniques like the Algorithm of Weir et al. [1] it is easy to capture most of the plaintext password.

II. LITERATURE SURVEY

2.1The Science of guessing: analysing an anonymised corpus of 70 million passwords

Authors: Joseph Bonneau 2012

This paper describes the evaluation of large password data sets by collecting a massive password data set legitimately and analysing it in a mathematically rigorous manner [3]. In previous paper, Shannon entropy and guessing entropy not worked with any realistically sized sample, therefore, they developed partial guessing metrics including a new variant of guesswork parameterized by an attacker’s desired success rate. In their study most troublesome is how little password distributions seem to vary, with all populations of users [3].

2.2 A Large-Scale Study of Web Password Habits

Authors: Dinei Florencio and Cormac Herley

This paper describes the study of password used and password reused habits [8]. They measured average number of passwords and average number of accounts each user has, as well as measured number of times user enters password per day. They calculated this data and estimated password strength, password vary by site and number of times user forgotten password. In their findings, it showed users choose weak passwords; they measured exactly how weak. They measured number of distinct passwords used by a client vs. age of client in days also, number of sites per password vs. age of client in days [8]. They also analyzed password strength. We are able to estimate the number of accounts that users maintain the number of passwords they type per day, and the percent of phishing victims in the overall population.

2.3Honeywords: Making Passwords Cracking Detectable

Authors: Ari Juels, Ronald L. Rivest

This paper describes honeywords technology to improve security level for authenticating fake users. The authors have also described briefly attacks on different scenarios, but have focused on stolen files of password hashes scenario [7]. They have described various types of attacks on honeyword system that shows how it will manage and overcome it. The attacks are, namely, general password guessing, targeted password guessing, attacking the honeychecker, likelihood attack, DOS attack and multiple systems.The study shows to limit the impact of a

DOS attack against chafing-by- tweaking, one possible approach is to select a relatively small set of honeywords randomly from a larger class of possible sweetwords [7].

2.4Kamouflage: Loss-Resistant Password Management

Authors: HristoBojinov, ElieBursztein, Xavier Boyen, and Dan Boneh

This paper describes kamouflage-based password manager a new technique to prevent theft-resistant. The study states to use salts and slow hash functions to slow down a dictionary attack on the master password but unfortunately these methods do not prevent dictionary attacks. Authors states the main difficulties to overcome to make kamouflage work are, human-memorable passwords, related passwords, relation to master password and site restrictions. The authors have done with a survey that shows how users choose passwords. Authors have also described threat model, decoy set generation and fingerprinting. They ended with the conclusion stating kamouflage and fingerprinting technique provides security at high level [10].

2.5 Examination of a New Defense Mechanism: Honeywords

Authors: ZiyaAlperGenc, SuleymanKardas and Mehmet SabirKiraz

This paper describes hash passwords are used to improve security. For user authentication false passwords are added in hashed password file i.e. honeywords. They analyzed the honeyword system according to both functionality and the security perspective. They also elaborated how the system will respond to six password related attacks [4]. Improvements for honeywords is described briefly i.e. number of honeywords, typo-safe honeyword generation and old passwords problem. Assumptions are illustrated to an active attack against honeyword system. They concluded that honeyword system is the powerful defence mechanism where an adversary steals the file of password hashes and inverts most or many of the hashes [4].

2.6Security for Multimedia Content in Cloud using double Encryption

Authors: Shankar M. PatilKomal D. Jadhav, Jogendra.N.Nandanwar

It helps to detection of our node is in working state or not in working state. For security measurement we referMultimedia Content in Cloud using double Encryption method for providing protection to authenticated user’s [15].

2.7QoS-Oriented Adaptive Expedient Broadcast Routing for Hybrid Wireless Network

Authors: S. M. Satre and V. P. Jadhav

For better quality of service among the network users we used QoS-Oriented Adaptive Expedient Broadcast Routing for Hybrid Wireless Network (QoS-Oriented AEBR) algorithm. It allows in routing forwards the packets by using advance opportunistic schemes and providing framework to detection of a failure node in hybrid wireless network [14].

III. SYSTEM ARCHITECTURE

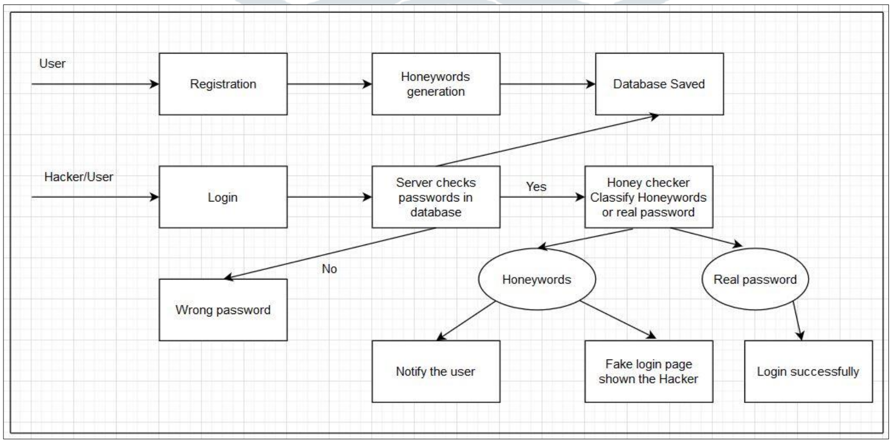


Figure: System Architecture

IV. SYSTEM METHODOLOGY

1. REGISTRATION
   Here user is going to register into system. Then while registration for give password by user system will generate Honeywords and Store into the table.
2. LOGIN
   Here user is going to Login into the System. If password matches with password then user can Login.
3. HONEYWORD GENERATOR

In this phase honeywords are generated by using chafing, hybrid and take-a-tale methods. Here honeywords are generated to ensure the security of the system. There are total 30 honeywords generated randomly and are stored in the same file. 30 honeywords as there are 29 honeywords generated randomly and 1 is the actual password which user going to enter while logging into the system. So there are total 30 honeywords are generated and this honeywords are stored randomly and stored in database

4. HACKER
When a hacker is trying to get access into the valid user's account then he has given only 1 attempts to get login into the system. If any of the password entered by hacker matches with the honeyword then he will get access to the system but it will be the dummy page, which are fake files and they are not the actual ones.
5. SERVER
Though hacker got fake files. Server checks for honeyword and keep the hacker logged in on fake page and sends a notification to the valid user by mail or message that someone has tried to login into your account and also user receives new password through message and mail.

V. METHODS USED FOR GENERATION OF HONEYWORDS

1. CHAFING METHOD:

The chaffing approach in general offers no provable guarantee that the honeyword generation procedure Gen is flat. This particularly true if the user chooses her password in a recognizable manner. The success of chafing depends on the quality of the chaff generator; the method fails if an adversary can easily distinguish the password from the honeywords [7].

2.TAKE-A-TALE METHOD:

The take-a-tail method of the next section fixes the problem of poorly-chosen password tails by requiring new passwords to have system-chosen random password tails. If the user picks the last three characters of her pass- word randomly, then tail-tweaking is impossible to reverse- engineer—an adversary cannot tell the password from its tweaked versions, as all tails are random. Otherwise, an adversary may be able to tell the password from the honey- words: in the following list, which is the likely password?

57*flavors, 57*flavrbn, 57*flavctz

3.PASSWORD MODEL:

Our second method generates honeywords using a probabilistic model of real passwords; this model might be based on a given list L of thousands or millions of passwords and perhaps some other parameters.[7] (Note that generating honeywords solely from a published list L as honeywords is not in general a good idea: such a list may also be available to the adversary, who could use it to help identify honeywords.) Unlike the previous chafing methods, this method does not necessarily need the password in order to generate the honeywords, and it can generate honeywords of widely varying strength.

4. HYBRID METHOD:

It is possible to combine the benefits of different honey- word generation strategies by composing them into a "hybrid" scheme. As an example, we show how to construct a hybrid legacy- UI scheme that combines chaffing-by-tweaking-digits with chaffing-with-a-password-model. We assume a password- composition policy that requires at least one digit, so that tweaking digits is always possible [7].

VI. SYSTEM FLOWCHART:

A flowchart is a type of diagram that represents an algorithm or process, showing the steps as boxes of various kinds, and their order by connecting them with arrows. This diagrammatic representation illustrates a solution to a given problem. Process operations are represented in these boxes, and arrows; rather, they are implied by the sequencing of operations. Flowcharts are used in analysing, designing, documenting or managing a process or program in various fields.

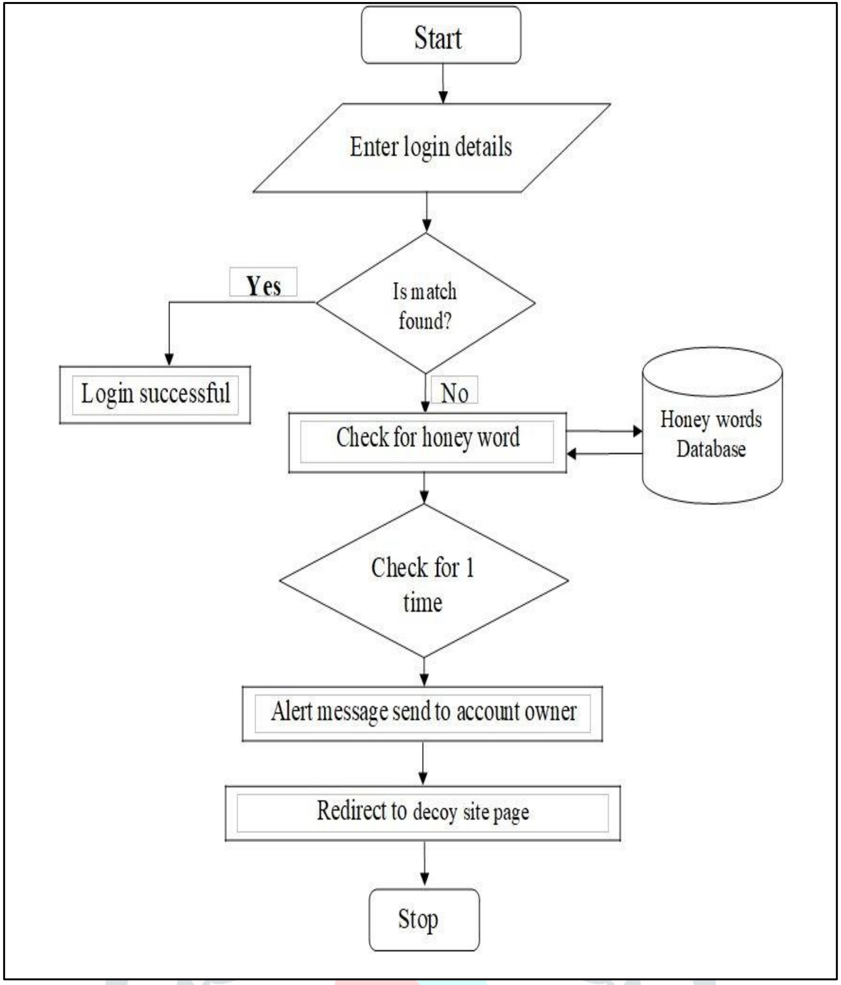
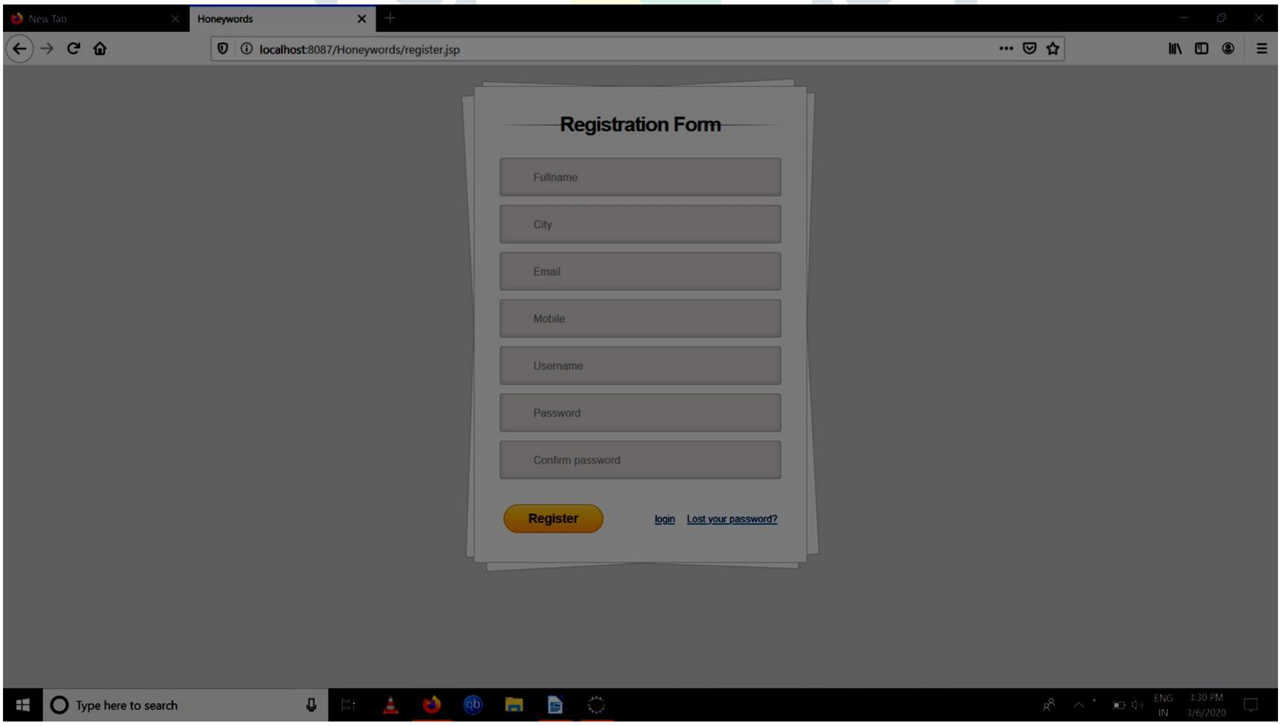


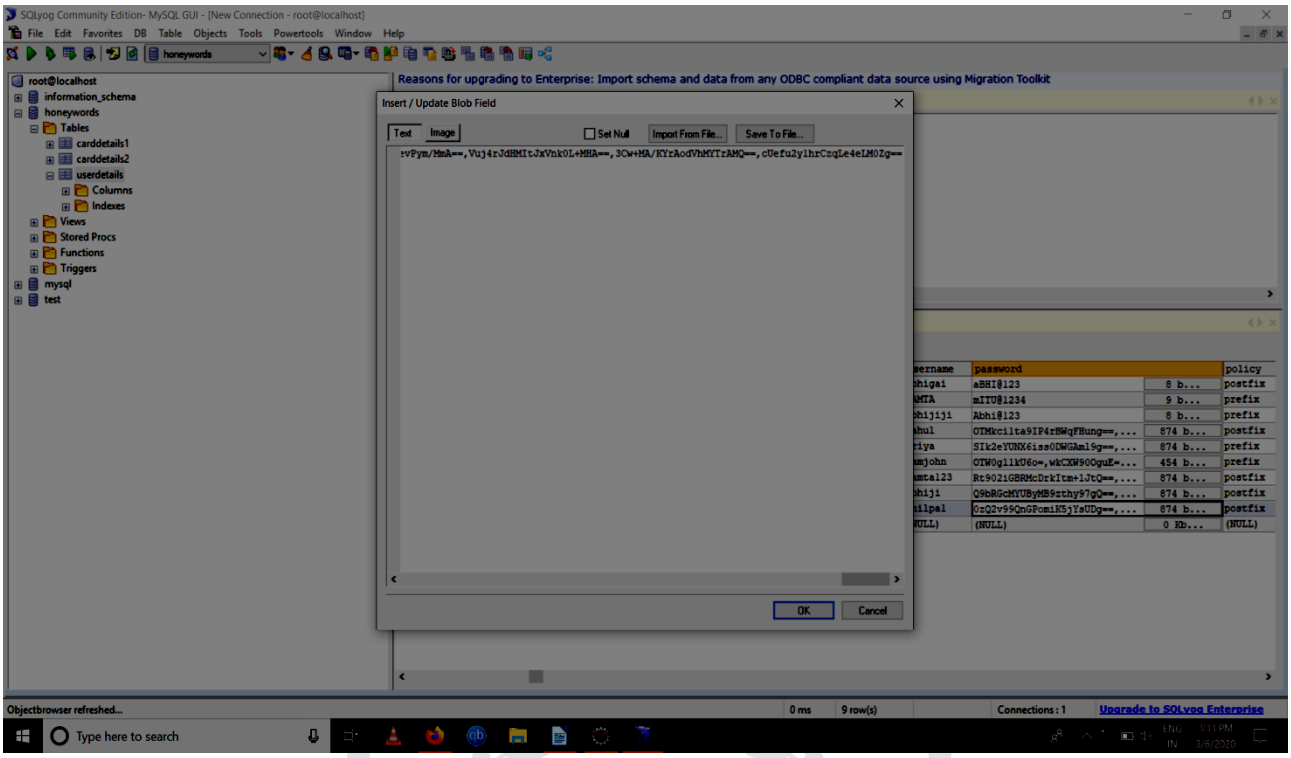
Figure: System flowchart

VI. RESULTS AND DISCUSSION:

1. Registration form:



2. Honeywords Generation:

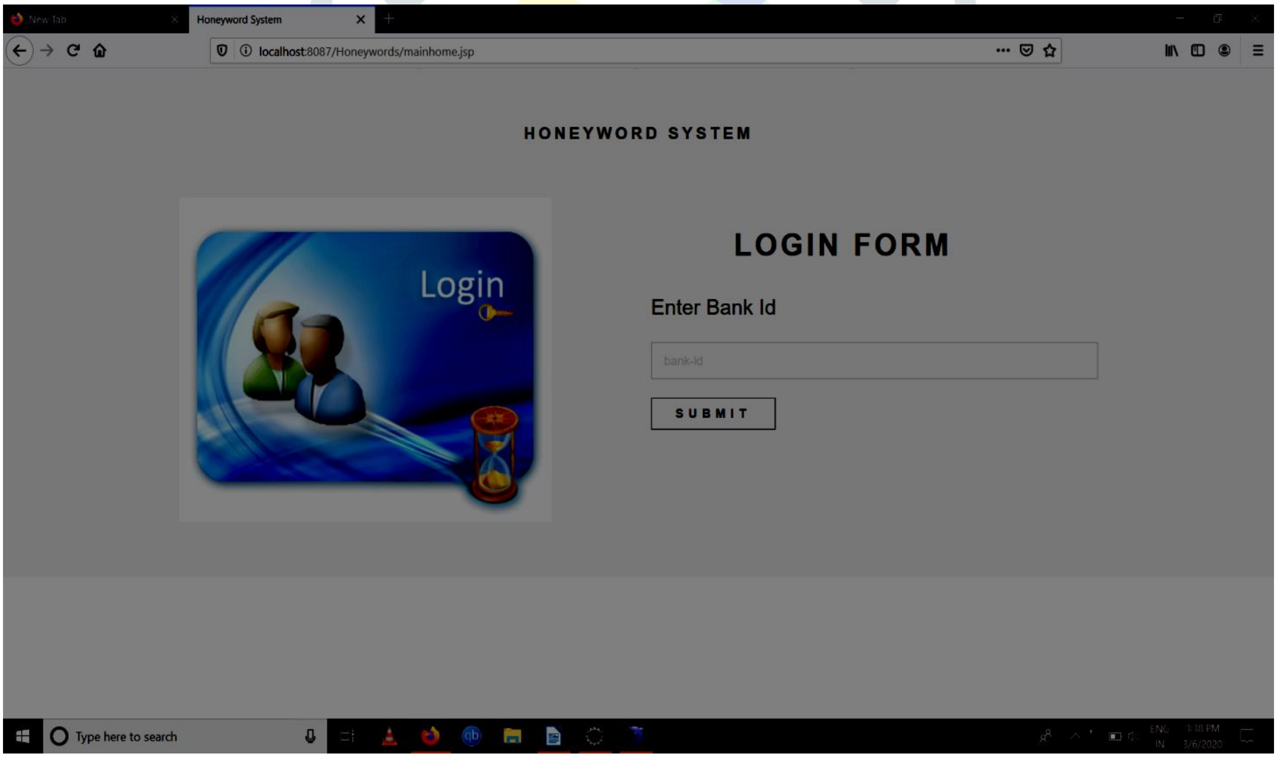


Reasons for upgrading to Enterprise: Import schema and data from any ODBC compliant data source using Migration Toolkit

```
:vPym/MmA==,Vuj4rJdHMItJxVnk0L+MHA==,3Cw+MA/KYrAodVhMYTrAMQ==,cUefu2ylhrCzqLe4eLM0Zg==
```

sername	password		policy
bhigai	aBHI@123	8 b...	postfix
AMTA	mITU@1234	9 b...	prefix
bhijiji	Abhi@123	8 b...	prefix
ahul	OTMkcilta9IP4rBWqFHung==,...	874 b...	postfix
riya	SIk2eYUNX6iss0DWGAml9g==,...	874 b...	prefix
amjohn	OTW0gllkU6o=,wkCXW90OguE=...	454 b...	prefix
amta123	Rt902iGBRMcDrkItm+lJtQ==,...	874 b...	postfix
bhiji	Q9bRGcMYUByMB9zthy97gQ==,...	874 b...	postfix
ilpal	0zQ2v99QnGPomiK5jYsUDg==,...	874 b...	postfix
NULL)	(NULL)	0 Kb...	(NULL)

3. Fake Login Page:



localhost:8087/Honeywords/mainhome.jsp

HONEYWORD SYSTEM

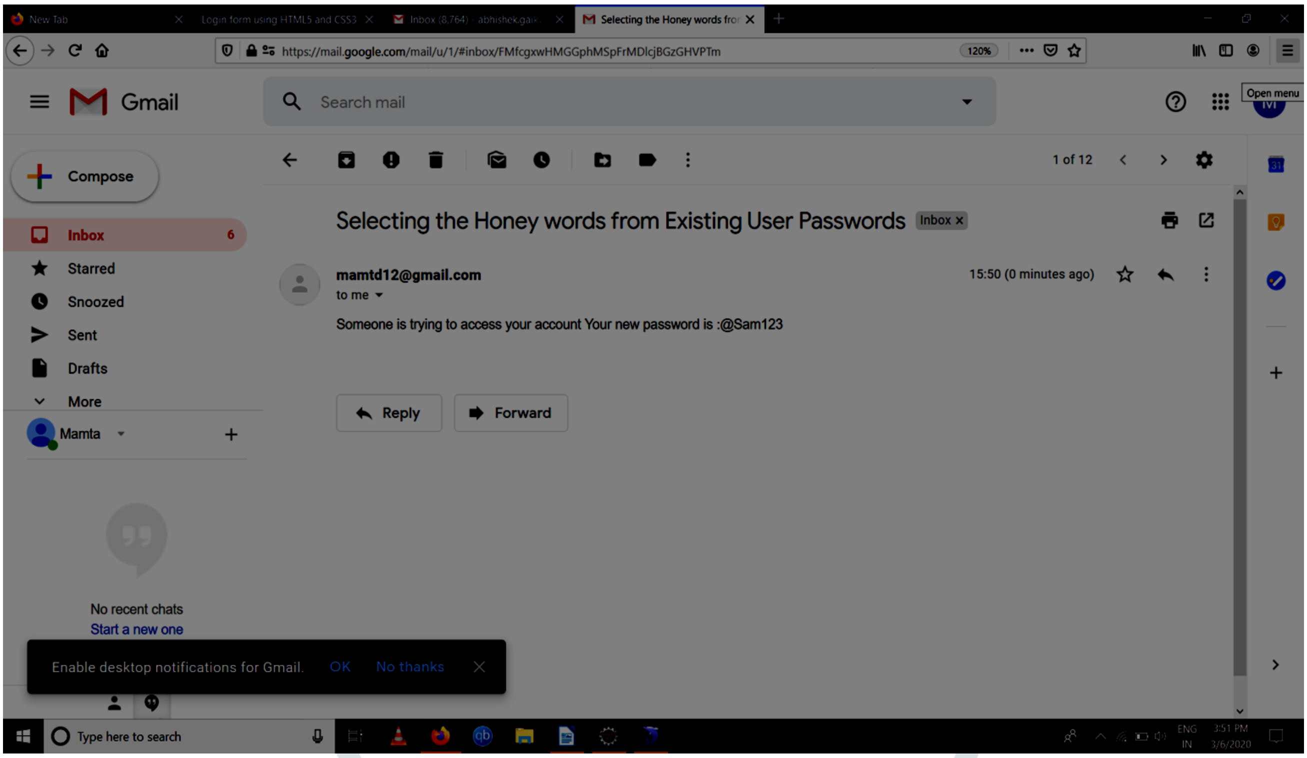
LOGIN FORM

Enter Bank Id

bank-id

SUBMIT

4. **Notification is sended to user through mail:**



Selecting the Honey words from Existing User Passwords Inbox ×

mamtd12@gmail.com
to me
15:50 (0 minutes ago)

Someone is trying to access your account Your new password is :@Sam123

Enable desktop notifications for Gmail. OK No thanks

VII. CONCLUSION:

Password security has been always an interesting challenge in security of various areas using passwords. Honeywords based authentication can provide several advantages over password based system. The big difference between the traditional password based system and when honeywords are used is that a successful attack does not give the attacker confidence that can log in into the system successfully without being detected. In this study, we present novel honeywords generation method which requires much less storage space and it can also reduce the majority of the drawbacks such as prevention from shoulder sniffing, brute force attacks, password attacks of the existing honeywords generation techniques.

VIII. RERFRENCE:

[1] M. Weir, S. Aggarwal, B. de Medeiros, and B. Glodek, “Password Cracking UsingProbabilistic Context-Free Grammars,” in Security and Privacy, 30th IEEE Symposium on.IEEE, 2009, pp. 391–405.

[2] National Conference Organized by Indira Gandhi P. G. Kelley, S. Komanduri, M. L.Mazurek, R. Shay, T. Vidas, L. Bauer, N. Christin, L. F. Cranor, and J. Lopez, “Guess again (andagain and again): Measuring Password Strength by Simulating Password-cracking Algorithms,”in Security and Privacy (SP), 2012 IEEE Symposium on. IEEE, 2012, pp.

[3] J. Bonneau, “The science of guessing: Analyzing an anonymized corpus of 70 millionpasswords,” in Security and Privacy (SP), 2012 IEEE Symposium on. IEEE, 2012, pp. 538– 552.

[4] Genc, ZiyaAlper and Mehmet SabirKiraz, “Examination of a New Defense Mechanism: Honeywords,” IACR CrptologyePrint Archive, p. 696, 2013.

[5] “www.webeopdia.com/term/s/shoulder–surfing.html (last access October, 2013).”

[6] http://clam.rutgers.edu/~birget/grPssw/srgp.pdf

[7] A. Juels and R. L. Rivest, “Honeywords: MakingPassword-cracking Detectable,” in Proceedings of the 2013ACM SIGSAC Conference on Computer & CommunicationsSecurity, ser. CCS ’13. New York, NY, USA: ACM, 2013, pp.145–160. [Online]. Available:

http://doi.acm.org/10.1145/2508859.2516671

[8] D.Florencio and C.Herley,”A Large-scale Studyof web Pass-word Habit,” in proceeding of the 16th international conference on World Wide Web. ACM Press,2007,pp.657-666.

[9] J. Bonneau, C. Herley, P. Oorschot, and F. Stajano, “The quest to replace passwords: Aframework for comparative evaluation of web authentication schemes,” in Proc. IEEE S&P2012, pp. 553–567.

[10] H. Bojinov, E. Bursztein, X. Boyen, and D. Boneh, "Kamouflage: Loss-resistant Password Management," in Computer Security–ESORICS 2010. Springer, 2010, pp. 286–302.

[11] D. Wang, H. Cheng, P. Wang, X. Huang, and G. Jian, "Zipf's law in passwords," IEEETrans. Inform. Foren. Secur, vol. 12, no. 11, pp. 2776–2791, 2017.

[12] J. Ma, W. Yang, M. Luo, and N. Li, "A study of probabilistic password models," in Proc.IEEE S&P 2014, pp. 689–704.

[13] I. Erguler, "Achieving flatness: Selecting the honeywords from existing user passwords,"IEEE Trans. Depend. Secure. Compute, vol. 13, no. 2, pp. 284–295, 2016.

[14] S. M. Satre and V. P. Jadhav "QoS-Oriented Adaptive Expedient Broadcast Routing for Hybrid WirelessNetwork," IEEE Advances in Electrical, Electronics, Information, Communication and Bioinformatics-2016 International Conference (AEEICB - 2016), ISBN- 978-1-4673-9745-2, Feb. 2016.

[15] Shankar M. PatilKomal D. Jadhav, Jogendra.N.Nandanwar, "Security for Multimedia Content in Cloud using double Encryption",International Journal of Creative Research Thoughts (IJCRT), Volume 6, Issue 2, April 2018.