7th International Conference on Recent Trends in Engineering, Science & Management
Genba Sopanrao Moze College of Engineering, Balewadi-Baner, Pune (ICRTESM-17)
01st-2nd April 2017, www.conferenceworld.in ISBN: 978-93-86171-12-2

PASSWORD PREVENTION TECHNIQUE TO REDUCE CYBER ATTACKS USING HONEYWORD BY HYBRID GENERATION ALGORITHM

Prof. Priyanka Mane[1], Kalpana Sharma[2] , Parvati Karhale[3]

[1,2,3]*Information Technology, Genba Sopanrao Moze Collage of Engineering, Balewadi –Pune (India)*

ABSTRACT

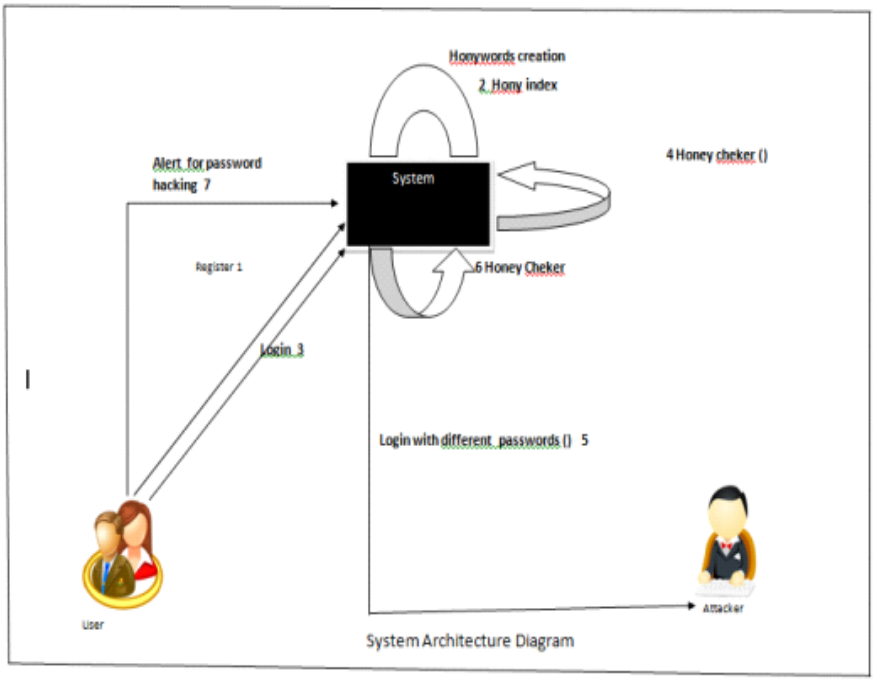
This paper focus on the user security issue which is very critical and all system that deals with sensitive data of user has to provide strong security services. So, HoneyWords is a approach that secure user passwords with honeywords(decoy password) .For Honeywords generation we have used Hybrid algorithm. Attacker will not able to differentiate actual user password and honeywords. Hence, attacker will try different combination of password and user will be alerted for the same.

Keywords: Honey Words, Secure Passwords.

I. INTRODUCTION

Leak of password files is a major security problem that has affected millions of users and companies like bank data, company's data, LinkedIn, Honey and Adobe since exposed passwords make the user's target of many possible forgery-attacks. For this, there are two issues that should be concerned to overcome these security problems: First, passwords should be secured by taking desired precautions and storing them with their hash values computed through some other complex mechanisms. Hence, for an adversary it must be difficult to invert hashes to get plaintext passwords. The second point is that a safe system should detect whether the password file exposure incident happened or not to take proper actions.

ISBN: 978-93-86171-12-2



System Architecture Diagram

Combination of Simple word generation algorithm and Random function algorithm is

Hybrid Algorithm: Combining both above mentioned algorithm together.

Algorithm 1 : Simple Model algorithm for honey words Generation

procedure SIMPLEMODEL(L)

w random(L) .

d length(w) .

honey word(1) w(1) .

for j 2 to d do

if mod1 then

w random(L), honey word(j) w(j) word

ISBN: 978-93-86171-12-2

else if mod2 then

w random(L),

else

honey word(j) <- w(j)

end for

end procedure

Algorithm 2: Model algorithm for honey Random Generation

Inputs: words between [1-26 letter],

chose the random functions and its limit.

Random value generation.

Convert the random ascii value to its corresponding letter.

Output:

Random cipher text of original password.

Step 1 =Honey pots creation: fake user account

1]For each account honey index set is created like

Xi =(xi;1; xi;2; : : : ; xi;k); one of the elements in Xi is the correct index (sugar index) as

ci

2]create two password file file f1 and file f2

· F1 Store username and honeywords set <hui,xi) Where hui is honey pot account

· F2 keeps the index number and the corresponding hash of the password(create the

hash of the password), < ci;H(pi) >

Step 2=Generation of honeywords set

Gen(k; SI) -> ci;Xi

Generate Xi

1]select xi randomly selecting k-1 numbers from SI and also randomly picking a number ci

SI .

2] ui; ci pair is delivered to the honey checker and F1, F2 files are updated.

Step 3=Honey checker

Set: ci, ui

Sets correct password index ci for the user ui

Check: ui, j

Checks whether ci for ui is equal to given j

2. LITERATURE SURVEY

[1]. Avanish Pathak, "An analysis of various tools, methods and systems to generate fake accounts for social media," in Northeastern University Boston, Massachusetts December 2014.

In this Paper, To study the mechanisms used by modern account creation programs and their overall effectiveness. This study analyzes the different ways in which these tools create fake accounts and how they manage to circumvent existing security measures. It also helps to get an insight into what websites do in order to handle fake accounts, both during the account sign-up process, as well as and after the fake accounts have been created. Tests that reveal the number of accounts that can be fabricated prior to an OSN's countermeasures and their longevity due to the inability of the OSN's detection mechanisms are presented. This study highlights whether major websites are following security best practices to mitigate

fake account creation, and if existing security countermeasures are effective.Major websites provide critical functionality to billions of Internet users every day.

Disadvantages:

Social spam campaigns can have a variety of objectives. The most obvious uses are promoting shady e-commerce sites, foreign pharmaceuticals, surveys, and scams i.e. the same kinds of content found in email spam. Social spam may also be used to spread malicious social applications that leverage the graph structure of OSNs propagate from friend to friend To give an idea of the scope of this problem: 8% of 25 million URLs that are posted to Twitter point to sites that are known for phishing, scams, or malware. Unfortunately it has been shown that 90% of the visitors click on these malicious links before they are blacklisted by OSNs. Another spam phenomenon that is unique to social networks is the manipulation of trending topics.. Thus, attackers often use fake accounts to try and create their own trending topics, or inject spam content into existing trending topics.

[2]. R. Butler and M.J. Butler "An Assessment of the Human Factors Affecting the Password Performance of South African Online Consumers" in Proceedings of the Eighth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2014),

In this Paper, Research suggests that passwords breaches are frequently the result of poor user security behavior. Internationally, poor password behavior among users is common. The objective of this study was to investigate the password performance of South African online consumers and to understand the factors contributing to poor password performance. A web-based survey was designed to determine online consumers' perceptions of their password-related knowledge, measure their ability to apply safe practices and asses their motivational levels to employ secure practices. Poor password practices among South African online consumers were evident from this study. Using a construct for password performance, this analysis indicated a deficiency in the knowledge, capability and motivation of users

Disadvantages:

Human computer interface and relevant education, training and awareness programs are required to protect password it time consuming and not 100 % correctness that password Wright and secure.Human users are the 'weakest link' in password control

IV. FIGURES AND TABLES

- User Registration:

This is registration page. In this system first step is user registration then user login.

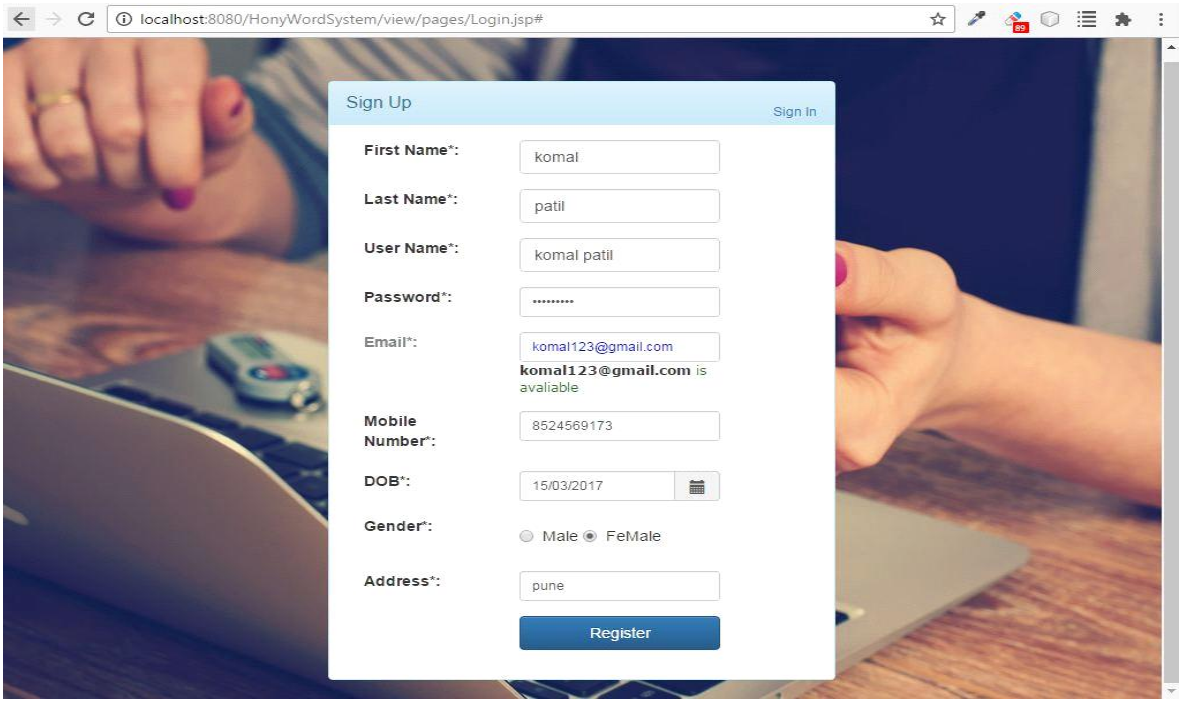
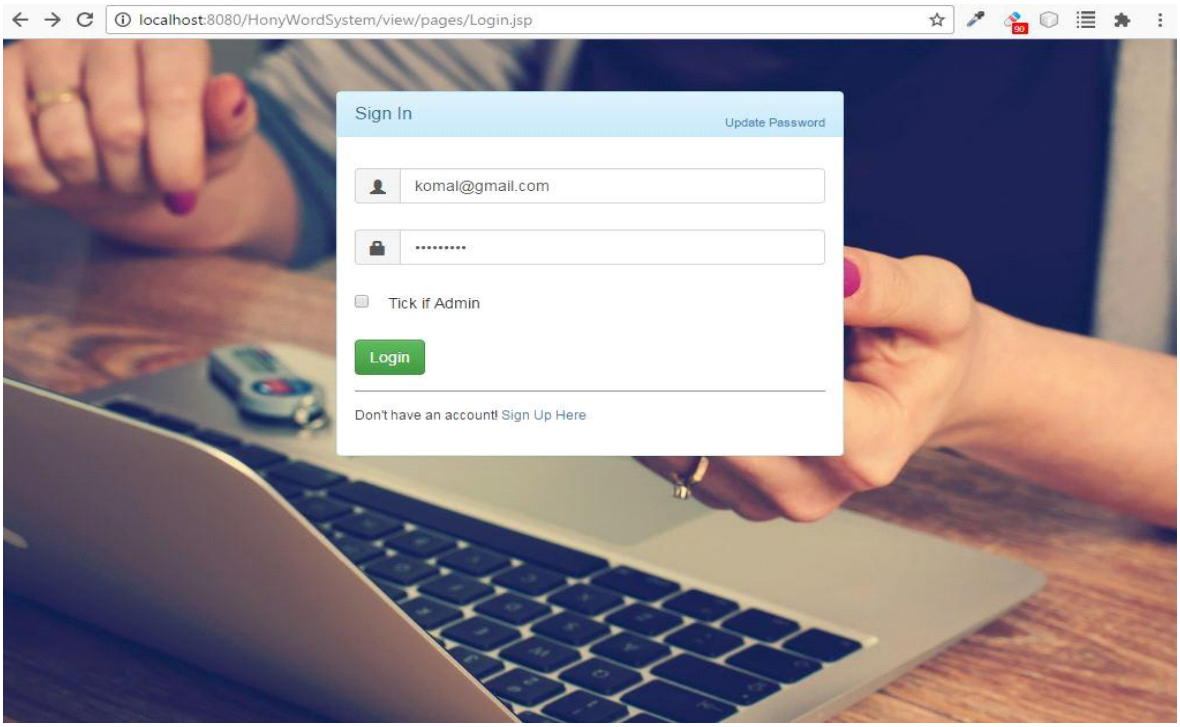


Fig1.User Registration.

- User Login:

This is User Login Page. In this System First Registered User is Login, then after Login other System is work. In this System, If username or password is correct then Successfully Login Otherwise Login Failed.

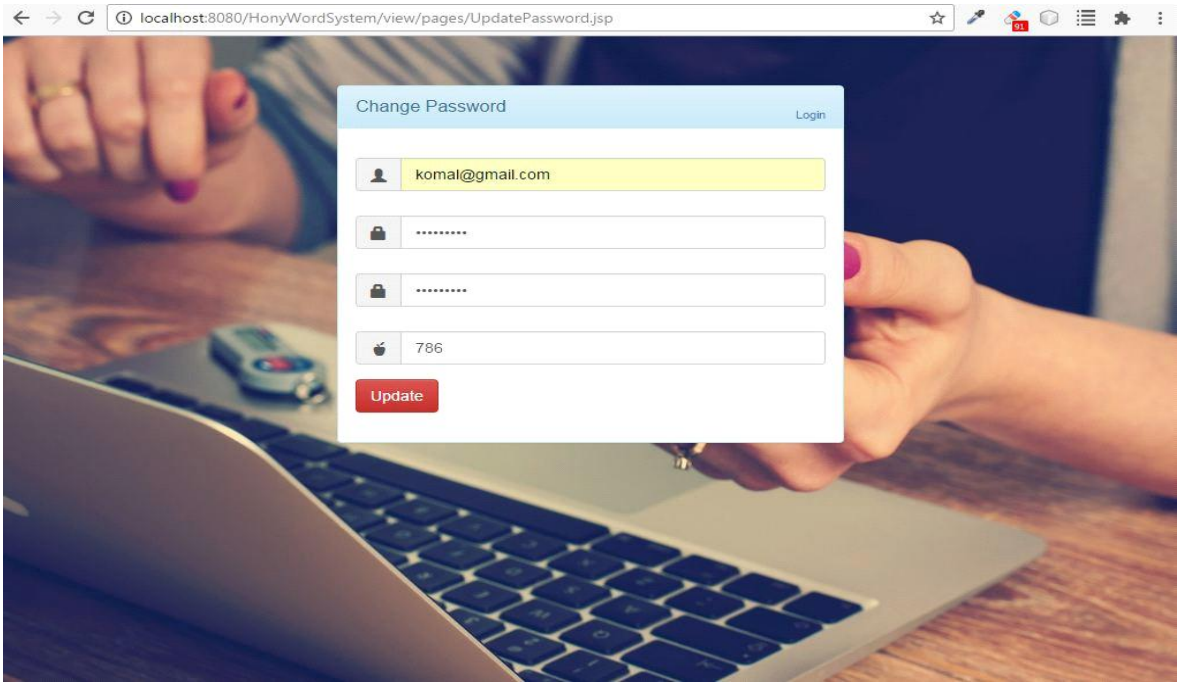
ISBN: 978-93-86171-12-2



3.Update Password:

This Page is the Update Password. IF User Change the password then go to the Update Password Option.

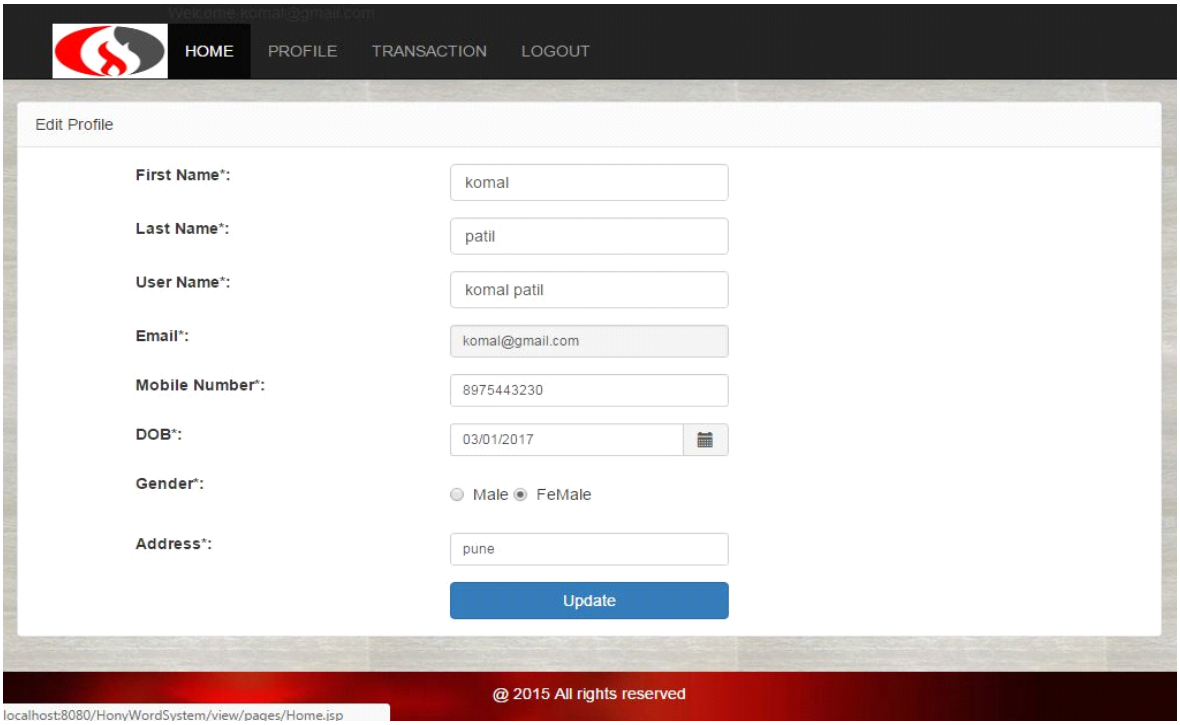
ISBN: 978-93-86171-12-2



4.Update User Profile:

This is User Update Profile Page. Suppose User Change the Profile Then select the Profile Option and Successfully created the Profile.

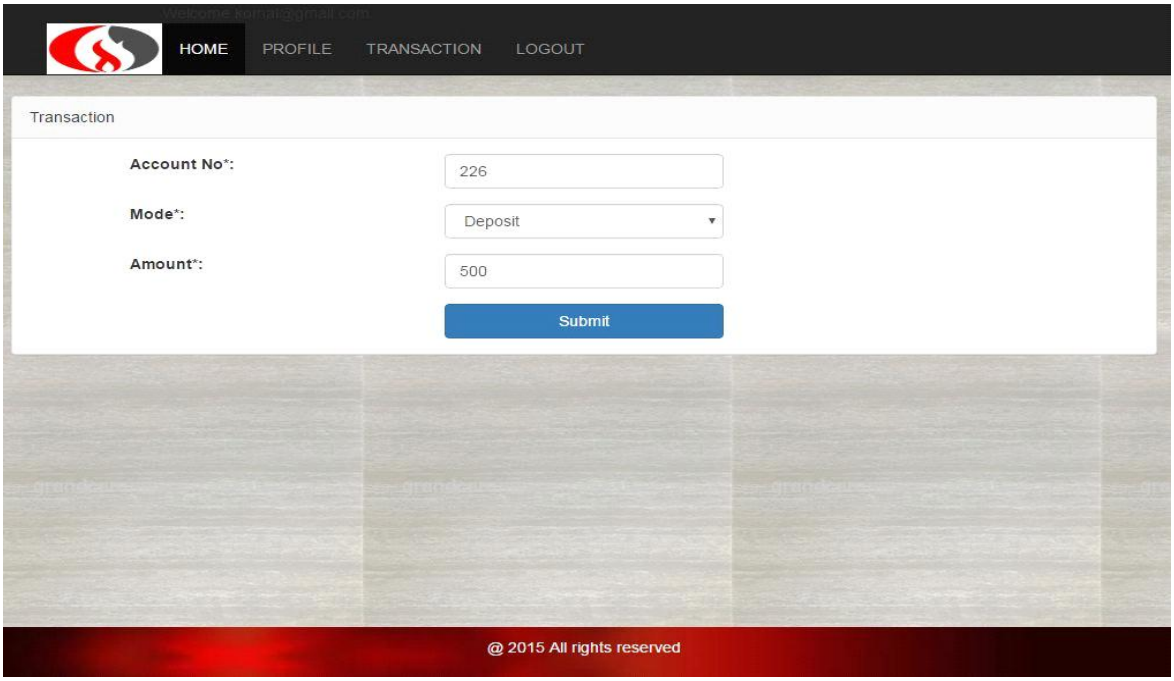
ISBN: 978-93-86171-12-2



5.Deposite Money:

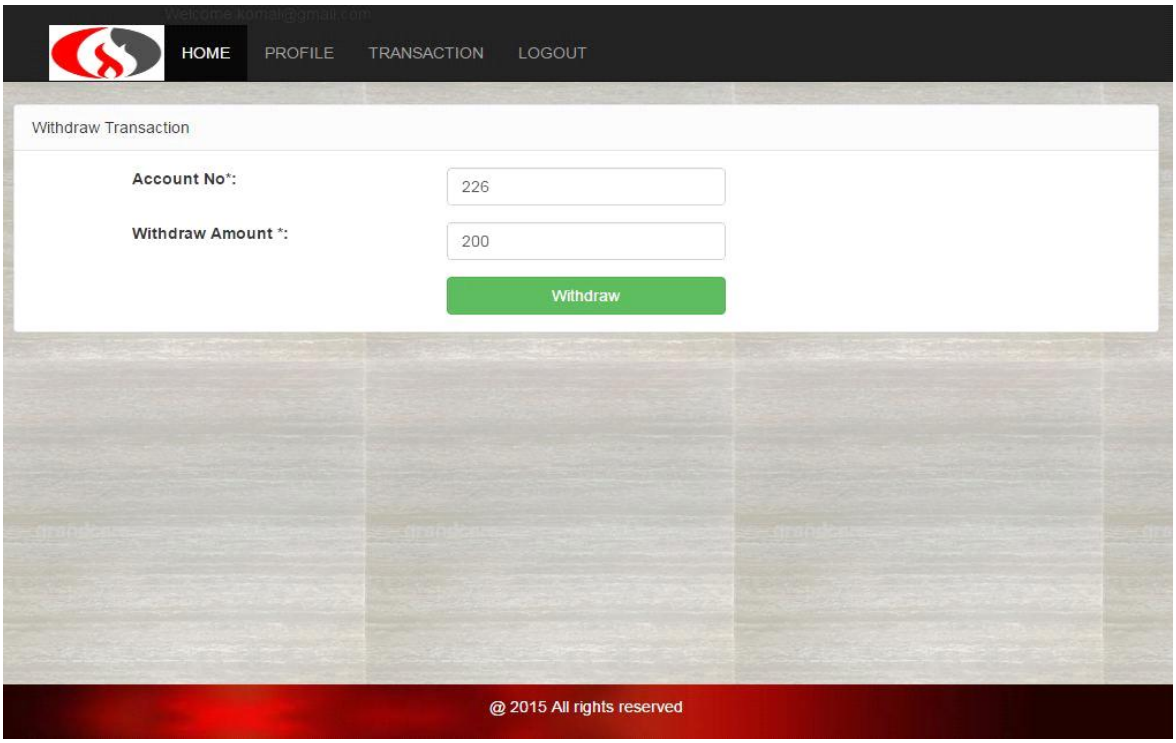
This is Deposited Money Page. User Deposited the money in our System.

ISBN: 978-93-86171-12-2



6.Withdraw Money:

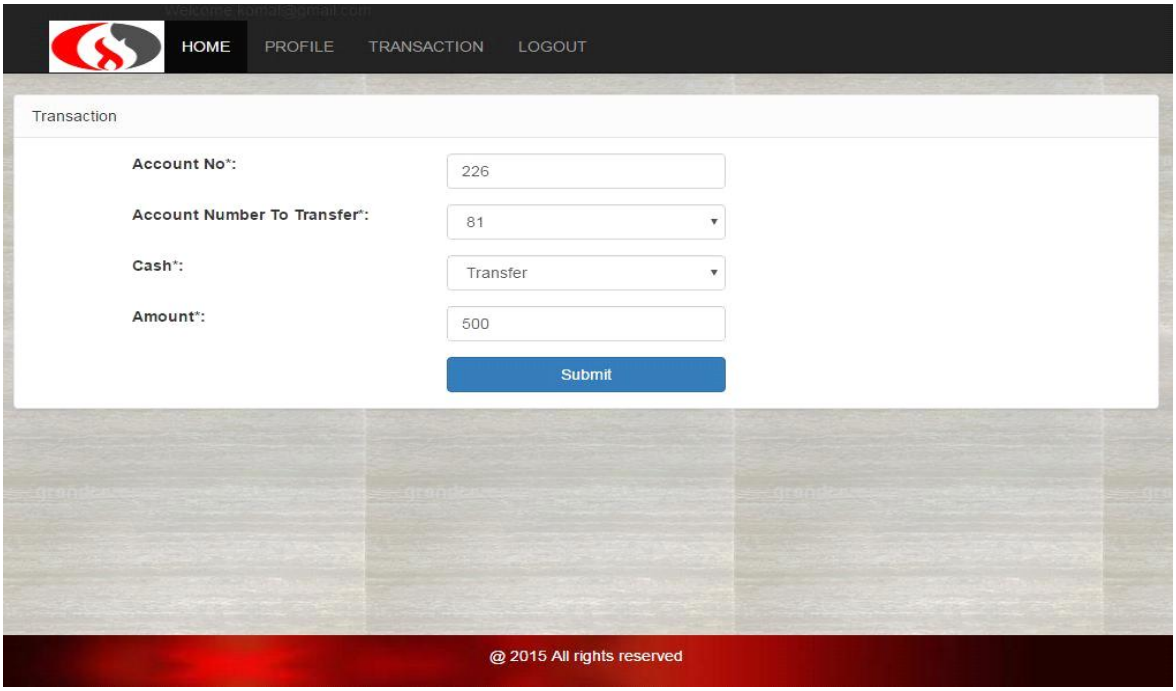
This is Withdraw Money Page. User Withdraw the Money in our System.



ISBN: 978-93-86171-12-2

7.Transfer Money:

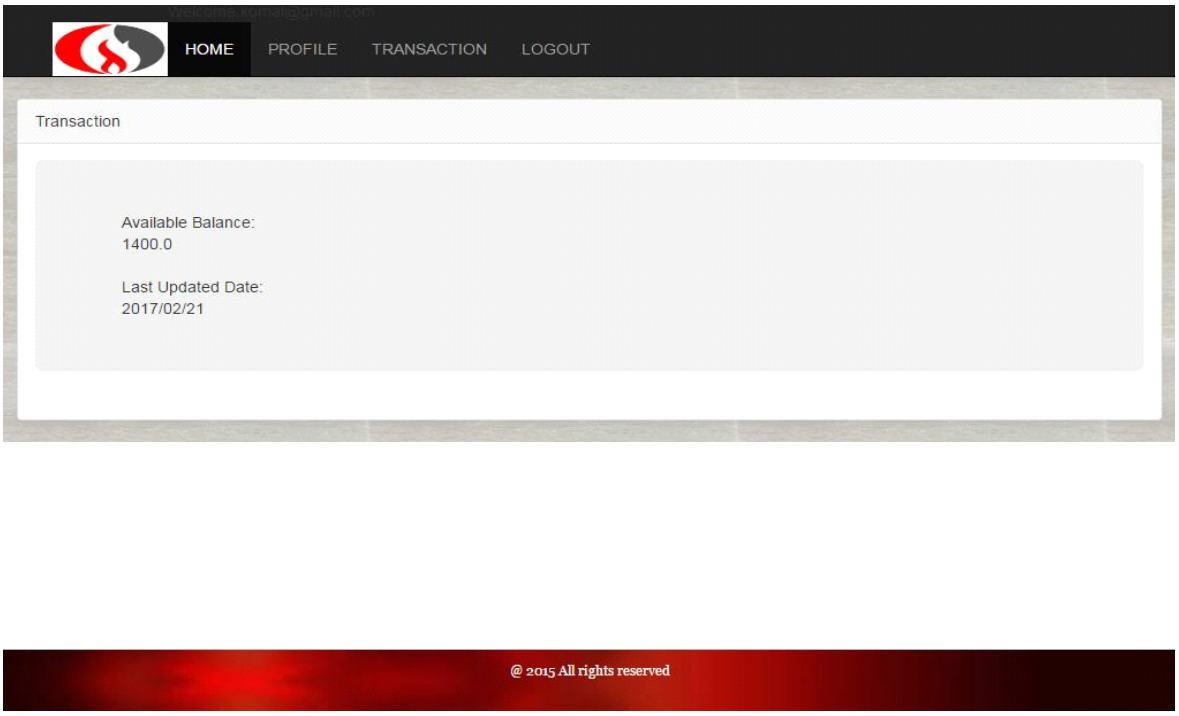
This is Transfer Money Page. In this Page Successfully Transfer Money From One Account To Another Account.



8.Check Balance:

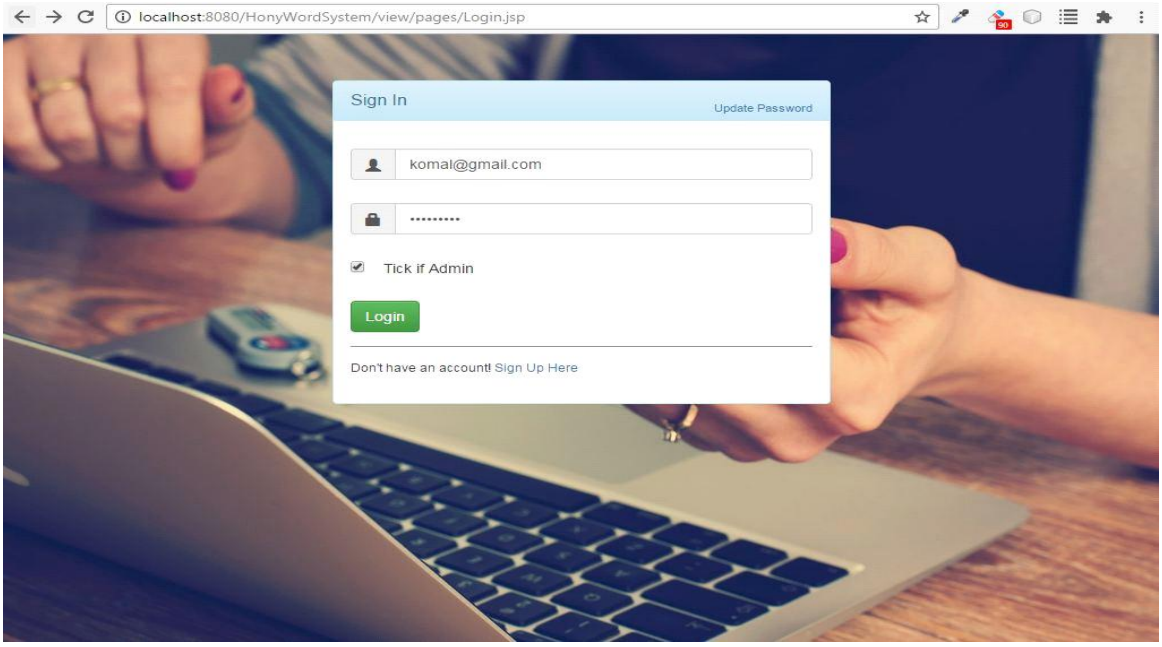
After Money Transfer Successfully Check the Account Balance and Balance Information Give in Your Mail Address.

ISBN: 978-93-86171-12-2



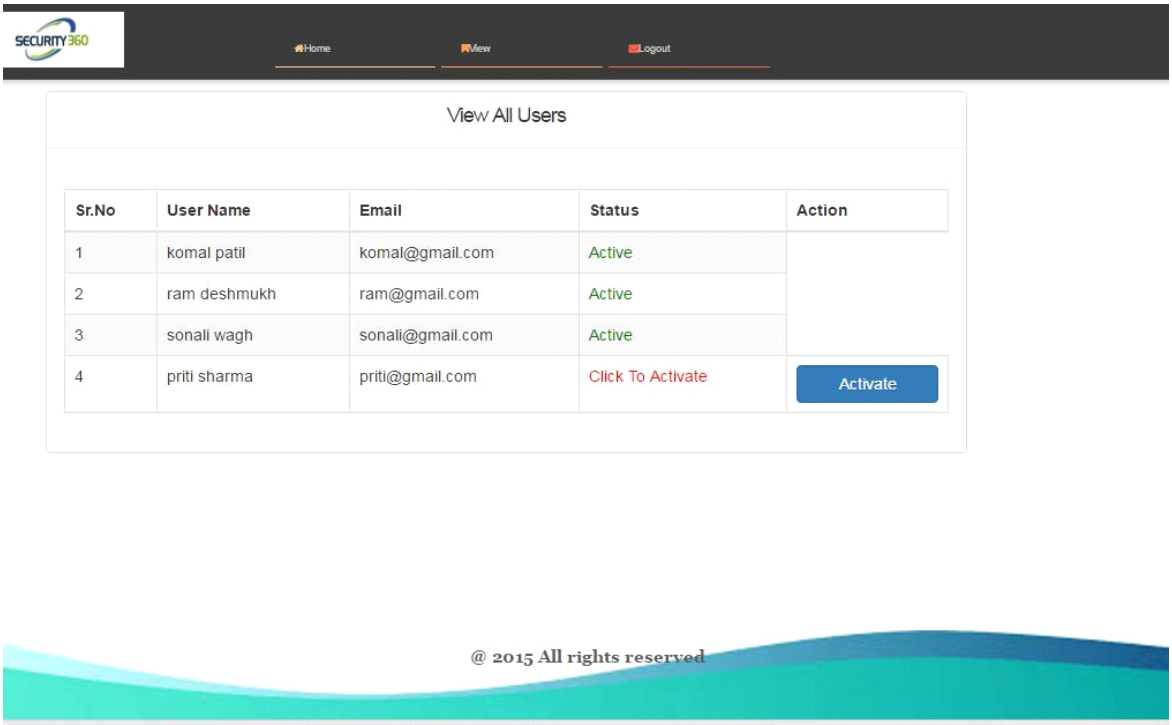
9.Admin Login:

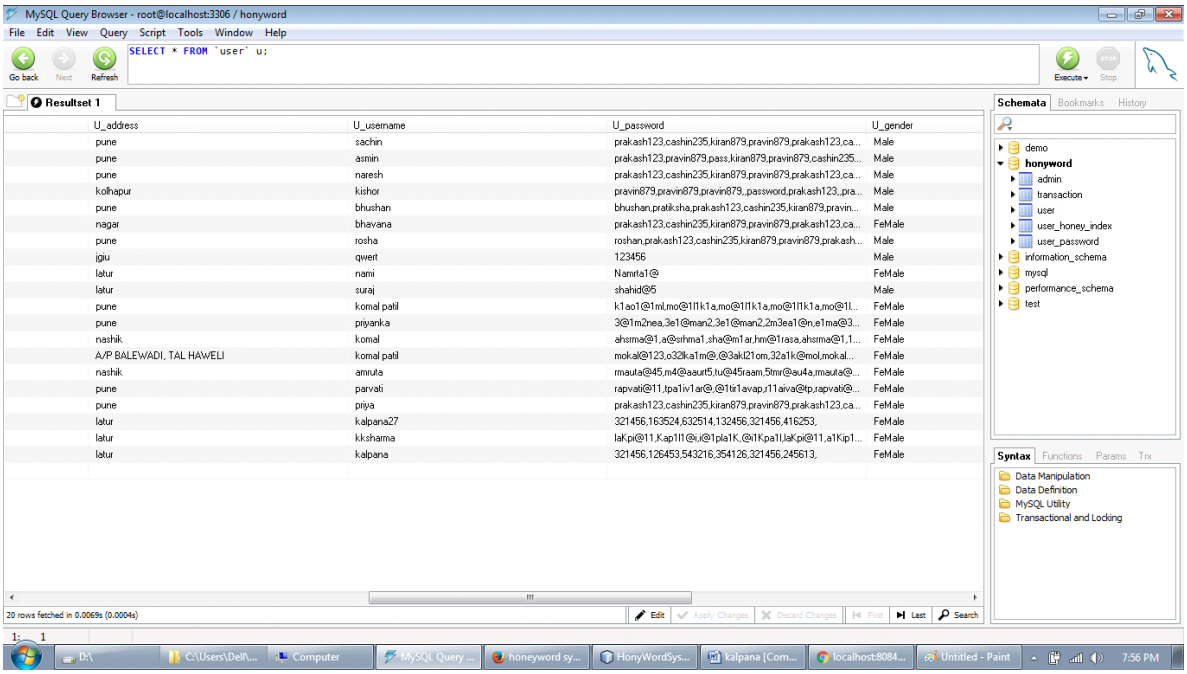
This is Admin Login Page. In this System First Admin User is Login, then after Login Open the Admin Panel.



10.View Users:

This is View User Page. In This Page User Activate or Deactivate options are handle the System Admin.





Result Analysis:

1.DOS Resistance:

the chaffing-with-tweakingmodel may suffer from a DoS attack, due to predictability of the honeywords. Unlikely, the chaffing-with-a-passwordmodel provides resistance against such an attack, because honeywords are generated by using a list of passwords such that they may be independent from the correct password.

2. Flatness:

it is presented that reuse rate of weaker passwords is higher than those of stronger passwords, since the stronger ones are usually created for higher-security sites e.g. banking accounts.

the chaffing-with-tweakingmodel may leave traces to an adversary in distinguishing the genuine password from the honeywords.

ISBN: 978-93-86171-12-2

Method	DOS Resistance	Flatness	
Tweaking	Weak	Weak	
Password Model	Strong	Strong+	
Our Model	Strong	Strong++	

Comparison with hybrid generation Model

V. CONCLUSION

We have analyzed the use of the honeyword system and addressed a number of faults that need to be handled before successful release of the scheme. In this way, we have figured out that the strength of the honeyword directly relied on the generation algorithm Finally, we have presented a new way to make the hybrid algorithm algorithm for generating honeywords .

REFERENCES

[1]. D. Mirante and C. Justin,"Understanding Password Database Compromises," Dept. of Computer Science and Engineering Polytechnic Inst. of NYU, Tech. Rep. TR-CSE-2013-02, 2013.

[2]. F. Cohen, "The Use of Deception Techniques: Honeypots and Decoys," Handbook of Information Security, vol. 3, pp. 646–655, 2006.

[3]. K. Brown, "The Dangers ofWeak Hashes," SANS Institute InfoSec Reading Room, Tech. Rep., 2013.

[4]. C. Herley and D. Florencio, "Protecting financial institutions from brute-force attacks," in SEC'08, 2008, pp. 681–685.

[5]. M. Weir, S. Aggarwal, B. de Medeiros, and B. Glodek, "Password Cracking Using Probabilistic contextfree.