Secure of web Account using personal-PCFG

[1]Pratima Nikam, [2]Vaishnavi mahajan, [3]kalyani padmawar
[1,2,3]Computer Department,
Sinhgad Institute of Technology & Science,
Pune, India - 411041..

Abstract:

For security of the data as well as maintaining privacy over the internet, authentication is very important. Usually the password which is used by the user is small password, easy to memorize or password which can be guessed easily. People use personal information as their password for easy memorization. In this paper, we analysis the various passwords from the leaked dataset to research their personal information for finding the relation between them and the password. We use Probabilistic Context-Free Grammars (PCFG) method with semantic-rich method to propose Personal-PCFG method in which it will find if there is any correlation between password and personal information. This method will help us to crack the password much faster than any other method which increases the chances of successful password crack. To protect user’s from this type of attacks we use distortion function. This paper also provide security by notifying authenticated user if someone is trying to access the account from another or trying to attempt their account by entering wrong password.

Keywords: *Cyber security, Information security, PCFG, Distortion function*

Introduction

Network security are also called the InfoSec i.e. information Security. Information security has number of strategies to extract the process Tools. It is very necessary to prevent, detect document and find the threats to digital and non-digital information. Information securities are responsible for a set of business processes that provide security to information assets. It secures all the business and personal information.

Information security threats come in large quantity in different forms. Some of the most common threats today are software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion. Most people have experienced software attacks of some sort. Viruses, worms, phishing attacks, and Trojan horses are a few common examples of software attacks. The theft of intellectual property has also been an extensive issue for many businesses in the IT field. Identity theft is the attempt to act as someone else usually to obtain that person's personal information or to take advantage of their access to vital information. Theft of equipment or information is becoming more prevalent today due to the fact that most devices today are the main objective is to help user to choose strong password which will be difficult for the hacker to crack password. User mostly use easy password for its memorization. Mostly this password contains personal information which makes it vulnerable. Hacker can get user information from various sources like Facebook. This information can be used by hacker for guessing password.

The prime focus of this paper is to help user to get strong password. Mostly people use their information in passwords. Hackers can get the peoples information from various sources like Social Networking Site. This information can be used to guess user passwords. If the user's password does not contain personal information then it is difficult for the hacker to crack the password.

Problem Definition:

After R&D of various hacked account most of the passwords were containing user information. This password can be guessed easily by hackers as they can get user information from various sources. Hacker can be your friend or colleague or stranger who knows about you. They get your information from known sources like social networking sites etc. So, our focus is to provide strong password to the authenticate user.

Objectives

- To protect users account from various attacks.
- To increase password security.
- To improve online authentication systems.
- To provide Strong password to the user.

System design:

Data Flow Diagram 0:

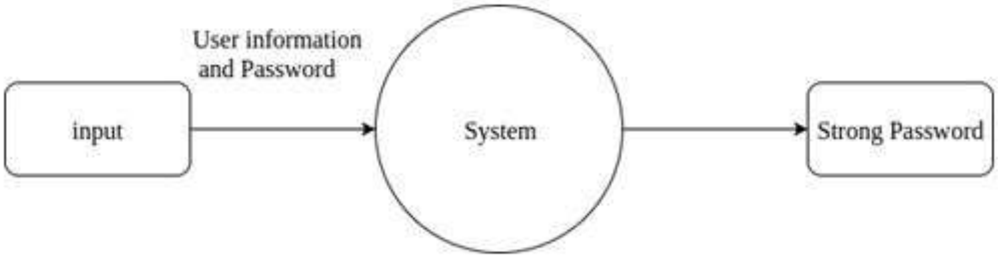


Fig :- DFD 0

Data Flow Diagram 1:

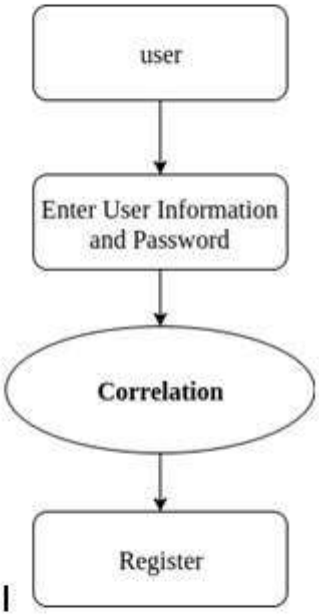
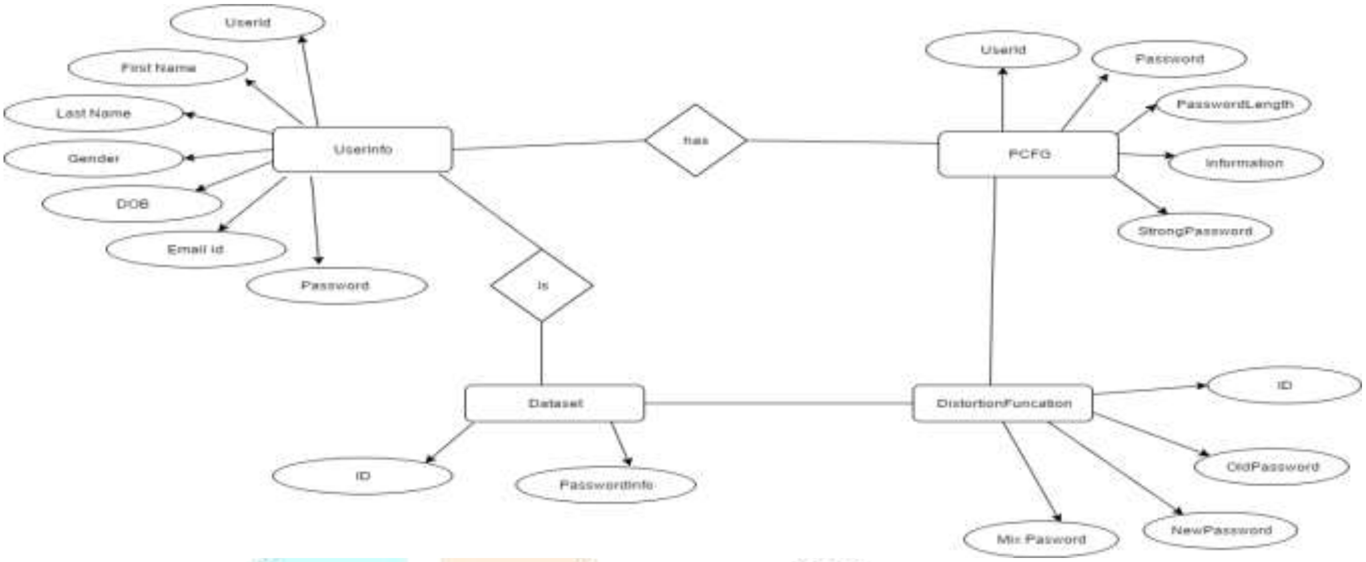
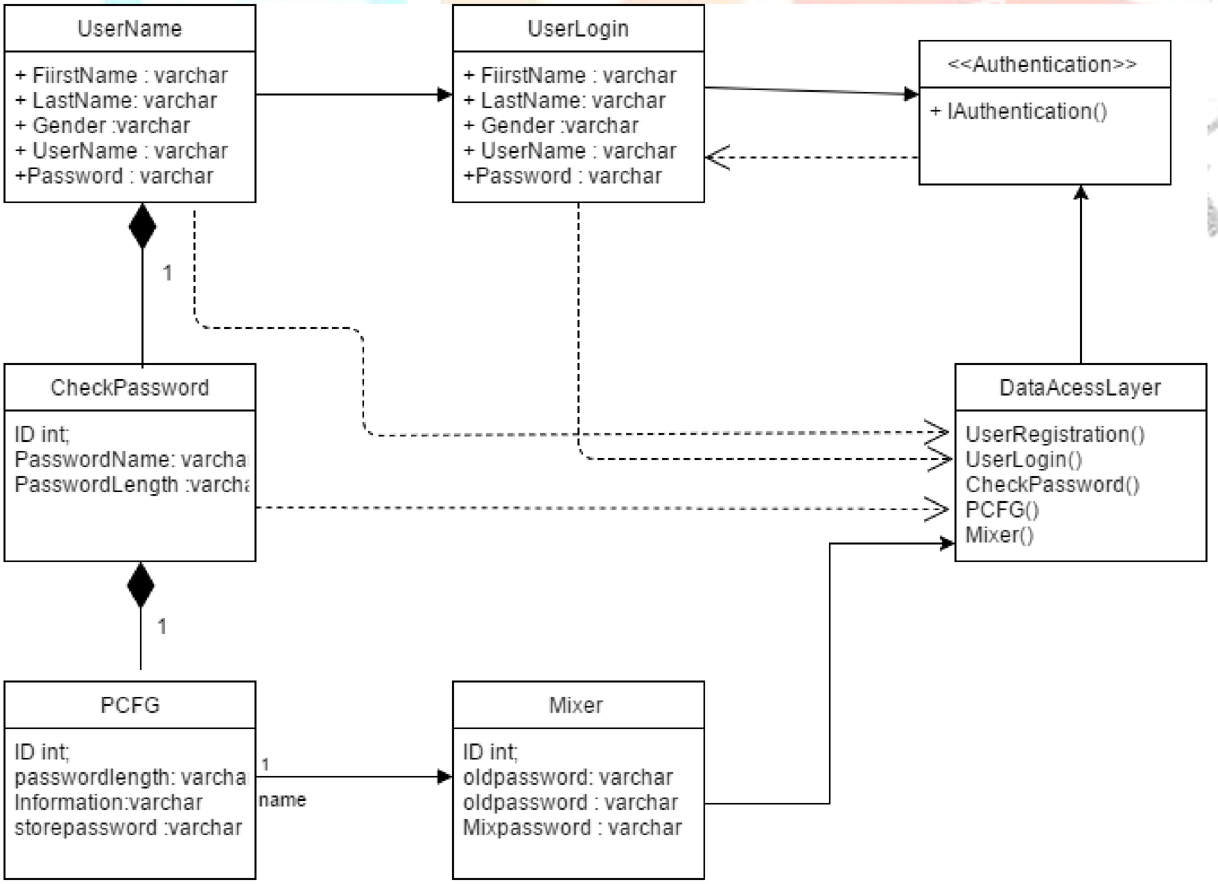


Fig DFD 1

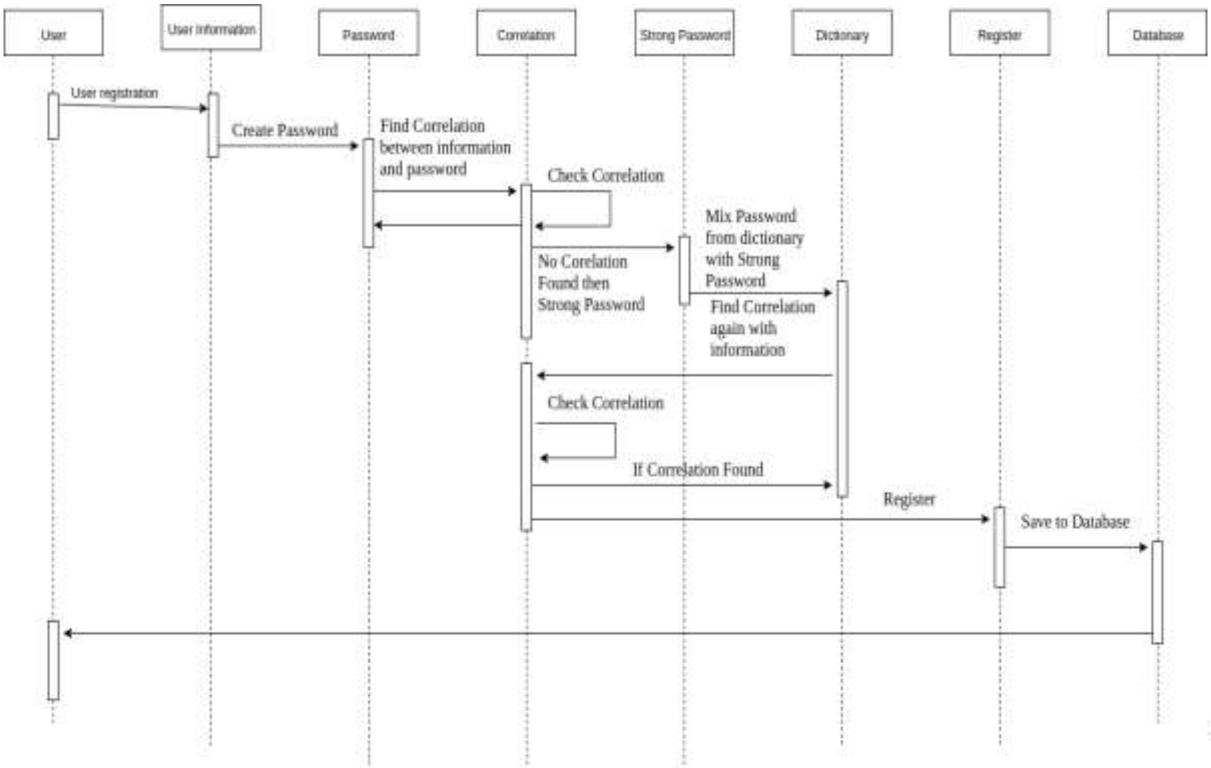
ER Diagram:



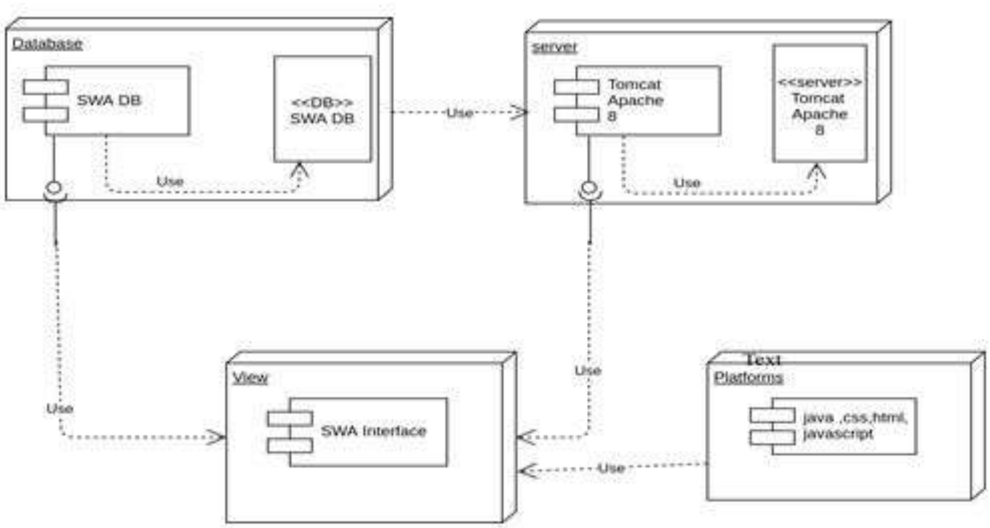
Class Diagram:



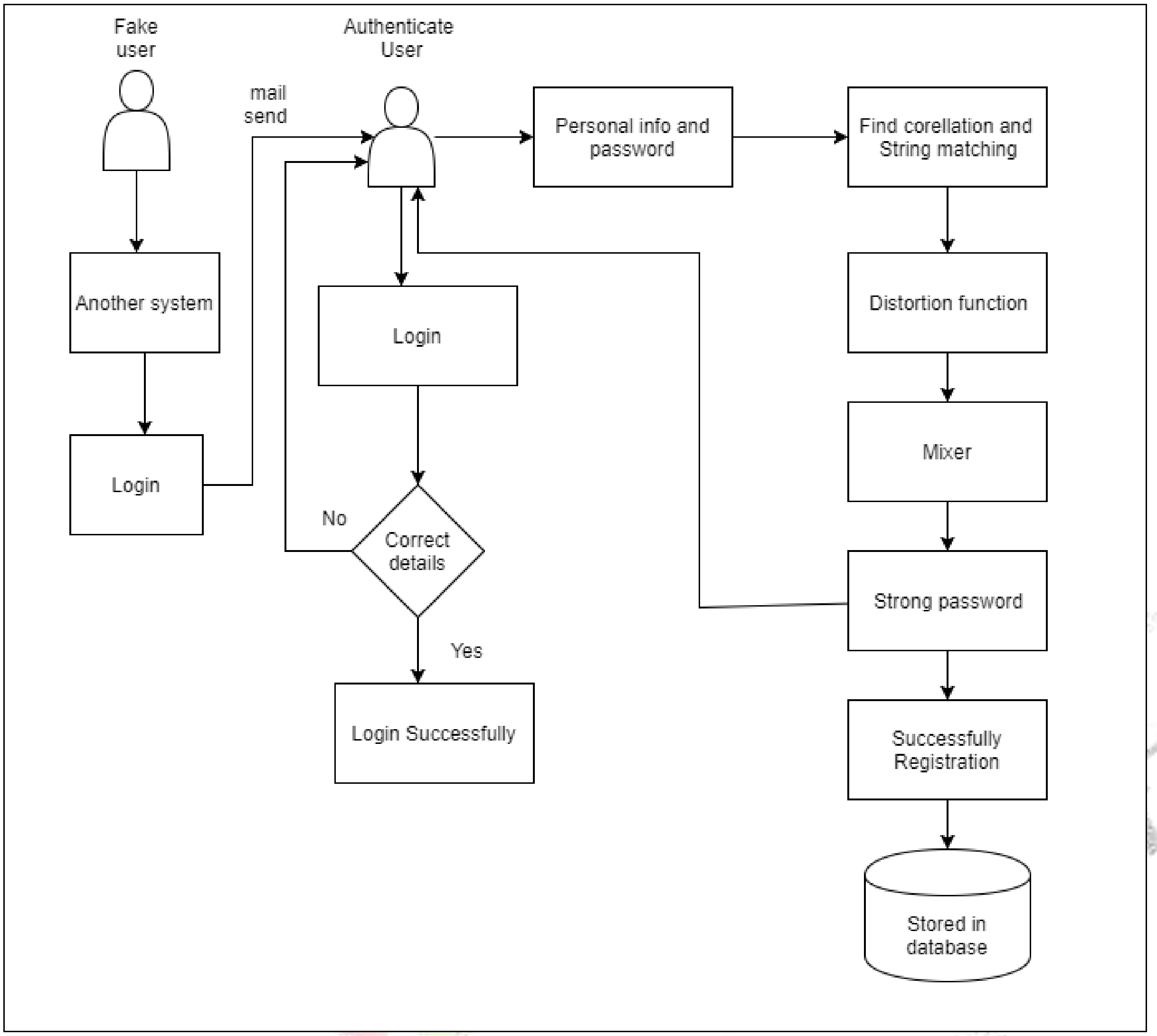
Sequence Diagram:



Deployment diagram



SYSTEM ARCHITECTURE



Above fig shows system flow. In this system user enter the personal information and enter the Username and Password. First the system search the password and find its correlation PCFG with user's personal information and if find it show notification to the user for week password, if user enter the password which not related to user's info then the system uses the distortion function and add some character to the password and shuffle the password and make them strong and send to the user and user will be successfully register. Also this system will give notification mail to the authenticate user if some fake user is trying to access their account.

Related Works

2.1 The science of guessing: analyzing an anonymized corpus of 70 million password

Introduction: - in this paper authors user the large no of data set .This large data set motivates a thorough statistical treatment of estimating guessing difficulty by sampling from a secret distribution. In place of previously used metrics such as Shannon entropy and guessing entropy, which cannot be estimated with any realistically sized sample, and partial guessing metrics including a new variant of guesswork parameterized by an attacker's desired success rate? This requires retiring traditional, inappropriate metrics such as Shannon entropy and using entropy which don't model realistic attackers and aren't approximable using sampled data.

- Technique: - privacy-preserving technique use.
  - Advantage :-

    1. The system use the different language for creating the password

    2. This system uses privacy-preserving approach to collecting a password distribution for statistical Analysis.

  - Disadvantage :-

    1. This system is very complex and time consuming system.

    2. Natural experiment on actively encouraging stronger passwords seems to have made little difference.

2.2. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schema

Introduction:- this authors to give the proposals to replace text passwords for general-purpose user authentication on the web using a broad set of twenty-five usability, deploy ability and security benefits that an ideal scheme might provide. The scope of proposals we survey is also extensive, including password management software, federated login protocols, graphical password schemes, cognitive authentication schemes, one-time passwords, hardware tokens, phone-aided schemes and biometrics.

Techniques: - usability-deplorability-security (USD)

Advantage: - 1.It is use of Negligible-Cost-per-User, in terms of technology.

Disadvantage: -

1. This system only providing the suggestion to improvement password.

2.3 Two-Factor Data Security Protection Mechanism for Cloud Storage System

Introduction:-Short and efficient Certificate Based Signature (CBS) scheme to improve level of trust in cloud environment. This scheme was need one group element for public key and the signature size and it reduced the public information to one group elements for each and every user in the cloud environment. This key size is smaller than the PKI based signature scheme because it needs one group element for generation of public key and the another group element is needed for the certificate

Techniques: - Efficient Certificate Based Signature (CBS) Methodology

Advantage:-

1. The solution not only enhances the confidentiality of the data, but also offers the revocability of the device so that once the device is revoked; the corresponding cipher text will be updated automatically by the cloud server without any notice of the data owner.

2. The cloud server cannot decrypt any cipher text at any time.

Disadvantage:-

1. This system performance is very low and complex.

HYPOTHESES

1- We are developing a system that helps a user to get the strong password.
2- The system matches the password and personal information by using personal-PCFG and provides the strong password.
3- This system provides the security in such a way that authenticate user will get the notification if someone is trying to access the account.
4- Strong password is stored in encrypted format in database

LIMITATION OF THE STUDY

1. Users have to memorize their password once it sends to users email by link.
2. Strong password will displayed for 3o sec.
3. Link will be accessible only one time to user.

DESIGN OF THE STUDY

Propose Algorithm:-

```
1. Input :-  i(info, pass) -  collection and information and password

2. Output :-- Strong password

3. For (i=0;i< info; i++)

4. For (j=0;j<pass; j++)

5. Info = collection of information

6. Pass = collection password

7. If (correlation == Password) then

8. Pass is week

9. Else

10. Pass is storage

11. End if

12. End for
```

```
13. End for
14. If (strong password! = 0)
15. Using distortion (strong password)
16. Else
17. Password is empty
18. End if
```

SAMPLE OF THE STUDY

This paper is based on security, as we know how security is important; many users' passwords get leaked or hacked by using their personal information from source like internet, Facebook etc. Therefore we proposed this concept in which the user's password does not match with their personal information and provide strong password on a link, only authenticate user can access that link.

TOOLS UDED

Software Requirement:

➢ Operating System	:	windows 8 and above..
➢ Application Server	:	Tomcat5.0/6.X
➢ Language	:	Java
➢ Front End	:	HTML, JSP
➢ Database	:	MySQL

- **Hardware Requirement:** The hardware design of the system includes designing the hardware units and the interface between those units.

➢ Processor	-	Pentium –III
➢ RAM	-	1 GB (min)
Hard Disk	-	20 GB

STATISTICAL TECHNIQUE USED

We have used the PCFG in which it find the correlation between the password and personal information and distortion function is used in which it add some character from the password dataset and shuffle them and send to the user.

Experiment Result:

Results demonstrate that the password does not match with personal information and also it provides the strong password to the registered user and also it successfully stored the information of user to the database in the encrypted form so that hacker will not able to access them even from database. In this system while registering a link is send to user to access the password in which the user can get the strong password and also while accessing the link user is asked to enter the security answer and question to enter, if its correct then only user can access the link. This user can access the link for only 30 sec and user can access this link only one time.so in this way we have provided security to keep the password safe and provide the strong password to the user by using PCFG and distortion function. Overall this system provides the total security to the user.

Future scope:

The experiment results show that this system can be used in future for the purpose of security where the system will give the strong password to the user and also show the alert message if the users enter the week password. And also notify the user if another user trying to access their account. Overall this system work as secured system and in future it will be every useful for the user.

Acknowledgment: (optional)

It gives us great pleasure in presenting the preliminary project report on ‘Secure of web Account using personal-PCFG ’.

I would like to take this opportunity to thank my internal guide Prof…..for giving me all the help and guidance I needed I am really grateful to them for their kind support. Their valuable suggestions were very helpful.

I am also grateful to Prof……, Head of Computer Engineering Department, *Computer Department, Sinhgad Institute of Technology & Science, Pune*, for his indispensable support and suggestions.

In the end our special thanks to Prof. …….for providing various resources such as laboratory with all needed software platforms,

Pratima Nikam

Vaishnavi Mahajan

Kalyani Padmawar

(B.E. Computer Engineering).

Conclusion:

Our Coverage based qualification disclosure on the use of personal information in the password and that shows how vulnerable our password is. We developed a Personal-PCFG based on PCFG which guesses more accurate password and personal information correlation. Our method is faster than any other system in password cracking and also strong password are send to authenticated user by a link in which system will ask the security question, depending on the answer system will provide the strong password and this link is available only for one time. Also distortion functions are effective in defending against personal-information –related and semantic aware attacks.

Reference:

[1] D. Balzarotti, M. Cova, and G. Vigna. Clearshot: Eavesdropping on keyboard input from video. In IEEE Security & Privacy, 2008.

[2] J. Bonneau. The science of guessing: analyzing an anonymized corpus of 70 million passwords. In IEEE Security & Privacy, 2012.

[3] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentications chemes. In IEEE Security & Privacy, 2012.

[4] J. Bonneau, S. Preibusch, and R. Anderson. A birthday present every eleven wallets? The security of customer-chosen banking pins. In Financial Cryptography and Data Security. Springer, 2012.

[5] S. Boztas. Entropies, guessing, and cryptography. Department of Mathematics, Royal Melbourne Institute of Technology, Tech. Rep, 1999.

[6] J. Brainard, A. Juels, R. L. Rivest, M. Szydlo, and M. Yung. Fourthfactor authentication: somebody you know. In ACM CCS, 2006.

[7] C. Cachin. Entropy measures and unconditional security in cryptography. PhD thesis, Swiss Federal Institute of Technology Zurich, 1997.

[8] P. Cao, H. Li, K. Nahrstedt, Z. Kalbarczyk, R. Iyer, and A. J. Slagell Personalized password guessing: a new security threat. In ACM Proceedings of the 2014 Symposium and Bootcamp on the Science of Security, 2014.

[9] C. Castelluccia, A. Chaabane, M. D¨urmuth, and D. Perito. When privacy meets security: Leveraging personal information for password cracking. arXiv preprint arXiv:1304.6584, 2013.

[10] C. Castelluccia, M. D¨urmuth, and D. Perito. Adaptive password-strength meters from Markov models. In NDSS, 2012.