iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 Issue: IX Month of publication: September 2020

DOI: https://doi.org/10.22214/ijraset.2020.31437

Implementation Paper on BanCo – One platform for all your Transaction

Mr. Chaudhari Shubham[1], Mr. Kumbhar Nikhil[2], Mr. Galphade Abhishek[3], Mr. Thul Sameer[4], Prof. Deshpande Rashmi[5]
[1, 2, 3, 4, 5]Dr. D. Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune

Abstract: The new developments in the field of information technology offered the people growth, comforts and convenience, but there are many security and online transaction management related problems. First is we use many applications for online transaction, it's very difficult for managing various transaction information. To solve this here we develop online transaction management system Namely BanCo – one platform for all your transaction. Second is password hacking. Password files have got a lot of security problem that has affected millions of users as well as many companies. Password is generally 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 or each wrong password user and admin get notification.

Keywords*: Banking, Data Security, Honey words, Database.*

I. INTRODUCTION

The money transaction using mobile phone is one of the most important technological developments of our age. It has become the primary tool of people around the world for communication and business applications. The trend of global mobile phone usage increased from the year 2012 from 1.2 billion people to 4.5 billion people in 2019. There are many applications from the payment service providers that were developed for supporting mobile payments including. Examples of the application are Google pay, Phone Pay, Google Wallet, Paypal, and Paytm. However, most of the applications mentioned above use the traditional form transaction processing: one bill, one transaction. This may affect the performance potential of the mobile payment process and difficult to handle various transaction in one system. We implement Banco application i.e. one platform for all your money transactions.

II. LITERATURE REVIEW

In this section, we briefly review the related work on credit card fraud system and their different techniques.

1) *Mohammad Reza Nami:* factor in the future development of financial services industry, and especially banking industry. Growing international trading and problems in transferring money have motivated researchers to introduce a new structure. E-banking is such idea. Most of banks are using the Internet as a new distribution channel. This paper presents a through survey of e-banking describing definition, barriers, benefits from the customers', economy, and bank point of views, and main issues and challenges such as risk management and factors responsible for e-banking development. Finally, conclusion and future perspective of e-banking development will be discussed.
2) *LIU Rui-bo, SUN Li-hua:* The banking merger and acquisition (M&A) has become the focus of the fifth wave of global merger tide, followed by people's puzzle about whether there is a positive and sustainable performance of banking M&A. By sifting the current microscopic analytical method of banking M&A performance, we choose the adjusted case study law for an overall analysis of the case of Wing Hang Bank Ltd. purchasing Chekiang First Bank N.A. We draw a conclusion that the positive impact of M&A on improving bank efficiency and shareholder's value can be confirmed, so that the discrepancy between empirical results and the real M&A activities at present can be perfectly explained.
3) *Imran Erguler:* In this paper, they check the honey word system and present some remarks to highlight possible weak points. Also, they suggest an alternative approach that selects the honey words from existing user passwords in the system in order to provide realistic honey words a perfectly flat honey word generation method – and also to reduce storage cost of the honey word scheme.

4) *Lianying Zhao and Mohammad Mannan:* Using deception techniques (as in honeypots), they propose the user-verifiable authentication scheme (Uvauth) that tolerates, instead of detecting or counteracting, guessing attacks. Uvauth provides access to all authentication attempts; the correct password enables access to a legitimate session with valid user data, and all incorrect passwords lead to fake sessions.
5) *Patrick Gage Kelley, Saranga Komanduri, Michelle L. Mazurek, Richard Shay, Timothy Vidas Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Julio Lopez:* In this paper We develop an efficient distributed method for calculating how effectively several heuristic password- guessing algorithms guess Passwords and Honey word generation method i.e. chaffing-with tweaking provide some possible improvements which are easy to implement and introduce an enhanced model as a solution to an open problem also overcomes almost all the drawbacks of previously proposed honey word generation approaches.

III.EXISTING APPROACH

A lot of work has been done in this field thanks to its extensive use and applications. This section mentions some of the approaches that have been implemented to achieve the same purpose. These works are mainly differentiated from the technique for banking systems.

A. In existing system you can add your account details with various applications but you can show this details with this specific application.
B. You can’t merge all transaction details in one application.
C. Generally in many companies and software industries store their data in databases like ORACLE or MySQL or may be other. So, the entry point of a system which is required user name and password are stored in encrypted form in database. Once a password file is stolen, by using the password cracking technique it is easy to capture most of the plaintext passwords.
D. System doesn’t provide the security

IV. PROPOSED APPROACH

In the proposed solution, at the time a user sends a login request and simultaneously create honey words. Those factors are used to identify the customers at the initial step. Based on initial identification a personal profile is created and stored in the database.

Based on the mentioned factors the users are compared with the personal profile which is in the system database, from the next login attempt onwards. If there are no unauthorized access detected and all the factors are compatible with the profile, access will be allowed. But if there are some unauthorized access, based on the security mechanism will be carried out. This security mechanism includes an automated email notification system.

You can view all transaction details in one application using this authorization system.

A. System Diagram

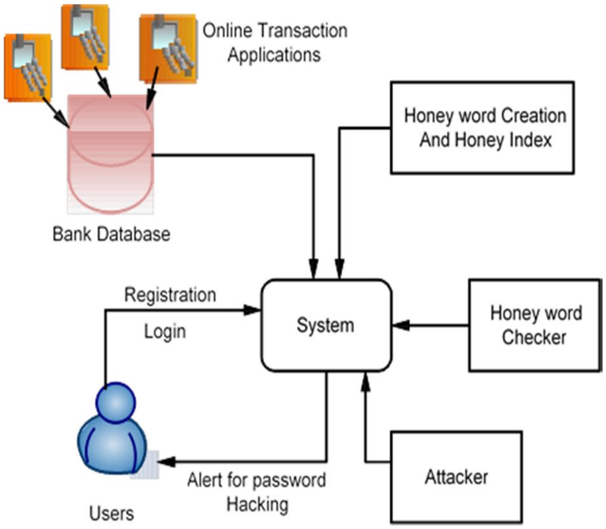
Online Transaction Applications
Honey word Creation And Honey Index
Bank Database
Registration
Login
System
Honey word Checker
Users
Alert for password Hacking
Attacker

Fig 1. System Architecture

B. Algorithm

```
1) Take input as a Position(pos) and Password(pass).
2) Reverse the Password.
3) Apply for loop from 1 to 20.
4) if(i == position) realPassword[i] = pass;hashPassword[i] = generatorHash(pass);
5) elserealPassword[i] = replace(password1); hashPassword[i] = generatorHash(pass);
6) passResult.put("real", realedPassword); passResult.put("hash", hashedPassword); passResult is HashMap.
```

V. RESULTS AND DISCUSSION

Experiments are done by a personal computer with a configuration: Intel (R) Core (TM) i3-2120 CPU @ 3.30GHz, 4GB memory, Windows 7, MySQL 5.1 backend database and Jdk 1.8. The application is web application used tool for design code in Eclipse and execute on Tomcat server.

VI. CONCLUSION

We present a standard way to deal with making sure about and blend exchange from different applications in the one framework and We propose checking information access designs by profiling client conduct to decide whether and when a malevolent insider illicitly gets to somebody's records in a framework administration. Bait archives put away in the framework close by the client's genuine information additionally serve assessors to distinguish ill-conceived admittance. When unapproved information access or presentation is suspected, and later checked, with challenge inquiries for example, we immerse the malignant insider with counterfeit data so as to weaken or occupy the client's genuine information.

REFERENCES

[1] Mohammad Reza Nami" E-Banking: Issues and Challenges" 2009 10th ACIS International Conference on Software Engineering, Artificial Intelligences, Networking and Parallel/Distributed Computing.

[2] LIU Rui-bo" 2, SUN Li-hua2" The Performance of Banking Merger and Acquisition: From a Microscopic View".

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

[4] 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.

[5] L. Zhao and M. Mannan, "Explicit Authentication Response Considered Harmful," in Proceedings of the 2013 Workshop on New Security Paradigms Workshop– NSPW '13. New York, NY, USA: ACM, 2013, pp. 77–86. [Online]. Available: http://doi.acm.org/10.1145/2535813.2535822

[6] K. Brown, "The Dangers of Weak Hashes," SANS Institute InfoSec Reading Room, Tech. Rep., 2013.

[7] 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. 538–552.

[8] Malone and K. Maher, "Investigating the Distribution of Password Choices," in Proceedings of the 21st International Conference on World Wide Web, ser. WWW '12. New York, NY, USA: ACM, 2012, pp. 301–310. [Online]. Available:

[9] http://doi.acm.org/10.1145/2187836.2187878

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

[11] 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 Password-cracking Algorithms," in Security and Privacy (SP), 2012 IEEE Symposium on. IEEE, 2012, pp. 523–537.