iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** III **Month of publication:** March 2020

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue III Mar 2020- Available at www.ijraset.com

Survey 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 improvements in the field of data innovation offered the individuals development, comforts and convenience, but there are many security and online transaction management related problems. First is we utilize numerous applications for online exchange, it's extremely hard for overseeing different 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 a great deal of security issue that has influenced a huge number of users just as numerous organizations. 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.

A. Objectives

1) This system provides users the facility to access their finance information and banking transactions from various applications.
2) Focus on fake passwords or accounts as a simple and cost effective solution to detect compromise of passwords.
3) Design a system that focus the cracked password files can be detected by the system administrator if a login attempt is done with a honey word by the adversary.
4) Use this technology to launch disinformation attacks against malicious insiders, preventing them from distinguishing the real sensitive customer data from fake worthless data.

B. Problem Statement

Design and Develop a web based application to help customers in managing multiple bank transactions in one system and provide the password may be hacked by hacker and if it is in hashed format adversary it is easy to capture most of the plaintext passwords. Here to detect attacks against password.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue III Mar 2020- Available at www.ijraset.com

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 later on advancement of money related administrations industry, and particularly banking industry. Developing worldwide exchanging and issues in moving cash have inspired scientists to present another structure. E-banking is such thought. The vast majority of banks are utilizing the Internet as another circulation channel. This paper presents a through overview of e-banking portraying definition, hindrances, profits by the clients', economy, and bank purpose of perspectives, and fundamental issues and difficulties, for example, hazard the board and factors answerable for e-banking improvement. At long last, end and future point of view of e-banking advancement will be examined.
2) *LIU Rui-bo, SUN Li-hua:* The financial merger and obtaining (M&A) has become the focal point of the fifth flood of worldwide merger tide, trailed by individuals' riddle about whether there is a positive and maintainable execution of banking M&A. By filtering the current minuscule expository strategy for banking M&A execution, we pick the balanced contextual investigation law for a general examination of the instance of Wing Hang Bank Ltd. buying Chekiang First Bank N.A. We make a determination that the positive effect of M&A on improving bank productivity and investor's worth can be affirmed, so the disparity between experimental outcomes and the genuine M&A exercises at present can be impeccably clarified.
3) *Imran Erguler:* In this paper, check the nectar word framework and present a few comments to feature conceivable powerless focuses. Likewise, they propose an elective methodology that chooses the nectar words from existing client passwords in the framework so as to give reasonable nectar words a superbly level nectar word age strategy – and furthermore to diminish capacity cost of the nectar word conspire.
4) *Lianying Zhao and Mohammad Mannan:* Utilizing misdirection strategies (as in honeypots), they propose the client evident confirmation conspire (Uvauth) that endures, rather than distinguishing or balancing, speculating assaults. Uvauth gives access to all verification endeavors; the right secret phrase empowers access to an authentic meeting with substantial client information, and every single mistaken secret word lead to counterfeit meetings.
5) Patrick Gage Kelley, Saranga Komanduri, Michelle L. Mazurek, Richard Shay, Timothy Vidas Lujo Bauer, Nicolas Christin,
6) *Lorrie Faith Cranor, and Julio Lopez:* In this paper They build up a proficient disseminated technique for computing how viably a few heuristic secret key speculating calculations surmise Passwords and Honey word age strategy for example teasing with tweaking give some potential upgrades which are anything but difficult to actualize and present an improved model as an answer for an open issue additionally beats practically all the disadvantages of recently proposed nectar word age draws near.

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

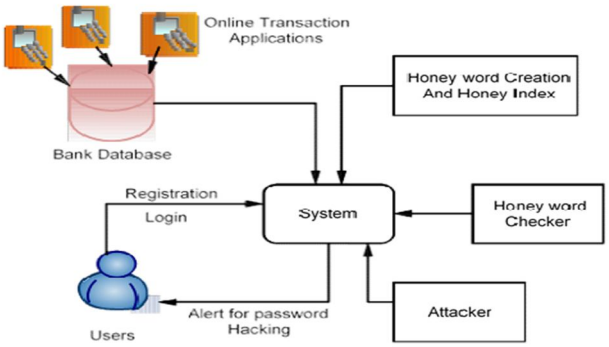


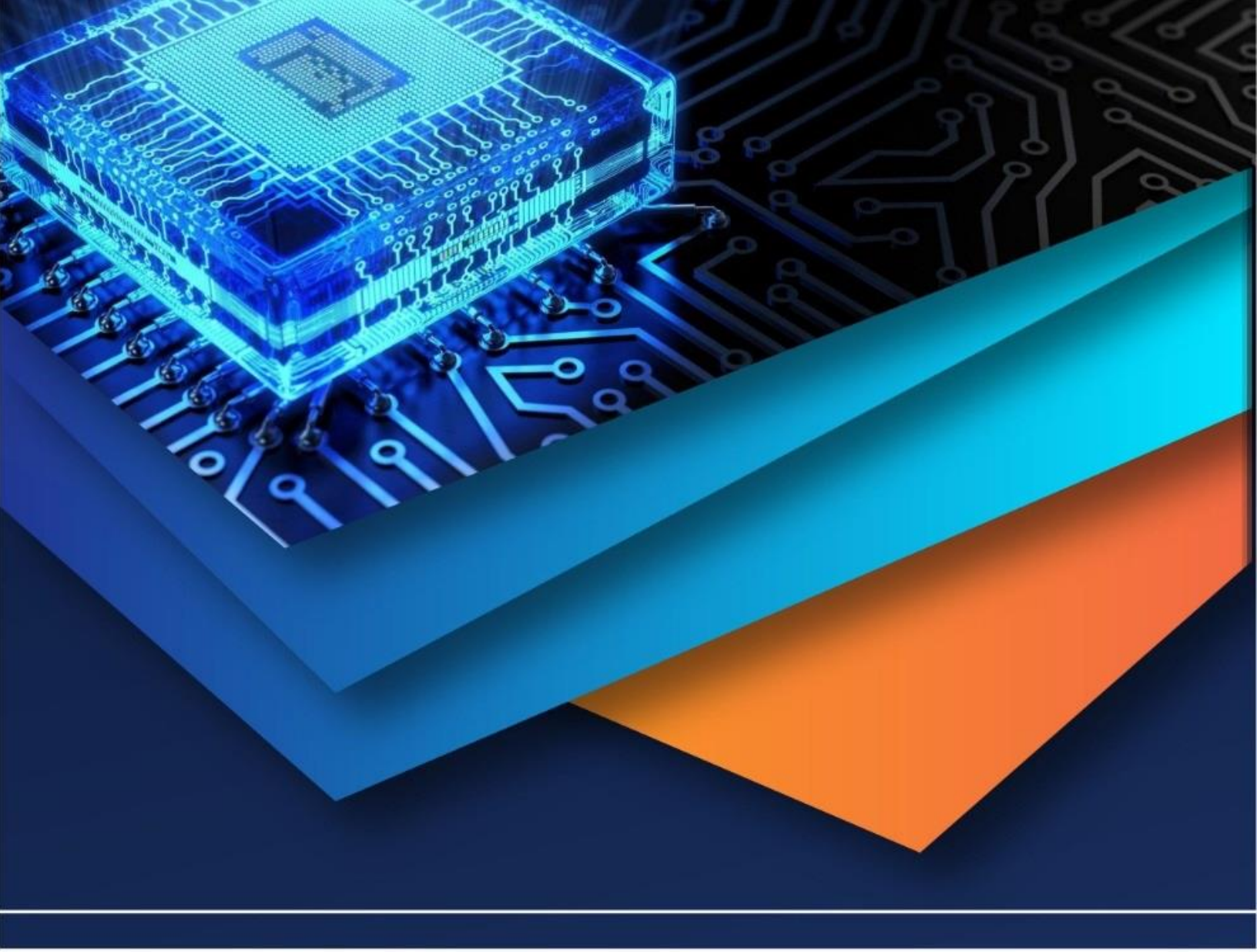
Fig 1. System Architecture

V. CONCLUSION

We present a standard approach to securing and merge transaction from multiple applications in the one system and We propose monitoring data access patterns by profiling user behavior to determine if and when a malicious insider illegally accesses someone's documents in a system service. Decoy documents stored in the system alongside the user's real data also serve assessors to detect illegitimate access. Once unauthorized data access or exposure is suspected, and later verified, with challenge questions for instance, we i undate the malicious insider with fake information in order to dilute or divert the user's real data.

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] [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.
[12] 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.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY