Card Payment Using Three Way Security

Yash Zode
Computer Engineering
G.H. Raisoni College of engineering & Management
Pune,Maharashtra

Sambhaji Bhosle
Computer Engineering
G.H. Raisoni College of engineering & Management
Pune,Maharashtra

Sunita Nandgave
Project Guide
G.H. Raisoni College of engineering & Management
Pune,Maharashtra

Swapnja Gungawar
Computer Engineering
G.H. Raisoni College of engineering & Management
Pune,Maharashtra

Ashish Awashar
Computer Engineering
G.H. Raisoni College of engineering & Management
Pune,Maharashtra

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. Main 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 plain text from encrypts passwords. To implement OTP Generation and Bio-metric verification system. To provide three way verification system first is password, second is One Time Password (OTP), third is biometric scanning.

Keywords- Banking, Data Security, Honey words, Database, Cyber-Security, One-time-password, Biometric.

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 password security in system. We implement application i.e. card payment using three way security.

II. LITERATURE REVIEW

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

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. The 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.

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.

Imran Erguler - The paper, checks 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.

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.

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.

Comparison Table:

components	confidentiality	Availability	Integrity	Delay
Honeyword	Yes	Yes	Yes	Minor
Bio-metrics	Yes	Yes	Yes	Null
OTP	Yes	Yes	Yes	minor
Server	Yes	Minor	Yes	Null

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.

1. 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.
2. 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.

A. System Architecture

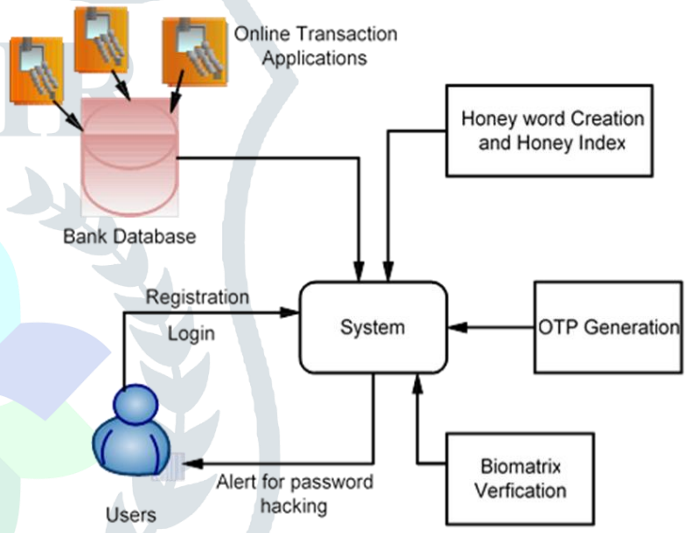

Figure 1. System Architecture

The system consists of Honey word creation, honey index, one-time password generation and bio metric verification. System also contains database which is having online transaction application. User gets an alert after login into system and if password is incorrect still the user gets the alert.

B. Algorithms

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. Else
   realPassword[i] = replace(password1);
   hashPassword[i] = generatorHash(pass);
6. passResult.put("real", realedPassword);
   passResult.put("hash", hashedPassword);
   passResult is HashMap.
7. Return passResult

Conclusion

It presents a standard approach to securing transaction from multiple applications in the one system and it propose monitoring data access patterns by profiling user behaviour 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, it inundate the malicious insider with fake information in order to dilute or divert the user's real data.

REFERENCES

[1] 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.

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

[3] 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

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

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

[6] 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.

Conference on World Wide Web, ser. WWW '12. New York, NY, USA: ACM, 2012, pp.

301–310. [Online]. Available: http://doi.acm.org/10.1145/2187836.2187878

[8] 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.

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

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