ISSN 2395-1621

System Security Using Encrypted Negative Password

[#1]Prof Nirmal S.S, [#2]Aboli Panhale, [#3]Priya Gaikar, [#4]Pooja Jadhav, [#5]Priti Madgul

[2]abolipanhale17@gmail.com
[3]priyaraikar710@gmail.com,
[4]jadhavpoo164@gmail.com,
[5]madgulpriti1996@gmail.com,

[#12345]Department Of Computer Engineering
PREC Loni, Savitribai Phule Pune University,Maharastra.

ABSTRACT

Secure data and password storage is a very crucial and most important aspect in systems based on password authentication. Password Authentication is still the most widely used authentication technique, despite its some security flaws. In this project, we propose a password authentication framework that is designed for secure data and password storage of a banking system to make it more secured and safe to use . In this framework we are going to use a negative password authentication technique to gene rate password. First the entered password will be hashed. The hashed password will then be converted to negative password. The Negative password will then be made more secured by usingAES algorithm for encryption and decryption. When a user authenticates the system the same process of generating the password will be reversely followed to obtain the original password. After a successful authentication the banking application will be started. We are going to use cloud to save the password and data needed by the application.

ARTICLE INFO

Article History

Received: 7th June 2019

Received in revised form :

7th June 2019

Accepted: 9th June 2019

Published online :

10th June 2019

Key Words: Password, Authentication, Hashing, Negative Password, AES and Cloud.

I. INTRODUCTION

Problem Statement

Due to the development of the Internet, a vast number of online services have emerged from banking to health care applications etc., in which password authentication is the most widely used authentication technique, for it is available at a low cost and easy to deploy. Hence, password security always attracts great interest from academia and industry. Despite great research achievements on password security, passwords are still cracked because of users careless behavior. For instance, many users often select weak passwords, they tend to reuse same passwords in different systems they usually set their passwords using familiar vo cabulary for its convenience to remember in illegally access weak systems .

Motivation of the Project :

Safe password authentication system is the need of the day. Negative password generation is a very good technique to fake the original password as it is unusable without our application. So we thought of using this technology in our project to make the banking application more secured by providing the authentication scheme using Encrypted Negative Password.

II. LITERATURE SURVEY

Graphical Password Authentication Technique which is resistant to Shoulder Surfing: In 2016 Mrs. Aakansha S.Gokhale and Prof. Vijaya S.Waghmare authored this paper which mainly explains that Nowadays computer as well as information security is the most significant challenge. Authorized users should access the system or information. Authorization can't occur without authentication. For this authentication various techniques are available. Among them the most popular and easy technique is the password technique. This technique ensures that computer or information can be accessed by those who have been granted the right to view or International Journal of Research In Science & Engineering e-ISSN: 2394-8299 p-ISSN: 2394-8280 access them. The textual passwords are easy to crack through various types of attacks. So to overcome the vulnerabilities, a graphical password technique is introduced.

As the name suggests , in this technique images(pictures) are used as a password instead of text. Also psychological study says that humans can easily remember images than text. So according to this fact, graphical passwords are easier to remember and di fficult to guess. But because of the graphic nature, nearly all the graphical password techniques are vulnerable to shoulder surfing attack.So , a new graphical password authentication technique is proposed . It is resistant to shoulder surfing and also other types of possible attacks to some extent. It is a combination of recognition and the recall based approach. It can be useful for smart devices like smart phones, PDA, iPod,iPhone etc.

OPUS: Preventing weak password choices In 2007 Dinei Florencio and Cormac Herley authored this paper said that We report the results of a large scale study of password use andpassword re-use habits. The study involved halfmillion users over a three month period. A client component on the machines of users recorded a variety of password strength, usage and frequency metrics. This allows us to estimate quantities such as the average number of passwords and the average number of accounts each user has, also how many passwords she types per day, how often the passwords are shared among si tes, and how often they are forgotten. The data is the first large scale study of its kind, and yields numerous other insights into the role that the passwords play in the online experience of user.

A large-scale study of web password habits

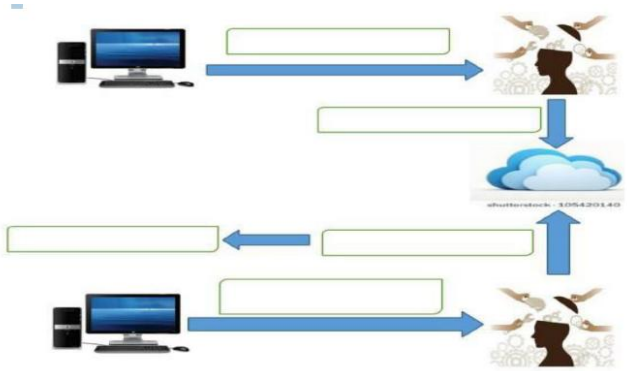
In 2007 Dinei Florencio and Cormac Herley authored this paper said that We report the results of a large scale study of password use andpassword re-use habits. The study involved halfmillion users over a three month period. A client component on the machines of users recorded a variety of password strength, usage and frequency metrics. This allows us to estimate quantities such as the average number of passwords and the average number of accounts each user has, also how many passwords she types per day, how often the passwords are shared among si tes, and how often they are forgotten. The data is the first large scale study of its kind, and yields numerous other insights into the role that the passwords play in the online experience of user.

III. PROPOSED SYSTEM

Password and data security is a hot topic. But as password attacks by hackers is getting more sophisticated it is very difficult to maintain a secured data system. Due to loss of data the banking system is vulnerable to loss and theft of money. To solve this problem many have suggested System Security Using Encrypted Negative Password as our project topic.

Goal and Objectives:

- To make effective use Password Security.
- To make effective use of Data Hashing & Negative Password Technique.
- To make effective use of cloud computing.
- To build a fully functional banking application.



Statement of scope:

Password Generation : The System can be used to analyze the generation of an Encrypted Negative password using a combination of Hashing, Negative password and AES together.

Authentication : The System can be used to analyze the authentication process of an Encrypted Negative password using a combination of Hashing, Negative password and AES together.

Methodology/ Algorithm details :

AES (Advanced Encryption System):
The Advanced Encryption Standard , which is also known as Rijndael , isa specification for the encryption of the electronic data established by the United States National Institute of Standards and Technology in 2001. It is a subset of the Rijndael block cipher which is developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen, who submitted a proposal to NIST during the AES selection process. Rijndael is the family of ciphers with different key and block sizes. For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but having three different key lengths: 128, 192 and 256 bits. It has been adopted by theU.S. government and is now used worldwide. It is superior to the Data Encryption Standard (DES), which was published in 1977. This announcement followed a five-year standardization process in which the fifteen competing designs were presented . Advanced Encrypted Standard became effective as the federal government standard on May 26, 2002 , after the approval by the Secretary of Commerce . AES is includedin ISO/IEC 18033 -3 standard. AES is available in many different encryption packages. It is the first publicly accessible cipher and is approved by the National Security Agency (NSA) for the top secret information when it is used in an NSA approved cryptographic

IV. CONCLUSION

In this project, we are developing a novel approach to provide a secured environment for a banking system using Encrypted Negative Password. The basic idea of the project is integrating Hashing Method, Negative Password Concept, Encryption/Decryption and cloud computing together to achieve a secured banking system. We have assembled cloud computing and desktop application together to build a

whole newsystem which is secured and reliable. It is more intelligent in minimizing the risks of hacker attacks on the banking system.

REFERENCES

M. A. S. Gokhale and V. S. Waghmare, The shoulder surng resistant graphical password authentication technique, Procedia Computer Science, vol. 79, pp. 490498, 2016.

J. Ma, W. Yang, M. Luo, and N. Li, A study of probabilistic password models, in P roceedings of 2014 IEEE Symposium on Security and Privacy, May 2014, pp. 689704. Information Forensics and Security, vol. 12, no. 10, pp. 23202333, Oct. 2017.

M. A. S. Gokhale and V. S. Waghmare, The shoulder surng resistant graphical password authentication technique, Procedia Computer Science, vol. 79, pp. 490498, 2016.

Y. Li, H. Wang, and K. Sun, Personal information in passwords and itssecurity implications, IEEE Transactions on Information Forensics and Security, vol. 12, no. 10, pp. 23202333, Oct. 2017.

D. Florencio and C. Herley, A large-scale study of web password habits, in Proceedings of the 16th International Conference on World Wide Web. ACM, 2007, pp. 657666.

R. Shay, S. Komanduri, A. L. Durity, P. S. Huh, M. L. Mazurek, S. M. Segreti, B. Ur, L. Bauer, N. Christin, and L.F. Cranor, Designing password policies for strength and usability, ACM Transactions on Information and System Security, vol. 18, no. 4, pp. 13:113:34, May 2016.

H. M. Sun, Y. H. Chen, and Y. H. Lin, oPass: A user authentication protocol resistant to password stealing and password reuse attacks, IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 651663, Apr. 2012

