www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 04, April 2023, pp : 238-243

e-ISSN : 2583-1062

Impact Factor : 5.725

MANAGING PASSWORD LOCKER

V. Latha[1], Mr. E.R. Ramesh[2], Ms. Sarika Jain[3], Dr. S. Geetha[4]

[1]M.Sc-CFIS, Department of Computer Science and Engineering, Dr. M.G.R Educational and Research Institute, Chennai 600 095, Tamilnadu, India

[2,3]Center of Excellence in Digital Forensics, Perungudi, Chennai 600 089, Tamilnadu, India

[4]Head of the Department, Department of Computer Science and engineering, Dr. M.G.R Educational and Research Institute, Chennai 600 089, Tamilnadu, India.

ABSTRACT

This application utilizing for recovering a neglected information's and in this application landing page contains three choices that is home, client and administrator. Home choice is welcome page and administrator choice contains a client data and information's. Administrator is in general access in the application. In the event that you click the client choice you see the login page. On the off chance that you as of now register you can login straightly. On the off chance that you not register you can see lower part of login page register choice there. You register there. Then you got online entertainment choices and one recovering choice. Virtual entertainment applications choices contain register page that is you update your information resembles email, name secret word and this information's putting away scrambled type that is garbled arrangement. On the off chance that you failed to remember your information's you going to recovering choice and utilizing your email to get unscramble information's That is intelligible sort. This is the application utilizations.

Keywords: Password manager, email encryption, text encryption.

1. INTRODUCTION

This application using for recuperating a dismissed data's and in this application presentation page contains three decisions that is home, client and head. Home decision is welcome page and overseer decision contains a client information and data. Overseer is in everyday access in the application. If you click the client decision you see the login page. If you at this point register you can login straightly. In case you not register you can see lower part of login page register decision there. You register there. Then, at that point, you got online amusement decisions and one recuperating decision. Virtual amusement applications decisions contain register page that is you update your data looks like email, name secret word and this data's taking care of mixed sort that is jumbled plan. If you neglected to recollect your data's you going to recuperating decision and using your email to get unscramble data's that is comprehensible sort. This is the application uses.

2. LITERATURE SURVEY

WeiliHan et.al, long passwords are gaining popularity in password policy recommendations; however, data-driven guessing studies are woefully inadequate in adapting to long passwords, lacking in both guessing efficiency and their composition guidelines.

For state-of-the-art data-driven password guessing methods such as PCFGs (Probabilistic Context-free Grammars), their guessing efficiency is limited by the presence of a large-scale training data, or the lack thereof. Given that long passwords leaked in the real world are typically scarce, coupled with the fact that the data-driven methods' performance depends on training data, obtaining good performance on long passwords has become a key challenge. To overcome the dataset limitation, we propose a framework TransPCFG, that transfers the knowledge, (i.e., grammars in PCFGs), from short passwords to facilitate long password guessing. We further perform an empirical evaluation based on three real-world datasets and the results demonstrate superior performance over the state-of-the-art data-driven guessing methods under 1014 offline guesses. For passwords with 16 characters, TransPCFG can compromise an average of 23.30% of the passwords, outperforming PCFG_v4.1 by 56.10%. Additionally, for better password-composition guidelines, we find that long password-composition policies requiring more segments are more resistant to guessing attacks. For the segment, the password 12zxcvbnword1997 has four segments since it follows the template Digit2Keyboard6Letter4Year4. We thus recommend users to create long passwords with four or more segments instead of the widely recommended more character classes for secure.

Mariam.m.taha et.al, in this paper, we propose a new algorithm to compute the strength of passwords based on two measurements, mainly: password entropy and password quality. The passwords considered by the algorithm consist of eight characters alpha numeric with special characters. For such passwords, the analysis phase identified the low/high

entropy patterns and low/high quality passwords. The analysis yields two rules: high entropy passwords are also high-quality passwords, and low-quality passwords are low entropy passwords.

(Building and studying a password store that perfectly hides passwords from itself) We introduce a novel approach to password management, called SPHINX, which remains secure even when the password manager itself has been compromised. In SPHINX, the information stored on the device is theoretically independent of the user's master password. Moreover, an attacker with full control of the device, even at the time the user interacts with it, learns nothing about the master password - the password is not entered into the device in plaintext form or in any other way that may leak information on it. Unlike existing managers, SPHINX produces strictly high-entropy passwords and makes it compulsory for the users to register these passwords with the web services, which defeats online guessing attacks and offline dictionary attack upon service compromise. We present the design, implementation and performance evaluation of SPHINX, offering prototype browser plugins, smartphone apps and transparent device-client communication. We further provide a comparative analytical evaluation of SPHINX with other password managers based on a formal framework consisting of security, usability, and deplorability metrics.

(Strong password generation based on user inputs) Every person using different online services is concerned with the security and privacy for protecting individual information from the intruders. Many authentication systems are available for the protection of individuals' data, and the password authentication system is one of them. Due to the increment of information sharing, internet popularization, electronic commerce transactions, and data transferring, both password security and authenticity have become an essential and necessary subject. But it is also mandatory to ensure the strength of the password. For that reason, all cyber experts recommend intricate password patterns.

But most of the time, the users forget their passwords because of those complicated patterns. In this paper, we are proposing a unique algorithm that will generate a strong password, unlike other existing random password generators. This password will be based on the information, i.e. (some words and numbers) provided by the users so that they do not feel challenged to remember the password. We have tested our system through various experiments using synthetic input data. We also have checked our generator with four popular online password checkers to verify the strength of the produced passwords. Based on our experiments, the reliability of our generated passwords is entirely satisfactory. We also have examined that our generated passwords can defend against two password cracking attacks named the "Dictionary attack" and the "Brute Force attack". We have implemented our system in Python programming language. In the near future, we have a plan to extend our work by developing an online free to use user interface. The passwords generated by our system are not only user-friendly but also have achieved most of the qualities of being strong as well as non- crackable passwords.

3. PROPOSING SYSTEM

3.1 Concept

This application utilizing for recovering an information and putting away information's on data set. You retrieving your failed to remember information easily with utilizing this application.

3.2 Technique

AES algorithm

Advantage

It uses for recovering your online entertainment application information's utilizing Email.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 04, April 2023, pp : 238-243

e-ISSN : 2583-1062

Impact Factor : 5.725

4. ARCHITECTURE DIAGRAM

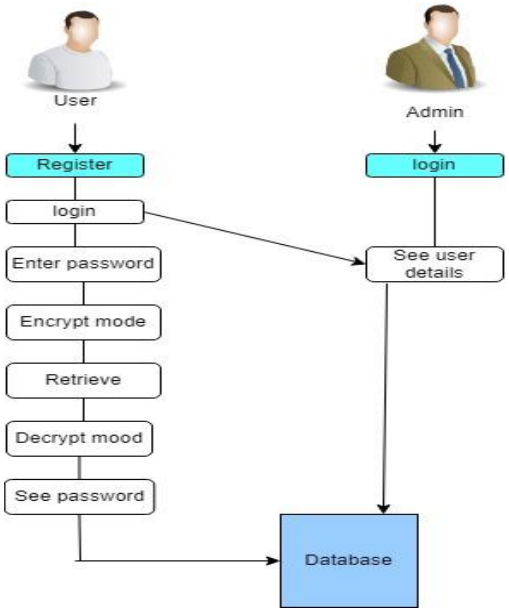


Figure 1. Architecture Diagram

4.1 List of phases

There are 8 phases

- Admin
- User
- Instagram
- Whatsapp
- Facebook
- Snapchat
- Twitter
- Telegram
- Retrieve Datas

Admin

Administrator is top of this application and it will get to client names furthermore, information's. This choice s can see all data inside the application.

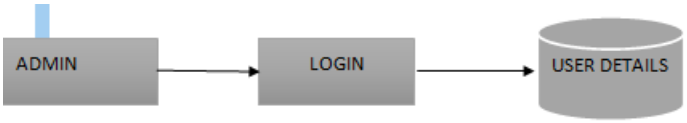


Figure 2. ADMIN diagram

User

Client choice is the application clients. Client initially saw the login page assuming as of now register you can login straightly however by chance you not register. You need to enroll first and afterward you login. Then, at that point, you saw the couple of online entertainment applications names. Then, at that point, you can store your online entertainment data and passwords that is client utilizations.

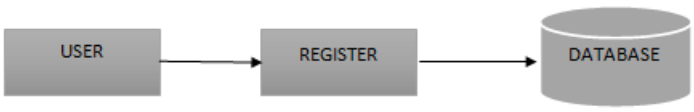


Figure 3. User Diagram

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
www.ijprems.com
editor@ijprems.com
Vol. 03, Issue 04, April 2023, pp : 238-243
e-ISSN : 2583-1062
Impact Factor : 5.725

Instagram

You click the Instagram choice then you store your Instagram data and secret key that is utilization of Instagram choice and afterward at whatever point you recover your data utilizing your email id.

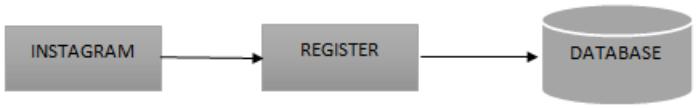


Figure 4. Instagram Diagram

Facebook

You click the Facebook choice then you store your Facebook data and secret key that is utilization of Facebook choice and afterward at whatever point you recover your data utilizing your email id.

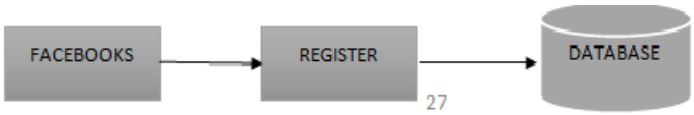


Figure 5. Facebook Diagram

Whatsapp

You click the Whatsapp choice then you store the your Whatsapp data and secret key that is utilization of Whatsapp choice and afterward at whatever point you recover your data utilizing your email id.

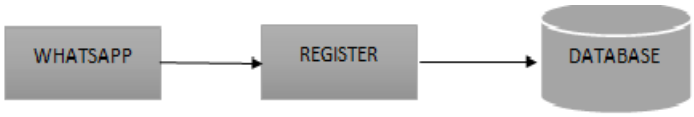


Figure 6. Whatsapp Diagram

Telegram

You click the Telegram choice then you store your Telegram data and secret key that is utilization of Telegram choice and afterward at whatever point you recover your data utilizing your email id.

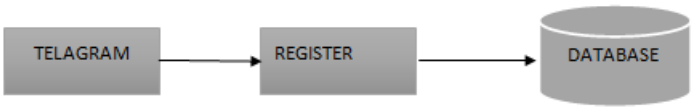


Figure 7. Telegram Diagram

Snapchat

You click the Snapchat choice then you store your Snapchat data and secret key that is utilization of Snapchat choice and afterward at whatever point you recover your data utilizing your email id.

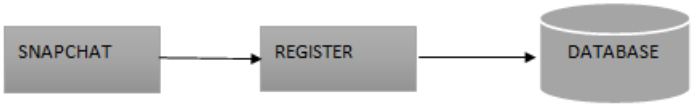


Figure 8. Snapchat Diagram

Twitter

You click the Twitter choice then you store your Twitter data and secret key that is utilization of Twitter choice and afterward at whatever point you recover your data utilizing your email id.

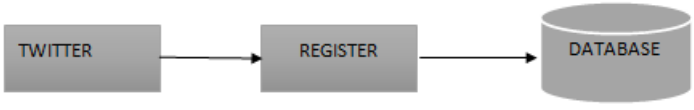


Figure 9. Twitter Diagram

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

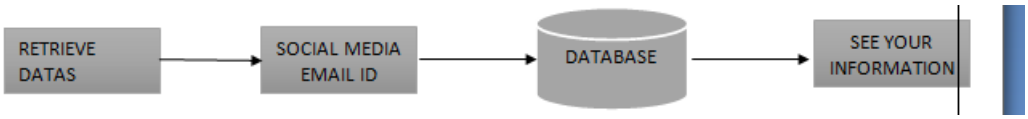
Vol. 03, Issue 04, April 2023, pp : 238-243

e-ISSN : 2583-1062

Impact Factor : 5.725

Retrieve Datas

Recover information choice is a vital that is utilizing for recovering your virtual entertainment data and passwords how is that utilizing your register email id. Then you got your data and passwords.



Screen Shots

User main page

User login page

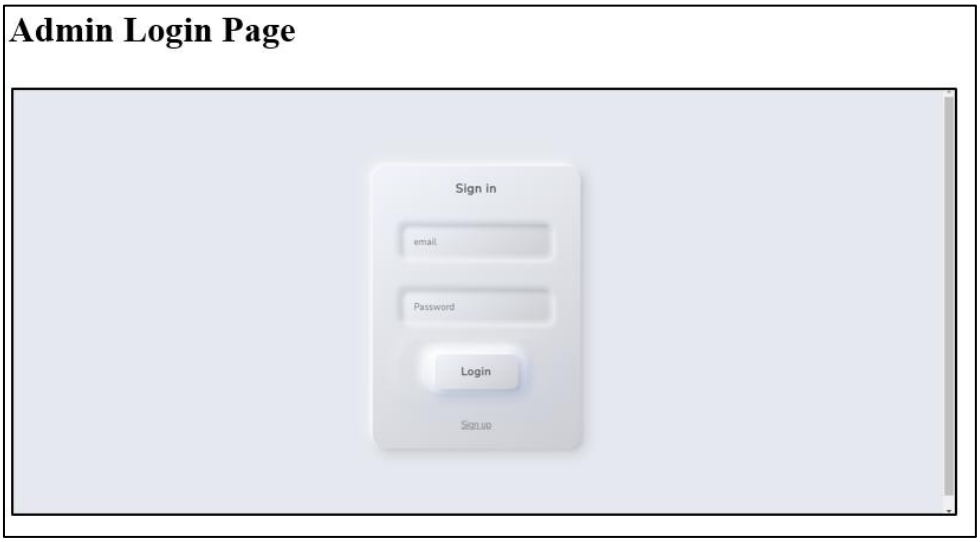
User Register page

User Page

Data insert Page

Data Retrieve page

Admin Login Page



5. CONCLUSION

In this task we will discuss secret key storage and how to recover your information's with utilizing email id. This application utilizing to get your information's constantly and you will recover your information whenever. In this application you store your data whenever. You will recuperate your web-based entertainment data.

6. REFERENCES

[1] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," IEEE Access, vol. 7, pp. 82721–82743, 2019.

[2] A. Alketbi, Q. Nasir, and M. A. Talib, "Blockchain for government services—Use cases, security benefits and challenges," in Proc. IEEE15th Learn. Technol. Conf. (L&T), 2018, pp. 112–119.

[3] Coindesk. The Indian Government Is Preparing a National Framework to Support the Wider Deployment of Blockchain Use Cases. Accessed:Nov. 27, 2019. [Online]. Available: https://www.coindesk.com/indiaplans-to-issue-a-national blockchain-framework

[4] H. Cho, "Correction to asic-resistance of multi-hash proof-of-work mechanisms for blockchain consensus protocols," IEEE Access, vol. 7, 2019, Art. no. 25086.

[5] V. Hassija, V. Chamola, S. Garg, N. G. K. Dara, G. Kaddoum, and D. N. K. Jayakody, "A blockchain-based framework for lightweight data sharing and energy trading in V2G network," IEEE Trans. Veh. Technol., vol. 60, no. 6, pp. 5799 5812, Jun. 2020.

[6] V. Hassija, V. Chamola, D. N. G. Krishna, and M. Guizani, "A distributed framework for energy trading between UAVs and charging stations for critical applications," IEEE Trans. Veh. Technol., vol. 69, no. 5, pp. 5391–5402, May 2020.

[7] E. Androulaki et al., "Hyperledger fabric: A distributed operating system for permissioned blockchains," in Proc. ACM 13th EuroSys Conf., 2018, p. 30.

[8] V. Hassija, V. Chamola, G. Han, J. J. Rodrigues, and M. Guizani, "DAGIoV: A framework for vehicle-to-vehicle communication using directed acyclic graph and game theory," IEEE Trans. Veh. Technol., vol. 69, no. 4, pp. 4182–4191, Jan. 2020.

[9] C. D. Clack, V. A. Bakshi, and L. Braine, "Smart contract templates: Essential requirements and design options," 2016. [Online]. Available: arXiv:1612.04496.

[10] C. Cachin, "Architecture of the hyperledger blockchain fabric," in Proc. Workshop Distrib. Cryptocurrencies Consensus Ledgers, 2016, p. 310.