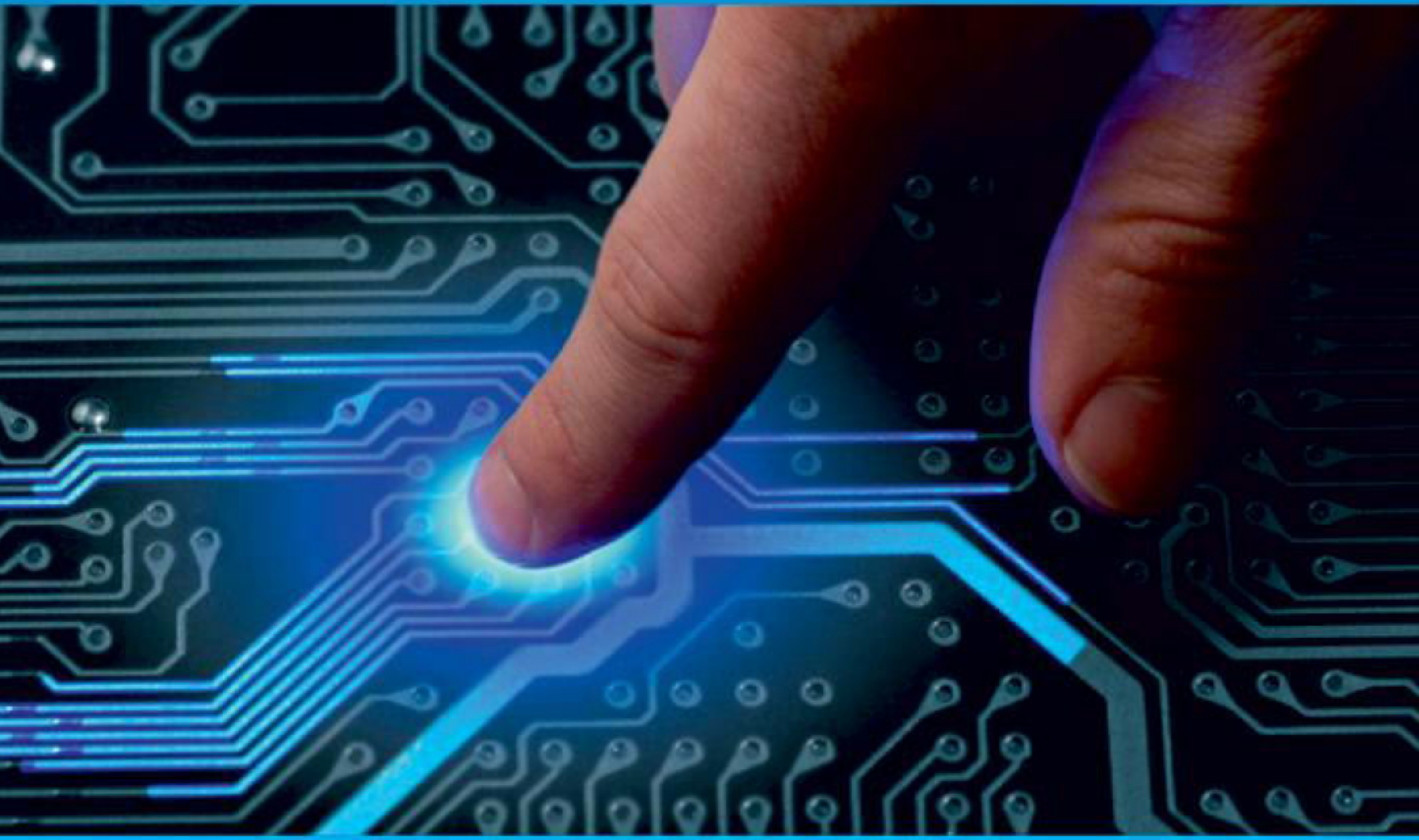
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 6, June 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 6, June 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0906290 |

Secure Password Manager for Safeguarding Sensitive and Personal Data using AES-256 Algorithm

Mayuri B. Shinde,Smrutika J. Bhawsar, Rohit T. Badgujar, Sunita V. Pawar

UG Student, Department of Computer Engineering, MVPS's KBTCOE, Savitribai Phule Pune University, Maharashtra, India

UG Student, Department of Computer Engineering, MVPS's KBTCOE, Savitribai Phule Pune University, Maharashtra, India

UG Student, Department of Computer Engineering, MVPS's KBTCOE, Savitribai Phule Pune University, Maharashtra, India

Assistant Professor, Department of Computer Engineering, MVPS's KBTCOE, Savitribai Phule Pune University, Maharashtra, India

ABSTRACT: Information security has become top priority in day to day life and basic need are the passwords. For every app or device we need to have a password to lock and unlock it. Hence it has become a cumbersome process to remember all of them as well as to generate a new one for every purpose which is strong is not possible. This brings in the need of a secure password storage app to help us selflessly and efficiently keep track of all the passwords. For this we are using AES 256 bit encryption algorithm to securely encrypt the password with the functionality of generating strong random password. Advanced Encryption Standard (AES) which is used provides encryption with key length of 256 bits which is the maximum that can be provided. The process we have adopted improves the password security as the key is randomly updated every time which is used to encrypt the password. After cryptography 2 factory authentication will also be provided in the app. In this system we are developing software by using AES and RSA algorithm which can stored the passwords of all social accounts, cards etc. There is no need to save the password on Google account every time. Password it can be leaked from the account and are vulnerable when it comes to protecting the information from hackers.

KEYWORDS: AES, RSA, password, cryptography, password manager

I. INTRODUCTION

In 21^{st} century hacking has increased a lot which has hugely increased the awareness of local people towards keeping their information secured. The factor which is hampering the security the most is exposure of user's passwords. If anyone gets hold of the users password accessing once is information becomes an easy task. For this users need to have different passwords for everything. Remembering all these passwords and generating a strong password every time is not possible for the users. After all the protocols used are HTTPS and HTTP which are not very secured.

As the threat of information leakage starts as soon as it is being transferred therefore on the transferring process itself the data should be encrypted. This also shows that the password stored by the users currently are also exposed and can be easily obtained if one wants to. Current data encryption technology can be classified into symmetric and asymmetric encryption. The AES algorithm is currently the mainstream symmetric algorithm which was designed to overcome the DES standards. This leads us to the purpose of this project which is to store all the users passwords securely using AES encryption and provide them with a strong password whenever in need. For this we have developed the application which ensures information safety and eases day to day life of the users.

II. RELATED WORK

In [1], Ying Liu and Wei Zhang have used the concept of symmetric encryption algorithm AES, using two layers of AES keys and updating them periodically. This way of processing enhances the security of the password stored. Here to avoid the leakage of the key during the transmission the AES key is encrypted with a random number which is then used to encrypt the password which also maintains the efficiency. They have also used asymmetric encryption algorithm which is RSA with its wide key length of 40 to 2048 bit changes. This algorithm is as safe as AES.
In [2], Mengli Zhang and Gang Zhou they have used SP – RNN, they first serialized the password in the training set, and then trained the recurrent neural network. Using this it was see that it not only improves the generalization ability of the model, but also increases the string generation rate. As researched the user password can be divided into three cases and based on these cases a hybrid PCFG and BiLSTM RNN algorithm was used proposing fast password set generation model best on SPSR – RNN.
In [3], Ramesh Yegireddi and R. Kiran Kumar used various algorithms on different types of files. Their study reflected that encrypting and decrypting the .EXE files, Blowfish performed best while for .DOC file AES algorithm was superior but only for encrypting for decrying this type of file Blowfish is still superior to others. They studied all the algorithms and defines a new conventional encryption algorithm which will be defined for multi-core processors to give efficient performance

III. ARCHITECTURE

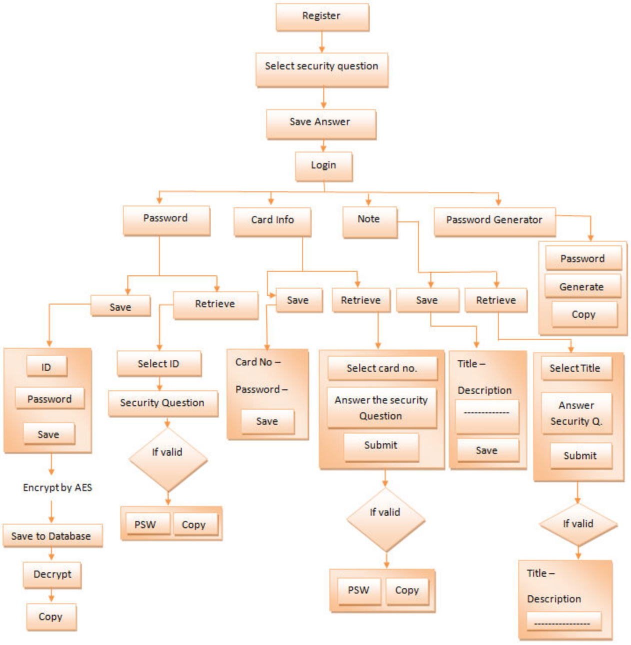


Fig: System Architecture

Above fig. shows the overall system structure of security password manager. We create a different model for secure multiple social media accounts and bank details. ATM card details etc. in this system we can safely save or retrieve passwords and notes of our accounts.

IV. PROPOSED APPLICATION

With an intent of securing personal and sensitive data of the user, this app stores all the user information in an encrypted format, so that it does not get tampered by an intruder. This data has been encrypted using AES-256 algorithm. The user will first have to go through a registration process wherein he will have to fill his details which would be stored in the database. Also, the user will have to set a few questions and answers to those questions at the time of registration. The answers of these questions will also be stored in an encrypted format in the database using AES-256 algorithm. The user can store his data, retrieve his data and can delete his data as and when needed.
In this app, different sections have been made for the storage of different kinds of data. So, the user can store his passwords, personal notes and information of his cards in different sections of this app. This will help the user to store

his information in an organised manner and avoid confusion of the user. In all these sections, the user can perform the following operations on his data:

i) Save: In order to store the data in a tamperproof manner, all the data will be encrypted using the AES-256 algorithm in the database.

ii) Retrieval: At the time of retrieval of data, the questions which have been set at the time of registration will appear randomly and the user will have to answer it in order to prove that he is the genuine user. Once the questions are answered, the data will be decrypted and displayed.

iii) Deletion: The stored data can also be deleted when needed.

The app provides a feature for the users' ease which will generate a random strong password which will be a combination of upper case and lower case alphabets, digits and special symbols. The combination of all these characters will make the password very strong. This feature will have a separate section in the app called as Random Password Generator.

V. Results

We proposed this for password manager and for cyber security. Now a days with the growth of internet peoples are increasingly use the social media accounts for entertainment or for business development projects. Many data are stored on their mobile phone or in the laptops, computers etc. but that is not secure as we need. To secure the system or passwords of social accounts or bank accounts we developed the software. In this software we can store all passwords of our social accounts and bank accounts also we can add any important or personal note on it. And also we can create random password from it. Sometimes we cannot set the personal passwords that time password generator helps to generate random password. We can save or retrieve data from this software. It helps us to securely store our personal data and passwords. We use database which is store all data and get results as per user wants. This is very useful for secure our data.

VI. Conclusion and Future Work

In this software we can store all passwords of our social accounts and bank accounts also we can add any important or personal note on it. And also we can create random password from it which is unique every time.

In our project we are also planning to provide the cloud storage feature in future. As keeping the data backed up on cloud will make this project more feasible towards feature if the local storage gets damaged.

ACKNOWLEDGEMENT

It is indeed a great pleasure to express our thanks and gratitude to all those who helped us. No serious and lasting achievement or success one can ever achieve without the help of friendly guidance and co-operation of so many people involved in the work. We are extremely grateful to Dr. S. R. Devane, Principal, M. V. P. Samaj's Karmaveer Baburao Thakare College of Engineering, Nashik and Dr. V. S. Pawar, Head of Department, Computer Engineering for permitting me to undertake this work. We express our heartfelt gratitude to my respected project guide Ms. S. V. Pawar for her kind and inspiring advice which helped us to understand the project and its semantic significance. They enriched us with valuable suggestions regarding our project and presentation issues. Finally, we would like to appreciate all our great teachers and mentors throughout our academic career without whom we would not have achieved this milestone. We are also very thankful to all our colleagues who helped and co-operated with us in conducting the project presentation by their active participation.

References

1. Ying Liu 1,Wei Zhang, Xienxia Peng, Yan Liu, Sida Zheng, Tongjia Wei, Liang Wang IEEE "Design of password encryption model based on AES Algorithm", State electric research power institute,Nanjing, China. J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.
2. Mengli Zhang, Gang Zhou1, Muhammad Khuram Khan, Saru Kumari, Xuexian Hu, and Wenfen Liu5 IEEE - "SPSR-FSPG: A Fast Simulative Password Set Generation Algorithm", 1 State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China 2 State Key Laboratory of Integrated Service Networks, Xidian University, Xian 710126, China 3 Center of Excellence in Information Assurance, King Saud University, Riyadh 11653, Saudi Arabia 4 Department of Mathematics, Chaudhary Charan Singh University, Meerut 250004, India 5 Department of Computer Science and Information Security, Guilin University of

Electronic Technology, Guilin 541004, China Corresponding authors: Gang Zhou (gzhougzhou@126.com) and Muhammad Khurram Khan (mkhurram@ksu.edu.sa). K. Elissa, “Title of paper if known,” unpublished.

3. Ramesh Yegireddi , R Kiran Kumar IEEE - “A survey on Conventional Encryption Algorithms of Cryptography ”, Aditya Institute of Technology and Management Tekkali, Department of Computer Science Krishna University, Andhra Pradesh, India.Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

BIOGRAPHY

Mayuri B. Shinde is pursuing Bachelor's in Computer Engineering from M. V. P. Samaj's Karmaveer Baburao Thakare College of Engineering, Nashik, affiliated to Savitribai Phule Pune University, Maharashtra, India and will be graduating in the year 2021.

Smrutika J. Bhawsaris pursuing Bachelor's in Computer Engineering from M. V. P. Samaj's Karmaveer Baburao Thakare College of Engineering, Nashik, affiliated to Savitribai Phule Pune University, Maharashtra, India and will be graduating in the year 2021.

Rohit T. Badgujar is pursuing Bachelor's in Computer Engineering from M. V. P. Samaj's Karmaveer Baburao Thakare College of Engineering, Nashik, affiliated to Savitribai Phule Pune University, Maharashtra, India and will be graduating in the year 2021.

Sunita V. Pawar has pursued Masters in Computer Engineering. She is working as Assistant Professor at M. V. P. Samaj's Karmaveer Baburao Thakare College of Engineering, Nashik, affiliated to Savitribai Phule Pune University, Maharashtra, India. Her area of research is Information Security.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING