IJAREEIE

e-ISSN: 2278-8875
p-ISSN: 2320-3765

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

Volume 11, Issue 12, December 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.18

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.18|

||Volume 11, Issue 12, December 2022||

|DOI:10.15662/IJAREEIE.2022.1112021 |

Secure Your Passwords through Safe Wallet with a Smart Key and a Secret Key

Janaki Raman Palaniappan

Software Engineer, Former Student of Thiagarajar College of Engineering, IT Dept, Madurai, India

ABSTRACT: We are in the phase where IT development is growing rapidly with the new technologies coming in always, let it be a new devices, new applications in phones, email services and so on, but one thing that has not changed is a use of passwords and its securities for these devices and applications. As a human being, it is difficult for us to remember so many passwords in our day-to-day life despite having other tensions, work, meeting, etc., towards our life. Remember when our passwords get exposed, that means we lost our identity and if it goes to unauthorized hands then it is very risky. So, keeping the passwords safe is the fore most important thing that everyone has to abide. To be concise, what if passwords are kept in a safe place like locker in a bank and are available to only authorized person. Here we discuss about having the passwords stored in the wallet using secret key and to open the locked list of accounts in the wallet there needs to be a smart key. The user must decide the smart key and the secret key and remember to be able to see the passwords. The method that is used to protect the passwords is by a distinct approach using AES algorithm. This entire method shows the additional security of having our passwords stored safely and reduces our stress on passwords retrieve.

KEYWORDS: Information Security, AES 128-bit, AES 192-bit, Brute Force Attack, Identities, P-Wallet

I. INTRODUCTION

While the passwords are to be provided, everywhere in the internet services we like to use. The tough part is to remember many passwords as we intend to forget and end up in resetting the passwords many times due to number of different passwords and its length to maintain the security. Also, the number of passwords has been growing in our life due to growth of computer technology and its activities that we do daily. We cannot use the same password everywhere which is a hazard of easy exposing the content easily when a password is hacked. Passwords are important for authentication. Here the better solution can be to use the wallet to store the passwords safely and have a strong authentication to open the wallet.

There are different types of wallets available in the market for a different purpose such as digital wallet, Mobile wallet, Desktop wallet, etc. Digital wallet is also called e-wallet that stores safely the card details such as credit card, debit card, etc. Mobile wallet is a type that stores payment card information on a mobile device and is a kind of secure way to store money. Another type called Desktop wallets are software applications that allows users to manage the private keys securely on a computer hard drive.

In general wallet is to restore the information safely and securely. In this paper, we are going to see a wallet that is upcoming in the IT development called P-wallet. There are few password managers that are available in the market with different abilities and functionalities.

I.I. P-WALLET

P-wallet also called a password wallet is used to store the passwords in one secure place. This makes the things easy for the user not to remember so many passwords.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.18|

||Volume 11, Issue 12, December 2022||

|DOI:10.15662/IJAREEIE.2022.1112021 |

I.II. AES ALGORITHM

AES algorithm means Advanced Encryption standard Algorithm. There are 3 different key lengths in AES that are 128 bits, 192 bits and 256 bits. AES uses a symmetric key process. Generally, many companies use AES 128-bit algorithm to encrypt the plain text as it is more sufficient to secure the confidential information. Using the current computer technology, it would take millions of years (Fig 1) to crack it. Then comes the AES 192 bits which is second most secured algorithm that is being used in the market. Finally, AES 256-bit algorithm which is the largest key size length and also very difficult to crack due its complex length size mathematically. This method is being used in top-secret government to encrypt the information.

AES algorithm uses symmetric key method, which involves only one secret key to encrypt and decrypt the information.

Key Size	Possible Combinations
128 bits	3.4×10^{38}
192 bits	6.2×10^{57}
256 bits	1.1×10^{77}

Fig 1: Possible Combinations for AES algorithm

II. PROPOSED METHOD OVERVIEW

When we store the passwords in a wallet, it is not a viable method to store it directly. The reason is when there is a cyber attack or hack happens to login into the portal/app, the passwords are directly exposed to unauthorized personnel. For this reason, Encryption and Decryption are the road to success to protect it from the unauthorized personnel. The process follows as user would have to login into the portal/app using the username and the password. User must be able to see the list of accounts of passwords that are stored let us say accounts such as gmail, amazon, banks, etc., To be able to see the passwords in a decoded format for a particular account, user must provide the smart key and secret key. A key to remember here, even smart key provided by the user will be encrypted at rest for the additional security. Smart key plays the role of additional security wall to be able to decode the password.

AES Type	Key Length	Number of Rounds
128 bits	128	10
192 bits	192	12
256 bits	256	14

Fig 2: Rounds of transformation of AES types

Passwords are encrypted and the encrypted content is stored in the wallet backend. As the passwords are encrypted internally upon saving, it will be shown to the user when the correct smart key and secret key are provided as inputs. There are real time chances that users may open the screen for a longer time. As there are threats for the account password to expose when portal/app is open for a longer time than expected. The password is shown to the user only for a few seconds then hidden. This protects the password from being exposed. If needed user must go through the smart key process to be able to view the password again.

III. IMPLEMENTATION DISCUSSION

Let us discuss the method that is implemented here. When the user logins into the portal, then provides the account name, password and saves it. Functionality happens in a way that Account Password would be encrypted

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.18|

||Volume 11, Issue 12, December 2022||

|DOI:10.15662/IJAREEIE.2022.1112021 |

simultaneously using AES 192-bit algorithm internally. For this encryption step there would be a secret key that user must remember. Upon saving the password, there would be a message to the user asking for smart key. The user must enter the smart key and once the smart key is entered, the smart key would be encrypted using AES 128-bit algorithm. 2 different AES algorithm are done for a dual protection purpose for the passwords that user saved. If at all someone wants to hack the password of the account they may to crack these security walls apart from network firewall and so on. Three security forces here are login password, secret key and the smart key.

When the user wants to retrieve the password the decryption phase has to go through. Once the user logins into the portal, the account names are shown in a locked state. User must choose the account for the one password is needed to be shown. Upon choosing the account, it would ask for a smart key and user must enter. If the smart key is right, it would decrypt by the AES 128-bit algorithm and the account will be unlocked. AES 128-bit does 10 rounds of transformation for the algorithm to process. Next step is to decrypt the password for a particular account, a secret key must be entered by the user for the AES 192-bit algorithm to decrypt and show the password text. A point to be noted here, AES 192-bit does 12 rounds of transformation for the algorithm to process (Fig 2). This multiple steps of encryption and decryption provides additional protection to the end user passwords.

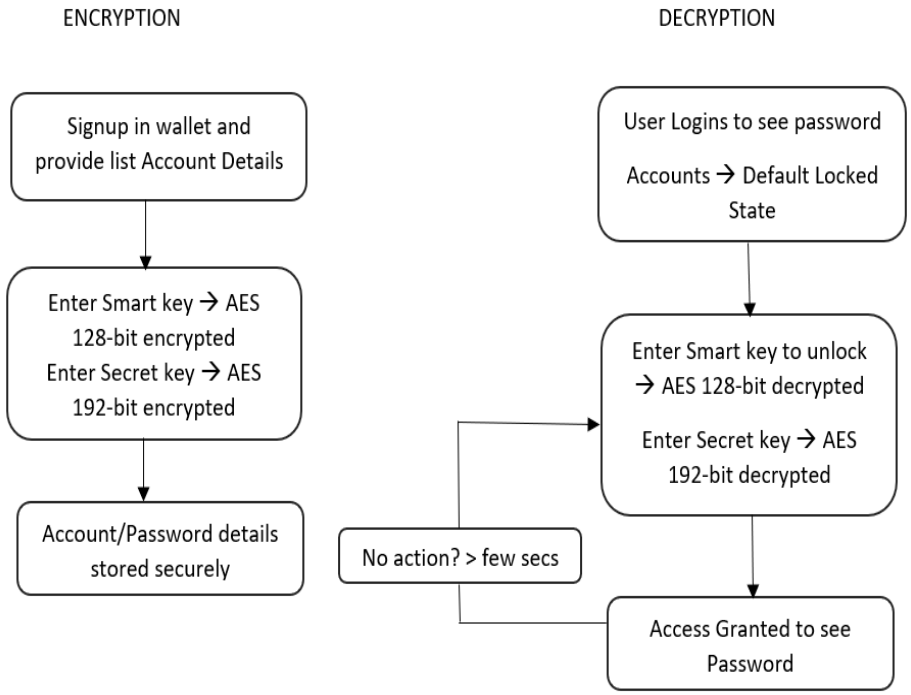


Fig 3: AES Dual combination Algorithm Process

IV. CONCLUSION

When the technology improves more and more, even the number of attacks is increasing as there is a development on hacking and cracking process in cyber-attack point as well. So always looking up on how the protection has to be better, is the only key to protect our data. In this method, using AES 128-bit algorithm is stronger and complex for a protection. Having another additional protection of 192-bit algorithm is stronger. Using the algorithm for dual authentication assures us the additional security. Combination of same method algorithm with a different key length of bits makes our system strong as it plays an important role to protect our data. This dual protection ensures that cracking the password is nearly impossible (Fig 3). Thus makes our 'n' number of password management easy for the customers by storing in the p-wallet.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.18|

||Volume 11, Issue 12, December 2022||

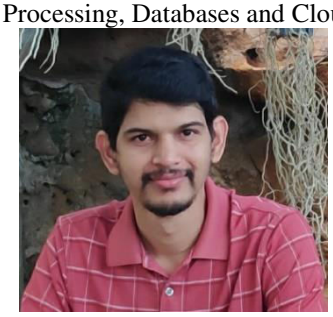
|DOI:10.15662/IJAREEIE.2022.1112021 |

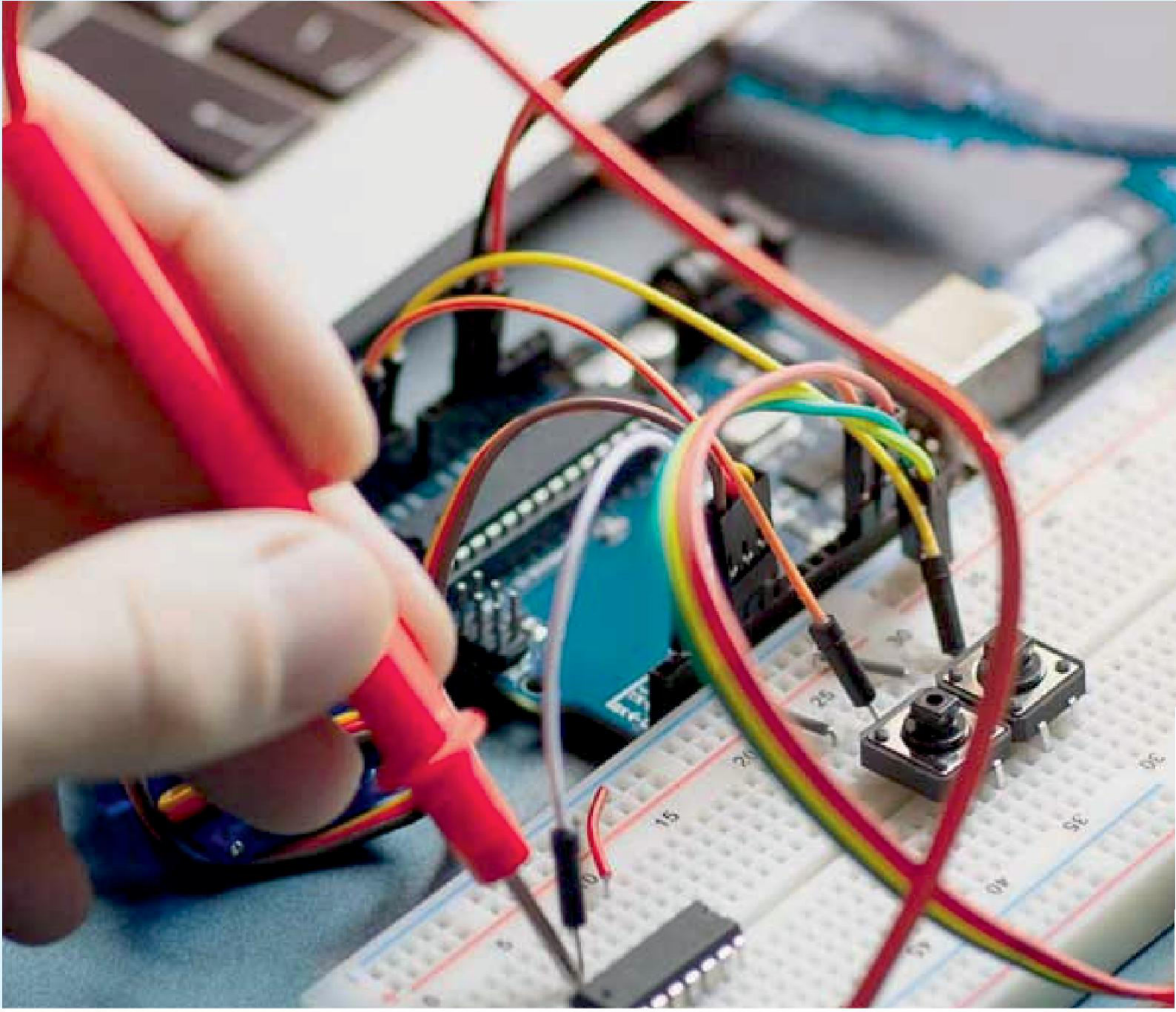
REFERENCES

[1] Comparison of AES 128, 192 And 256 Bit Algorithm for Encryption And Description File by Ria Andriani; SteviEmaWijayanti; Ferry Wahyu Wibowo. Published by IEEE, 2018 3rd International Conference on Information Technology, Information System and Electrical Engineering (ICITISEE)
[2] Highly Secure Cryptography Algorithm Method to Safeguard Audios and Visuals, Vol. 12, No.3, Sep 2022 of International Journal on Cryptography and Information Security (IJCIS) by author Janaki Raman Palaniappan
[3] Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data by Ako Muhamad Abdullah in Eastern Mediterranean University - Cyprus - Publication 16 June 2017.
[4] Research Paper on Cyber Security by Mrs. Ashwini Sheth, Mr. Sachin Bhosale, Mr. Farish Kurupkar, Department of C.S., I.C.S. College, Khed, Ratnagiri of Emerging Advancement and Challenges in Science, Technology and Management, 23rd& 24th April 2021.
[5] Crypto your Belongings by Two Pin Authentication using Ant Algorithm based Technique by Janaki Raman Palaniappan, CAIML - Volume 12, Number 12, July 2022.
[6] Implementation of 128, 192 & 256 bits Advanced Encryption Standard on Reconfigurable Logic by Monika Gupta, Swapnil Mahto, Ambresh Patel of International Journal of Engineering Trends and Technology (IJETT) – Volume 50 Number 6 August 2017.
[7] Hacking AES-128 by Timothy Chong and Kostis Kaffes, Stanford University
[8] Conceal the Data with Ultra Advanced Smart Key Using Cryptography Algorithm, Vol 2, Issue 1, Nov 2022 by author Janaki Raman Palaniappan of International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
[9] https://www.trentonsystems.com/blog/aes-encryption-your-faqs-answered

BIOGRAPHY

Janaki Raman Palaniappan is a working as a Software Engineer. He obtained his B. Tech in Information Technology in 2009 from TCE, Madurai. He is currently a Researcher, Database Administrator,Cloud Engineer and a DevOps Engineer. He has published in reputable Journals and Learned Conferences. His area of research is mainly on Cryptography, Information Security, Image Processing, Databases and Cloud.





INNO SPACE
SJIF Scientific Journal Impact Factor

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

Impact Factor: 8.18

International Journal of Advanced Research

in Electrical, Electronics and Instrumentation Engineering

9940 572 462 6381 907 438 ijareeie@gmail.com

www.ijareeie.com

Scan to save the contact details