International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET229139

PassVaRRdS - Password Generator, Encrypting and Storage using AES and Cloud

Sonia Maria D'souza[1], Rohan V. Chikalkar[2], Sayani Panda[2], Vipul Singh[2], Rohan Santra[2]

[1]Assistant Professor, Department of Computer Science Engineering, HKBK College of Engineering, Bengaluru, Karnataka, India

[2]Department of Computer Science Engineering, HKBK College of Engineering, Bengaluru, Karnataka, India

ABSTRACT

Article Info
Volume 9, Issue 1
Page Number : 139-142
Publication Issue :
January-February-2022
Article History
Accepted : 01 Feb 2022
Published: 11 Feb 2022

The users of computer technology and internet are increasing day by day. As the users are growing, the need for security is also felt very much. The data assets and other valuable facts are stored in the computer systems. One of the ways to safe guard the data assets is to have a proper authorization method to access the data. This is achieved by user identification and password mechanism. The selection of password is important, since the entire authorization is dependent on the password. The password needs to be strong enough to avoid brute force attack and other attacks. Also remembering complicated passwords or passwords of multiple accounts can be much hectic, thus we need a way to store or save the password securely. It should also be kept in mind that the passwords should be easily accessible to the user but cannot be breached by others. So we are using Advanced Encryption Standard algorithm to safely encrypt the passwords and store the encrypted passwords in the cloud database.

Keywords : Advanced Encryption Standard, AES, Cloud

I. INTRODUCTION

The proposed project is to design an application that is going to generate a random password of user specified length that cannot be easily guessed by any hacker, encrypt it using the AES algorithm and finally store it in a cloud based vault for easy access by the user.

The vault would be used to store passwords of multiple accounts and it will have a master password to protect all the other passwords stored in it.

Introduction to AES

Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S National Institute of Standards and Technology (NIST) in 2001. AES is widely used today as it is a much stronger than DES and triple DES despite being harder to implement.

Points to remember

- AES is a block cipher.
- The key size can be 128/192/256 bits.
- Encrypts data in blocks of 128 bits each.

That means it takes 128 bits as input and outputs 128 bits of encrypted cipher text as output. AES relies on substitution-permutation network principle which means it is performed using a series of linked operations which involves replacing and shuffling of the input data.

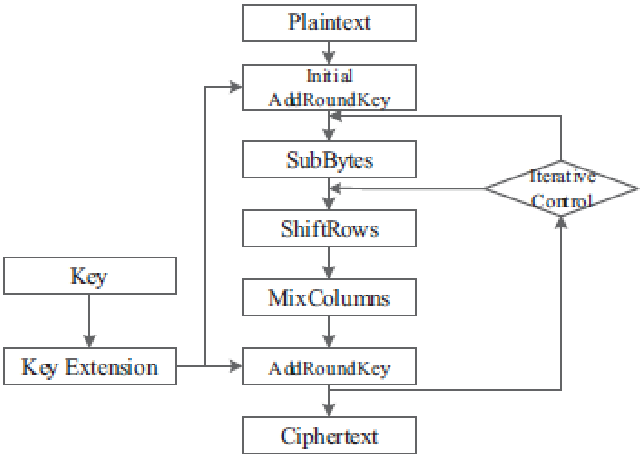
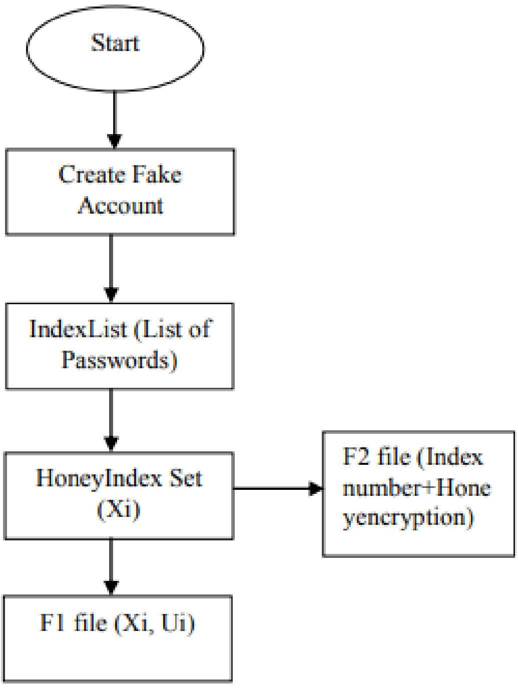


Fig. 1

II. LITERATURE SURVEY

[1] This paper by Mrs.Vasundhara R.Pagar ,In digital era people's livelihood is completely depend on internet due to speedy growth of it. Web services are widely used by business, government, individuals. Communication with the different web services is occurring through authentication i.e. user name and password. But web services are becoming susceptible due to effortless hacking of website through weak password. Password is vital key to get authorization but hackers are much successful in password cracking due to the weak password selected by user. To strengthen the password storage, proposed system uses Honeyword technique along with Honeyencryption. Honeywords are bogus passwords which are stored with original password to lure the attacker. In case attacker got the password file but he cannot guest which is the original password. Alarm is generated to the legitimate user immediately if attacker is trying to access the account either one of the Honeyword or wrong password. For encryption of password Honeyencryption technique is applied which provides more security to password. Every attempt of decryption of password gives incorrect or false plaintext which confuses the attacker with original password. The purpose of this study is secure online communication by providing strong password security and avoids misuse of user financial and personal data by attacker.

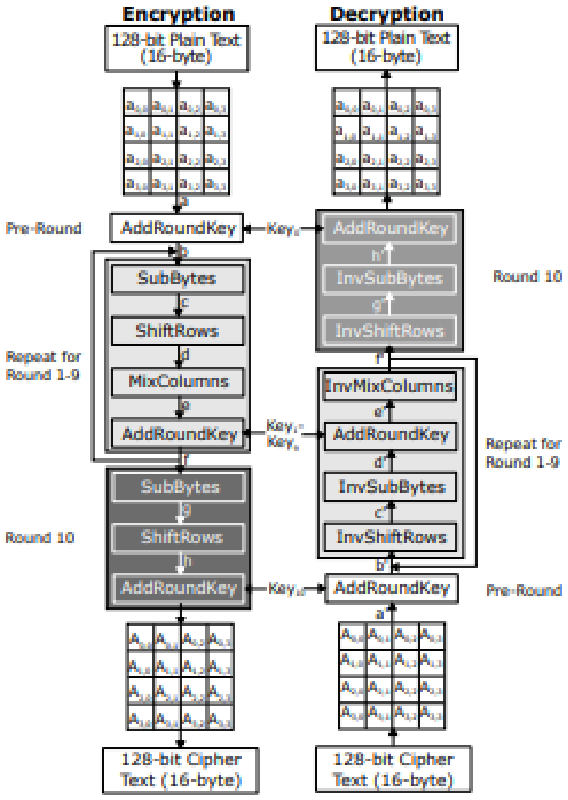

Start
Create Fake Account
IndexList (List of Passwords)
HoneyIndex Set (Xi)
F2 file (Index number+Honeyencryption)
F1 file (Xi, Ui)

[2]This paper by Vatchara Saicheur proposes the implementation of the Advance Encryption Standard (AES) algorithm on Apple iPhone7. We extend the standard AES-128 algorithm to support the block size of 512 bits (AES-512). There are 4 steps in the encryption process: SubBytes, ShiftRows, MixColumns and Add-round key. The comparison between original AES-128 and the new AES-512 using 128, 192, 256, 512, 1024 bits key size is presented. Our implementation shows that AES-512 has higher performance than that of AES-128. The speed up is 1.20 – 1.58 depending on key size. The 128-bit key size is the fastest. The 1024-bit key size is the slowest. We conclude that expanding the block size to 512 bits can enhance the throughput and the speed up of AES algorithm.

TABLE I. COMPARISON OF BLOCK SIZE BETWEEN AES-128 AND AES-512

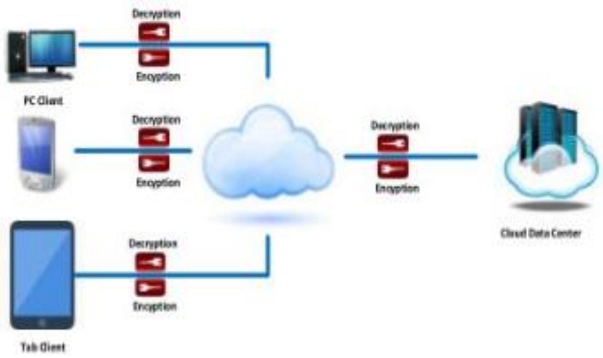
AES	AES Blocksize 128 bit	AES Blocksize 512 bit
Nb	4	8
Row	4	8
Column	4	8
Byte	16	64

[3] This Paper by Liting Yu states that ,with the rapid development and globalization of semiconductor industry, data security is becoming a more critical issue for highly confidential devices, especially for cryptography related applications. Advanced Encryption Standard (AES) is widely used for information security. For AES, the most important data are plaintext and keys, which are the targets of attacks. In this paper, AES security vulnerabilities are analyzed first. Information leakage would be a major concern for AES. Hence one of the most common types of attacks that could leak information at the AES implementation, inserted into AES and utilizing scan chains in or around AES to extract keys or plaintext, is discussed. To deal with the attacks and improve AES circuit's information security, one protection, namely Registered Data Obfuscation, is presented. Experiment results show that with the proposed protection, the scanbased attack is invalidated to leak the critical data. Meanwhile, the proposed protection can also disalbe key Trojan attack introduced in [1, 2]. The cost analysis shows that the additional area and power overhead incurred by the proposed protection are 1.09% and 0.46%, respectively.

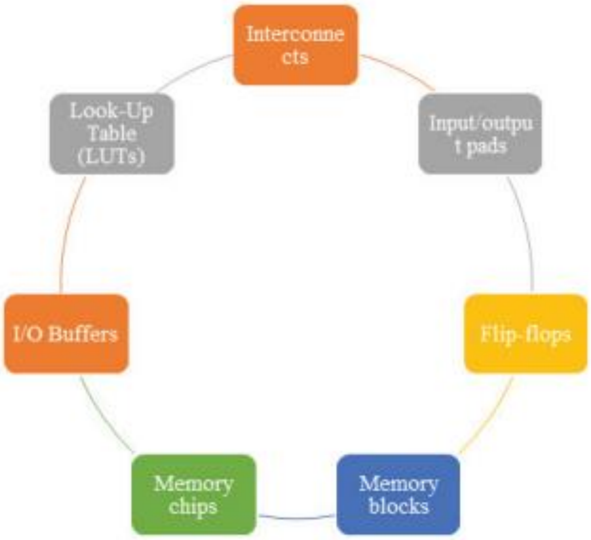


[4] This Paper by Dr.P.Sivakumar, Professor proposes cloud security is a developing part of computer devices and network security. Cloud platform usage is for third-person information model. In Here we talk about how to provide protection for the information, from the illegal abuser and offer probity to the client. It requires an extremely high level of confidentiality and verification. One of the examples for cloud platform as a service is Heroku. The Heroku is based on a fully administered structure, which includes high data services and a great system, for implementing and operating current applications. The leading concern in cloud computing is data protection, so it can be used to handle the cryptographic methods. A probabilistic method to encrypt the information using AES. At AES algorithm is not only for protection it can be also used in huge speed. AES provides well-built security from third party. In this proposed work, we implemented Heroku is a cloud platform, and then we apply the AES method for data protection in Heroku cloud. AES cryptography is able to use for

data security in cloud platform. And also using a dual cloud if one active or both active. If anyone cloud is active then the data should be more efficient in uploading and downloading operation perform in the cloud. Moreover, calculation delay in information to the encryption shows to better amount of information increase and the information time lag for encrypting information.



[5] As the technology is getting advanced continuously the problem for the security of data is also increasing. The hackers are equipped with new advanced tools and techniques to break any security system. Therefore people are getting more concern about data security. The data security is achieved by either software or hardware implementations. In this work Field Programmable Gate Arrays (FPGA) device is used for hardware implementation since these devices are less complex, more flexible and provide more efficiency. This work focuses on the hardware execution of one of the security algorithms that is the Advanced Encryption Standard (AES) algorithm. The AES algorithm is executed on Vivado 2014.2 ISE Design Suite and the results are observed on 28 nanometers (nm) Artix-7 FPGA. This work discusses the design implementation of the AES algorithm and the resources consumed in implementing the AES design on Artix-7 FPGA. The resources which are consumed are as follows- Slice Register (SR), Look-Up Tables (LUTs), Input/Output (I/O) and Global Buffer (BUFG).



III. REFERENCES

[1]. Vasundhara R. Pagar, “Strengthening Password Security through Honeyword and HoneyEncryption Technique” – IEEE,DOI: 10.1109/ICOEI.2017.8300819

[2]. Vatchara Saicheur, “An implementation of AES-128 and AES-512 on Apple mobile processor”-IEEE, DOI: 10.1109/ECTICon.2017.8096255

[3]. Liting Yu, “AES Design Improvements Towards Information Security Considering Scan Attack”-IEEE, DOI: 10.1109/TrustCom/BigDataSE.2018.00056

[4]. Dr.P.Sivakumar, Professor ,“Securing Data and Reducing the Time Traffic Using AES Encryption with Dual Cloud”-IEEE, DOI: 10.1109/ICSCAN.2019.8878749

[5]. Dr.P.Sivakumar ,“A Design Implementation and Comparative Analysis of Advanced Encryption Standard (AES) Algorithm on FPGA”-IEEE, DOI: 10.1109/ICRITO48877.2020.9198033

Cite this article as :

Sonia Maria D'souza, Rohan V. Chikalkar, Sayani Panda, Vipul Singh, Rohan Santra, "PassVaRRdS - Password Generator, Encrypting and Storage using AES and Cloud", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 9 Issue 1, pp. 139-142, January-February 2022. Available at doi : https://doi.org/10.32628/IJSRSET229139
Journal URL : https://ijsrset.com/IJSRSET229139