BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE

"Application of AES Cryptography algorithm for password manager"

BY

LOCADIA LISA MURISA

B1953743

SUPERVISOR: MR MATOMBO

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF BSc HONORS DEGREE IN INFORMATION TECHNOLOGY

Approval Form

The undersigned certify that they have supervised the student LOCADIA LISA MURISA's dissertation entitled application of AES cryptography algorithm for password manager submitted in Partial fulfilment of the requirements for the Bachelor of Computer Science Honors Degree of Bindura University of Science Education.

…… ……..

Name of student Date

.

…….. ……..

Name of supervisor Date

…….. ……..

Name of chairperson Date

…… ……

External examiner Date

Dedication

Dedicated to my family for the love and support they always give. To my friends and colleagues for helping me throughout the period.

Acknowledgments

I would like to thank and give praises to God the Almighty for the gift of life. A further acknowledgement goes to my family, parents and friends for the unconditional love and support throughout the journey. I would also like to express my gratitude to my lecturers for the support, encouragement and direction in the course of the research.

ABSTRACT

The research focuses on managing passwords using the password manager. AES cryptography algorithm is used to encrypt the user passwords. Henceforth, the main objective of the system is to design and implement a password manager cemented with AES cryptography algorithm to secure the user passwords. The researcher will therefore use the system to assess and evaluate the level of security to be reinforced with AES cryptography algorithm compared to other algorithms.

Contents

List of tables

List of figures

CHAPTER 1: INTRODUCTION

1.1 Introduction

The research is focusing on building a robust password manager in the future that is free from outside intruders. Therefore, the author was pleased to explore the field of cryptographic algorithms, by exploiting the AES cryptography algorithm. The researcher is required to design, analyse and produce a detailed account on the performance of the algorithm as it is applied on the password manager application to be designed by the researcher for evaluation purposes.

AES (Advanced Encryption Standard) Cryptography algorithm is designed to be an iterative rather than Feistel Cipher. Thus, henceforth it is designed to encrypt passwords (Lu, C. C., & Tseng, S. Y.,2002, pp. 277-285). It comprises a set of interconnected operations, some of which substitute certain outputs for inputs (substitutions), while others require shifting bits about (permutations). AES generates 128 bits of encrypted cipher text from 128 bits of input. AES operates utilizing a chain of linked operations that replace and shuffle the input data, which is known as the substitution-permutation network principle.

1.2 Background of the study

Software used to store and manage internet credentials is known as a password manager. These passwords are often kept in an encrypted database and secured by a master password. The author is required to implement AES algorithm during the course of designing the password manager application. The algorithm is to be used to encrypt the passwords. Assessment of the efficiency of the algorithm is to be done by the author by tabulation of results.

Once upon a time, during the early years of the Internet, you may have had a handful of passwords for a few essential web applications that you used to shop, study, stay connected, and get work done. Today, things are much more complicated. A 2017 report from LastPass found, on average, people had to remember 191 different passwords—just for work—not to mention their personal passwords.

While technology promises to make our lives easier, and it generally does, every new website and application we sign up for is another password we have to remember. For most, it’s become impossible to remember all of them. The 2019 Google Online Security Survey found 52 percent

of respondents reused the same password for multiple (but not all) accounts. This is a big no-no.

Using giant lists of stolen passwords (aka “dumps”) bought off the dark web, cybercriminals can brute force their way into other sites or use old passwords to extort users in scams. This is the data breach domino effect. One breach leads to another and another and so on. According to the 2019 Verizon Data Breach Investigations report, 80 percent of data breaches are caused by compromised, weak, and reused passwords (et al https://www.malwarebytes.com/what-is-password-manager 2022).

AES uses bytes rather than bits for all of its calculations. As a result, AES considers a plaintext block's 128 bits to be 16 bytes. For processing as a matrix, these 16 bytes are set up in a four-column by four-row arrangement. In contrast to DES, the number of rounds in AES varies and is based on the size of the key. For 128-bit keys, AES employs 10 rounds; for 192-bit keys, 12 rounds; and for 256-bit keys, 14 rounds. A separate 128-bit round key, derived from the initial AES key, is used for each of these rounds.

Some researchers have implemented three tier authentication passwords for security purposes. The three tier login authentication in the following routine. User is required to sign in providing his/her facial biometric images, basic text password and graphical text password. Therefore, upon these sign-up properties the user is required to login using the biometric facial login, graphical text login and finally basic text login. The three-tier login authentication was designed to cement systems from any form of invasion or intruders (et al Oreen Nyandoro Three Level Architecture Password Authentication System, 2021).

On the same field of security over the network, other researchers have exploited the hybrid architecture for encryption algorithms. Therefore, on this one researcher has to design two encryption algorithms and bond them together to produce a robust hybrid architecture.

1.3 Problem Statement

With exceeding number of attacks over the network, it has come to limelight for the author to further made a robust research on how best can the research reduce the cyber-attacks over the network. Globally due to advancement in technology a survey conducted using giant lists of stolen passwords (aka “dumps”) bought off the dark web (Verizon Data Breach Investigation , 2019), cybercriminals can brute force their way into other sites or use old passwords to extort users in scams. This is the data breach domino effect. One breach leads to another and another and so on. According to the 2019 Verizon Data Breach Investigations report, 80 percent of data

breaches are caused by compromised, weak, and reused passwords. The researcher will apply AES Cryptography to enhance high quality security for online passwords.

1.4 Research Aim

The research serves to implement a password manager application, cemented with the Advanced Encryption Standard Cryptography Algorithm. The algorithm is to be applied for encrypting the passwords. The researcher is exploiting the field of Cybersecurity in a notion to reduces risks of intruders on one's passwords. Therefore, helps in reinforcing heavily any risks for a user to be exposed to externals intruding and keeping the passwords safely.

1.5 Research Objectives

- To design and implement a password manager application
- To implementation the Advanced Encryption Standard Cryptography Algorithm
- Evaluate the efficiency and effectiveness of the AES Cryptography Algorithm

1.6 Research Questions

- How the author is going to design and implement a password manager application?
- How the researcher is going to implement the Advanced Encryption Standard Cryptography Algorithm?
- How the author is going to evaluate the efficiency and effectiveness of the AES Cryptography algorithm?

1.7 Significance of the study

Due to a survey which has been done using giant lists of stolen passwords (aka "dumps") bought off the dark web, cybercriminals can brute force their way into other sites or use old passwords to extort users in scams. This is the data breach domino effect. One breach leads to another and another and so on. According to (Berent .A , 2013) , 76 percent of data breaches are caused by compromised, weak, and reused passwords

(https://www.malwarebytes.com/what-is-password-manager 2022).Therefore the researcher has discovered that it is worth it to develop a robust and most secured password to avoid any breaches that can happen to the users over the network.

1.8 Scope of the study

The research will be exploiting the field of cybersecurity and its attacks over the network. Globally due to advancement in technology a survey conducted using giant lists of stolen passwords (aka "dumps") bought off the dark web, cybercriminals can brute force their way into other sites or use old passwords to extort users in scams. This is the data breach domino effect. One breach leads to another and another and so on. The research will help the author to come up with conclusions on whether the application of AES Cryptography algorithm will help in reducing the risks on being attacked by externals or intruders.

1.9 Research justification

Application of AES algorithm on implementing the password manager software application will be a great value to every individual using the internet. Due to rise of internet account, there is need for a password manager (Reddy, M. S., & Babu, Y. A. 2013), to store one's passwords on a specific software application. The AES algorithm is expected to deliver a robust and reinforced security feature on the passwords that will help on reducing risks of being attacked or hacked over the network.

1.10 Research Limitation

- The use of Facebook and another social media account due to lack of apis which are not easily provided by the giant companies

1.11 Definition of terms

AES – Advanced Encryption Standard

DES – Data Encryption Standard

Cryptography- provides for secure communication in the presence of malicious third-parties

Encryption - the process of converting information or data into a code, especially to prevent unauthorized access.

Decryption- the conversion of encrypted data into its original form

Password - a string of characters that allows access to a computer system or service

1.12 Conclusion

This current chapter elaborates the current system's flaws, as well as the prospective system's goal and objectives. The next chapter will cover the literature review and demonstrates some of the past work that has been done in relation to this research.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

Literature review entails the methodical gathering, organization, and analysis of papers containing information about the study subject under consideration. Its goal is to provide in-depth understanding of the subject being researched. It aids the researcher in discovering what other researchers have done in relation to the subject under investigation. It assists a researcher in avoiding unnecessary and unintended duplication, as well as providing a framework for interpreting study findings (Mugenda and Mugenda, 2013).

This chapter will look at literature reviews related to the application of the writer's system. Functionalities, benefits of implementation, key steps for successful implementation, challenges of implementation, successes and opportunities for success, objectives of implementing electronic and document management systems, best practices, and electronic records management standards are all covered in the reviewed literature.

2.2 Preview and background of the research

Software used to store and manage internet credentials is known as a password manager. These passwords are often kept in an encrypted database and secured by a master password. The author is required to implement AES algorithm during the course of designing the password manager application. The algorithm is to be used to encrypt the passwords. Assessment of the efficiency of the algorithm is to be done by the author by tabulation of results.

Once upon a time, during the early years of the Internet, you may have had a handful of passwords for a few essential web applications that you used to shop, study, stay connected, and get work done. Today, things are much more complicated. A 2017 report from LastPass found, on average, people had to remember 191 different passwords—just for work—not to mention their personal passwords.

While technology promises to make our lives easier, and it generally does, every new website and application we sign up for is another password we have to remember. For most, it's become impossible to remember all of them. The 2019 Google Online Security Survey found 52 percent of respondents reused the same password for multiple (but not all) accounts. This is a big no-no.

Using giant lists of stolen passwords (aka "dumps") bought off the dark web, cybercriminals can brute force their way into other sites or use old passwords to extort users in scams. This is the data breach domino effect. One breach leads to another and another and so on. According to the 2019 Verizon Data Breach Investigations report, 80 percent of data breaches are caused by compromised, weak, and reused passwords (et al https://www.malwarebytes.com/what-is-password-manager 2022).

AES uses bytes rather than bits for all of its calculations. As a result, AES considers a plaintext block's 128 bits to be 16 bytes. For processing as a matrix, these 16 bytes are set up in a four-column by four-row arrangement. In contrast to DES, the number of rounds in AES varies and is based on the size of the key. For 128-bit keys, AES employs 10 rounds; for 192-bit keys, 12 rounds; and for 256-bit keys, 14 rounds. A separate 128-bit round key, derived from the initial AES key, is used for each of these rounds.

Some researchers have implemented three tier authentication passwords for security purposes. The t three tier login authentication in the following routine. User is required to sign in providing his/her facial biometric images, basic text password and graphical text password. Therefore, upon these sign-up properties the user is required to login using the biometric facial login, graphical text login and finally basic text login. The three-tier login authentication was designed to cement systems from any form of invasion or intruders (et al Oreen Nyandoro Three Level Architecture Password Authentication System 2021).

On the same field of security over the network, other researchers have exploited the hybrid architecture for encryption algorithms. Therefore, on this one researcher has to design two encryption algorithms and bond them together to produce a robust hybrid architecture.

2.3 Advanced Encryption Standard (AES)

The National Institute of Standards and Technology (NIST) of the United States developed it as a specification for the encryption of electronic data in 2001. Despite being more difficult to build, AES is still commonly used because it is substantially stronger than DES and triple DES.

The output is 128 bits of encrypted cipher text after receiving 128 bits as input. AES operates utilizing a chain of linked operations that replace and shuffle the input data, which is known as the substitution-permutation network principle.

Working of the cipher:

AES performs operations on bytes of data rather than in bits. Since the block size is 128 bits, the cipher processes 128 bits (or 16 bytes) of the input data at a time.

The number of rounds depends on the key length as follows:

- 128 bits key – 10 rounds
- 192 bits key – 12 rounds
- 256 bits key – 14 rounds

Creation of Round keys:

A Key Schedule algorithm is used to calculate all the round keys from the key. So, the initial key is used to create many different round keys which will be used in the corresponding round of the encryption.

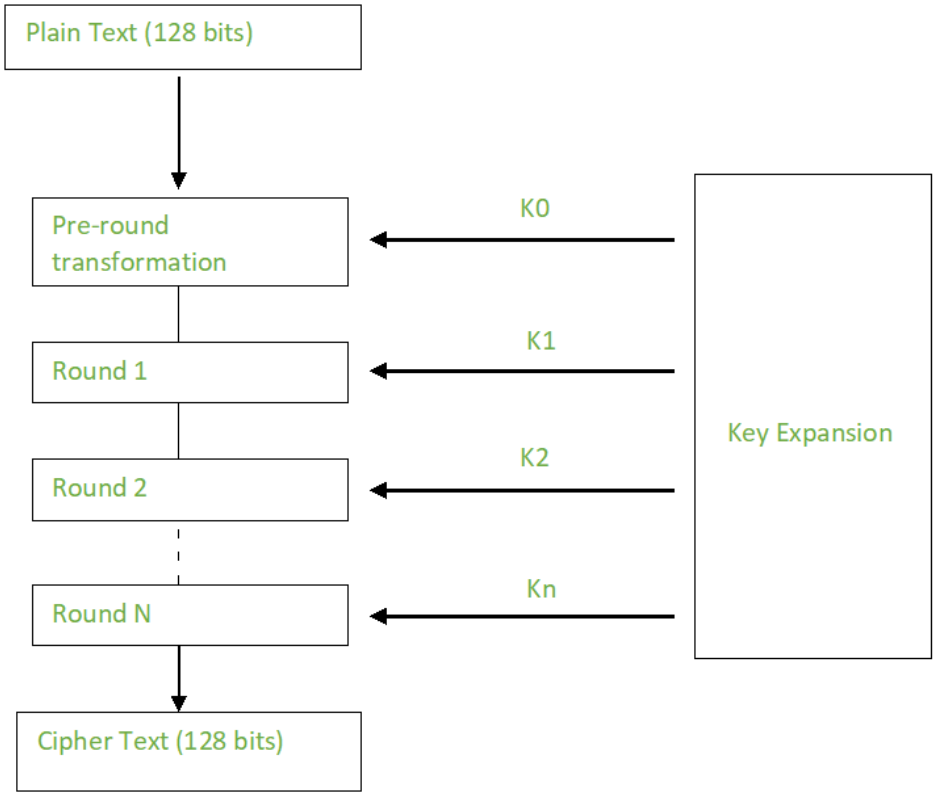


Figure 1

Encryption:

AES considers each block as a 16 byte (4 byte x 4 byte = 128) grid in a column major arrangement.

[b0 | b4 | b8 | b12 |

| b1 | b5 | b9 | b13 |

| b2 | b6 | b10| b14 |

| b3 | b7 | b11| b15]

Each round comprises of 4 steps:

- Sub Bytes
- Shift Rows
- Mix Columns
- Add Round Key

The Sub Bytes does the substitution and Shift Rows and Mix Columns performs the permutation in the algorithm.

Sub Bytes:

This step implements the substitution.

In this step each byte is substituted by another byte. It performed using a lookup table also called the S-box. This substitution is done in a way that a byte is never substituted by itself and also not substituted by another byte which is a compliment of the current byte. The result of this step is a 16-byte (4 x 4) matrix like before.

The next two steps implement the permutation.

Shift Rows:

This step is just as it sounds. Each row is shifted a particular number of times.

- The first row is not shifted
- The second row is shifted once to the left.
- The third row is shifted twice to the left.
- The fourth row is shifted thrice to the left.

2.4 AES analysis

In present day cryptography, AES is widely adopted and supported in both hardware and software. Till date, no practical cryptanalytic attacks against AES have been discovered. Additionally, AES has built-in flexibility of key length, which allows a degree of 'future-proofing' against progress in the ability to perform exhaustive key searches.

However, just as for DES, the AES security is assured only if it is correctly implemented and good key management is employed.

2.5 Data Encryption Standard (DES)

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only).

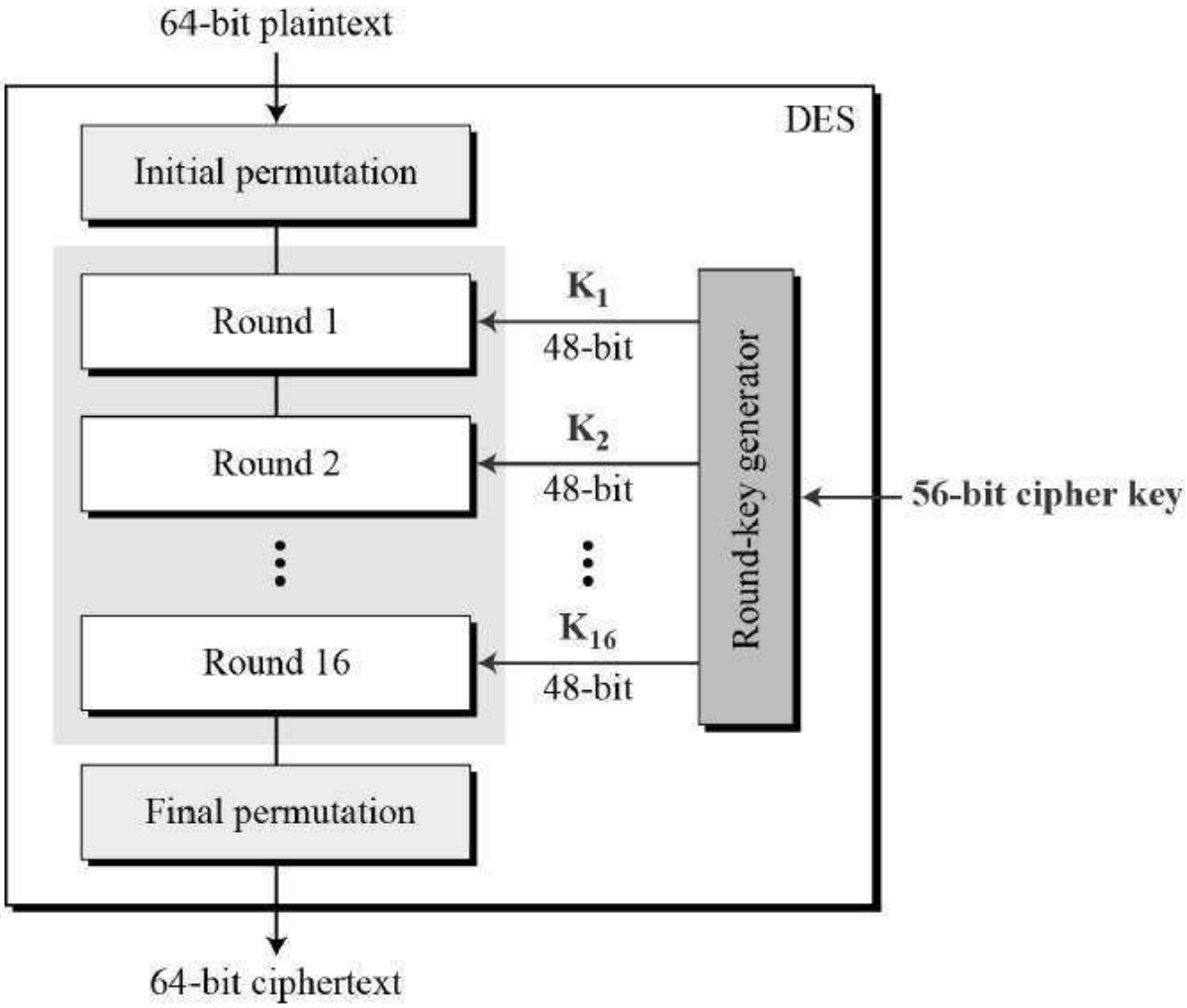


Figure 2

Since DES is based on the Feistel Cipher, all that is required to specify DES is −

- Round function
- Key schedule
- Any additional processing − Initial and final permutation

Initial and final permutation

The initial and final permutations are straight Permutation boxes (P-boxes) that are inverses of each other. They have no cryptography significance in DES. The initial and final permutations are shown below:

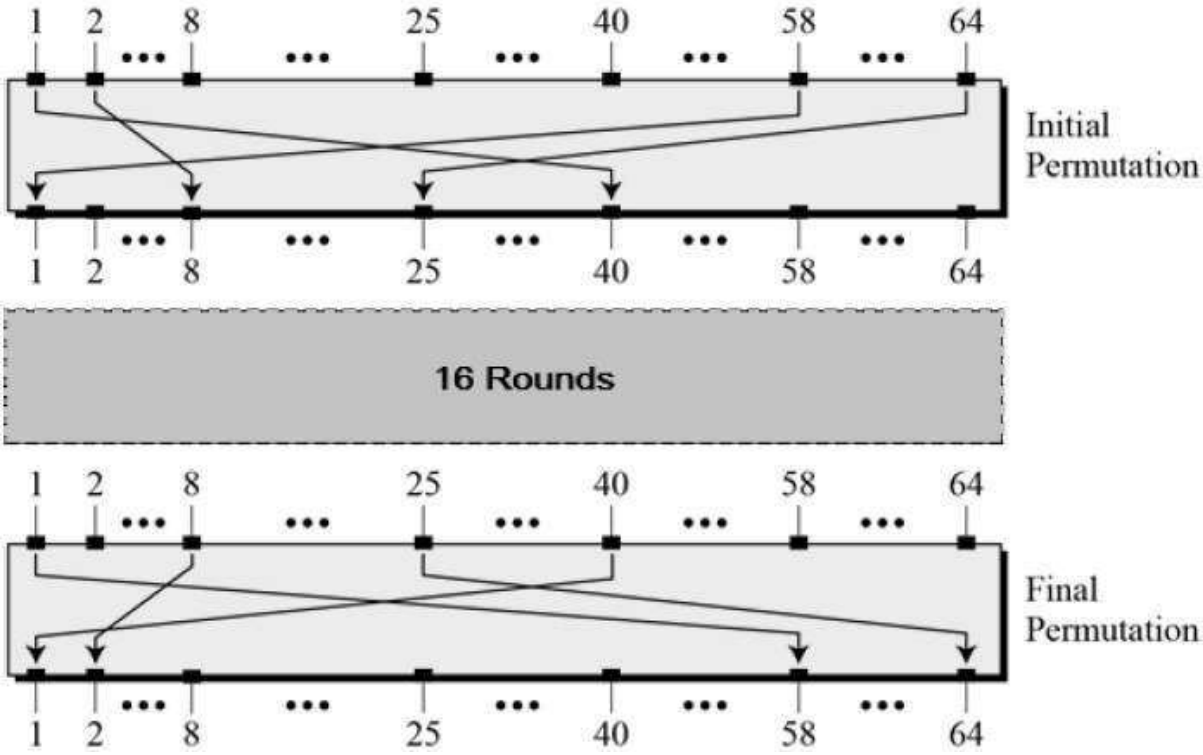


Figure 3

Round Function

The heart of this cipher is the DES function, *f*. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.

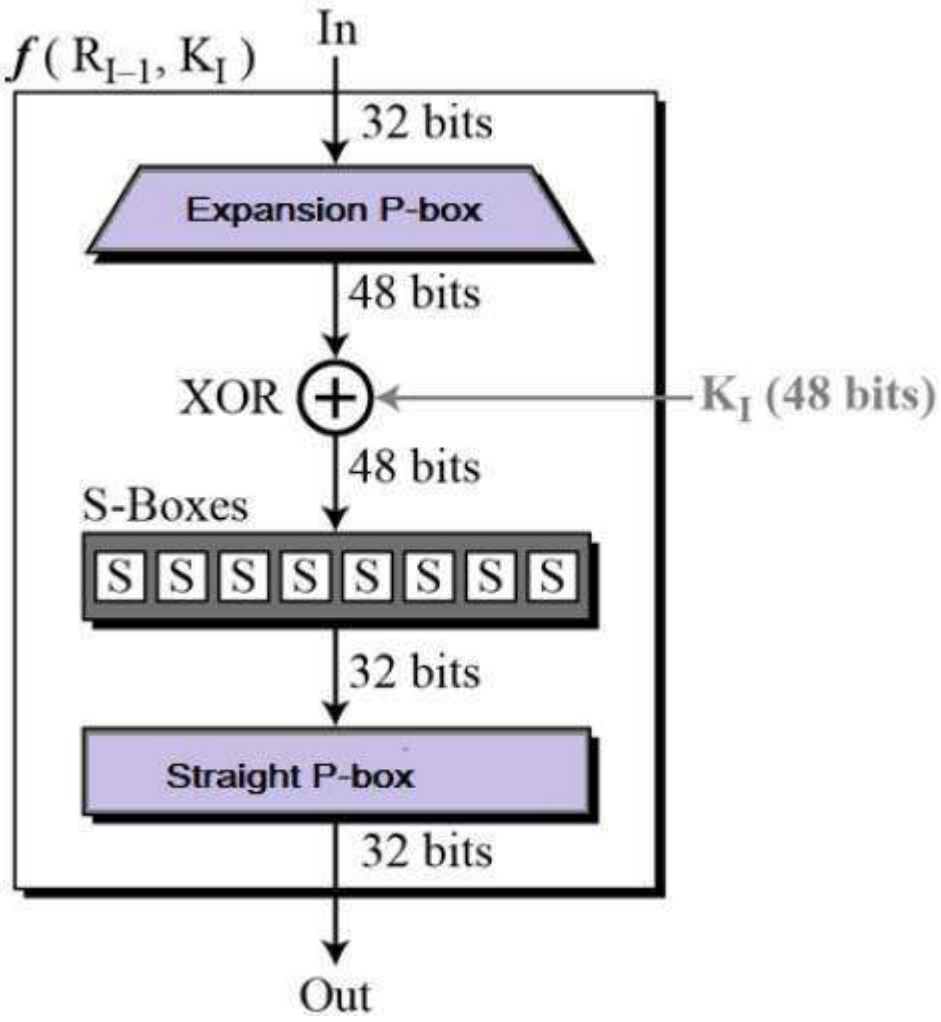


Figure 4

Expansion Permutation Box

Since right input is 32-bit and round key is a 48-bit, we first need to expand right input to 48 bits. Permutation logic is graphically depicted in the following illustration:

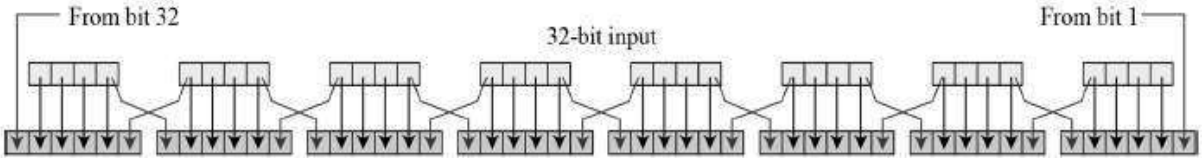


Figure 5

The graphically depicted permutation logic is generally described as table in DES specification illustrated as shown below:

32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	31	31	32	01

Table 1

XOR (Whitener)

After the expansion permutation, DES does XOR operation on the expanded right section and the round key. The round key is used only in this operation.

Substitution Boxes

The S-boxes carry out the real mixing (confusion). DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output. Refer the following illustration

z

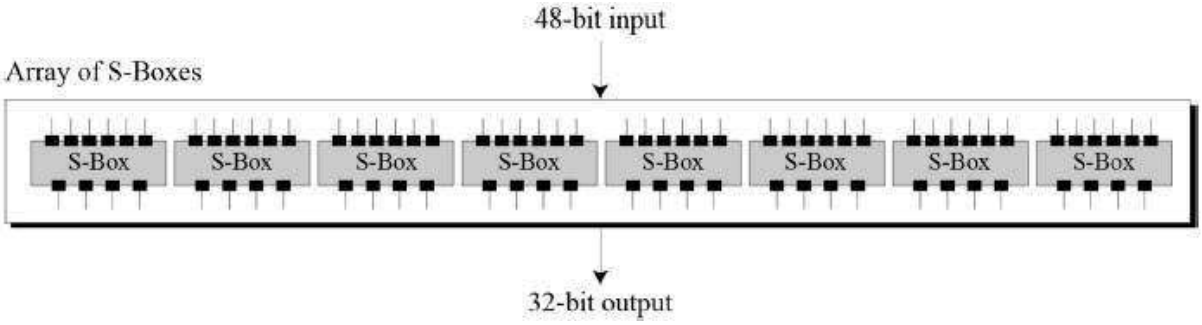


Figure 6

Previous Related Studies

Different researchers recommend different methods of protection. In this section I will prepare the research literature of the works done in this field.

In 2010 S. Subashini and V. Kavitha proposes a security framework by different methods provided dynamically, that one of the components of this framework refers to provide data

security by storage and access to data based on meta-data, which is similar to storing related data in different areas based on meta data, and if the destruction of user data takes place, it can be retrieved. Each part of the framework in "security as a service" is provided for practical applications by providers of security as a layer or multiple layers of required applications.

Pradeep Bhosale et.al, (2012), discuss that today's world relies on cloud computing to store their public as well as some personal information which is needed by the user itself or some other persons. Cloud service is any service offered to its users by cloud. As cloud computing comes in service there are some drawbacks such as privacy of user's data, security of user data is a very important aspect. He talks about the enhancement of data security. Not only this makes researchers to make some modifications in the existing cloud structure, invent new model cloud computing and much more but also there are some extensible features of cloud computing.

Jasmin James, et.al, (2012), discuss about the security in cloud computing. Cloud computing is fast growing area in computing research. With the advancement of the Cloud, many new possibilities are coming into picture, like how applications can be built and how different services can be offered to the end user through Virtualization. There are the cloud services providers who provide large scaled computing infrastructure defined on usage, and provide the infrastructure services in a very flexible manner.

Tejinder Sharma, et.al, (2013), in this paper author discuss about the cloud computing. As, the computer networks are still in their infancy, but they grow up and become sophisticated. Cloud computing is emerging as a new paradigm of large-scale distributed computing. It has moved computing and data away from desktop and portable PCs, into large data centers. It has the capability to harness the power of Internet and wide area network to use resources that are available remotely. There are many security issues in the cloud computing.

In 2014 Sudhansu Ranjan Lenka et. al. wrote a paper. In this model they have implemented a combination of RSA encryption and digital signature technique which can easily with all types of cloud computing features like, PaaS, SaaS and IaaS. This combination mechanism provides

three-way security, that is, data security, authentication and verification. In this paper, they have proposed RSA encryption algorithm for confidentiality of data and for authentication.

In 2014 Swarnalata Bollavarapu and Bharat Gupta propose data storage security system in cloud computing. These system use algorithms like RSA, ECC and RC4 for encryption and decryption techniques.

In 2015 Karun Handa et. al. described that Cloud Computing is a technology that readily makes available resources that otherwise may require huge amount of investment. Besides, it increases the availability of resources since anyone can access the data using web. But this advantage comes at a cost. Firstly, the data is uploaded insecurely which has a high risk of being hacked by some malicious people. Secondly, the data saved at remote servers is under the surveillance of unknown people who can do anything with our data. So, these data security risks are causing a hindrance in the development of the field of cloud computing.

In 2016 Sarojini et.al proposed a technique known as Enhanced Mutual Trusted Access Control Algorithm (EMTACA). This technique presents a mutual trust for both cloud users and cloud service providers to avoid security related issues in cloud computing. The aim was to propose a system which include EMTACA algorithm which can assure enhanced guaranteed and trusted and reputation based cloud services among the users in a cloud environment. The results showed data confidentiality, integrity and availability which is the three most important aspects of data security.

(Dimitra A. Geogiou, 2017), wrote a paper to present security policies for cloud computing. The purpose of the security policies is to protect people and information, set rules for expected behaviour by users, minimize risks and help to track compliance with regulation. The paper focused on Software as a Service. The paper presented a detailed review and analysis of existing studies as far as security is concern in cloud computing. To be able to identify new rules that supposed to be integrated in the cloud policy, a methodology was proposed for

assessing different threats in the cloud. The paper scrutinized the security requirements of a cloud service provider taking into consideration a case study of E-health system of Europe.

2.6 Benefits of the proposed system

While technology promises to make our lives easier, and it generally does, every new website and application we sign up for is another password we have to remember. For most, it's become impossible to remember all of them. The 2019 Google Online Security Survey found 52 percent of respondents reused the same password for multiple (but not all) accounts. This is a big no-no. Using giant lists of stolen passwords (aka "dumps") bought off the dark web, cybercriminals can brute force their way into other sites or use old passwords to extort users in scams. This is the data breach domino effect. One breach leads to another and another and so on. According to the 2019 Verizon Data Breach Investigations report, 80 percent of data breaches are caused by compromised, weak, and reused passwords (et al https://www.malwarebytes.com/what-is-password-manager 2022).Therefore the research will help implement a strong, robust and secure password.

2.7 The proposed system

The research serves to implement a password manager application, cemented with the Advanced Encryption Standard Cryptography Algorithm. The algorithm is to be applied for encrypting the passwords. The researcher is exploiting the field of Cybersecurity in a notion to reduces risks of intruders on one's passwords. Therefore, helps in reinforcing heavily any risks for a user to be exposed to externals intruding and keeping the passwords safely.

2.8 Conclusion

This chapter outlined and brought into perspective some reliable security technology to prevent security attacks, as well as the damage of infrastructure and services. There is no doubt that the AES cryptography algorithm is the development trend in the future. Application of AES algorithm on password manager software brings the approximately infinite computing capability, good scalability, service on-demand and also challenges at security, privacy and legal issues associated with it. But to solving the existing issues also becomes an utmost

urgency to protect against the compromise of the compliance integrity and security of their applications and data, firewall, intrusion detection and prevention, integrity monitoring, log inspection, and malware protection.

CHAPTER 3: RESEARCH METHODOLOGY

3.1 INTRODUCTION

The chapter aims to define the strategies and tools used to achieve the proposed objectives of research and system. With the help of the information attained in the previous chapter the author will formulate the necessary methods to build a solution and be able to make choices among competing strategies to achieve the expected results of the research

While technology promises to make our lives easier, and it generally does, every new website and application we sign up for is another password we have to remember. For most, it's become impossible to remember all of them. The 2019 Google Online Security Survey found 52 percent of respondents reused the same password for multiple (but not all) accounts. This is a big no-no.

Using giant lists of stolen passwords (aka "dumps") bought off the dark web, cybercriminals can brute force their way into other sites or use old passwords to extort users in scams. This is the data breach domino effect. One breach leads to another and another and so on. According to the 2019 Verizon Data Breach Investigations report, 80 percent of data breaches are caused by compromised, weak, and reused passwords (et al https://www.malwarebytes.com/what-is-password-manager 2022).

3.1.1 RESEARCH DESIGN

Research design should be a reflexive process operation through every stage of a project. The design stage involves coming up with the different modules of the system and their intended functionality. The core objective of this stage is to ensure that an operative, proficient, sustainable and reliable system is designed. Thus there should be a designed application by the researcher that will be used to demonstrate the author's research topic.

3.2 REQUIREMENTS ANALYSIS

Requirements analysis is critical to the failure or success of a project and the formulated requirements need to be realistic, documented, testable, actionable, traceable, measurable, related to identified business needs and detailed enough to facilitate the system design (Abram Moore, Bourque, & Dupuis 2004).

At this point, it is thus essential to record all the functional and non-functional specifications of the required system. It is advisable to structure all the incoming data, asses it as well as considering all the limitations which may arise on the consumer's side and come up with a ready to follow specification which may arise on the consumer's needs. The researcher also took into consideration all the limitations that may arise such as budget restrictions that may impede the design method.

3.2.1 FUNCTIONAL REQUIREMENTS

Defines the functions of a system or its modules, whereby the function is typically a specification of the interaction between inputs and outputs (Fulton & Vandermolen, 2017). Thus, functional requirements outline the system service provided on completion of certain tasks at hand by how the system respond to the set of inputs, the behaviour and output.

The proposed system must be able to meet the following requirements:

- Admin should be able to monitor all user accounts
- User should be able to store all passwords for different sites
- User should be able store encrypted passwords

3.2.2 NON-FUNCTIONAL REQUIREMENTS

They are often referred to as quality requirements and used to judge the performance of a system rather than its intended behaviour. The proposed system must be able to meet the following:

- System should have very relatively small response time and decision time
- The system should be easy to assemble

3.3TOOLS USED (Hardware and Software)

- PyCharm
- Python 3.9
- AES crypto library

3.4 SYSTEM DEVELOPMENT

This describes the overview of the system and how it was developed so as to produce the results. Thus, it specifies all the software tools and models used in the development of the system.

3.4.1 SYSTEM DEVELOPMENT TOOLS

The researcher is using python as a programming language to develop an application to be used for testing. This application serves as a tool to test for results. The AES crypto library is to be used to encrypt the passwords to be stored with the user. Henceforth the research is based on determining on how strong and secure are passwords when they are being encrypted with AES algorithm. Therefore, the AES Crypto library will enhance its abilities on coming up with a possible decision, thus if the encryption is strong and secure or not.

3.4.2 BUILD METHODOLOGY

- Prototyping Development- Evolutionary prototyping

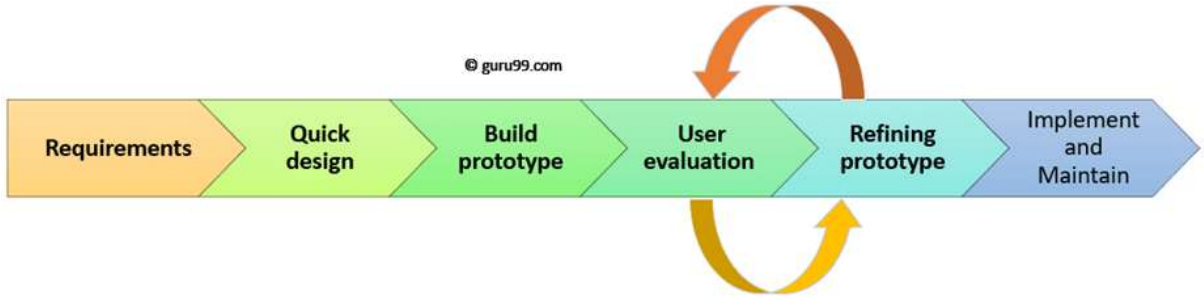


Figure 7

3.4.3 PROTOTYPE

The prototype are usually not complete systems and many of the details are not built in. The goal is to provide a system with overall functionality.

3.4.4 ADVANTAGES OF PROTOTYPE

- Users are actively involved in the development
- Since in this methodology a working model of the system is provided, the users get a better understanding of the system being developed.
- Errors can be detected much earlier.

- Quicker user feedback is available leading to better solutions.
- Missing functionality can be identified easily

3.4.5 DISADVANTAGES OF PROTOTYPE

- Leads to implementing and then repairing way of building systems.
- Practically, this methodology may increase the complexity of the system as scope of the system may expand beyond original plans.

3.5 TECHNOLOGY USED

- Python
- AES Crypto library

3.6 ALGORITHMS USED

- AES Algorithm

3.7 AES ALGORITHM

The National Institute of Standards and Technology (NIST) of the United States developed it as a specification for the encryption of electronic data in 2001. Despite being more difficult to build, AES is still commonly used because it is substantially stronger than DES and triple DES.

The output is 128 bits of encrypted cipher text after receiving 128 bits as input. AES operates utilizing a chain of linked operations that replace and shuffle the input data, which is known as the substitution-permutation network principle.

Working of the cipher:

AES performs operations on bytes of data rather than in bits. Since the block size is 128 bits, the cipher processes 128 bits (or 16 bytes) of the input data at a time.

The number of rounds depends on the key length as follows:

- 128 bits key – 10 rounds
- 192 bits key – 12 rounds
- 256 bits key – 14 rounds

Creation of Round keys:

A Key Schedule algorithm is used to calculate all the round keys from the key. So, the initial key is used to create many different round keys which will be used in the corresponding round of the encryption.

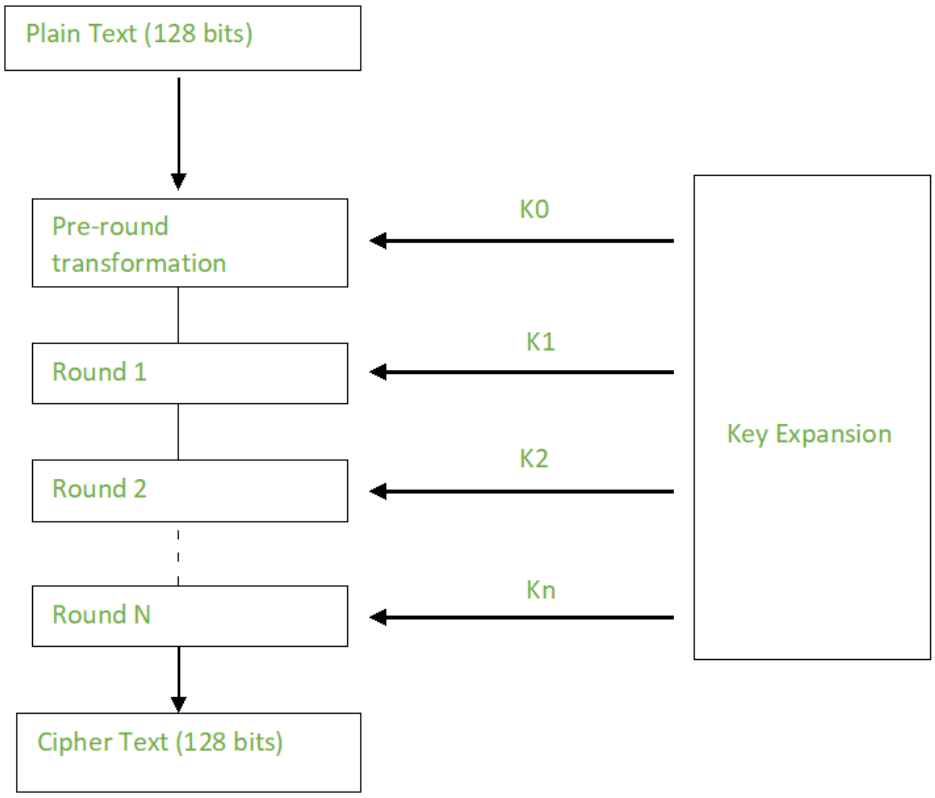


Fig 1

Encryption:

AES considers each block as a 16 byte (4 byte x 4 byte = 128) grid in a column major arrangement.

[b0 | b4 | b8 | b12 |

| b1 | b5 | b9 | b13 |

| b2 | b6 | b10| b14 |

| b3 | b7 | b11| b15]

Each round comprises of 4 steps:

- Sub Bytes
- Shift Rows
- Mix Columns
- Add Round Key

The Sub Bytes does the substitution and Shift Rows and Mix Columns performs the permutation in the algorithm.

Sub Bytes:

This step implements the substitution.

In this step each byte is substituted by another byte. It performed using a lookup table also called the S-box. This substitution is done in a way that a byte is never substituted by itself and also not substituted by another byte which is a compliment of the current byte. The result of this step is a 16-byte (4 x 4) matrix like before.

The next two steps implement the permutation.

Shift Rows:

This step is just as it sounds. Each row is shifted a particular number of times.

- The first row is not shifted
- The second row is shifted once to the left.
- The third row is shifted twice to the left.
- The fourth row is shifted thrice to the left.

3.8 GENERAL OVERVIEW OF PASSWORD MANAGER APPLICATION USING AES ALGORITHM

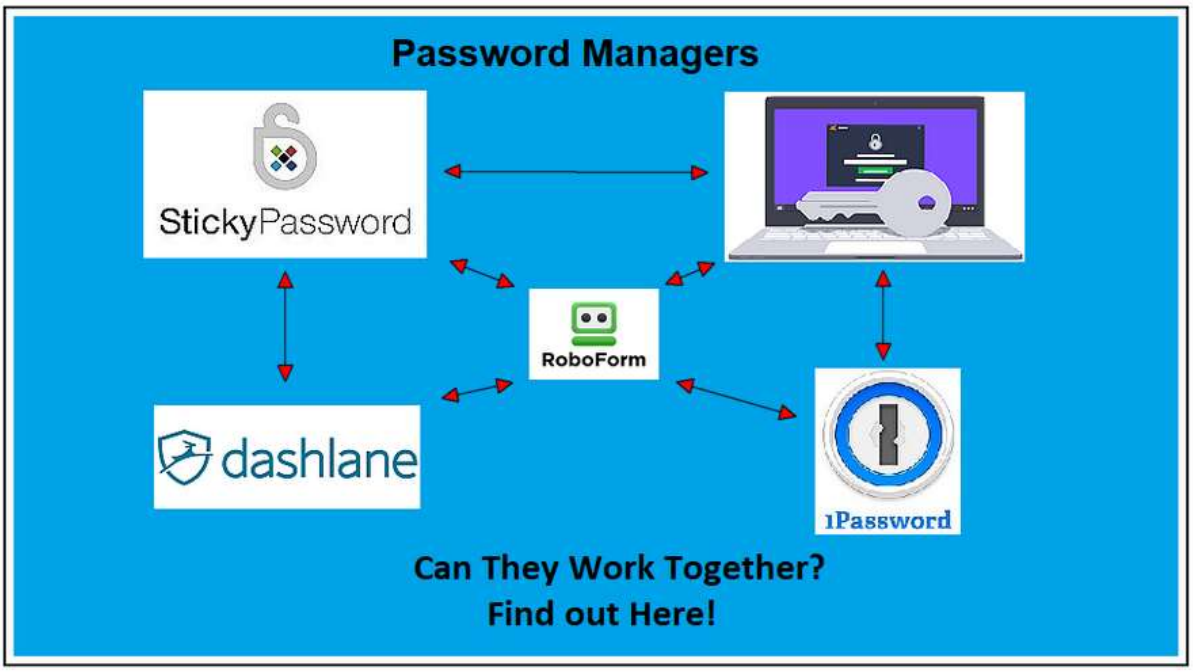


Figure 8

3.9 PROPOSED SYSTEM FLOWCHART

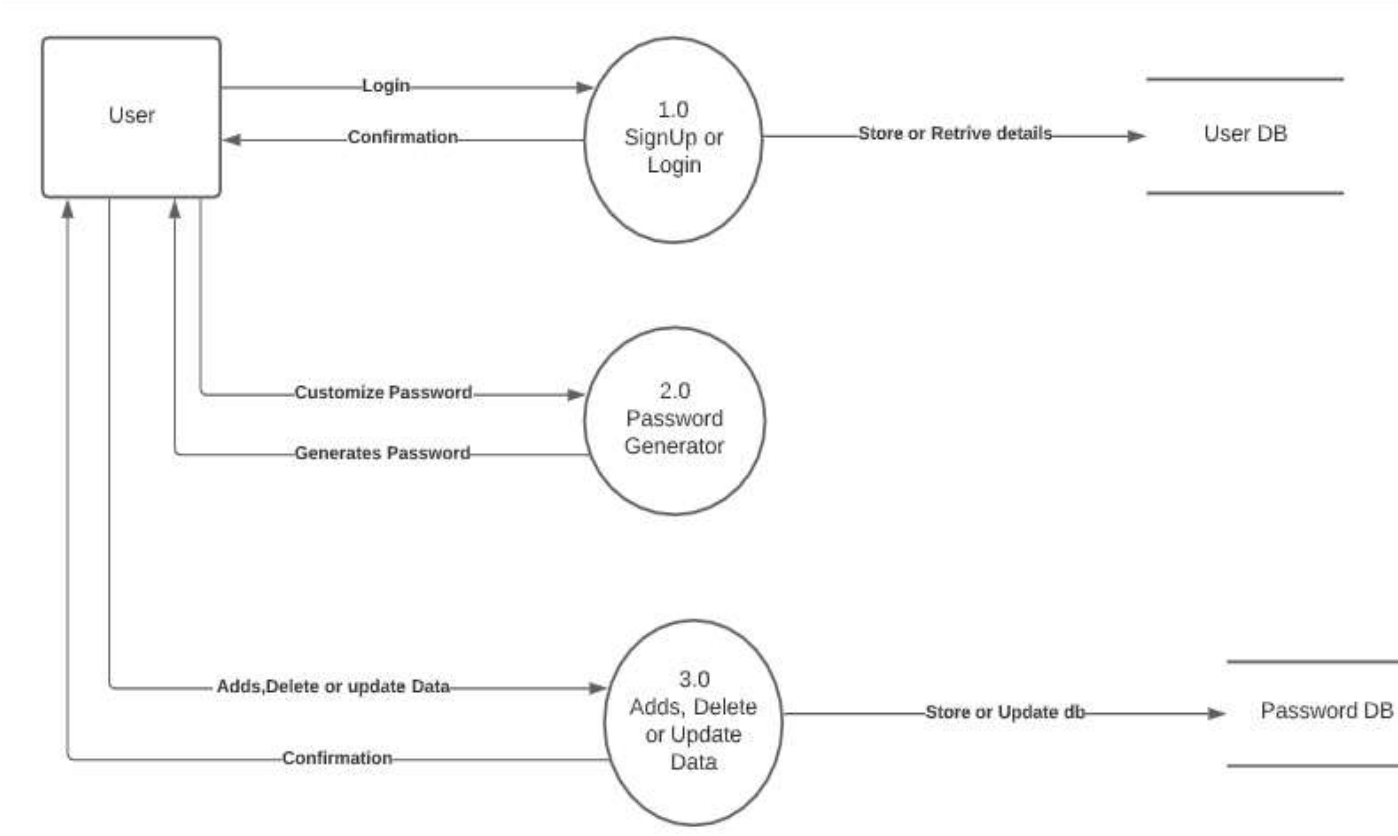


Figure 9

3.10 IMPLEMENTATION

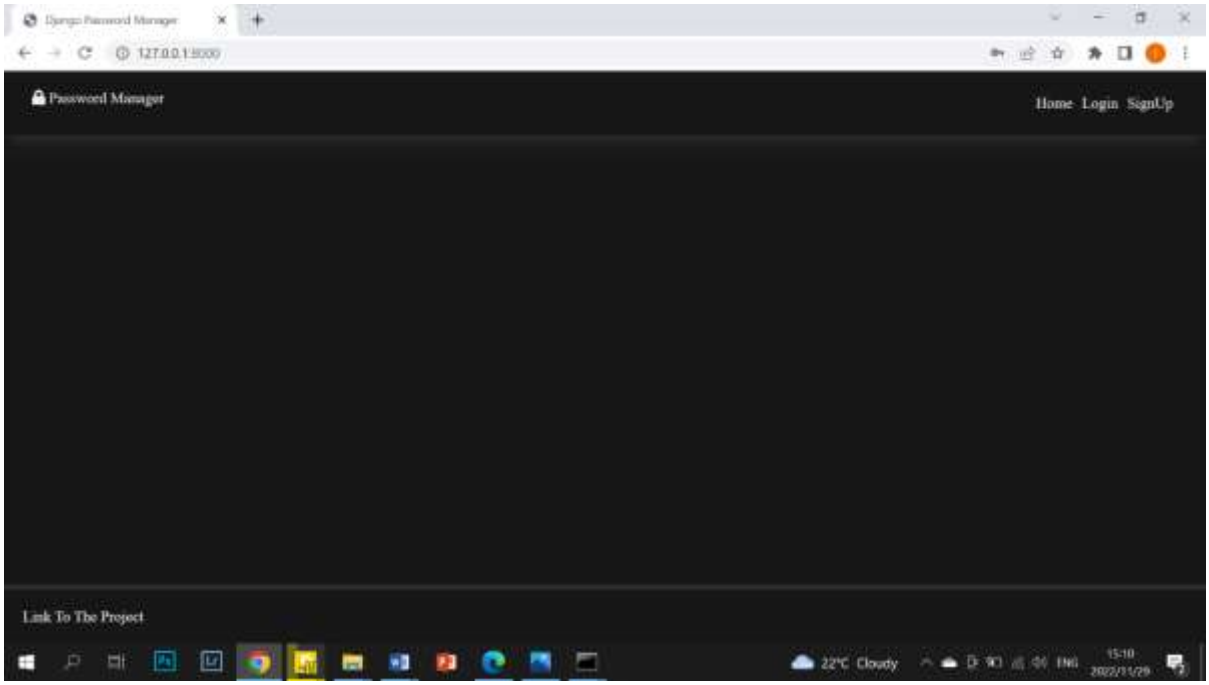
This section implicates setting the system into action thus coordination and directing the resources elaborated in the previous chapter to meet the objectives of the research plan. Thus, all the documentation from all previous chapters being finalized to align it in order to deliver the system. The application is required to secure data or passwords for individuals, which are securely encrypted with AES algorithm.

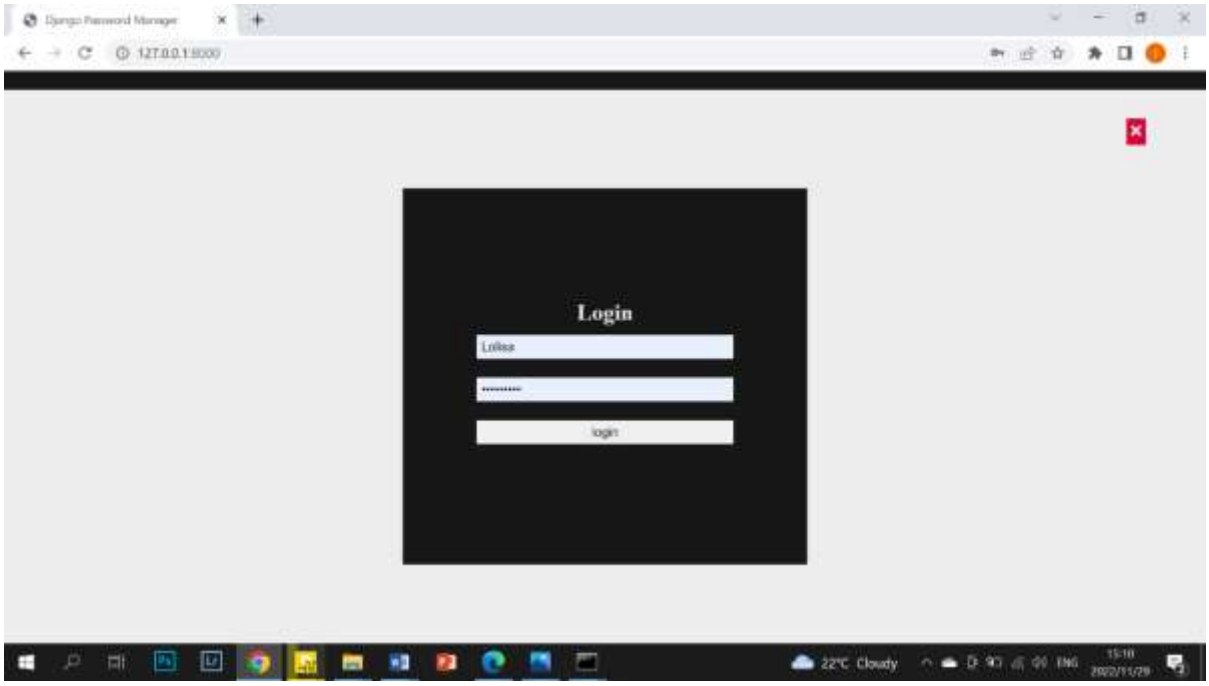
3.11 AES CRYPTOGRAPHY PASSWORD MANAGER APPLICATION

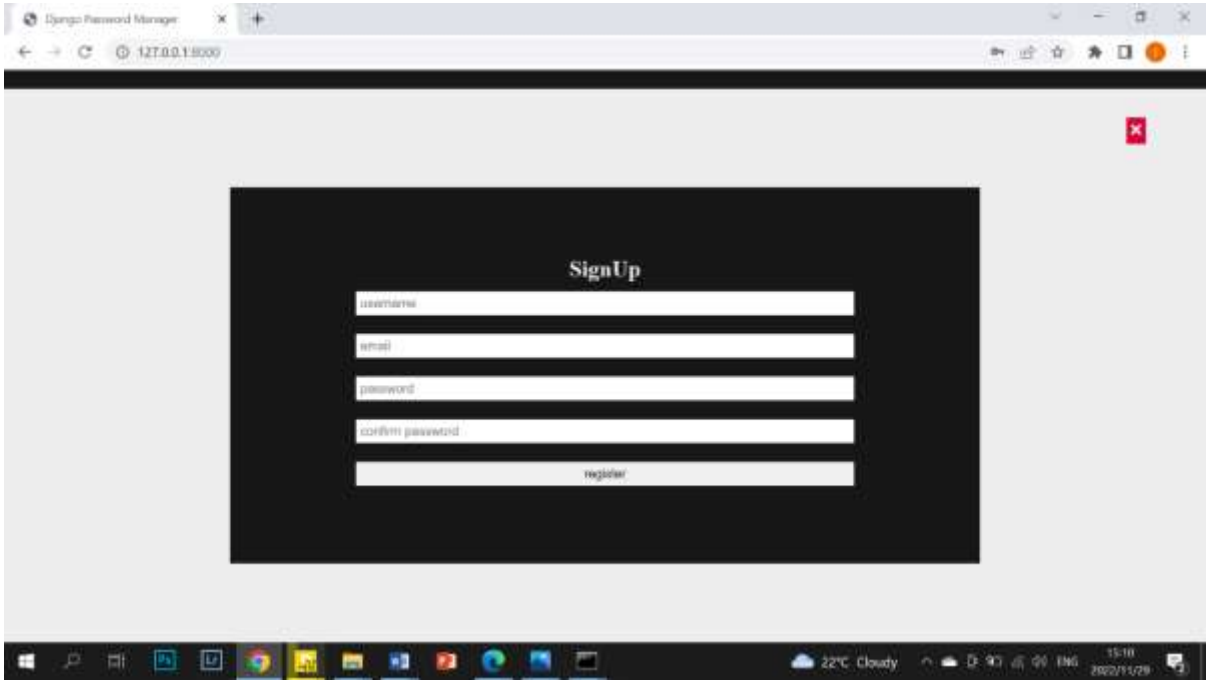
```
#!/usr/bin/env python
"""Django's command-line utility for administrative tasks."""
import os
import sys


def main():
    """Run administrative tasks."""
    os.environ.setdefault('DJANGO_SETTINGS_MODULE', 'PROJECTNAME.settings')
    try:
        from django.core.management import execute_from_command_line
    except ImportError as exc:
        raise ImportError(
            "Couldn't import Django. Are you sure it's installed and "
            "available on your PYTHONPATH environment variable? Did you "
            "forget to activate a virtual environment?"
```

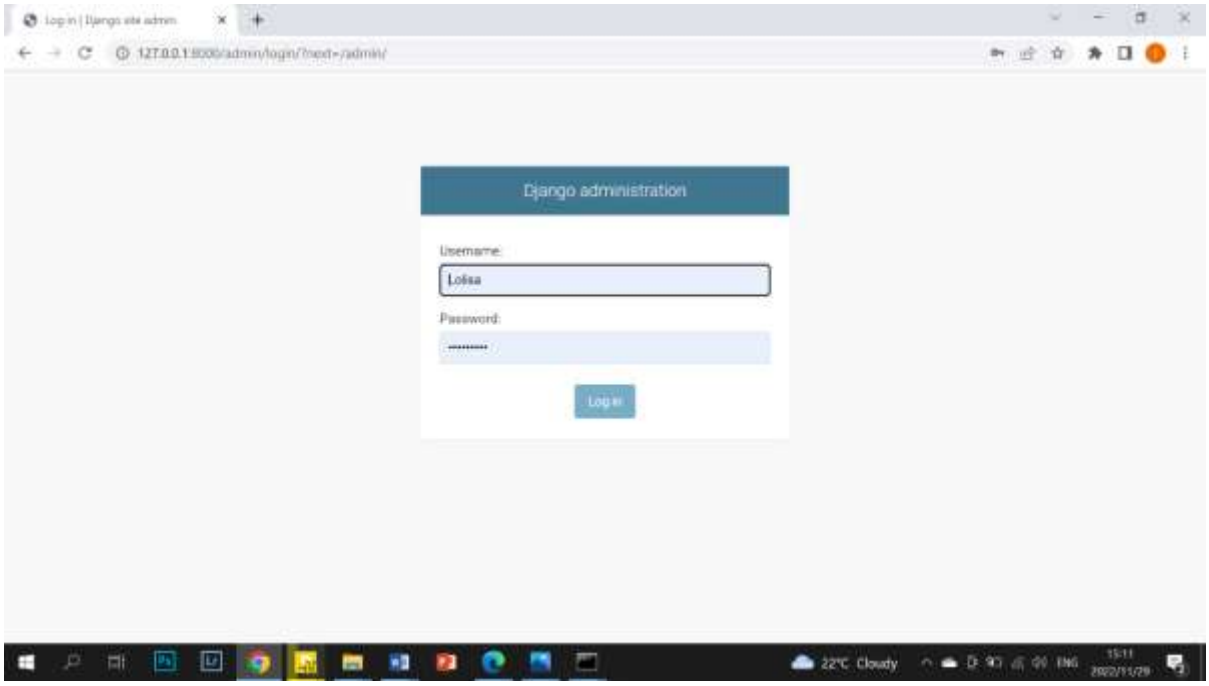
Figure 10

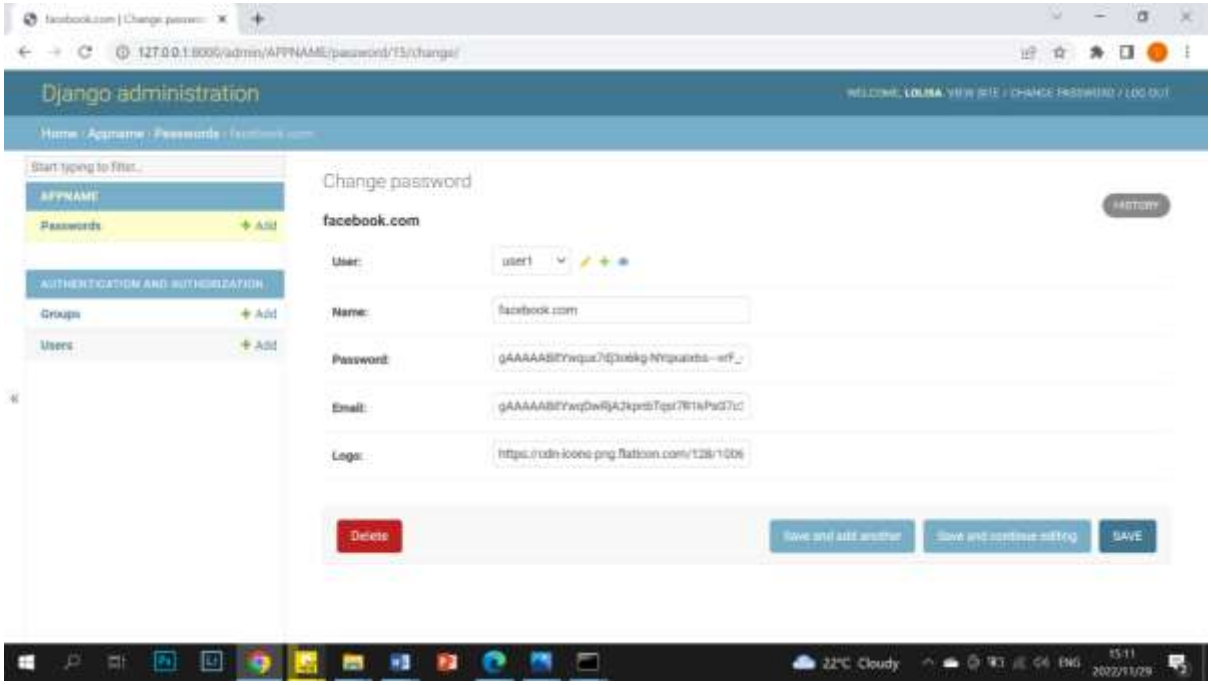
3.12 SUMMARY OF HOW THE SYSTEM WORKS

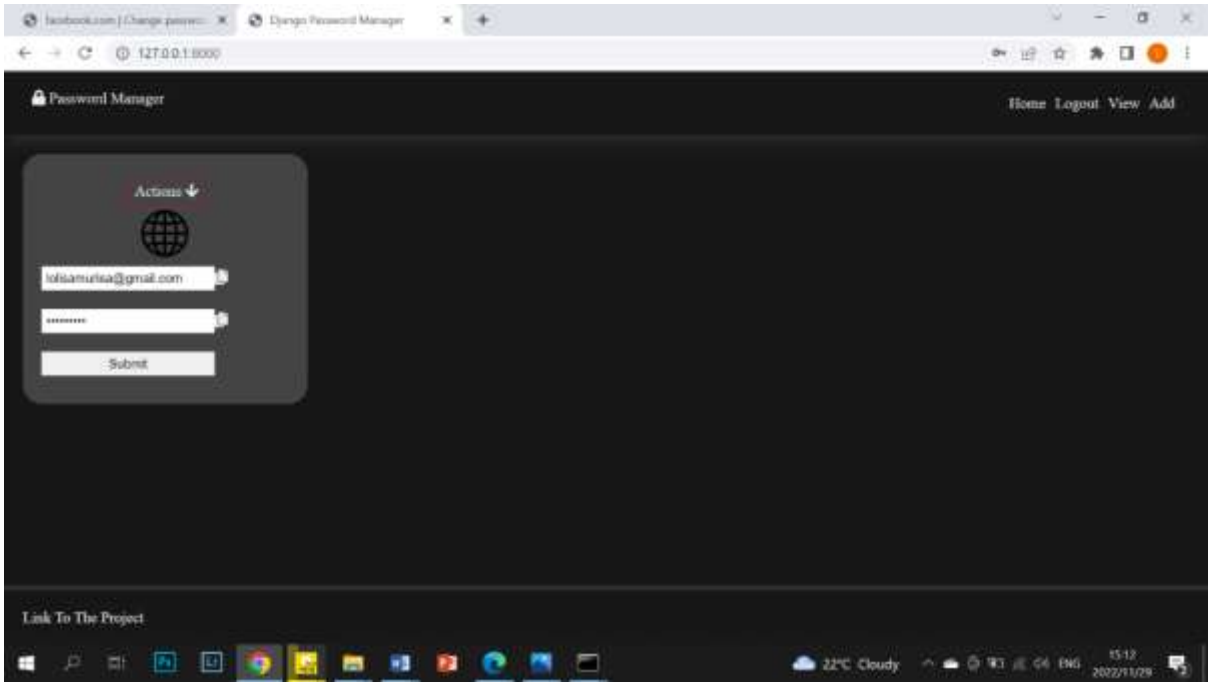



Login
login


SignUp
register


Django administration
Username:
Lolisa
Password:
Log in


Django administration
Change password
facebook.com
User:
Name:
Password:
Email:
Logo:
Delete
SAVE



3.12.1 Summary

This chapter mainly focused on the methodology used in the development of the system and how it was designed as well as implemented. Different techniques were used to come up with the system, also different tools like the python and Django framework made it possible to come up with the proposed system.

CHAPTER 4: RESULTS AND ANALYSIS

4.0 INTRODUCTION

After the author had successfully implemented the system there arose the need to analyze the efficiency of the developed solution. Accuracy, performance and response time were the matrices used to determine the efficiency and effectiveness of the developed solution. The developed solution's behaviour was also well observed under the different times and the outcome was presented in a table format.

4.1 TESTING

Testing is a vital part of the development process and this chapter shows the tests that were undertaken and the result they produced. The testing is thus measured against the functional and non-functional requirements as outline in the previous chapter.

4.2 BLACK BOX TESTING

Black box testing enables a user without the knowledge of the internal structure of the system to test it against the functional and sometimes the non-functional requirements of the system. The system is developed to help secure passwords using the AES cryptography algorithm.

4.3 FUZZY TESTING

Fuzzy testing is a black box testing technique which the researcher used on the Password Manager Application to check if the system is accurately responding and giving the correct results as per given coordinates.

4.4 EVALUATION MEASURES AND RESULTS

An evaluation metric measures the performance of a classifier (Hossin & Sulaiman, 2015). Moreover, according to Hossin & Sulaiman (2015), model evaluation metrics can be grouped into three types namely threshold, probability and ranking.

4.4.1 Strength Evaluation for the AES Cryptography algorithm

AES is a highly secure ciphering algorithm whether it's 128-AES, 256-AES or 512-AES. While 512-AES is an overkill, the debate settles between the 128- & 256-bit variations. To make the picture clearer, both ciphers have never been broken so far as the possibilities (2-128 & 2-256) available exceed the number of atoms in the universe thus brute-force is not an option. One might think that 256-AES is twice as secure compared to 128-AES but in fact, it's 340

billion-billion-billion-billion times harder. Even if we did manage to build a world-wide network of super-computers designed solely for the sake of testing combinations, it would take 100+ billion years to find the correct text. For comparison, the universe has only been around for 13.8 billion years. It is thus no surprise how AES (developed in 2000) replaced DES (developed in 1977) especially since DES was proven inadequate with a key-length of 56 bits & a block size of 64 bits.

4.4.2 Speed Comparison between AES Cryptography algorithm and other algorithms

During Encryption:

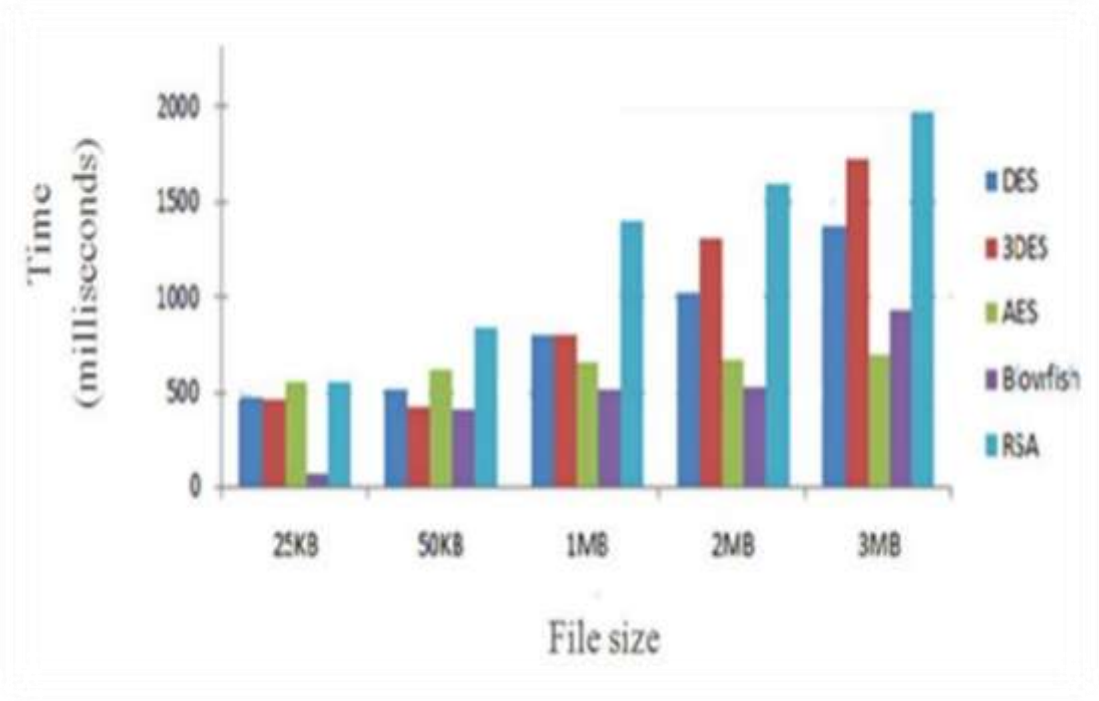


Table 2

The author discovers that DES is faster than AES which makes sense when comparing the 56-block size of DES compared to 128 block size of AES. Henceforth as file size increases ,AES algorithm defies the odds as it takes minimum amount of time to encrypt ,with Blowfish becomes another strong encryption algorithm to take into consideration.

During Decryption:

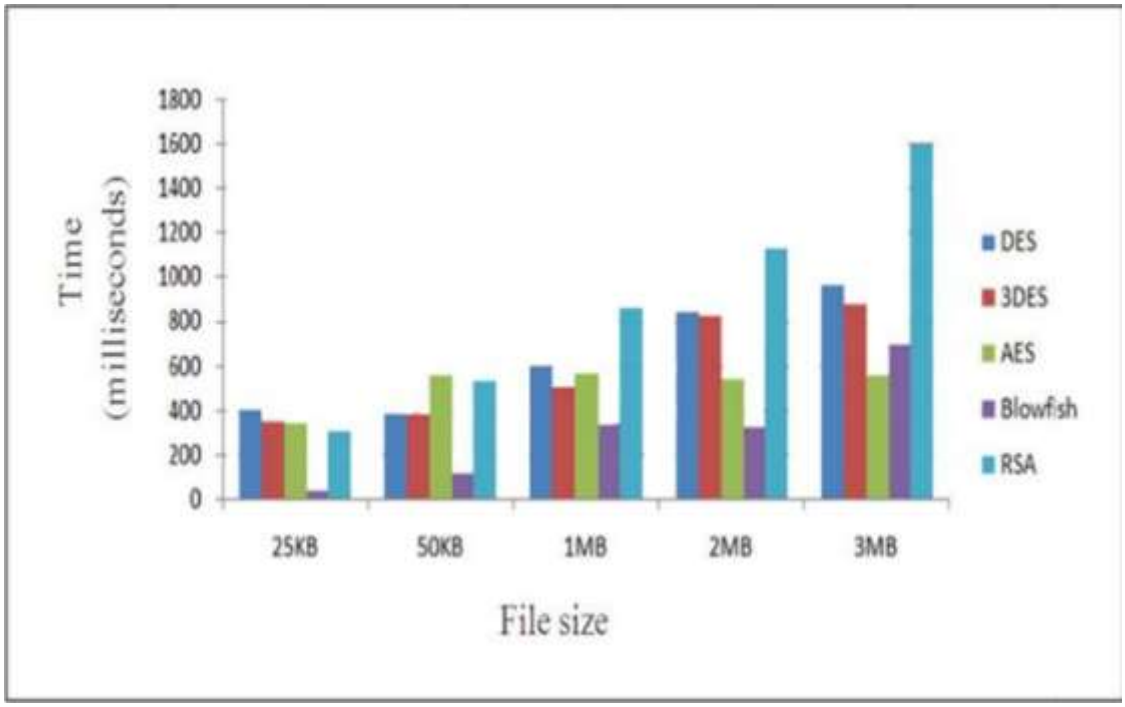


Table 3

Similarly, the decryption time is slightly higher for DES, henceforth for Blowfish it seems it's a mountain to climb. This demonstrate the strength o Blowfish to AES.As well AES is strong enough also compared to other algorithms.

4.4.3 Memory Requirement comparison for AES Cryptography and other algorithms

The AES algorithm uses less memory than DES algorithm due to the characteristics & implementation requirements of the algorithm, yet Blowfish Algorithm remains the most memory-friendly.

Algorithm	Memory Used (KB)
DES	**18.2**
3DES	**20.7**
AES	**14.7**
Blowfish	**9.38**
RSA	**31.5**

Table 4

4.4.4 Entropy Comparison for AES Algorithm

The author performed entropy test checks for randomness & possibility of patterns. It's measured using entropy per byte of encryption & is considered better when higher.

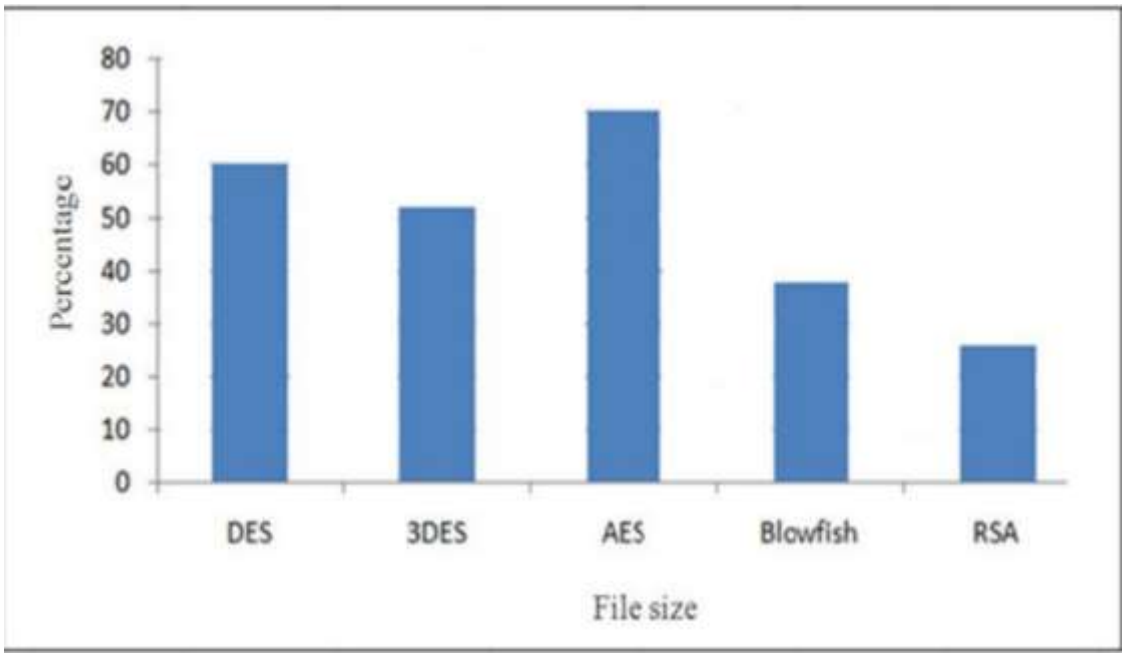


Table 5

AES proves to much way best in terms of entropy test that was performed by the author. This demonstrates its level of strength in terms of security over the network.

Algorithm	Average Entropy size per byte of encryption
DES	**2.9477**
3DES	**2.9477**
AES	**3.84024**
Blowfish	**3.93891**
RSA	**3.0958**

Table 6

We can notice that AES performs much better than DES, RSA and 3DES when it comes to randomness. Henceforth on the other hand it is weak compared to Blowfish which proves to be more dominant.

4.5 Conclusion

Use of internet and network is growing rapidly. Every day, lots and lots of digital data is being exchanged between users. A considerable amount of the exchanged information includes secret or confidential data that needs to be protected. Encryption algorithms play vital roles to protect original data from unauthorized access and we do have more than a couple of existing ones. Advanced encryption standard (AES) algorithm is one of the most efficient algorithms and it is widely supported and adopted on hardware and software. As mentioned throughout the paper, what makes this method special is its ability to deal with different key sizes such as 128, 192, and 256 bits with 128 bits block cipher. Another noticeable thing regarding the AES algorithm is that the encryption and decryption processes are pretty similar except for a few variations and order difference. Several important features of the AES algorithm were discussed and the performance was evaluated based on previous researches and results. According to the results obtained from researches, AES can provide much more security compared to other algorithms like DES, 3DES, etc.

CHAPTER 5: RECOMMENDATIONS AND FUTURE WORK

5.1 Introduction

In the previous chapter, the researcher focused on presentation and analysis of obtained data. This chapter covers the research and development of the solution in line with the set objectives. This chapter will also examine the difficulties encountered by the researcher in designing and carrying out this study.

5.2 Aims and Objectives Realization

The research serves to implement a password manager application, cemented with the Advanced Encryption Standard Cryptography Algorithm. The algorithm is to be applied for encrypting the passwords. The researcher is exploiting the field of Cybersecurity in a notion to reduces risks of intruders on one's passwords. Therefore, helps in reinforcing heavily any risks for a user to be exposed to externals intruding and keeping the passwords safely.

5.3 Conclusion

Advanced encryption standard (AES) algorithm is one of the most efficient algorithms and it is widely supported and adopted on hardware and software.

5.4 Recommendations

As mentioned throughout the paper, what makes this method special is its ability to deal with different key sizes such as 128, 192, and 256 bits with 128 bits block cipher. Another noticeable thing regarding the AES algorithm is that the encryption and decryption processes are pretty similar except for a few variations and order difference.

5.5 Future Work

The AES algorithm got some weaknesses for sure, but they are minimal when compared to the strengths of it. Finally, we do not expect to see any change in the use of this algorithm in the near future unless quantum/supercomputers manage to break the cipher.

REFERENCES

Almorabea, A. M. and Aslam, M. A. (2015). Symmetric key encryption using aes-gcm and external key derivation for smart phones, pp. 264–270.

Alvarez, R., Andrade, A. and Zamora, A. (2018). Optimizing a password hashing function´ with hardware-accelerated symmetric encryption, *Symmetry* **10**(12): 705.

Alvarez-S´anchez, R., Andrade-Bazurto, A., Santos-Gonza´lez, I. and Zamora-Go´mez,´ A. (2017). Aes-ctr as a password-hashing function, *International Joint Conference SOCO17-CISIS17-ICEUTE17 Le´on, Spain, September 6–8, 2017, Proceeding*, Springer, pp. 610–617.

Alwen, J., Chen, B., Pietrzak, K., Reyzin, L. and Tessaro, S. (2017). Scrypt is maximally memory-hard, *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, pp. 33–62.

Arora, M., Sharma, S. and Engles, D. (2017). Parametric comparison of emds algorithm with some symmetric cryptosystems, *Egyptian informatics journal* **18**(2): 141–149.

Biryukov, A., Dinu, D. and Khovratovich, D. (2016). Argon2: new generation of memoryhard functions for password hashing and other applications, *2016 IEEE European Symposium on Security and Privacy (EuroS&P)*, IEEE, pp. 292–302.

Chhabra, S. and Lata, K. (2018). Enhancing data security using obfuscated 128-bit aes algorithm-an active hardware obfuscation approach at rtl level, *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, IEEE, pp. 401–406.

Ertaul, L., Kaur, M. and Gudise, V. A. K. R. (2016). Implementation and performance analysis of pbkdf2, bcrypt, scrypt algorithms, *Proceedings of the International Conference*

on Wireless Networks (ICWN), The Steering Committee of The World Congress in Computer Science, Computer , p. 66.

Gore, A., Meena, S. and Purohit, P. (2016). Hybrid cryptosystem using modified blowfish algorithm and sha algorithm on public cloud, *International Journal of Computer Applications* **155**(3): 6–10.

Hatzivasilis, G., Papaefstathiou, I. and Manifavas, C. (2015). Password hashing competition-survey and benchmark., *IACR Cryptology ePrint Archive* **2015**: 265.

Kant, D. C. and Sharma, Y. (2013). Enhanced security architecture for cloud data security, *International journal of advanced research in computer science and software engineering* **3**(5).

Kaur, J. and Sharma, S. (2018). Hessis: Hybrid encryption scheme for secure image sharing in a cloud environment, *International Conference on Advanced Informatics for Computing Research*, Springer, pp. 204–216.

Kumar, N. and Chaudhary, P. (2018). Password security using bcrypt with aes encryption algorithm, *Smart Computing and Informatics*, Springer, pp. 385–392.

Marton, K., Suciu, A. and Ignat, I. (2010). Randomness in digital cryptography: A survey, *Romanian journal of information science and technology* **13**(3): 219–240.

Musliyana, Z., Arif, T. Y. and Munadi, R. (2015). Security enhancement of advanced encryption standard (aes) using time-based dynamic key generation, *ARPN Journal of Engineering and Applied Sciences* **10**(18).

Padmavathi, B. and Kumari, S. R. (2013). A survey on performance analysis of des, aes and rsa algorithm along with lsb substitution, *IJSR, India* .

Percival, C. (2009). Stronger key derivation via sequential memory-hard functions.

Percival, C. and Josefsson, S. (2016). The scrypt password-based key derivation function.

Sachdeva, S. and Kakkar, A. (2018). Implementation of aes-128 using multiple cipher keys, *International Conference on Futuristic Trends in Network and Communication Technologies*, Springer, pp. 3–16.

Singh, G. (2013). A study of encryption algorithms (rsa, des, 3des and aes) for information security, *International Journal of Computer Applications* **67**(19).

Sriramya, P. and Karthika, R. (2015). Providing password security by salted password hashing using bcrypt algorithm, *ARPN Journal of Engineering and Applied Sciences* **10**(13): 5551–5556.

Turan, M. S., Barker, E., Burr, W. and Chen, L. (2010). Recommendation for passwordbased key derivation, *NIST special publication* **800**: 132.

Widiasari, I. R. (2012). Combining advanced encryption standard (aes) and one time pad (otp) encryption for data security, *International Journal of Computer Applications* **57**(20).