RANDOM PASSWORD GENERATOR

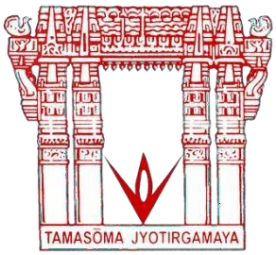
A Course Based Project Report Submitted in partial fulfillment of the requirements for the award of the degree of

BACHELOR OF TECHNOLOGY IN CSE (CYBERSECURITY)

Submitted by

K. SHIVANI 2207A6203

Under the guidance of
Dr.Lalitha
(Assistant Professor, Department of CSE-CYS, VNR VJIET)



DEPARTMENT OF CSE (CYBERSECURITY)

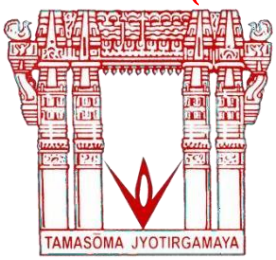
VALLURUPALLI NAGESWARA RAO VIGNANA JYOTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY

(An Autonomous Institute, Accredited by NAAC with 'A++' Grade NBA)
Bachupally, Pragati Nagar, Nizampet (S.O), Hyderabad – 500 090, TS, India

VALLURUPALLI NAGESWARA RAO VIGNANA JYOTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY

(An Autonomous Institute, Accredited by NAAC with 'A++' Grade NBA)
Bachupally, Pragati Nagar, Nizampet (S.O), Hyderabad – 500 090, TS, India

DEPARTMENT OF CSE (CYBERSECURITY)



CERTIFICATE

This is to certify that the project report entitled "**Title of the CBP"** is a bonafide work done under our supervision and is being submitted by **K. SHIVANI (22075A6203)** in partial fulfillment for the award of the degree of Bachelor of Technology in CSE (CYBERSECURITY), of the VNRVJIET, Hyderabad during the academic year 2022-2023. Certified further that to the best of our knowledge the work presented in this thesis has not been submitted to any other University or Institute for the award of any Degree or Diploma.

Project Guide

LALITHA,
Professor,
Dept of CYS,
VNRVJIET
Hyderabad.

Head of the Department

Dr. RAJASHEKHAR
Head of the dept,
Dept of CYS,
VNRVJIET
Hyderabad

VALLURUPALLI NAGESWARA RAO VIGNANA JYOTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY

(An Autonomous Institute, Accredited by NAAC with 'A++' Grade NBA)
Bachupally, Pragati Nagar, Nizampet (S.O), Hyderabad – 500 090, TS, India

DEPARTMENT OF CSE (CYBERSECURTIY)

DECLARATION

We declare that the major project work entitled "**Random Password Generator**" submitted in the department of CSE-CYS, Vallurupalli Nageswara Rao Vignana Jyothi Institute of Engineering and Technology, Hyderabad, in partial fulfillment of the requirement for the award of the degree of **Bachelor of Technology** in **CSE-CYS** is a bonafide record of our own work carried out under the supervision of Mrs. **Lalitha ,Assistant Professor**. Also, we declare that the matter embodied in this thesis has not been submitted by us in full or in any part thereof for the award of any degree/diploma of any other institution or university previously.

Place: Hyderabad

K.SHIVANI
(22075A6203)

ACKNOWLEDGEMENT

We express our deep sense of gratitude to our beloved Chairman, Shri. D.Suresh Babu, VNR Vignana Jyothi Institute of Engineering &Technology for the valuable guidance and for permitting us to carry out this project.

With immense pleasure, we record our deep sense of gratitude to our beloved Principal, Dr.C.D.Naidu for permitting us to carry out this project.

We express our deep sense of gratitude to Dr. Rajashekar, Associate Professor and Head, Department of Cyber security, VNR Vignana Jyothi Institute of Engineering & Technology, Hyderabad for the valuable guidance and suggestions, keen interest and through encouragement extended throughout period of project work.

We take immense pleasure to express our deep sense of gratitude to our beloved Guide Lalitha, Professor in Cyber security, VNR Vignana Jyothi Institute of Engineering & Technology, Hyderabad, for his valuable suggestions and rare insights, for constant source of encouragement and inspiration throughout my project work.

We express our thanks to all those who contributed for the successful completion of our project work.

K. SHIVANI (22075A6203)

ABSTRACT

A random password generator is a tool that creates unique and secure passwords for individuals or organizations to use as login credentials. This tool uses algorithms to randomly combine letters, numbers, and symbols to produce a string of characters that is difficult to crack or guess. The passwords generated by this tool are stronger and more secure than those chosen by humans, which are often easily guessed or found in dictionaries. With a random password generator, users can ensure their accounts are protected from unauthorized access and data breaches, keeping their sensitive information secure. This tool also eliminates the need for users to come up with their own passwords, making it a convenient solution for managing multiple accounts. In short, a random password generator is a must-have for anyone looking to secure their digital footprint.

Table of Contents

1. INTRODUCTION

Having a weak password is not good for a system that demands high confidentiality and security of user credentials. It turns out that people find it difficult to make up a strong password that is strong enough to prevent unauthorized users from memorizing it.

A random password generator is a software tool that creates unique and secure passwords for individuals or organizations to use as login credentials. With the increasing number of cyber threats and data breaches, it is essential to have strong and unpredictable passwords to protect online accounts and sensitive information. This is where a random password generator comes in, using advanced algorithms to create passwords that meet the highest security standards. The generator offers customization options such as password length, character types, and complexity, making it a versatile solution for different security requirements. Using a random password generator eliminates the need for users to come up with their own passwords, which are often easily guessed or found in dictionaries, and ensures that accounts are protected with strong and unpredictable passwords. Overall, a random password generator is an indispensable tool for anyone looking to secure their digital footprint and protect their sensitive information.

2.2 SYSTEM STUDY

A random password generator is a tool that creates a unique and secure password for users. The problem statement for this tool is to provide users with a password that is:

1. Strong: made up of a combination of letters, numbers, and symbols to prevent guessing and cracking attempts.
2. Unique: not easily guessable or already used in previous breaches.
3. Convenient: easy for users to remember, but not easily guessable.
4. Customizable: allow users to specify the length and complexity of the password, as well as other constraints such as excluding certain characters.

The challenge is to create a random password generator that meets these criteria while being user-friendly and efficient.

The requirements for a random password generator are as follows:

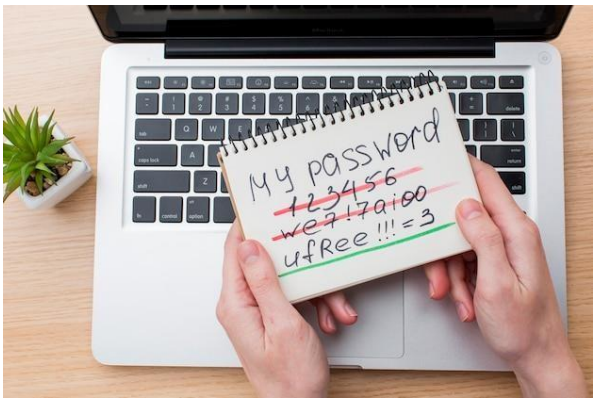
1. Strength: The password must be strong and secure, using a combination of uppercase and lowercase letters, numbers, and symbols.
2. Length: The password should have a minimum length specified by the user or a default length of 12 characters or more.
3. Complexity: The password must meet certain complexity requirements such as having a minimum number of upper and lowercase letters, numbers, and symbols.
4. Uniqueness: The password should not be easily guessable, repetitive or have been used in previous breaches.
5. Customizability: The password generator should allow the user to specify the length and complexity of the password, as well as other constraints such as excluding certain characters.
6. User-friendly: The password generator should be easy to use, with clear instructions and a user-friendly interface.
7. Efficiency: The password generator should be able to generate a password quickly, without causing delays or slowing down the system.
8. Security: The password generator should be secure, using industry-standard encryption methods to protect the generated passwords from unauthorized access or theft.

3.DESIGN

3.1. REQUIREMENT SPECIFICATION SOFTWARE DESCRIPTION:

A random password generator is an important tool for ensuring the security of sensitive information. To meet this need, the password generator must have a combination of functional and user requirements to effectively create unique, secure, and user-friendly passwords. These requirements will help guide the development process and ensure that the end result meets the needs of users.

The password generator should be able to create a unique and secure password, users to specify the length and complexity of the password, as well as other constraints such as excluding certain characters.The password generator should be compatible with different operating systems and devices.



USECASE DIAGRAM:

ACTIVITY DIAGRAM:

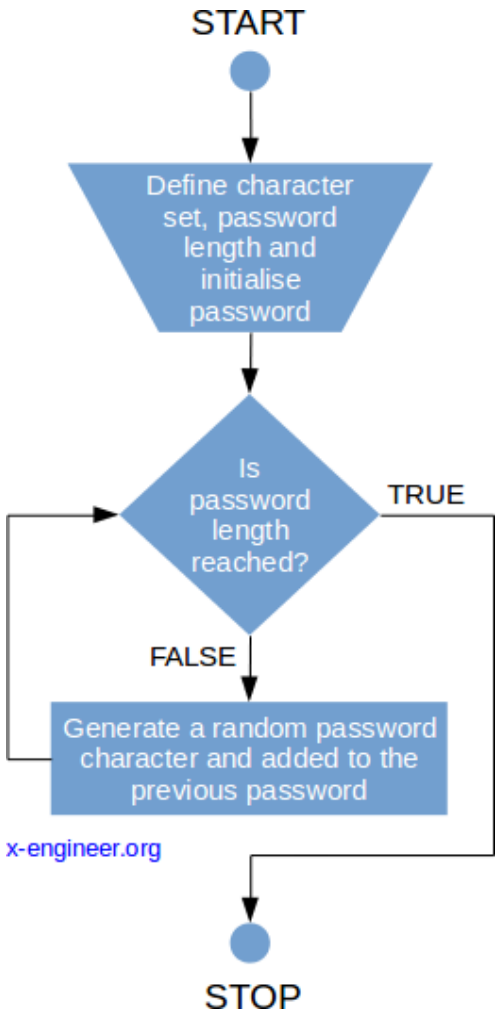


Figure 3.8 Activity Diagram

3.2.1 SEQUENCE DIAGRAM:

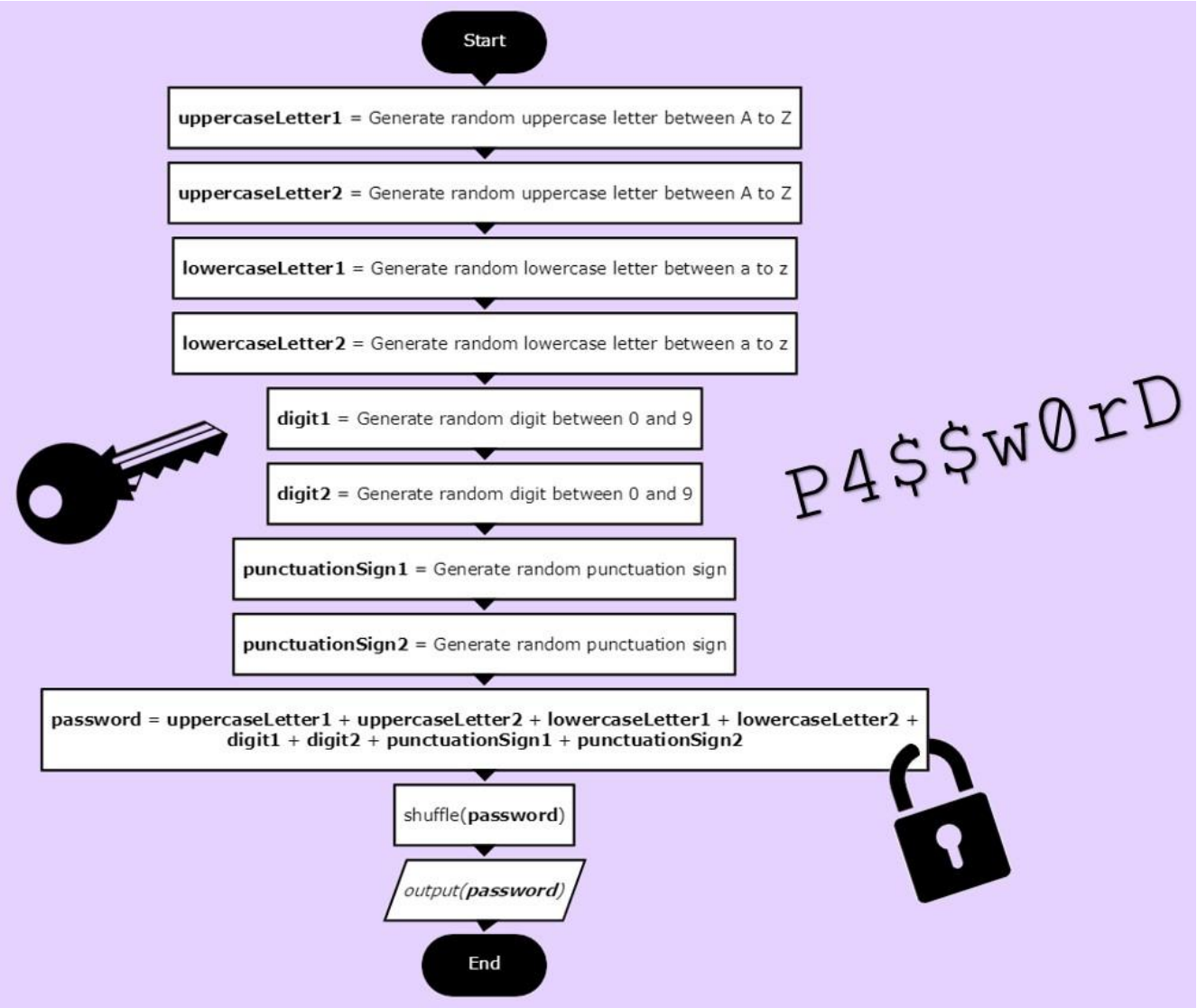
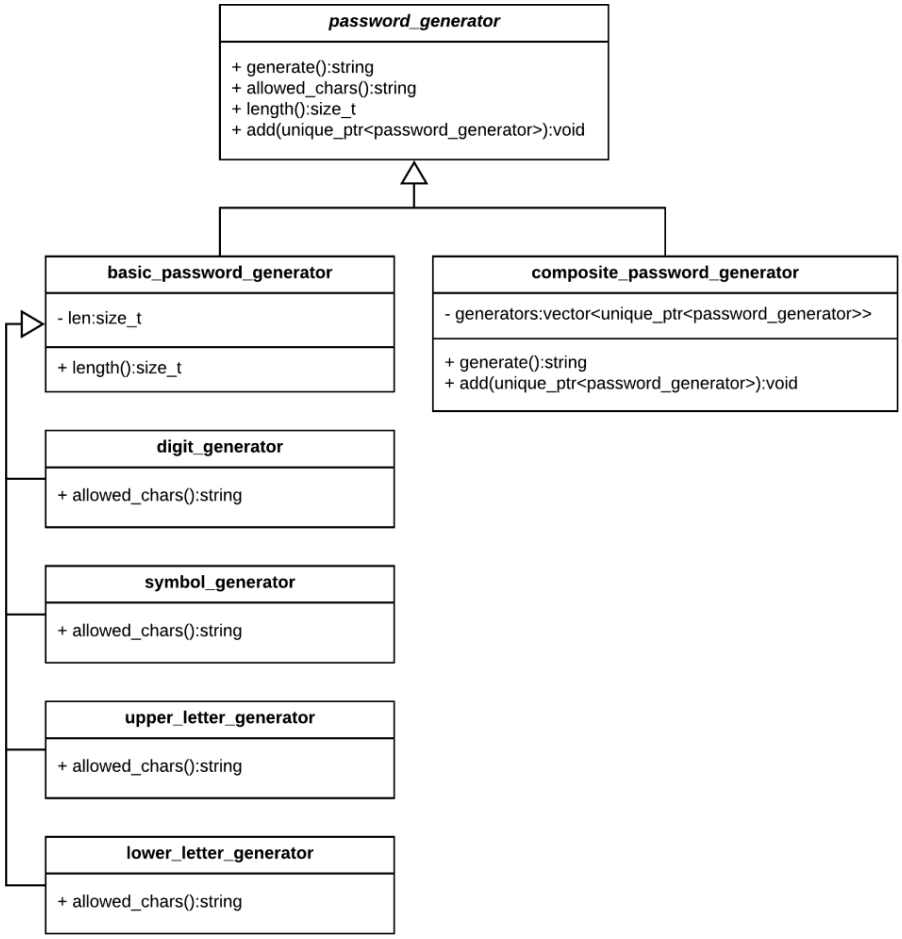


Figure 3.7 Sequence Diagram

3.2.2 CLASS DIAGRAM:



3.2.3

Figure 3.5 shows the Use Case Diagram use-case diagrams model the behavior of a system and help to capture the requirements of the system. Use-case diagrams describe the high-level functions and scope of a system. These diagrams also identify the interactions between the system and its actors

Figure 3.6 shows the Class Diagram which is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among objects.

Figure 3.7 shows the Sequence Diagram illustrates the sequence of messages between objects in an interaction. A sequence diagram consists of a group of objects that are represented by lifelines, and the messages that they exchange over time during the interaction.

Figure 3.8 shows the Activity Diagram that provides a view of the behavior of a system by describing the sequence of actions in a process.

4.IMPLEMENTATION

```
import random
#A function do shuffle all the characters of a string
def shuffle(string):
  tempList = list(string)
  random.shuffle(tempList)
  return ''.join(tempList)

#Main program starts here
#uppercase letters
uppercaseLetter1=chr(random.randint(65,90)) #Generate a random Uppercase letter (based on ASCII code)
uppercaseLetter2=chr(random.randint(65,90)) #Generate a random Uppercase letter (based on ASCII code)
#Generate more characters here
#lowercase letter
lowercaseLetter1=chr(random.randint(97,122))
lowercaseLetter2=chr(random.randint(97,122))
#numbers
num1=chr(random.randint(48,57))
num2=chr(random.randint(48,57))
#characters
```

```
char1=chr(random.randint(33,47))
char2=chr(random.randint(33,47))

#Generate password using all the characters, in random order
password = uppercaseLetter1 + uppercaseLetter2 +
lowercaseLetter1+lowercaseLetter2+num1+num2+char1+char2
password = shuffle(password)

#Ouput
print(password)
```

5. TESTING

```
The random password generated is :
0&7tZ&nH
>
```

```
The random password generated is :
d0%4DWd!
>
```

7 . CONCLUSION AND FUTURE SCOPE

In conclusion, a random password generator is a critical tool for ensuring the security of online accounts and sensitive information. By using advanced algorithms to create unique and secure passwords, a random password generator eliminates the need for users to come up with their own passwords, which are often easily guessed or found in dictionaries. With the increasing number of cyber threats and data breaches, it is essential to have strong and unpredictable passwords to protect online accounts.

In addition to its security benefits, a random password generator also offers convenience for users managing multiple accounts, as it eliminates the need to remember multiple complex passwords. Furthermore, a random password generator can be customized to meet the needs of different users and organizations, making it a versatile solution for a wide range of security requirements.

Overall, a random password generator is a must-have for anyone looking to secure their digital footprint and protect their sensitive information. By using a random password generator, users can have peace of mind knowing that their accounts are protected with strong and unpredictable passwords.

REFERENCES (If any)

[1] https://docs.python.org/3/library/tkinter.html

[2] https://www.tutorialspoint.com/python3/python_gui_programming.htm

[3] https://www.geeksforgeeks.org/python-tkinter-tutorial/

[4] https://www.geeksforgeeks.org/python-strings/

[5] https://stackoverflow.com/questions/51777956/link-gui-to-main-class