Password Generator Using NLP

(Natural Language Processing)

Under The Guidance Of:

MAYANK AGARWAL
(H.O.D)
Comp. Dept.

Submitted By:

HIMANSHU KUMAR
PULKIT AGARWAL
RAKESH SINGH RAWAT
SHUBHAM VERMA

INTRODUCTION

Generally, A Password is an alphanumeric word with some special symbols…

A Strong Password is a key to protect your personal assets online. Generally, Every Login on Internet is secured by many means like Password, OTP, etc.

Password and its security is the matter of concern in order to provide one individual a full Protection.

CONTENTS

- Problem Statement
- Need Of Password Generator
- The Way Of Use
- Why To Use
- Framework

  i. Module 1

  ii. Module 2

  iii. Module 3
- Future Work

PROBLEM STATEMENT

There are three problems that arises to a User

1. It’s not safe to use a same password on every LOGIN.

2. It’s difficult to remember a unique password for every new LOGIN. Generally, we forget one.

3. It’s not feasible to save all passwords under a Password Manager. Somehow, causing a Breach in your security.

Need of Password Generator

A strong password is a key to protect your personal assets online. Password Generator is used in a way through which highly secure passwords are generated that is really hard to crack or hack.

The Way of Use

The use of **Password Generator** is extremely easy. It requires simple step when you have to select the criteria for the password. After selecting the field, all you need is to select the generate password option. That will help you in getting a password that is absolutely secured and safe to use.

Why to Use?

With the help of a generator, it is much easier to create such passwords that are hard to crack even with the use of the software.

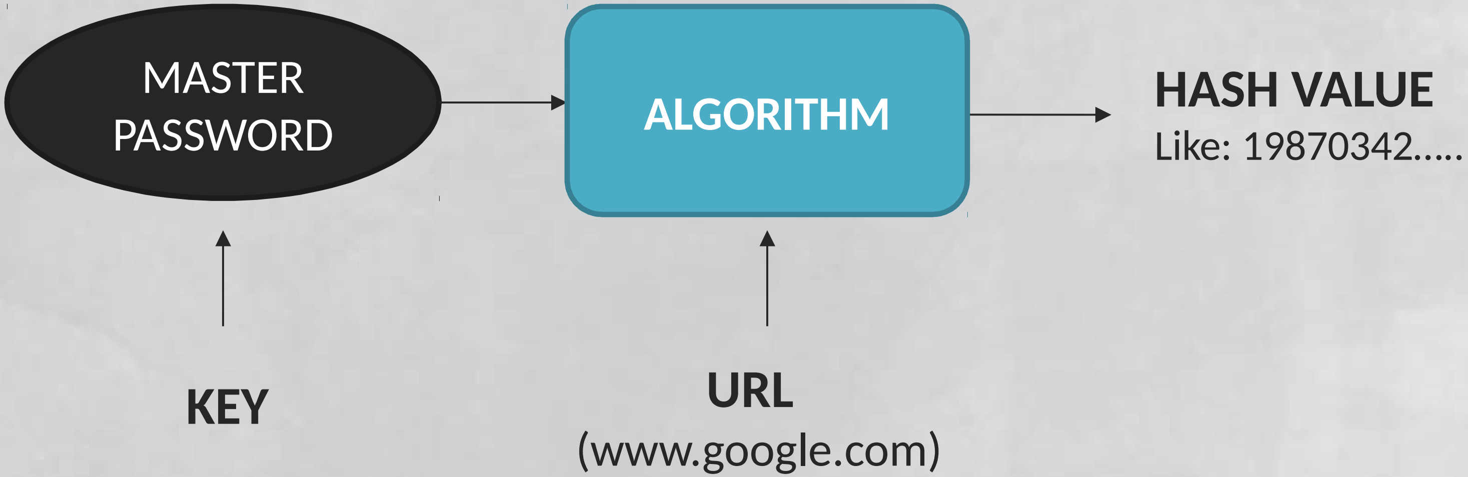
What’s The Difference?

It does not store a password in any encrypted form, but rather than it generates a unique password for any LOGIN by using NLP(Natural Language Processing) Technique followed by markov assumption and substitution. Thus, making it memorable and hard to crack.

FRAMEWORK

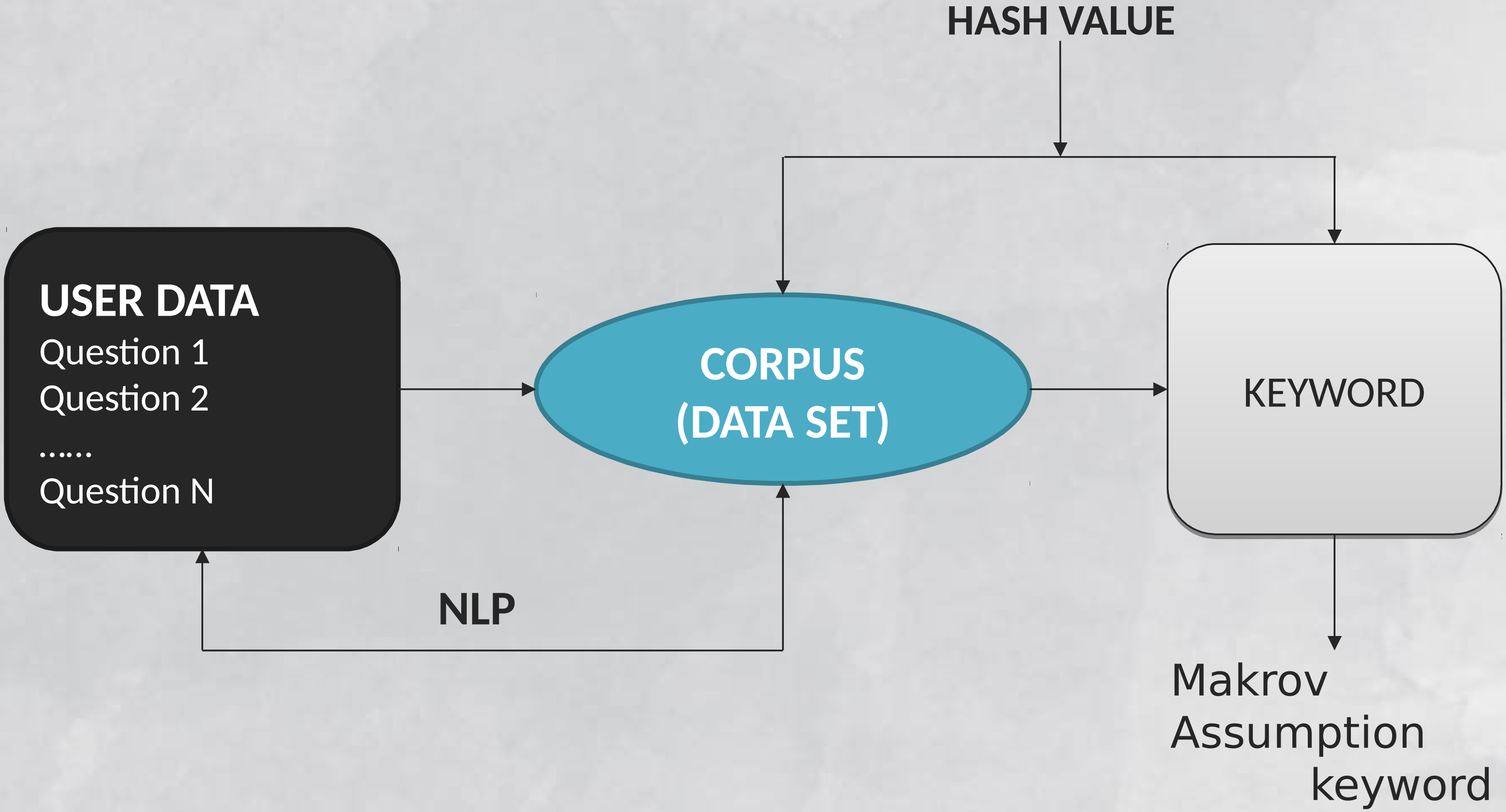
The framework implementation is done in three basic modules using SHA encryption, NLP (Natural Language Processing) technique, and Markov’s Assumption followed by Substitution.

MODULE 1



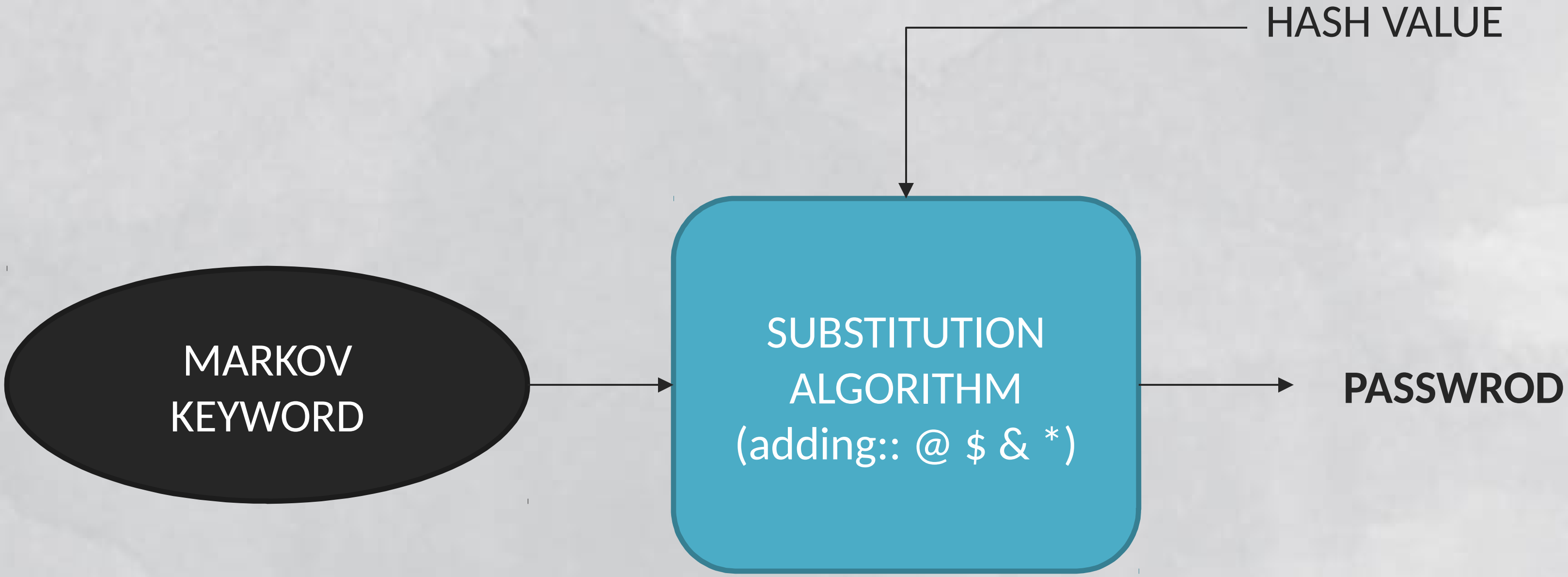
A Unique (One Time) Master Password is used as a key and a LOGIN URL in SHA Encryption to generate a HASH Value in Module 1.

MODULE 2



NLP Technique is used on a corpus and user data to generate a KEYWORD, by using the HASH value from MODULE 1.

MODULE 3



In Module 3, a keyword generated in Module 2 goes under Substitution Algorithm in order to make it more hard to crack and memorable and thus, generating a PASSWORD.

Future Work

1. Adding multiple users
2. Storing Pre-define passwords with AES encryption followed by Salting, Incremental counting, etc.
3. Mobile Application
4. Master Password as FINGER PRINT
5. Master Password as IRIS PRINT
6. New Data sets (CORPUS)

THANK YOU