**FACULTY**

**DEPARTMENT**

**STUDENT NAME**

**COURSE CODE**

**PROJECT TOPIC: PASSWORD STRENGTH CHECKER**

# Abstract

User-chosen passwords are known to be relatively predictable, and attackers and password recovery programs can significantly reduce the number of guesses necessary by employing tools like dictionaries or probabilistic models. Surprisingly, however, existing research does not offer a conclusive response to the question of how likely it is for a modern attacker to succeed in cracking a password given a number of guesses. Using several datasets of well-known passwords, we compare and assess the efficacy of known attacks to respond to the earlier query. We discover that the "diminishing returns" concept is in effect: weak passwords are widespread in the absence of an enforced password strength policy, but as an attack progresses, the likelihood that a guess would be successful declines by orders of magnitude. A large portion of the passwords won't be guessable by even the most capable attackers. Our methodology for estimating password strength can be used as a foundation for more effective proactive password checkers for users and security auditing tools for administrators. The outcome of this work will assist in evaluating the security of authentication methods based on user-chosen passwords

Table of Contents

[Abstract 1](#_Toc118298356)

[CHAPTER ONE: INTRODUCTION 3](#_Toc118298357)

[1.4 Significance of the Project 4](#_Toc118298362)

[1.5 Password Strength Measures 4](#_Toc118298363)

[CHAPTER TWO: LITERATURE REVIEW 5](#_Toc118298364)

[2.1 Introduction 5](#_Toc118298365)

[2.1.1 Attack Based Approaches 6](#_Toc118298368)

[2.1.2 Heuristic Based Approaches 6](#_Toc118298369)

[2.1.3 Heuristic Based Approaches 7](#_Toc118298370)

[CHAPTER THREE: RESEARCH METHODOLOGY 7](#_Toc118298371)

[3.1 Research Design 7](#_Toc118298372)

[3.2 Research Tools and Procedures 7](#_Toc118298373)

[3.2.1 Literature Search 7](#_Toc118298374)

[3.2.2 Case Analysis 8](#_Toc118298375)

[3.3 Checker Requirements. 8](#_Toc118298376)

[CHAPTER FOUR: RESULTS AND DISCUSSIONS 8](#_Toc118298377)

[4.1 Introduction 8](#_Toc118298378)

[4.2 Flowchart of Password Strength Checker 9](#_Toc118298379)

[CHAPTER FIVE: CONCLUSION AND FUTURE WORK 9](#_Toc118298380)

[5.0 Conclusion 9](#_Toc118298381)

[5.1 Future Work 9](#_Toc118298382)

**CHAPTER SIX: REFERENCES…….10**

# CHAPTER ONE: INTRODUCTION

## Background to the Study

Passwords have been used to grant unauthorized personnel access to computer systems and other devices ever since the dawn of time. It is commonly known that a variety of entities, including people, companies, institutions, espionage agencies, government state agencies, etc., utilize passwords. Passwords are now used to access a variety of devices, including tablets, mobile phones, bank accounts, computer systems, and many more places. They are no longer just used to keep computers safe and secure. Most of the time, individuals believe that the only security measure that can be used to protect sensitive applications from unauthorized access is a password. Additionally, these individuals lack an adequate knowledge of the significance of the produced passwords. They frequently create passwords that are extremely weak and may either be excessively short or comprise a mix of dictionary words. These weak passwords are frequently vulnerable to brute force attacks, which are made possible by the constantly expanding attack surfaces. However, with a bit more caution and awareness, potential hackers' task can be made more difficult.

Numerous researchers have suggested various methods for imposing security using various technologies and assessing the strength of the password. This study offers a thorough analysis of the methods employed by earlier academics to evaluate the security of stronger passwords and reduce the risks associated with weak passwords.

## 1.2 Problem Statement

## The majority of entities, including companies, continue to assess the password strength using weak rule-based mechanisms. These defenses are frequently quite frail and open to several password-related assaults including brute force attacks. Additionally, businesses and individuals continue to tolerate passwords with low levels of complexity. Strong password usage can protect organizations from time-consuming password cracking methods.

## Goals

1. To research and evaluate the password strength checkers that have been in use recently.
2. To enhance and make use of stronger passwords by users of the system.
3. To use a combination of special characters, combinations of uppercase and lowercase letters while generating the password

## Significance of the Project

Fear of forgetting complex passwords, especially when there are several to remember, is a common worry that people have while generating them. Of course, one should try to come up with something that would be simple for them to memorize. Changing a sentence or phrase into something that is difficult for others to understand is one technique to achieve this. Use the first letter of each word in the sentence while substituting numbers or symbols for some terms to accomplish this. For example, the word "for" may be substituted by the number 4 or the word "number" with the # symbol. The password "Save the number for later in the year" might appear as St#4LITY using this technique. By using the combination of characters makes the password to be stronger hence save from password attacker.

## Password Strength Measures

Passwords are unquestionably crucial for security, but they are not the only way to secure one's computers and other electronic devices. People should understand how to secure their passwords and use them appropriately in addition to setting strong passwords. This entails keeping a written copy in a safe place if you can't remember it and never disclosing it.

Using encrypted websites solely when submitting personal information is one of the additional security measures outside of passwords. When https is included at the start of the Web URL, it is easy to identify an encrypted website. Computer security software is essential for protecting computers, and both security software and mobile device firmware should be updated frequently.

When it comes to avoiding illegal access to one's computer and mobile devices, security precautions like passwords are essential. Hackers and other cybercriminals constantly discover new ways to access these devices in the modern world in order to steal or use the information they contain. However, using passwords carelessly can be just as harmful as not protecting one's digital gear. People should take care when creating and safeguarding their passwords because of this.

# CHAPTER TWO: LITERATURE REVIEW

## 2.1 Introduction

## The most used kind of authentication in computer systems is text-based passwords. According to earlier studies [1], passwords are frequently simple for attackers to crack. A typical threat model involves an attacker stealing a list of hashed passwords so that he can try to decipher them offline at his convenience. These concerns are quite real because to the numerous recent instances of data thefts involving massive numbers of hashed passwords and the accessibility of botnets that provide attackers with large computational resources. Once these passwords have been broken, access to the original website as well as additional accounts where people reuse their passwords can be obtained. As people open more online accounts, password reuse (exactly and with small variations) is a widespread and rising trend.

## System administrators define password-composition procedures to lessen the risk of such attacks. These regulations impose numerous conditions on newly established passwords in an effort to make them more difficult to decipher. Passwords typically need to have a number or a symbol, be longer than a set minimum, and not be words that can be looked up in a dictionary.

Despite the widespread belief that password composition policies increase password security by making them more difficult to guess, research has had difficulty determining the exact degree of guessing resistance offered by various password-composition policies or the specific requirements they contain. Estimating the entropy of the generated passwords and using password-guessing software to empirically analyze the produced passwords are the two approaches that are most frequently used to measure the impact of password-composition restrictions. The latter, however, is challenging to apply due to the lack of readily available password sets made under various password-composition policies, and the former is not grounded in actual evidence. password strength estimation approaches can be classified in three big groups: attack-based, heuristic-based and probabilistic-based.

### 2.1.1 Attack Based Approaches

These attack-based strategies raise two significant problems: 1) On the one hand, they are unable to generalize effectively to various attacks or even to various configurations of the same attack, such as employing various dictionaries. In other words, if we assume that it takes 1,000 guesses to crack a password using a specific attack, we get an idea of how strong the password is against that specific assault. However, what if the attack is modified? How can the number of attempts to guess a password be made independent of the assaults taken into account? 2) On the other hand, executing an attack to determine the number of guesses necessary to crack a password takes time, and many applications require a quick response, such as informing a user of the strength of a password he has just selected.

### 2.1.2 Heuristic Based Approaches

The trend based on heuristics, commonly known as LUDS: counts of lower- and uppercase letters, digits, and symbols, is now the one that is most widely used and adopted in the field of password strength measures. The majority of password policies used in reality are based on this idea, despite several extremely important heuristic-based works moving away from it at the moment. For instance, the current NIST standard, numerous online password strength estimators, and even leading technology businesses all adhere to this technique. These measures, which estimate password complexity under the premise that a more complicated password will be less vulnerable to attacks, are based on expert guidelines that have been developed ad hoc from experience. These guidelines include things like the following: longer passwords are stronger, as passwords with more character kinds such as lowercase, uppercase, digits, and special characters.

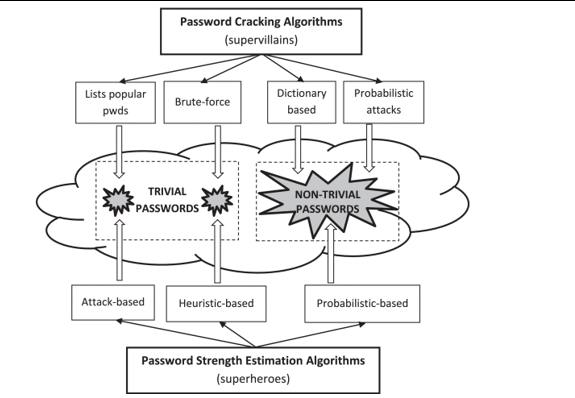


Fig 1: General diagram of the “password-cracking *vs* strength-estimation” problem.

### 2.1.3 Heuristic Based Approaches

A very intriguing idea was introduced in the last section on heuristic-based techniques: the connection between passwords and probability. Given that "smart" assaults also take advantage of the lack of randomness in password selection, it makes sense to estimate the number of guesses needed to crack a password using the likelihood that it was chosen by a human. In this manner, the chance of occurrence can be effectively employed as a measure of password strength. A very high likelihood would indicate low strength, and vice versa, a low probability would indicate strong strength. But the issue is not straightforward: A password's likelihood of being chosen by a human is inherently very individualized.

# CHAPTER THREE: RESEARCH METHODOLOGY

## 3.1 Research Design

Explanatory research design is used in this study. Explanatory research is defined as a research strategy used to gain a deeper comprehension of a current issue. It is also employed to go into further detail on the areas of a subject that have not yet been examined and to fill in the blanks. In this type of research design, the researcher begins with a general idea and uses the research as a medium to identify issues that can be the focus for future research.

## 3.2 Research Tools and Procedures

### 3.2.1 Literature Search

One of the cheapest ways to find a hypothesis and offer reliable information about the topic at hand is to conduct a literature search. Journals, research papers, and articles from Google Scholar are the sources of material for this research paper's literature review.

The literature search focus on:

1. Doing comprehensive research on the vulnerabilities of the weak passwords.
2. Understanding how the current password strength checker have been designed.
3. Studying how to improve the strength of password strength checker by including special characters.

### 3.2.2 Case Analysis

A case analysis is a method of empirical inquiry and research that examines a phenomenon in its setting. A case study might provide a researcher with more knowledge by carefully examining previous cases that have encountered a similar issue. This study will examine various case studies on employing checkers to strengthen passwords that have been conducted in recent years by various researchers. This will make it easier to determine whether my gap is real.

## 3.3 Checker Requirements.

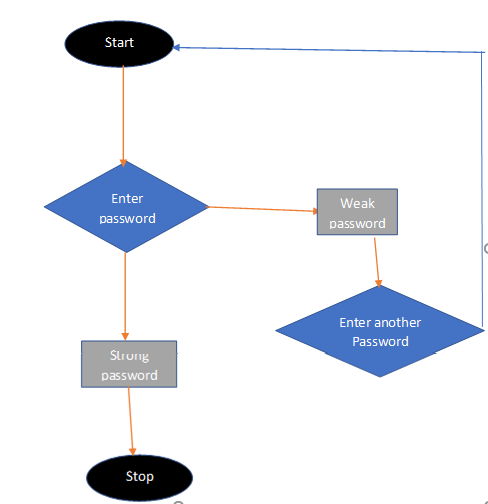
1. Computer
2. Operating System
3. Coding skills (Bootstrap, HTML, CSS, and JavaScript)
4. Data Structure’s knowledge

**CHAPTER FOUR: RESULTS AND DISCUSSIONS**

## 4.1 Introduction

In this chapter, the proposed password strength checker is going to be illustrated.

4.2 Flowchart of Password Strength Checker



At first, someone input their own generated password into the password field. Afterwards the system detects the strength of the password while entering in to the field, the system will automatically give a situation concerning the password entered, if it is week or medium a user is required to enter the password again until the correct password standards are made.

# CHAPTER FIVE: CONCLUSION AND FUTURE WORK

## 5.0 Conclusion

The main lesson learned from this project is that the user will have the ability to increase the strength of the password that they choose to enter for their account, based on the analysis offered in the application before establishing the password. This will assist the user in avoiding becoming a target of cyber password attacks, which are quite likely when using weak or obvious passwords.

## 5.1 Future Work

There is a lot of room for improvement in this program in the future. Due to the new technologies' simple accessibility, we can easily add new features to them and ensure that they are accessible to all website developers who require a login for their projects.

**CHAPTER SIX: REFERENCES**

[1] Dell'Amico M, Michiardi P, Roudier Y. Password strength: An empirical analysis. In2010 Proceedings IEEE INFOCOM 2010 Mar 14 (pp. 1-9). IEEE.

[2] Kelley PG, Komanduri S, Mazurek ML, Shay R, Vidas T, Bauer L, Christin N, Cranor LF, Lopez J. Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. In2012 IEEE symposium on security and privacy 2012 May 20 (pp. 523-537). IEEE.

[3] de Carné de Carnavalet X, Mannan M. From very weak to very strong: Analyzing password-strength meters. InNetwork and Distributed System Security Symposium (NDSS 2014) 2014. Internet Society.

[4] Bonneau J. Statistical metrics for individual password strength. InInternational Workshop on Security Protocols 2012 Apr 12 (pp. 76-86). Springer, Berlin, Heidelberg.

[5] Wang D, He D, Cheng H, Wang P. fuzzyPSM: A new password strength meter using fuzzy probabilistic context-free grammars. In2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) 2016 Jun 28 (pp. 595-606). IEEE.

[6] Florêncio D, Herley C, Van Oorschot PC. Pushing on string: The'don't care'region of password strength. Communications of the ACM. 2016 Oct 28;59(11):66-74.

[7] Hu G. On password strength: A survey and analysis. InInternational Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing 2017 Jun 26 (pp. 165-186). Springer, Cham.

[8] Doucek P, Pavlíček L, Sedláček J, Nedomová L. Adaptation of password strength estimators to a non-English environment—the Czech experience. Computers & security. 2020 Aug 1;95:101757.

[9] Voyiatzis AG, Fidas CA, Serpanos DN, Avouris NM. An empirical study on the web password strength in Greece. In2011 15th Panhellenic Conference on Informatics 2011 Sep 30 (pp. 212-216). IEEE.

[10] David L, Wool A. An explainable online password strength estimator. In sEuropean Symposium on Research in Computer Security 2021 Oct 4 (pp. 285-304). Springer, Cham.