Multi-Purpose AI Password Analysis Tool

By:

Osama Khalid– Team Member 1
27971
Sardar M. Zeeshan khan – Team Member 2
27969
Salman Ali – Team Member 3
27667

Supervised by:
Sir Osamah Ahmed

Faculty of Computing
Riphah International University, Islamabad

Spring/Fall 20xx

A Dissertation Submitted To

Faculty of Computing,

Riphah International University, Islamabad

As a Partial Fulfillment of the Requirement for the Award of the Degree of

Bachelors of Science in Software Engineering

Faculty of Computing
Riphah International University, Islamabad

Date: [date of final presentation]

Final Approval

This is to certify that we have read the report submitted by ***name of student(s) (CMS #)***, for the partial fulfillment of the requirements for the degree of the Bachelors of Science in Software Engineering (BSSE). It is our judgment that this report is of sufficient standard to warrant its acceptance by Riphah International University, Islamabad for the degree of Bachelors of Science in Software Engineering (BSSE).

Committee:

1 ________________________________

[Name Supervisor]
(Supervisor)

2 ________________________________

[Name of HOD/chairman]
(Head of Department/chairman)

Declaration

We hereby declare that this document “**[Project Title]**” neither as a whole nor as a part has been copied out from any source. It is further declared that we have done this project with the accompanied report entirely on the basis of our personal efforts, under the proficient guidance of our teachers especially our supervisor **[insert name of Supervisor(s)]**. If any part of the system is proved to be copied out from any source or found to be reproduction of any project from anywhere else, we shall stand by the consequences.

Osama Khalid
27971

Sardar M. Zeeshan khan

27969

Salman Ali

27667

Dedication

Insert dedication here…

Acknowledgement

First of all we are obliged to Allah Almighty the Merciful, the Beneficent and the source of all Knowledge, for granting us the courage and knowledge to complete this Project.

We would like to express our sincere gratitude to the following individuals whose guidance and support were instrumental in the successful completion of this project:

- **Project Supervisor:** We are particularly grateful to our project supervisor, **Mr. Osama Ahmad**, for his invaluable expertise, insightful feedback, and unwavering encouragement throughout the entire project development process. His dedication and support played a pivotal role in shaping the direction and success of our work.
- **Faculty Advisors:** We extend our sincere thanks to our faculty advisors, **Dr. Muhammad Mansoor Alam**, whose passion for AI inspired us to pursue this project, and **Dr. Jawaid Iqbal**, whose knowledge and guidance were invaluable throughout the research phase.
- **Technical Support Staff:** We appreciate the assistance provided by **Mr. Haseeb Ahmed**, **Mr. Ihtesham Ullah**, and **Mr. Tajamul Hussain**. Their technical expertise and willingness to help were crucial in overcoming technical challenges.
- **Project Convener:** We acknowledge the leadership of **Mr. Muhammad Ahmad Nawaz** as the project convener, whose guidance ensured the project's smooth execution within the academic framework.
- **Colleagues and Friends:** Finally, we would like to thank our colleagues, **Mr. Osama Raza** and **Mr. Awais Nawaz**, for their encouragement, collaboration, and support throughout the course of this project. Their positive spirit and willingness to assist contributed significantly to our progress

Osama Khalid
27971

Sardar M. Zeeshan khan

27969

Salman Ali

27667

Abstract

This project proposes the development of a multi-purpose AI password analysis tool offering both offensive and defensive capabilities. It leverages AI to analyze and crack passwords, assess their security strength, and identify breached credentials. This tool empowers users to test the resilience of their own passwords and proactively identify vulnerabilities.

Table of Contents

List of Figures

List of Tables

Chapter 1:
Heading (30-Point Size, Times New Roman, Bold and Right aligned)

Table of Contents

Chapter 1: Introduction

Project Title: Multi-Purpose AI Password Analysis Tool

1.1 Introduction & Background

1.1.1 Introduction

In today's world, where everything is becoming digital and online threats are on the rise, having strong password security is absolutely crucial. That's where the AI Multipurpose Password Analysis Tool comes in. It's a game-changing software that's here to revolutionize how we manage passwords. By combining cutting-edge artificial intelligence with traditional password analysis tools, this tool offers a complete solution for keeping our digital accounts safe. Whether it's cracking passwords or assessing password’s strength, this tool covers multiple aspects of password security. And it doesn't stop there - it seamlessly works with popular tool like Hashcat, making it even more powerful. So, as we step into the future of password management, the AI Multipurpose Password Analysis Tool is leading the way, providing both analysis and cracking abilities to protect our sensitive information from the ever-evolving threats online.

1.1.2 Background

Traditional password cracking tools have relied on brute force techniques or precomputed dictionaries to decipher passwords. While these methods have been effective to some extent, they suffer from several limitations and challenges.

1. **Limited Efficiency**: Brute force attacks iterate through all possible combinations of characters, making them time-consuming and resource-intensive, especially for complex passwords.
2. **Dependence on Dictionaries**: Dictionary attacks rely on precompiled lists of commonly used passwords or words found in dictionaries. However, these lists may not encompass all possible variations, especially when users employ complex or unique passwords.
3. **Lack of Adaptability**: Traditional tools often struggle with adaptive password generation techniques, such as adding special characters or changing letter cases, making them less effective against modern password practices.
4. **Inability to Detect Breached Credentials**: Many password cracking tools do not have built-in mechanisms to cross-reference passwords with known breaches, leaving users unaware if their passwords have already been compromised.
5. **Scalability Issues**: As passwords become longer and more complex to enhance security, traditional methods face scalability challenges in terms of processing power and memory requirements.

1.2 Opportunity & Stakeholders

1.2.1 Opportunities

- **Enhanced Security Assessments:** Businesses and individuals can leverage the tool for penetration testing and vulnerability assessments, identifying potential weaknesses in their password security policies and practices.
- **AI-driven Offensive and Defensive Capabilities:** Utilizing AI for both offensive (password cracking) and defensive (password strength assessment) purposes provides a comprehensive approach to password security management.

1.2.2 Stakeholders

- **Businesses:** Companies aiming to improve their overall cybersecurity posture by identifying and mitigating password-related vulnerabilities.
- **Security Professionals:** Penetration testers and security consultants who can use the tool for vulnerability assessments and ethical hacking activities.
- **Law Enforcemen**t**:** Agencies might leverage the tool for lawful investigations adhering to court orders and legal guidelines.

1.3 Existing System

1.3.1 John the Ripper

Limitations:

1. Relies on traditional methods of password cracking such as dictionary attacks, brute-force attacks, and rainbow tables.
2. While powerful, it may not effectively adapt to evolving password patterns and behaviors without continuous updates and modifications.

Problems:

1. Lack of advanced AI integration for targeted password list generation based on learned patterns.
2. Limited defensive capabilities in analyzing password strength beyond basic dictionary checks.

1.3.2 Brutus

Limitations:

1. Primarily designed for online password cracking through network protocols like HTTP, FTP, SMB, etc.
2. May lack advanced AI-driven capabilities for generating targeted password lists.

Problems:

1. Limited applicability for offline password analysis and cracking scenarios.
2. May not integrate well with the defensive aspects of the proposed tool, such as analyzing password strength and checking for breached credentials.

1.3.3 Wfuzz

Limitations:

1. Primarily focuses on web application security testing, including fuzzing and brute-forcing directories and files.
2. May lack specialized features for password cracking and analysis.

Problems:

1. Not specifically tailored for password analysis and cracking tasks, thus requiring significant adaptation to fit into the proposed project's scope.
2. Limited or no integration with AI-driven password analysis and cracking techniques.

1.3.4 Comparison

Tool	John the Ripper	RainbowCrack	OphCrack
Type	Password Cracker	Password Cracker	Password Cracker
Supported Platforms	Windows, Linux, macOS	Windows, Linux	Windows, Linux
Password Hashes Supported	Various (Unix, Windows, etc.)	LM, NTLM, MD5, SHA1, SHA256, SHA512	LM, NTLM
Attack Methods	Dictionary, Brute Force, Hybrid	Precomputed Hash Tables	Rainbow Tables, Brute Force
Speed	Fast	Depends on Rainbow Table size	Moderate
User Interface	Command Line	Command Line	GUI
License	Open Source	Freeware	Open Source
Usage	Penetration Testing, Password Auditing	Password Cracking	Password Recovery

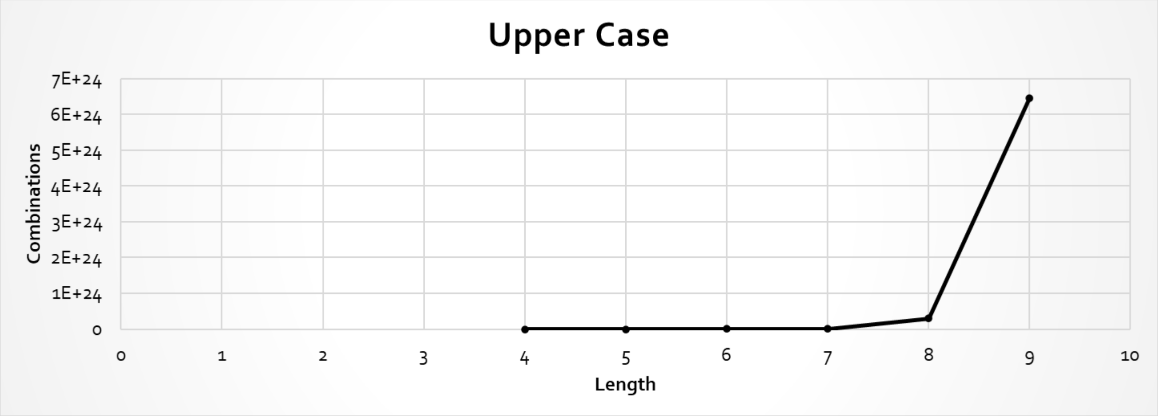
Comparison Table 1

Tool	L0phtCrack	Aircrack-ng
Type	Password Cracker	Wi-Fi Network Security Tool
Supported Platforms	Windows	Linux, macOS
Password Hashes Supported	LM, NTLM	WEP, WPA, WPA2
Attack Methods	Dictionary, Brute Force	Dictionary, Brute Force, WPS PIN
Speed	Fast	Depends on hardware and complexity of the password
User Interface	GUI	Command Line
License	Commercial	Open Source
Usage	Password Cracking	Wi-Fi Network Security Testi

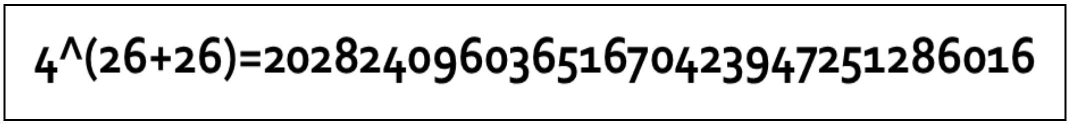
Comparison Table 2

1.4 Problem Statement

With increasing password complexity requirements, brute-force attacks become significantly slower and less efficient.



Users often employ longer and more complex passwords (e.g., 8+ characters, combination of uppercase, lowercase, symbols) making traditional brute-force methods impractical.


4^(26+26)=20282409603651670423947251286016

Uppercase and Lowercase length of 4

Length	Upper Case	Upper + Lower Case	Upper + Lower + Numeric	Upper + Lower + Numeric + Special Char
4	4.5036E+15	2.02824E+31	2.12676E+37	3.92319E+56
5	1.49012E+18	2.22045E+36	2.1684E+43	5.04871E+65
6	1.70582E+20	2.90981E+40	1.75945E+48	1.40029E+73
7	9.38748E+21	8.81248E+43	2.48931E+52	2.74926E+79
8	3.02231E+23	9.13439E+46	9.80797E+55	7.77068E+84
9	6.46108E+24	4.17456E+49	1.45558E+59	4.998E+89

Password Combination Table 1

1.5 Proposed Solution

Our AI-powered tool leverages advanced algorithms and Human like passwords data to:

- **Focus cracking efforts on statistically probable password patterns:** This reduces the search space and accelerates the cracking process compared to traditional brute-force methods.
- **Analyze password strength based on complexity metrics and AI-driven pattern recognition.** This identifies potential weaknesses in complex passwords, aiding in targeted cracking attempts.

1.6 Objectives

- Focus cracking efforts on statistically probable password patterns.
- Analyze password strength based on complexity metrics and AI-driven pattern recognition.
- Reduced cracking time.
- Improved vulnerability assessment.

1.7 Scope of the Project

- **Defensive capabilities:**

  Password strength assessment: Analyze password complexity, identify dictionary words, and check for patterns using AI.

  Optional

- **Breach checking:** Integrate with online databases to verify if entered passwords and email addresses have been exposed in known data breaches.

- **Offensive capabilities: (For Ethical purposes only)**

  AI-powered password cracking: Utilize correlation of password data and advanced algorithms to efficiently crack passwords within a specified scope and with proper authorization.

1.8 Evaluation Plan

Aligned with the objectives of our project, we will conduct a comprehensive assessment of the AI Multipurpose Password Analysis Tool's performance using diverse password datasets sourced from various sources, including real-world breaches, password dictionaries, and synthetic data generation. This dataset will serve as the cornerstone for evaluating the tool's effectiveness in analyzing password strength and facilitating password cracking across different scenarios.

Chapter 2: Develop and Train the AI Model

2.1 Research and select appropriate AI algorithms for password analysis.

2.2 Acquire or prepare relevant password datasets for training

2.3 Train and optimize the chosen AI model with the selected datasets.

Chapter 3: Implement Core Functionalities

3.1 Design and develop functionalities for password strength analysis.

3.2 Integrate password breach checking with online databases (securely).

3.3 (Optional) Develop functionalities for automated password cracking (ethical considerations apply).

Chapter 4: Design and Develop User Interface

4.1 Design a user-friendly interface for both offensive (optional) and defensive functionalities.

4.2 Integrate the trained AI model and core functionalities into the user interface.

Chapter 5: Testing and Refinement

5.1 Conduct thorough testing of all functionalities with various password scenarios.

5.2 Refine the AI model, user interface, and functionalities based on testing results.

5.3 Document user manuals and instructions for the completed tool.

References

References:

- . Hitaj, Briland et al. "PassGAN: A Deep Learning Approach for Password Guessing." *International Conference on Applied Cryptography and Network Security* (2017).
- Hitaj, Briland, et al. "Passgan: A deep learning approach for password guessing." *Applied Cryptography and Network Security: 17th International Conference, ACNS 2019, Bogota, Colombia, June 5–7, 2019, Proceedings 17*. Springer International Publishing, 2019.