

# **RIPHAH INTERNATIONAL UNIVERSITY**



## **Faculty of Computing FINAL YEAR PROJECT PROPOSAL & PLAN**

### **Multi-Purpose AI Password Analysis Tool**





#### **Project Team**

<b>Full Name of Student</b>	<b>SAP Id</b>	<b>Program</b>	<b>Contact Number</b>	<b>Email Address</b>
Osama Khalid	27971	BSCY	+9234-33433630	27971@students.riphah.edu.pk
Sardar M. Zeeshan khan	27969	BSCY	+92334-5027756	27969@students.riphah.edu.pk
Salman Ali	27667	BSCY	+92315-5374585	27667@students.riphah.edu.pk

**Sir Osamah Ahmed**

## Multi-Purpose AI Password Analysis Tool

### Change Record

Author(s)	Version	Date	Notes	Supervisor's Signature
Salman Ali, Osama Khalid, S.M.Zeeshan Khan.	1.0	4/3/2024	Original Draft	
Salman Ali, Osama Khalid, S.M.Zeeshan Khan.	1.2	7/3/2024	Background incorporated	
Salman Ali, Osama Khalid, S.M.Zeeshan Khan.	1.21	12/3/2024	Minor changes incorporated.	
Salman Ali, Osama Khalid, S.M.Zeeshan Khan.	1.22	28/03/2024	Minor changes.	
			Added Project Plan	
			Changes Based on Feedback From Supervisor	

# Project Proposal

**Project Title:** Multi-Purpose AI Password Analysis Tool

## 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.

## 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.

## **Opportunity & Stakeholders:**

### **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.

### **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 Enforcement:** Agencies might leverage the tool for lawful investigations adhering to court orders and legal guidelines.

## **Existing System/ Description of the Current Situation:**

### **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.

## **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.

## **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.

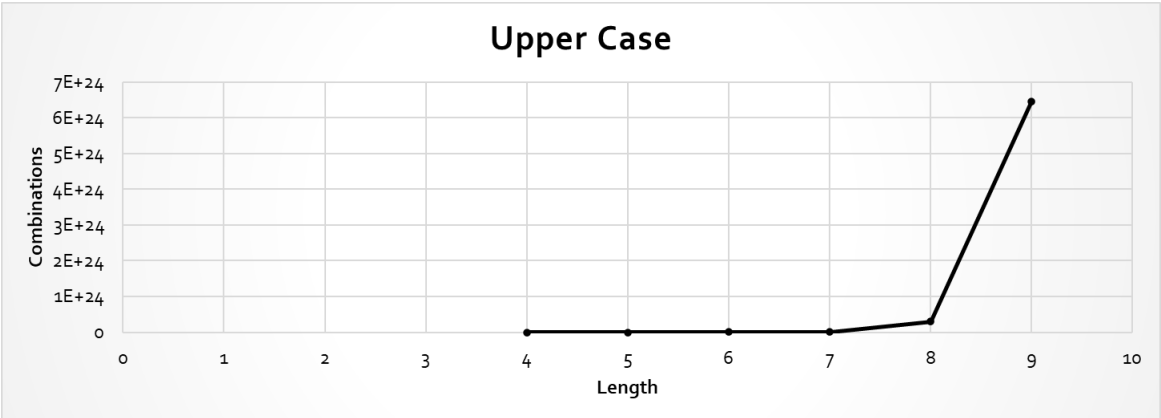
### **Problems:**

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.

Tool	John the Ripper	RainbowCrack	OphCrack	L0phtCrack	Aircrack-ng
Type	Password Cracker	Password Cracker	Password Cracker	Password Cracker	Wi-Fi Network Security Tool
Supported Platforms	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Linux, macOS
Password Hashes Supported	Various (Unix, Windows, etc.)	LM, NTLM, MD5, SHA1, SHA256, SHA512	LM, NTLM	LM, NTLM	WEP, WPA, WPA2
Attack Methods	Dictionary, Brute Force, Hybrid	Precomputed Hash Tables	Rainbow Tables, Brute Force	Dictionary, Brute Force	Dictionary, Brute Force, WPS PIN
Speed	Fast	Depends on Rainbow Table size	Moderate	Fast	Depends on hardware and complexity of the password
User Interface	Command Line	Command Line	GUI	GUI	Command Line
License	Open Source	Freeware	Open Source	Commercial	Open Source
Usage	Penetration Testing, Password Auditing	Password Cracking	Password Recovery	Password Cracking	Wi-Fi Network Security Testi

**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

## 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.

## 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.

## 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.



## **Methodology:**

- **AI Model Development:**
  - Utilize a deep learning framework (e.g., TensorFlow, PyTorch) to train an AI model on password datasets.
  - This will enable the model to identify patterns and weaknesses specific to different password landscapes.
- **Tool Development:**
  - Develop a user-friendly interface for both offensive and defensive functionalities.
  - Integrate libraries/APIs for password hashing, breach checking with online databases, and password cracking.

## **Implementation Plan:**

- 1. Data Collection and Preprocessing:**
  - Gather datasets containing passwords, including commonly used passwords, dictionary words, and human-like patterns.
  - Standardize data format and quality to ensure consistency across the dataset.
  - Preprocess the data by cleaning, tokenizing, and encoding passwords for model training.
- 2. Feature Extraction:**
  - Utilize advanced AI algorithms to extract high-level features from password data, focusing on characteristics such as length, complexity, and entropy.
- 3. AI Model Development:**
  - Design and implement the AI model architecture, incorporating deep learning techniques for password analysis tasks.
  - Experiment with different neural network architectures, such as convolutional neural networks (CNNs), recurrent neural networks

(RNNs), to optimize performance or Generative Adversarial Networks (GANs).

- Train the model on the curated password dataset using appropriate loss functions and optimization techniques.

#### **4. Adaptive Learning Integration:**

- Implement adaptive learning mechanisms within the AI model to continuously improve password analysis capabilities over time.
- Incorporate feedback loops to update the model based on new password patterns and emerging security practices.

#### **5. Evaluation and Validation:**

- Evaluate the trained model's performance using various metrics, such as accuracy, precision, recall, and F1-score.
- Validate the model's effectiveness in analyzing password strength, identifying vulnerabilities, and detecting breached credentials.

#### **6. Deployment and Integration:**

- Develop a user-friendly interface for the password analysis tool, allowing users to input passwords and receive analysis results.
- Integrate the trained AI model into the application or platform for real-time password analysis and vulnerability assessment.

#### **7. Documentation and Training:**

- Create comprehensive documentation and user guides explaining the tool's features, functionalities, and usage instructions.
- Provide training resources and tutorials to educate users on how to effectively utilize the password analysis tool for enhancing security.
- Develop support materials for troubleshooting common issues and FAQs, ensuring users have access to necessary assistance.

### **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.

### **Conclusion/Future work:**

In conclusion, the AI Multipurpose Password Analysis Tool represents a significant advancement in password security, offering users comprehensive capabilities to analyze, strengthen, and protect their passwords against potential threats. Through the implementation of advanced AI algorithms, the tool demonstrates promising accuracy in assessing password strength, detecting anomalies, and facilitating password cracking. Moving forward, there are several avenues for future work and enhancements. Firstly, the tool's usability and accessibility can be improved by developing user-friendly interfaces and integrating it into popular password management platforms or browsers. Additionally, further research and development can focus on enhancing the tool's adaptive learning capabilities, allowing it to continuously evolve and adapt to emerging password patterns and security practices. Moreover, expanding the tool's integration with breach databases and real-time threat intelligence sources can enhance its effectiveness in detecting breached credentials and mitigating security risks. Lastly, collaboration with cybersecurity experts and industry stakeholders can provide valuable insights and feedback for refining the tool's functionality and addressing evolving cybersecurity challenges. Overall, the future scope of the project holds potential for enhancing password security measures and contributing to the ongoing efforts to safeguard digital assets from unauthorized access and breaches.

### **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*

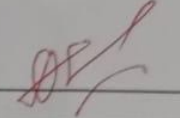
*Conference, ACNS 2019, Bogota, Colombia, June 5–7, 2019, Proceedings 17.*  
Springer International Publishing, 2019.

*Conference, ACNS 2019, Bogota, Colombia, June 5–7, 2019, Proceedings 17.*  
Springer International Publishing, 2019.

### **List of Faculty Proposed Changes**

**Project Title**

Supervisor's Signature: \_\_\_\_\_



Proposed Change	Proposed By	Supervisor's Decision
Please study "PassGAN, Hashcat and RockYou 2021! These are commonly used password cracking tools. How will we validate the proposed idea. Mention the datasets that we are going to use in this project. Reduce the scope of the project.	Dr. Jawaid Iqbal	Accepted
Idea is good. Great Presentation skills. Best of luck.	Haseeb Ahmed	Accepted
Excellent Idea, Excellent Presentation and explanation.	Awais Nawaz	Accepted
Good Idea. Good presentation delivery. Just need to dig in more to wind up in time.	Tajjamul Shahzad	Accepted
Draw comparison between your work and existing systems. Clearly mention your contributions. What will be the procedure for validation?	Ihtisham Ullah	Accepted
Good Idea. Limit your password length.	Engr. Muhammad Ahmed Nawaz	Accepted

# Project Plan

1.	<b>Title Page:</b>
	<ul style="list-style-type: none"><li>• <b>Project Title:</b> Multi-Purpose AI Password Analysis Tool</li><li>• <b>Author:</b> Osama Khalid, Salman Ali &amp; S.M. Zeeshan Khan.</li><li>• <b>University Name:</b> Riphah International University</li><li>• <b>Department:</b> Department of Cyber Security</li><li>• <b>Date:</b> 15<sup>th</sup> March, 2024</li></ul>
2.	<b>Abstract:</b>
	<ul style="list-style-type: none"><li>• <b>Summary of the Project:</b> 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.</li></ul>
3.	<b>Acknowledgments:</b>
	<p>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:</p> <ul style="list-style-type: none"><li>• <b>Project Supervisor:</b> We are particularly grateful to our project supervisor, <b>Mr. Osama Ahmad</b>, 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.</li><li>• <b>Faculty Advisors:</b> We extend our sincere thanks to our faculty advisors, <b>Dr. Muhammad Mansoor Alam</b>, whose passion for AI inspired us to pursue this project, and <b>Dr. Jawaid Iqbal</b>, whose knowledge and guidance were invaluable throughout the research phase.</li><li>• <b>Technical Support Staff:</b> We appreciate the assistance provided by <b>Mr. Haseeb Ahmed</b>, <b>Mr. Ihtesham Ullah</b>, and <b>Mr. Tajamul Hussain</b>. Their technical expertise and willingness to help were crucial in overcoming technical challenges.</li><li>• <b>Project Convener:</b> We acknowledge the leadership of <b>Mr. Muhammad Ahmad Nawaz</b> as the project convener, whose guidance ensured the project's smooth execution within the academic framework.</li><li>• <b>Colleagues and Friends:</b> Finally, we would like to thank our colleagues, <b>Mr. Osama Raza</b> and <b>Mr. Awais Nawaz</b>, for their encouragement, collaboration, and support throughout the course of this project. Their positive spirit and willingness to assist contributed significantly to our progress</li></ul>
4.	<b>Table of Contents:</b>
	<ul style="list-style-type: none"><li>• <b>Introduction</b><ul style="list-style-type: none"><li>• 1.1 Background and Context</li><li>• 1.2 Problem Statement</li><li>• 1.3 Objectives and Scope</li></ul></li><li>• <b>Literature Review</b></li><li>• <b>Methodology</b><ul style="list-style-type: none"><li>• 3.1 Research Design</li></ul></li></ul>

	<ul style="list-style-type: none"> <li>• 3.2 Tools and Technologies</li> </ul>
•	<b>System Design</b>
	<ul style="list-style-type: none"> <li>• 4.1 Architecture and Design</li> </ul>
•	<b>Implementation</b>
	<ul style="list-style-type: none"> <li>• 5.1 Implementation Details</li> </ul>
•	<b>Testing and Evaluation</b>
	<ul style="list-style-type: none"> <li>• 6.1 Testing Methods</li> <li>• 6.2 Results and Evaluation</li> </ul>
•	<b>Results and Discussion</b>
	<ul style="list-style-type: none"> <li>• 7.1 Presentation of Results</li> <li>• 7.2 Discussion of Findings</li> </ul>
•	<b>Conclusion</b>
	<ul style="list-style-type: none"> <li>• 8.1 Summary</li> <li>• 8.2 Achievements and Limitations</li> </ul>
•	<b>Future Work</b>
•	<b>References</b>
•	<b>Appendices</b>
5.	<b>Introduction:</b>
	<ul style="list-style-type: none"> <li>• <b>Background and Context:</b> Password cracking tools are essential for cybersecurity professionals and researchers to assess the strength of passwords and identify vulnerabilities in systems. They aid in penetration testing, forensic analysis, and recovery of lost passwords, crucial for maintaining network integrity and protecting against cyber threats but because of the users employ complex passwords, traditional brute-force methods are impractical.</li> <li>• <b>Problem Statement:</b> With increasing password complexity requirement, brute-force attacks become significantly slower and less efficient. Employment of complex password makes traditional brute-force attacking methods impractical.</li> <li>• <b>Objectives and Scope:</b> <ul style="list-style-type: none"> <li>• Focus cracking efforts on statistically probable password patterns.</li> <li>• Analyze password strength based on complexity metrics and AI-driven pattern recognition.</li> <li>• Reduced cracking time.</li> <li>• Improved vulnerability assessment.</li> </ul> </li> </ul>
	<b>Scope:</b>
	<ul style="list-style-type: none"> <li>• <b>Defensive capabilities:</b> <ul style="list-style-type: none"> <li>• <b>Password strength assessment:</b> Analyze password complexity, identify dictionary words, and check for patterns using AI.</li> </ul> </li> </ul>
	<b>Optional</b>
	<ul style="list-style-type: none"> <li>• <b>Breach checking:</b> Integrate with online databases to verify if entered passwords and email addresses have been exposed in known data breaches.</li> </ul>
	<ul style="list-style-type: none"> <li>• <b>Offensive capabilities: (For Ethical purposes only)</b> <ul style="list-style-type: none"> <li>• <b>AI-powered password cracking:</b> Utilize correlation of password data and advanced algorithms to efficiently crack passwords within a specified scope and with proper authorization.</li> </ul> </li> </ul>

6.	<b>Existing Systems :</b>
	<b>4. John the Ripper:</b>
	<ul style="list-style-type: none"> <li><b>Limitations:</b> <ul style="list-style-type: none"> <li>Relies on traditional methods of password cracking such as dictionary attacks, brute-force attacks, and rainbow tables.</li> <li>While powerful, it may not effectively adapt to evolving password patterns and behaviors without continuous updates and modifications.</li> </ul> </li> <li><b>Problems:</b> <ul style="list-style-type: none"> <li>Lack of advanced AI integration for targeted password list generation based on learned patterns.</li> <li>Limited defensive capabilities in analyzing password strength beyond basic dictionary checks.</li> </ul> </li> </ul>
	<b>5. Brutus:</b>
	<ul style="list-style-type: none"> <li><b>Limitations:</b> <ul style="list-style-type: none"> <li>Primarily designed for online password cracking through network protocols like HTTP, FTP, SMB, etc.</li> <li>May lack advanced AI-driven capabilities for generating targeted password lists.</li> </ul> </li> <li><b>Problems:</b> <ul style="list-style-type: none"> <li>Limited applicability for offline password analysis and cracking scenarios.</li> <li>May not integrate well with the defensive aspects of the proposed tool, such as analyzing password strength and checking for breached credentials.</li> </ul> </li> </ul>
	<b>6. Wfuzz:</b>
	<ul style="list-style-type: none"> <li><b>Limitations:</b> <ul style="list-style-type: none"> <li>Primarily focuses on web application security testing, including fuzzing and brute-forcing directories and files.</li> <li>May lack specialized features for password cracking and analysis.</li> </ul> </li> <li><b>Problems:</b> <ul style="list-style-type: none"> <li>Not specifically tailored for password analysis and cracking tasks, thus requiring significant adaptation to fit into the proposed project's scope.</li> <li>Limited or no integration with AI-driven password analysis and cracking techniques.</li> </ul> </li> </ul>
7.	<b>Methodology:</b>
	<ul style="list-style-type: none"> <li><b>AI Model Development:</b> <ul style="list-style-type: none"> <li>Utilize a deep learning framework (e.g., TensorFlow, PyTorch) to train an AI model on password datasets.</li> <li>This will enable the model to identify patterns and weaknesses specific to different password landscapes.</li> </ul> </li> <li><b>Tool Development:</b> <ul style="list-style-type: none"> <li>Develop a user-friendly interface for both offensive and defensive functionalities.</li> <li>Integrate libraries/APIs for password hashing, breach checking with online databases, and password cracking.</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>• <b>Tools and Technologies:</b></li> </ul>
	<ul style="list-style-type: none"> <li>• <b>AI Model Development:</b></li> </ul>
	<ol style="list-style-type: none"> <li>1. Utilize a deep learning framework (e.g., TensorFlow, PyTorch) to train an AI model on password datasets.</li> <li>2. This will enable the model to identify patterns and weaknesses specific to different password landscapes.</li> </ol>
	<ul style="list-style-type: none"> <li>• <b>Tool Development:</b></li> </ul>
	<ol style="list-style-type: none"> <li>1. Develop a user-friendly interface for both offensive and defensive functionalities.</li> <li>2. Integrate libraries/APIs for password hashing, breach checking with online databases, and password cracking.</li> </ol>
8.	<b>System Design:</b>
	<ul style="list-style-type: none"> <li>• <b>Architecture and Design:</b> Illustrate the architectural framework of your machine learning-based cyber security system. Utilize diagrams or flowcharts to enhance comprehension.</li> </ul>
9.	<b>Implementation:</b>
	<ul style="list-style-type: none"> <li>• <b>Data Collection and Preprocessing:</b></li> </ul>
	<ul style="list-style-type: none"> <li>• Gather datasets containing passwords, including commonly used passwords, dictionary words, and human-like patterns.</li> </ul>
	<ul style="list-style-type: none"> <li>• Standardize data format and quality to ensure consistency across the dataset.</li> </ul>
	<ul style="list-style-type: none"> <li>• Preprocess the data by cleaning, tokenizing, and encoding passwords for model training.</li> </ul>
	<ul style="list-style-type: none"> <li>• <b>Feature Extraction:</b></li> </ul>
	<ul style="list-style-type: none"> <li>• Utilize advanced AI algorithms to extract high-level features from password data, focusing on characteristics such as length, complexity, and entropy.</li> </ul>
	<ul style="list-style-type: none"> <li>• <b>AI Model Development:</b></li> </ul>
	<ul style="list-style-type: none"> <li>• Design and implement the AI model architecture, incorporating deep learning techniques for password analysis tasks.</li> </ul>
	<ul style="list-style-type: none"> <li>• Experiment with different neural network architectures, such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), to optimize performance or Generative Adversarial Networks (GANs).</li> </ul>
	<ul style="list-style-type: none"> <li>• Train the model on the curated password dataset using appropriate loss functions and optimization techniques.</li> </ul>



- **Adaptive Learning Integration:**
  - Implement adaptive learning mechanisms within the AI model to continuously improve password analysis capabilities over time.
  - Incorporate feedback loops to update the model based on new password patterns and emerging security practices.
- **Evaluation and Validation:**
  - Evaluate the trained model's performance using various metrics, such as accuracy, precision, recall, and F1-score.
  - Validate the model's effectiveness in analyzing password strength, identifying vulnerabilities, and detecting breached credentials.
- **Deployment and Integration:**
  - Develop a user-friendly interface for the password analysis tool, allowing users to input passwords and receive analysis results.
  - Integrate the trained AI model into the application or platform for real-time password analysis and vulnerability assessment.
- **Documentation and Training:**
  - Create comprehensive documentation and user guides explaining the tool's features, functionalities, and usage instructions.
  - Provide training resources and tutorials to educate users on how to effectively utilize the password analysis tool for enhancing security.
  - Develop support materials for troubleshooting common issues and FAQs, ensuring users have access to necessary assistance.

•

#### 10. **Testing and Evaluation:**

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.

•

#### 11. **Results and Discussion:**

	<ul style="list-style-type: none"> <li>• <b>Presentation of Results:</b> Showcase the outcomes of your project, highlighting successful instances of anomaly detection.</li> <li>• <b>Discussion of Findings:</b> Analyze and interpret the results, discussing their implications and significance in the broader context of cyber security.</li> </ul>
12.	<b>Conclusion:</b> <ul style="list-style-type: none"> <li>• <b>Summary:</b> Summarize the key findings and contributions of the project.</li> <li>• <b>Achievements and Limitations:</b> Highlight the accomplishments of the project and acknowledge any inherent limitations.</li> </ul>
13.	<b>Future Work:</b> <ul style="list-style-type: none"> <li>• <b>Suggestions for Future Enhancements:</b> Provide recommendations for future research or improvements to advance the capabilities of your machine learning-based cyber security system.</li> </ul>
14.	<b>References:</b> <ul style="list-style-type: none"> <li>• <b>Citations:</b> List all the sources referenced in your report, adhering to a specific citation style as per the guidelines of your university.</li> </ul>
15.	<b>Appendices:</b> <ul style="list-style-type: none"> <li>• <b>Additional Material:</b> Include supplementary materials, such as code snippets, datasets, or additional information supporting the main content of the report.</li> </ul>
16.	<b>Formatting Guidelines:</b> <ul style="list-style-type: none"> <li>• <b>University-Specific Guidelines:</b> Adhere strictly to your university's formatting requirements, including font size, margins, line spacing, and citation style.</li> </ul>

## Roles & Responsibility Matrix:

The purpose of roles & responsibility matrix is to identify who will do what.

WBS #	WBS Deliverable	Activity #	Activity to Complete the Deliverable	Duration (# of Days)	Responsible Team Member(s) & Role(s)
1	Phase 1: Develop and Train the AI Model	1.1	Research and select appropriate AI algorithms for password analysis.		Osama Khalid Zeeshan Khan Salman Ali
		1.2	Acquire or prepare relevant password datasets for training.		
		1.3	Train and optimize the chosen AI model with the selected datasets.		
2	Phase 2: Implement Core Functionalities	2.1	Design and develop functionalities for password strength analysis.		Osama Khalid Zeeshan Khan Salman Ali
		2.2	Integrate password breach checking with online databases (securely).		
		2.3	(Optional) Develop functionalities for automated password cracking (ethical considerations apply).		
3	Phase 3: Design and Develop User Interface	3.1	Design a user-friendly interface for both offensive (optional) and		Osama Khalid Zeeshan Khan

			defensive functionalities.		
		3.2	Integrate the trained AI model and core functionalities into the user interface.		
4	Phase 4: Testing and Refinement	4.1	Conduct thorough testing of all functionalities with various password scenarios.		Osama Khalid Zeeshan Khan Salman Ali
		4.2	Refine the AI model, user interface, and functionalities based on testing results.		
		4.3	Document user manuals and instructions for the completed tool.		

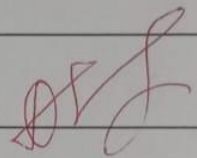
## Approval

### Project Supervisor

Comments SATISFACTORY.

Name: OSAMAH AHMAD

Date: 28/3/24

Signature: 

### Project Coordinator

Comments \_\_\_\_\_

Name: M. Ahmad Nawaz

Date: 28/3/24

Signature: 