International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 31 Issue 3 – MAY 2025.

Comparative Analysis of Password and Passphrase Generation for Secure Applications

A.Neela Madheswari[#1] , G.Raja [*2], C.Arunkumar [*3], S.Anbarasan [*4], V.Tamilselvan [*5]

[#]*Professor, CSE Department, Mahendra Engineering College, Namakkal, Tamilnadu, India*

[*]*UG Scholar, Cyber Security Department, Mahendra Engineering College, Namakkal, Tamilnadu, India*

***Abstract*— In the digital landscape, passwords and passphrases serve as critical barriers against unauthorized access to sensitive information. This paper aims to develop two robust tools such as character-based password generation and a secure pass phrase generation. The first tool generates customizable passwords adhering to industry standards, while the second transforms user-friendly phrases into secure passphrases using advanced transformation rules. The paper evaluates the performance of both tools through metrics such as strength assessment, time complexity, and usability. By addressing the dual challenges of complexity and usability, this study underscores the importance of secure credentials in modern cyber security practices.**

***Index Terms*— password security, pass phrase generation, cyber security, authentication, software development.**

I. Introduction

In the contemporary digital ecosystem, the proliferation of online services and digital platforms has led to an unprecedented reliance on password or pass phrase based authentication systems. As organizations and individuals increasingly store sensitive information in digital formats, the need for robust password or pass phrase security has become paramount. The digital passwords and pass phrases serves as the first line of defense against unauthorized access to sensitive data. However, despite their importance, many users still rely on weak or predictable passwords, leading to significant security vulnerabilities. Recent studies highlight that a considerable percentage of security breaches result from compromised passwords. This alarming trend emphasizes the need for robust password generation methods that uphold security standards.

The increasing prevalence of cybercrime highlights the critical need for robust authentication mechanisms. Secure passwords and passphrases serve as gatekeepers, protecting personal, corporate, and financial information. Weak credentials leave systems vulnerable to attacks, leading to data breaches, identity theft, and financial losses. Strong passwords must have the characteristics such as: i) sufficiently long to resist brute force attacks, ii) composed of diverse character sets such as letters, numbers, and symbols, iii) randomized to prevent predictability, Passphrases on the other hand, provide an alternative solution that emphasizes memorability while maintaining high security by leveraging length and complexity. Together, they form essential tools for safeguarding digital systems in an increasingly interconnected world.

The primary objective of this work is to develop two tools aimed at enhancing password security through customizable and user-friendly features. By addressing the dual challenges of complexity and memorability, this paper seeks to educate users on the significance of strong passwords and provide practical solutions for their implementation. The main aim of this paper is given as: i) educate users about the importance of strong passwords and passphrases, ii) demonstrate how randomness and complexity contribute to password strength, and iii) provide practical tools that balance security with user convenience.

II. Literature Review

The literature review provides a comprehensive overview of existing research on password security and the methodologies employed in password generation. Numerous studies have explored the weaknesses of traditional password systems, identifying common pitfalls such as poor user practices and inadequate security measures.

The growth of cybercrime costs is given in [1] and is shown in figure 1. As per the statistics given in [2], 81 percent of confirmed breaches were due to weak, reused, or stolen passwords in 2022. There are many types of password attacks that pose threat to company, client or employee data such as phishing, Man-in-the-Middle attack, Brute Force attack, Credential stuffing, Keylogging, and Rainbow Table attack [3].

A password is easy for an individual to remember is valued higher than a more complicated secure password. There is a conflict between security and usability when it comes to user authentication methods since there is a requirement to implement a high level of security while ensuring that the design is user-friendly. The user interface is where the system and user interact through commands on the web to operate the system, put in data, and use the contents. Usability of the user interface is essential since it assists the user to interact with the system, and security is necessary to protect the information against unauthorized individuals [4].

The paper [5] specifies that the different combinations of characters will strengthen the security and increase the difficulty faced by attackers trying to guess passwords using Brute force techniques. The paper [6] specifies that the security experts recommend using long, random, and unique passwords for every account, but remembering them all is

impossible. A security password generator can create highly secure, random passwords that meet modern security standards, helping users strengthen their digital security without the hassle of coming up with passwords manually.

A secure passphrase is the next generation in passwords. It uses a short phrase instead of a single word, making it more difficult for someone else to guess or use. It should be virtually impossible for others to guess, and not contain or be based on personal information. Passphrases should never be written down or given to anyone else [7].

A password composition policy (PCP) language is described in [8] that describes the language that websites use to generate compliant passwords. The libraries are provided for adopting in PCP language into websites and password managers and build proof-of-concept prototypes to verify the real-world feasibility of the PCP language.

In order to effectively balance between security and usability effective password composition policies must be ensured so that the user accounts will be secured without causing undue frustration or encouraging insecure workarounds such as password reuse, which undermines online safety [9].

The security and privacy of individual information from intruders is a concern to all those who use different online services. Password is an authenticated tool which does not need additional hardware and can be used easily. Database administrators utilize password composition policies to discourage users from choosing vulnerable passwords [10].

Although various tools and guidelines exist, gaps remain in user education and the practical application of password policies. This work aims to bridge these gaps by offering tools that not only generate secure passwords but also enhance user understanding of password security principles.

Fig. 1 Growth of Cybercrime costs [1]

III. Character Based Password Generator

This work is to develop a customized tool that generates random passwords by including specific character types like alphabets, digits, and special symbols while calculating the strength of the generated password. It shuffles the selected characters to create unique and unpredictable passwords. It also calculates password strength, based on character variety, length, and complexity. It is possible to receive the time taken to generate the password for performance insights.

A. *Algorithm for Password Generation*

i) Start the process.
ii) Get User input: Here the length of the password, count of alphabets, digits and speacial characters are received from the user.
iii) Validate input: The total number of character count does not exceed password length.
iv) Generate password: Randomly select characters based on the input. Fill the remaining length with random characters, shuffle the characters for randomness.
v) Calculate Password strength: Password srength is evaluated based on the criteria such as alphabets, digits, special characters, case sensitivity, and length.
vi) Display the output: Display the password, strength of the passowrd, and time taken for password generation.
vii) Stop the process.

IV. Secure Passphrase Generator

Passphrases provide an alternative to passwords, focusing on length and memorability to ensure security. Unlike passwords, which often prioritize complexity, passphrases use natural language, making them easier to remember while maintaining resistance to brute force and dictionary attacks. This work converts user input into a secure passphrase by applying rules to increase complexity and evaluate strength using entropy metrics. This work enhances input strings by replacing specific characters with symbols, capitalizing letters, and appending unique elements. It is possible to receive the time taken to generate and evaluate the passphrase. In order to enhance the complexity, common characters are replaced by special charcters and numebrs. For example, a is replaced by @, e is replaced by 3, etc.

A. *Algorithm for Passphrase Generation*

i) Start the process.
ii) Get User input: Here the passphrase string is received from the user.
iii) Validate input: It is ensured that the passphrase length is at least two characters.
iv) Apply transformation: The first letter is capitalized. Replace characters with predefined substitutions. Optionally append random numbers or special characters.
v) Calculate Passphrase strength: Passphrase strength is evaluated based on the criteria such as character types, length and randomness.
vi) Display the output: Display the passphrase, strength of the passphrase, and time taken for passphrase generation.
vii) Stop the process.

V. Character Based Password Generator Vs Secure Passphrase Generator

As though password generation and passphrase generation are used for securing applications for authentication, there is a difference among both the types in terms of features, use case

scenarios, security metrics analysis, usability and performance, and real world application scenarios. Table 1 specifies the features, table 2 specifies the use case scenarios, table 3 specifies the security metrics, table 4 specifies the usability and performance, table 5 specifies the real world implementation scenarios for both the models.

Table 1. Featured comparison between password and passphrase generation

Feature	Password Generator	Passphrase Generator
Objective	To generate a secure password with randomized characters	To generate a secure passphrase from user input with transformations
Length	Typically shorter (usually 8 to 16 characters)	Typically longer (usually 12 to 20 characters)
Complexity	Relies on character mix	Designed for memorability and security
Randomness	Emphasizes character randomness for security	Uses custom transformation rules and entropy-based enhancements
Security approach	Mixes alphabets, digits, and symbols for resistance to brute-force attacks	Transforms input phrases to make them harder to guess while keeping them memorable

Table 2. Use case scenarios for password generation and passphrase generation

Use case	Password Generator	Passphrase Generator
Corporate accounts and online banking	Ideal for generating complex passwords for high-security accounts	Suitable for situations where a memorable passphrase is needed alongside security
Temporary passwords or OTPs	Great for one-time or frequently changing passwords	Less suitable as passphrase tend to be longer and more permanent
Password requirements for web services	Excellent for websites that require passwords with a mix of characters	Suitable for personal accounts with less stringent password rules
Personal accounts or information accounts	Less memorable may not be ideal for non-technical users	Perfect for users looking for secure yet memorable passphrases

Table 3. Security metrics analysis for password generation and passphrase generation

Security metric	Password Generator	Passphrase Generator
Strength	Based on character diversity (such as alphabets, digits, symbols), and length	Based on entropy and transformation rules, longer length can helps much
Entropy	High entropy with random characters and a variety of symbols	Can have high entropy with sufficient transformation but depends on input strength
Vulnerability to attacks	Resistant to brute force and dictionary attacks, but shorter passwords can be weak	Vulnerable if input is too simple, but enhanced by transformations
Impact of length	Password length is crucial for strength	Passphrases benefit from longer length and transformations for enhanced security

Table 4. Usability and performance comparison for password generation and passphrase generation

Feature	Password Generator	Passphrase Generator
Ease of use	Simple, requires minimal input from the user	Requires user input string with optional transformation rules
Performance	Fast, especially for standard password lengths	Slightly slow due to transformations and entropy calculations
Memorability	Not easily memorable due to randomness	Easier to remember, as it is based on familiar phrases with added complexity
Customization	Customizable by user input for length and character counts	Customizable with string transformations and optional random additions
Security weakness	Weak if password is too short or predictable	Vulnerable if the input phrase is simple or common

Table 5. Real world implementation scenarios for password generation and passphrase generation

Implementation area	Password Generator	Passphrase Generator
Secure Authentication Systems	Generates strong, complex passwords for secure login processes, such as online banking, corporate accounts, and government systems	Generates secure, memorable passphrases for use in multi-factor authentication or systems where users need both security and ease of recall
Personal account security	Ideal for generating random, complex passwords for personal accounts (such as email, social media, e-commerce) to meet password complexity requirements	Useful for generating memorable yet secure passphrases for personal accounts where ease of recall is important (such as email, cloud storage)
Enterprise-level password policies	Ensures compliance with enterprise password policies by generating strong passwords with required character variety for employees corporate logins	Suitable for generating passphrases for internal enterprise systems where security is required but memorability is prioritized (such as VPN access, internal tools)
Cyber security awareness education	Demonstrates the importance of strong, complex passwords and the risks of using weak or simple passwords in educational programs	Used to teach how to create secure passphrases by applying transformation rules and evaluating their strength to reinforce best practices in cyber security education
Integration into larger security platforms	It can be integrated into password management tools to auto-generate passwords for user accounts and ensure strong credentials	It can be used in MFA systems to generate secure passphrases or backup codes, adding an extra layer of security for user authentication

VI. System Consideration for Evaluation

The password generation and passphrase generation are implemented using python and is tested for evaluation using execution time under various factors for each method. The system considered for execution is as follows: System model used - Oppo Reno 7, Processor – Qualcomm SnapDragon (6mm chipset), RAM – 8 GB, Storage – 256 GB. Online python compiler is used to ensure efficiency and real-time results [11]. Time complexity are calculated for character based password generation and secure passphrase generation using various length passwords and passphrases and are given in table 6 and table 7 respectively.

Table 6. Time complexity calculation for character based password generation

Character Length	Character based password generation	Time in milli seconds
8	!16S^hTD	0.072
12	)g%pb&60Ge8i	0.084
16	5^56WZA)&L^HT1Rq	0.120
20	*35$Xs@&X)H8uDz2zS7f	0.094
24	29J@R(H16C5C)1AYx9@R*@hp	0.107
28	ZT!0q6^Z1)fc7fc7h6@A2S2^fG%1ls^	0.096
32	M8F^8zxn(r%Cm!%dzV@**4R09RUR4D68	0.069
36	x)3Ygm!7KIUAW2@9v3BjmX%a0!1$@a(5)r1F	0.133
40	sov8YpMy@*5&$wPd@9K1h13(B50r#T(D%5P1s$mf	0.143

Table 7. Time complexity calculation for secure passphrase generation

Character Length	Secure passphrase generation	Time in milliseconds
8	Stay safe	0.085
12	Secure my data	0.092
16	Protect data, stay secure	0.087
20	Stay safe, secure your data	0.079
24	Your safety starts with you	0.084
28	Cybersecurity begins with awareness	0.104
32	Protect yourself from online threats daily	0.077
36	Digital safety ensures a secure tomorrow	0.070
40	Strong passwords and awareness lead to security	0.081

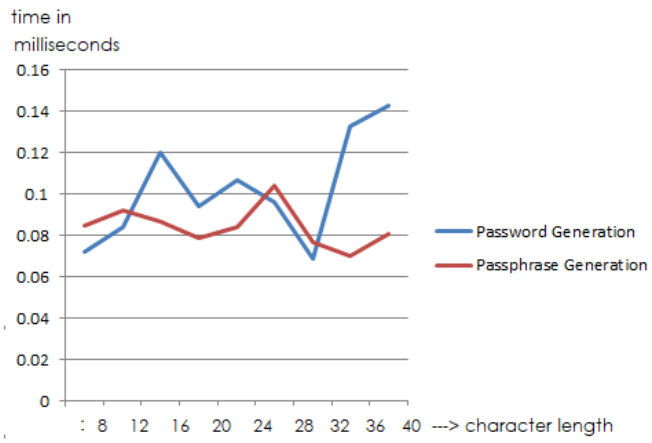

Fig. 2 Time Complexity for character based password generation and secure passphrase generation

VII. CONCLUSION

The proposed work specifies two concepts namely character based password generation and secure passphrase generation. These concepts are tested for time complexity by varying the length of the password or passphrase which has to be generated and from the figure 2, it is clearly understood the passphrase generation has a less time complexity when compared to password generation. Also it is easy to remember if we use passphrase generation. This work can be enhanced further by various combinations of password and passphrase combination and also for implementing various security measures like multi factor authentication, and the graphical form of password, by using these two concepts since in this current digital era is fully enhanced and experienced a lot of information storage and secure access is needed everywhere.

REFERENCES

[1] Cyberattack statistics 2025, Embroker Team, https://www.embroker.com/blog/cyber-attack-statistics/, accessed on April 2025.
[2] Rob Sobers, 82 Must-Know Data Breach Statistics [updted 2024], https://www.varonis.com/blog/data-breach-statistics, accedded during April 2025.
[3] Password Attacks, https://www.ontinue.com/password-attack/, accessed during April 2025.
[4] Cleopatra Borg Goga, Security and Usability: Recommendations for Password User Interfaces, Masters Degree Project, University of Skovde, Autumn 2023.
[5] Lama A.Almalki, Samah H.Alajmani, Ben Soh, Raneem Y.Alyami, Analysing the Impact of Password Length and Complexity on the Effectiveness of Brute Force Attacks, International Journal of Network Security and its Applications, vol.17, No.2, March 2025.
[6] Prof. Sayali Ambekar, Rinka Kamble, Supriya Chakre, Sanjivani Kendre, Pratiksha Bansode, Security Password Generator, International Journal of Research Publication and Reviews, Vol.6, Issue.3, March 2025.
[7] How to create a secure passphrase, https://www.buffalo.edu/content/www/ubit/service-guides/safe-computing/_jcr_content/rightcol/download_1820535914/file.res/how-to-create-a-secure-passphrase-2017-08-10_HQP.pdf, accessed during April 2025.
[8] Anuj Gautam, Shan Lalani, Scott Ruoti, Improving Password Generation through the Design of a Password Composition Policy Description Language, Proceedings of the Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022), Aug 2022.
[9] Huang, David H., Bridging User Preferences and Security Demands: A User-Centric Approach to Password Generation. Master's Thesis, University of Tennessee, 2024.
[10] Bathula Prasanna Kumar, Edara Srinivasa Reddy, An Efficient Security Model for Password Generation and Time Complexity Analysis for Cracking the Password, International Journal of Safety and Security Engineering, vol. 10, No. 5, October 2020.