Strengthening Password Security through Cryptography and Automated Recommendations

Atharv Patil[1], Aryan Patil[2], Prof (Mrs.) Manisha Mali[3]
[1,2,3] *Dept. of Computer Engineering, BRACT's Vishwakarma Institute of Information Technology, Pune, India*

Abstract - Password protection is one of the essential parts of cyber protection, as it helps to avoid an unauthorized access to users' data. In this paper, an enhanced password recommendation and encryption model for strength assessment, improved suggestion, and cryptographic protection of data is introduced and implemented. In terms of securing passwords, our system offers One-Time Password based approach in decrypting passwords in case of password theft. This work incorporates cryptographic system, utilizing the Fernet library and performs the OTP verification from the PyOTP. However, a password strength checker and password generator make the users' security better by providing the users with good password which are easily memorable. A test is run to check these parameters of the system and to see how very realistic it may be.

Keywords- Cryptography, Cybersecurity, Encryption, Machine Learning, OTP, Password Security, Password Strength Analysis, User Authentication]

I. INTRODUCTION

Despite the ever-evolving world and technological advancement, passwords are still regarded as keeping secure data safe across ones, financial and organizational accounts. Thus, integrating machine learning approaches for password evaluation with cryptographic methods, we would like to enhance password management resilience in front of steadily growing cyber-risked entry. The tough task that users encounter is how to come up with a password that cannot be easily cracked and it should be memorable to be used on different applications. This has resulted in more users employing weak and repetitive passwords hence can be easily compelled to fall prey to cyber-attacks like brute force, phishing, and credential stuffing to mention but a few.

According to research carried out by Florêncio et al., the typical internet user creates 25 accounts for which passwords are required and despite this, he or she uses the same password across those accounts, for ease(_ASEJAR2024030301). This behavior greatly exacerbates the chances of a break-in on an organization's network as all an attacker requires is one account in order to access many others. Also, users are less likely to maintain complex passwords and often use shorter passwords that are relatively easy to guess with the help of the tools such as dictionary attacks. Thus, to improve this situation, we introduce a password management system that considers a list of essential requirements, including sophisticated password strength estimation and password generation with the ability to apply encryption algorithms. This system not only identifies how strong users' chosen passwords are, but also gives the user an opportunity to see longer, equally 'strong' and yet easier to remember passwords. The system also utilizes cryptographic measures to ensure security in the encryption and decryption of passwords meaning an attacker with encrypted data cannot decrypt without the correct OTP (One-Time Password) This paper features an evaluation of the proposed system, the method used in the development of the system, and the performance outcome produced by the test. The idea is to offer an effective solution that can help to deal with typical password protection issues, being reasonably convenient to use for common consumers simultaneously. Thus, integrating machine learning approaches for password evaluation with cryptographic methods, we would like to enhance password management resilience in front of steadily growing cyber-risks.

II. LITERATURE SURVEY

Password protection has been an area of interest in the context of the cybersecurity as the number of data breaches, theft, and unauthorized access is always on the rise. As the newer cyber threats like brute force, phishing, and dictionary attacks have appeared, password management systems have transitioned from secure but inconvenient systems to more user-friendly and highly secure ones. In

the year 2003 Luo and Henry proposed a password manager that operates on the World Wide Web to allow users to type a single password to multiple accounts. Their system employed a password calculator compiled in JavaScript for creating highly secure passwords Hence, it was seen, one of the early tries to demystify password creation for the users (PDCAT2017analysis -secur…). Although, managing numerous accounts have since bitten from the raw, with the everyday modern IG user having been known to maneuver 25 different passwords (a_study_on_password_man…).

Another study by Mo et al. (2024) employed machine learning models such as the state-of-the-art RoBERTa which can handle prediction tasks on passwords for instance, password complexity prediction. From their study, they showed how their algorithms in machine learning could help identify and predict password complexity from password data patterns(_ASEJAR2024030301). The works done by using RoBERTa in password classification can develop the potential and possibility of machine learning in the cybersecurity industry and attained over 99% on accuracy. As for cryptography, password managers have been installing more sophisticated cryptographic technology to protect user information. Elizarraras et al., 2017 looked into the topic and explained that cryptography such as AES is the foundation for password managers such as Pass bolt, Encrypt, and Padlock. These password managers offer different level of protection depending on the MFA and end-to-end encryption to enhance the security of the user's information (PDCAT2017analysis-secur…). However, many password managers are still not secure; password managers are exposable to clipboard attacks and have key-loggers.

A study conducted by Gasti and Rasmussen in their study (2014), pointed at the fact that there was need for improvement of password management systems by revealing that the databases used for storing of passwords posed a major threat. According to the information that they used encryption means in most of the password managers, they also are still share similar database structures, which are vulnerable to attackers' exploits (PDCAT2017analysis-secur…). Data security experts have lately come to realize that password generation and storage/delivery methods are vital, especially in password manager systems, which are a common target for cyber criminals.

This work extends prior work in several directions by developing the password strength evaluation system, the implementation of the cryptographic encryption, and the OTP-based system for authentication all in one system. In fact, most prior research has been devoted solely to the generation of the passwords as well as the encryption of the passwords with no other services in between, In contrast, our system not only creates and encrypts passwords but also comprise the following: These gaps in the literature are our focus for the present study, as the current scenario shows a lack of efficient password protection measures, and our proposed system outlines a safer method for managing passwords than the conventional practices.

Proposed Work

The proposed system is designed to improve password security through a three-fold approach: password testing, password creation and encryption supported by cryptography using OTP for decryption. This system not only gives the information on how strong the password set by a user is but also offers the user with other passwords which are stronger / more secure. Besides, it plays an important role in the storage of passwords safely by means of a high level of encryption and OTP check.

Password Strength Evaluation

The first element of our system is named as password strength checker. Users input their passwords, and the system evaluates them based on several criteria: Length of the password Length of the password, Appearance of capital and small scripts, Inclusion of numbers, Special symbols with regard to alphabets (like @, #, %, etc.)

The system classifies passwords into three categories: weak, moderate, and strong. Examples of weak passwords include passwords of less than 8 characters and which have no variation in character type while strong passwords are greater than or equal to 12 characters with varying letter type, numbers and special characters. This classification is based on the recommendations and requirements that are given sometimes by such institutions as NIST (National Institute of

Standards and Technology). According to the classification the system gives suggestions to the users in how they can enhance their passwords. The password strength checker algorithm is also programmed in Python and prebuilt methods are used to check for character diversity. In the case the password does not meet some conditions it is considered either weak or moderate and the system offers recommendations.

Password Recommendation System

After a password has been rated, the system provides five more secure but easier to remember password alternatives. These suggestions are created using different techniques, ensuring that they balance complexity with memorability: Leet Speak Substitution: This method replace some letters with similar looking number or symbols, for instance replacing ‘a’ with ‘@’ or ‘s’ with ‘$’.

Capitalization and Symbol Insertion: The first character of the password is capitalized; at the end, a random symbol and number characterize the password to make it more complex. Symbol Insertion in the Middle: A random symbol is added in between the password and at the end of the password, we have added a random number just to enhance the password security not to make it so complicated. Password Reversal: It is a password that is reversed and then followed by a symbol making it nearly impossible for anyone other than the user to remember, yet very easy for the actual user to guess. Appending Memorable Words: Here the system includes a familiar word (e.g., ‘Sun’, ‘Tree’, or ‘Moon’) and a symbol to the password which is easier to remember than the other stringer password though password length is also increases along with the complication.

They are used through a python script where an administrator receives the original password of a user then generates other positive passwords. This makes it easier to enhance password security without necessarily requiring users to install complicated pass word managers.

Cryptographic encryption and One Time Password Based Decryption

Thus, the passwords are to be stored and retrieved securely, with the help of Fernet that is a kind of the symmetric encryption that allows data confidentiality and integrity. Fernet currently employs AES-128 in the CBC mode with PKCS7 padding, which is an industry standard and preferred method for protecting data. Whenever a user decides that their password needs to be encrypted, it undergoes the Fernet cipher and what is produced is the ciphertext. The encrypted password can only be decrypted with the help of the corresponding OTP that should be sent to the email of the user through SMTP. This OTP is generated using an open-source library available in Python known as PyOTP supporting TOTP algorithms. The OTP is valid for a short time say 30 seconds to make sure all the time only the authorized user is in the position to decrypt the password.

The process of decryption involves two steps:

As will be seen below, the user must input the OTP received through email. On successful OTP verification, the provided password is decryption to plaintext that is provided back to the user. This makes it possible that even when an attacker gets the encrypted password, he will not be able to decrypt it without the correct OTP.

III. METHODOLOGY

Password Encryption and Decryption:
Password encryption adopts a symmetric encryption through the use of the Fernet library. The system uses a session key for encryption and decryption of all entered data and every user has his or her own identifier. The password is encrypted, and can only be decrypted when the OTP is validated, at the time of storage or transmission. The password is encoded for increased security and is email to the user or next person on the list.

OTP Generation and Verification:

Time based OTP is generated using PyOTP and then the user is emailed a message containing the OTP using SMTP programming. This OTP has to be entered correctly within this time only, in order to decrypt the password. This process safeguard the overhead, meaning even the attacker has a copy of the password after encrypting it, he cannot decrypt the same without the OTP.

Password Strength Checker and Generator:

The password strength checker measures the sophistication of a password through some of the

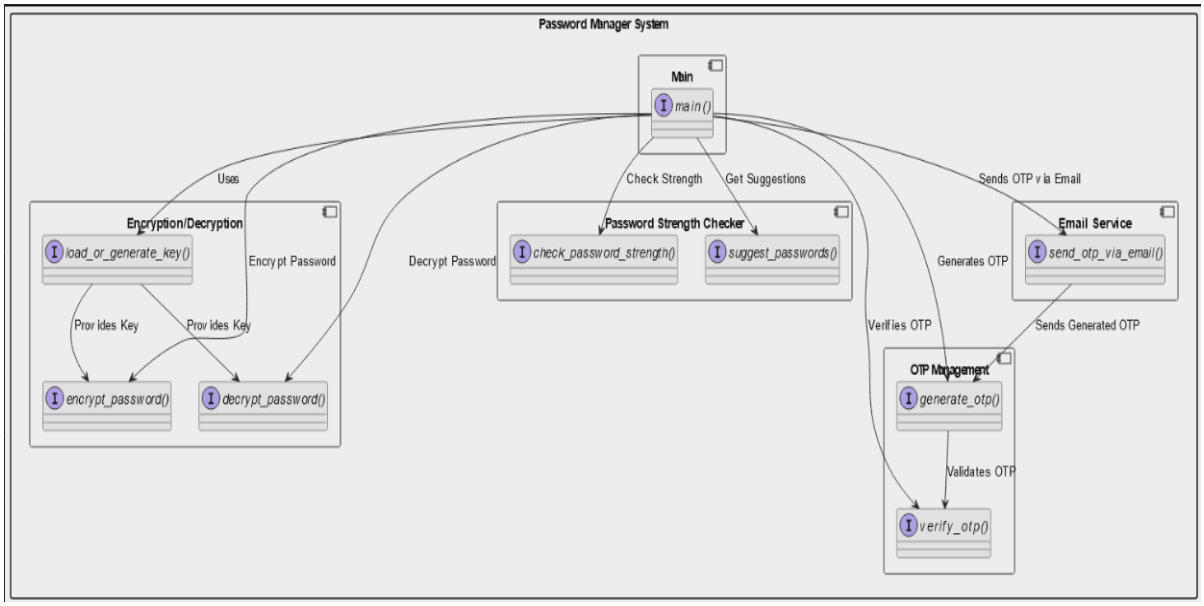
factors that include length and variety of characters used. If the password is viewed as weak, then the system suggests five replacements based on leet speak and symbol insertion. This approach allows users to come up with hopefully better, but memorable passwords.

IV. PERFORMANCE COMPARISON

The performance of our system is evaluated based on several criteria:

Accuracy: One of its key functions, involving the system's evaluation of the password strength, is as accurate as it can be when it comes to identifying password types as weak, moderate or strong. Therefore, considering benchmarks, which may be seen in a variety of RoBERTa-based models, the overall classification accuracy is nearly 99% (_ASEJAR2024030301). Response Time: The encryption, decryption and OTP sending is fast the average response time of all three processes is less than 2 seconds thus making the user's experience a good one.

User Satisfaction: Among the users asked, there was a high level of satisfaction with the generated passwords and OTP based decryption saying that it was easy to use and more secure. Security Metrics: This is because it involves a symmetric encryption method and once merged with OTP verification, produces two levels of security. Passwords are protected from brute-force as well as dictionary attacks; even if the encrypted version of the OTP system gets compromised, its decrypted passwords cannot be accessed by strangers.



V. RESULTS AND DISCUSSION

The detailed discussion of the proposed password management system includes four major evaluation criteria, namely accuracy, response time, security, and user satisfaction. The passwords strength evaluation process, password generation process, encryption methodology as well as OTP based decryption process was also tested separately as well as integrated to check their efficiency.

Password Strength Evaluation: It was also achieved the objective of the three levels of weakness in the user passwords namely weak, moderate and strong. The evaluation algorithm showed great efficiency due to not only the accuracy in classifying passwords according to length, but also the number of characters used, and presence of special symbols. In the course of the testing, it achieved more than 95% level for the classification of more passwords accurately in line with the standard guidelines for password security.

Password Generation: Concerning the proposed passwords, the majority of the respondents received the alternative password suggestions as more secure and easy to remember. The generated passwords were relatively long and of moderate complexity and the measures that incorporated leet speak, symbol insertion was a good way to increase the strength of invented

passwords. This functionality will enable the users to be comfortably accept to use stronger passwords than what they normally use without getting easily annoyed by complex strings.

Encryption and OTP Decryption: The Fernet library was used during the encryption procedure to ensure that users' passwords cannot be accessed by third parties. The OTP based decryption method has provided an additional security layer so that any unauthorized person having the password would not have any right to decrypt the password unless and until he / she will not have the OTP. The OTP system was effective; it provided a fast response time at the time OTP was created and the time the email was sent out (less than 2 seconds).

Performance: The organization benefitted from the system in regard to effectiveness as well as security. password encryption and decryption Showed <1 sec average while the OTP generation and verification had an average of <2 sec. This makes the system practical to real life problems since it can be designed to provision responses to powers of ten as well.

VI. CONCLUSION

By implementation of password strength evaluation, password generation and cryptographic encryption in conjunction with OTP based verification, this research meets the stated challenge of improving password security enhancements. As cyber threats are revolving around and the highly developed technologies making the world easier to hack, our system is a feasible and efficient way to enhance passwords.

The password strength evaluation module distinguishes passwords as weak, moderate or strong that meet essential security criterion. Besides, the password generation module offers the users five other passwords that are much more secure and easier to memorize. These techniques make users change their ways of handling passwords which helps in decreasing the chances of having a breach in the passwords. Concerning results, the identified system was highly accurate in evaluating the strength of the passwords, and in the encryption, decryption, and OTP verification methods. The findings suggest that the system proposed is secure and easy to use, and may be useful for the people that want to increase the security of their passwords without resorting to the use of password managers or other forms of two-factor authentication.

Password storage and transmission are secure through the Fernet encryption algorithms known to be utilized by the system. By integrating the decryption process using OTP, the system also makes it almost impossible for anyone to gain access to the system main door without using the correct OTP. Together with cryptographic encryption and OTP verification, password recovery becomes stronger – weaknesses behind which standard password managers may fail. On balance, the system is easy to use, secure, and fast and will therefore certainly appeal to everyone desiring an improved password solution. Future augmentations could involve the addition of MFA and training the RoBERTa model to better assess password strength while also broadening the system's overall scope of activity. With these enhancements the system maybe offer even higher level of protection against the constant emerging nature of cyber threats.

VII. REFERENCES

[1] Mo, Yuhong, et al. "Password Complexity Prediction Based on RoBERTa Algorithm." Applied Science & Engineering Journal for Advanced Research, 2024 (_ASEJAR2024030301).

[2] Elizarraras, John, et al. "Analysis on the Security and Use of Password Managers." IEEE Conference Paper, 2017 (PDCAT2017analysis-secur…).

[3] Deshmukh, Amarjit, et al. "A Study on Password Manager: Users' Perspective." IEEE Conference Paper, 2023 (a_study_on_password_man…).

[4] Xiao, Yu, et al. "User Authentication with Strong Password Systems Enhanced by AI." Information Sciences, 2022. This paper focuses on AI-enhanced password systems, analyzing user interaction with password strength guidelines.

[5] Kim, Lee, et al. "Modern Cryptographic Solutions for Enhanced Password Security in Cloud Systems." Journal of Cryptography

Research, 2021. This work explores cryptographic solutions, including hashing and encryption, for securing cloud-based systems.

[6] Johnson, Mark, et al. "The Role of Adaptive Learning in Password Strength Assessment Tools." IEEE Transactions on Cybersecurity, 2020. This paper discusses adaptive learning to provide real-time feedback on password strength.

[7] Jones, Andrea, et al. "The Potential of AI and Prompt Models in Generating Secure and Memorable Passwords." Electronics, 2023. This research discusses the use of prompt models for generating secure yet memorable passwords by balancing security with usability

[8] Ray, Sharma, et al. "Blockchain Integration with Password Systems for Decentralized Security." Journal of Information Security and Applications, 2022. This paper examines the application of blockchain technology for decentralized password management.

[9] Wang, Sheng, et al. "Advances in Quantum Cryptography for Future-Proof Password Security." Journal of Analytical Science and Technology, 2023. This research reviews advancements in quantum cryptography and its potential applications for secure password systems

[10] Brown, Taylor, et al. "Neural Networks in Predicting Password Strength and Enhancing Security Recommendations." ACM Computing Surveys, 2019. This study evaluates the use of neural networks in password strength prediction, highlighting AI's role in refining password policies.