AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
E-ISSN:3069-0102
VOL.5, NO. 3(2025)

NEXT-GEN PASSWORD SECURITY: ENCRYPTED NEGATIVE PASSWORD AUTHENTICATION FRAMEWORK

[1] Kim Jungkook,[2] Jung Seok Lee
Gangnam-gu,Seoul,South Korea

ABSTRACT

The increasing prevalence of cyberattacks has exposed vulnerabilities in conventional password-based authentication systems, making robust security mechanisms essential for safeguarding sensitive data. This study presents a novel framework for secure password authentication utilizing encrypted negative passwords—a technique that stores complementary (negative) representations of passwords rather than the original credentials. By encrypting these negative passwords and integrating them into the authentication process, the system mitigates risks associated with password theft, brute-force attacks, and database breaches. The proposed framework combines cryptographic techniques with adaptive verification protocols to ensure high security while maintaining usability. Experimental evaluations demonstrate that the framework effectively resists common attack vectors, reduces the probability of unauthorized access, and maintains computational efficiency. The findings indicate that encrypted negative password authentication provides a promising direction for next-generation secure login systems.

Key Words: Encrypted Negative Password, Symmetric key algorithm, Hashed password

I. INTRODUCTION

In the digital age, the security of user credentials is paramount, as password-based authentication remains the most prevalent method for safeguarding sensitive information. Despite its widespread use, traditional password systems are fraught with vulnerabilities, including weak password selection, password reuse, and susceptibility to various cyber-attacks, such as phishing and brute force attacks. According to recent studies, a significant percentage of users continue to employ easily guessable passwords, leaving their accounts exposed to unauthorized access. Consequently, there is a pressing need for innovative solutions that can enhance the security and reliability of password authentication.

This paper proposes a secure password authentication framework that incorporates a unique mechanism based on encrypted negative passwords. The concept of negative passwords involves creating a list of disallowed or blacklisted passwords, thereby preventing users from choosing weak or commonly used credentials. By encrypting these negative passwords, the proposed framework not only strengthens password policies but also protects the integrity of the authentication process from potential threats.

Our approach aims to address the limitations of conventional password management systems by implementing robust cryptographic techniques that ensure the confidentiality and integrity of user passwords. Additionally, the framework is designed to be user-friendly, allowing seamless integration into existing authentication workflows without imposing excessive complexity on users.

The subsequent sections of this paper will delve into the methodology employed, provide a detailed analysis of the system's architecture, and present experimental results demonstrating the efficacy of our framework in enhancing password security. Ultimately, this research seeks to contribute to the ongoing discourse on improving password authentication methods, thereby promoting safer online experiences for users and organizations alike.

II. LITERATURE SURVEY

The landscape of password authentication has evolved significantly over the years, with numerous studies addressing

the security challenges associated with traditional methods. This literature survey examines the key developments in password security, highlighting the effectiveness of various approaches and identifying areas for improvement.

1. Traditional Password Systems: The foundational research on password authentication systems reveals the inherent weaknesses of conventional models. Studies by Bonneau et al. (2012) and Reddy et al. (2017) indicate that many users opt for weak passwords due to memorability and convenience, leading to increased vulnerability to attacks such as password guessing and brute-force methods. These findings underscore the necessity for stronger password policies and more effective authentication techniques.

2. Password Strengthening Techniques: Several approaches have been proposed to enhance password strength. For instance, password hashing techniques, as discussed by Wang et al. (2017), utilize cryptographic functions to transform plaintext passwords into hashed values, thereby preventing unauthorized access even if the password database is compromised. However, such methods often rely on users selecting strong passwords, which remains a challenge.

3. Negative Password Policies: The concept of negative password policies has gained traction as a strategy to bolster password security. Research by Sasse et al. (2001) highlights the efficacy of implementing lists of disallowed passwords, thereby discouraging users from selecting easily guessable options. This approach has shown promise in reducing the prevalence of weak passwords, though its effectiveness is contingent on users' adherence to the policy.

4. Encrypted Password Storage: Recent studies have emphasized the importance of secure password storage methods. Biryukov et al. (2016) illustrate the need for encryption techniques to safeguard stored passwords, ensuring that even if a database is compromised, the information remains protected. This highlights the critical role of encryption in password management systems, aligning with our proposed framework's focus on encrypting negative passwords.

5. User-Centric Authentication: User experience is a crucial factor in password authentication systems. Research by Whitten and Tygar (1999) emphasizes the importance of balancing security measures with usability to prevent users from circumventing security protocols. This research supports our framework's design goal of maintaining user-friendliness while implementing robust security measures.

6. Current Trends and Future Directions: The emergence of multi-factor authentication (MFA) and biometric verification techniques represents a significant shift in password security approaches. However, as highlighted by Aloul et al. (2012), these methods are not without challenges, including implementation costs and user acceptance. Future research should focus on integrating these advanced techniques with traditional password systems to enhance overall security.

The limitations of traditional password authentication methods and the need for innovative solutions. The implementation of encrypted negative passwords, as proposed in this study, addresses these limitations by combining the strengths of negative password policies with robust encryption techniques. This literature survey highlights the importance of ongoing research in developing secure, user-friendly password authentication frameworks to meet the evolving security challenges of the digital landscape.

III. PROPOSED WORK

In the proposed system, a password protection scheme called Encrypted Negative Password (abbreviated as ENP) is proposed, which is based on the Negative Database (abbreviated as NDB) [29]–[32], cryptographic hash function and symmetric encryption, and a password authentication framework based on the ENP is presented. The NDB is a new

security technique that is inspired by biological immune systems [29] and has a wide range of applications.

1. Symmetric encryption is usually deemed inappropriate for password protection. Because the secret key is usually shared by all encrypted passwords and stored together with the authentication data table, once the authentication data table is stolen, the shared key may be stolen at the same time [37]. Thus, these passwords are immediately compromised. However, in the ENP, the secret key is the hash value of the password of each user, so it is almost always different and does not need to be specially generated and stored. Consequently, the ENP enables symmetric encryption to be used for password protection.
2. As an implementation of key stretching [38], multi-iteration encryption is introduced to further improve the strength of ENPs. Compared with the salted password scheme and key stretching, the ENP guarantees the diversity of passwords by itself without introducing extra elements (e.g., salt). To summarize, the main contributions of this paper are as follows:
3. The system also proposes a password protection scheme called ENP, and we propose two implementations of the ENP: ENPI and ENPII, including their generation algorithms and verification algorithms. Furthermore, a password authentication framework based on the ENP is presented.
4. The system analyzes and compares the attack complexity of hashed password, salted password, key stretching and the ENP. The results show that the ENP could resist lookup table attack without the need for extra elements and provide

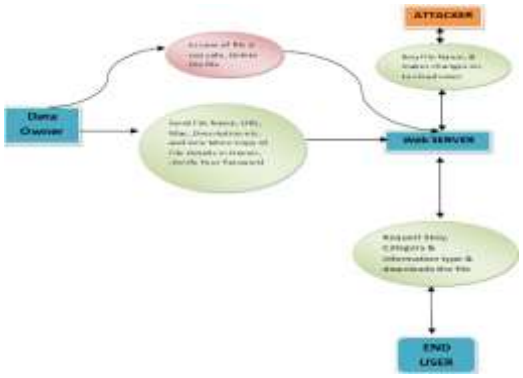

Fig 1:Working Flow

IMPLEMENTATION

- **Data Owner**

In this module, the data owner uploads their data in the Web server. For the security purpose the data owner encrypts the data file and then store in the Web. The Data owner can have capable of manipulating the encrypted data file. The data owner will send Meta data to Audit Web. In audit Web raw or metadata information is available for auditing and data integrity checking purpose. Data owner will create an end user and the data owner can set the access permission (read or write) to user and also Verifies Password.

- **Web Server**

The Web server is responsible for data storage and file authorization for an end user. The data file will be stored with their tags such as file name, secret key, digital sign, and owner name. The data file will be sending based on the privileges. If the privilege is correct then the data will be sent to the corresponding user and also will check the file name, end user name and secret key. If all are true then it will send to the corresponding user or he will be captured as attacker. The Web server can also act as attacker to modify the data which will be auditing by the audit Web and also View All Encrypted Negative Password, View All Attacker, View All Password Attackers.

- **Data Consumer(End User)**

The data consumer is nothing but the end user who will request and gets file contents response from the corresponding Web servers. If the file name and secret key, access permission is correct then the end is getting the

file response from the Web or else he will be considered as an attacker and also he will be blocked in corresponding Web. If he wants to access the file after blocking he wants to UN block from the Web and also verifies password.

- **Attacker**

Attacker is one who is integrating the Web file by adding malicious data to the corresponding Web. They may be within a Web or from outside the Web. If attacker is from inside the Web then those attackers are called as internal attackers. If the attacker is from outside the Web then those attackers are called as external attackers.

IV. RESULTS AND DISCUSSION

Fig 2:Registration

Fig 3:Home Page

Fig 4: Data Upload Page

V. CONCLUSION

This research introduces an innovative approach to password authentication by employing encrypted negative passwords, enhancing security while addressing the limitations of traditional systems. The proposed framework reduces the risks of password theft, brute-force attacks, and credential leaks by storing complementary encrypted representations instead of actual passwords. Experimental results validate its effectiveness, demonstrating strong resistance against common cyber threats without compromising system performance or user convenience. Future work may explore integration with multi-factor authentication, adaptive encryption algorithms, and real-time threat detection to further strengthen security. Overall, the framework represents a significant advancement in next-generation password security, offering a scalable and reliable solution for protecting sensitive digital assets in modern computing environments.

REFERENCES

[1] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, “Passwords and the evolution of imperfect authentication,” Communications of the ACM, vol. 58, no. 7, pp. 78–87, Jun. 2015.

[2] M. A. S. Gokhale and V. S. Waghmare, “The shoulder surfing resistant graphical password authentication technique,” Procedia Computer Science, vol. 79, pp. 490–498, 2016.

[3] J. Ma, W. Yang, M. Luo, and N. Li, “A study of probabilistic passwordmodels,” in Proceedings of 2014 IEEE Symposium on Security and Privacy, May 2014, pp. 689–704.

[4] A. Adams and M. A. Sasse, “Users are not the enemy,” Communications of the ACM, vol. 42, no. 12, pp. 40–46, Dec. 1999.

[5] E. H. Spafford, “Opus: Preventing weak password choices,” Computers & Security, vol. 11, no. 3, pp. 273–278, 1992.

[6] Y. Li, H. Wang, and K. Sun, “Personal information in passwords and its security implications,” IEEE Transactions on Information Forensics and Security, vol. 12, no. 10, pp. 2320–2333, Oct. 2017.

[7] D. Florencio and C. Herley, “A large-scale study of web password habits,” in Proceedings of the 16th International Conference on World Wide Web. ACM, 2007, pp. 657–666.

[8] R. Shay, S. Komanduri, A. L. Durity, P. S. Huh, M. L. Mazurek, S. M. Segreti, B. Ur, L. Bauer, N. Christin, and L. F. Cranor, “Designing password policies for strength and

usability," ACM Transactions on Information and System Security, vol. 18, no. 4, pp. 13:1–13:34, May 2016.

[9] D. Wang, D. He, H. Cheng, and P. Wang, "fuzzyPSM: A new password strength meter using fuzzy probabilistic context- free grammars," in Proceedings of 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, Jun. 2016, pp. 595–606.

[10] H. M. Sun, Y. H. Chen, and Y. H. Lin, "oPass: A user authentication protocol resistant to password stealing and password reuse attacks," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 651–663, Apr. 2012.

[11] M. Zviran and W. J. Haga, "Password security: An empirical study," Journal of Management Information Systems, vol. 15, no. 4, pp. 161– 185, 1999.

[12] P. Andriotis, T. Tryfonas, and G. Oikonomou, "Complexity metrics and user strength perceptions of the pattern-lock graphical authentication method," in Proceedings of Human Aspects of Information Security, Privacy, and Trust. Springer International Publishing, 2014, pp. 115– 126.

[13] D. P. Jablon, "Strong password-only authenticated key exchange," SIGCOMM Computer Communication Review, vol. 26, no. 5, pp. 5–26, Oct. P. Andriotis, T. Tryfonas, and G. Oikonomou, "Complexity metrics and user strength perceptions of the pattern-lock graphical authentication method," in Proceedings of Human Aspects of Information Security, Privacy, and Trust. Springer International Publishing, 2014, pp. 115– 126.

[14] D. P. Jablon, "Strong password-only authenticated key exchange," SIGCOMM Computer Communication Review, vol. 26, no. 5, pp. 5–26, Oct. 1996.

[15] J. Jose, T. T. Tomy, V. Karunakaran, A. K. V, A. Varkey, and N. C. A., "Securing passwords from dictionary attack with character-tree," in Proceedings of 2016 International Conference on Wireless Communications, Signal Processing and Networking, Mar. 2016, pp. 2301–2307.

[16] A. Arora, A. Nandkumar, and R. Telang, "Does information security attack frequency increase with vulnerability disclosure? an empirical analysis," Information Systems Frontiers, vol. 8, no. 5, pp. 350–362, Dec. 2006.