ISSN PRINT 2319 1775 Online 2320 7876

 Journal Volume 10, Iss 9, Sep 2021

A Secure Password Authentication Framework Based on Encrypted Negative Password

Ashutosh Lanjewar[1], Supriya Sawwashere[2], Rahul Bambodkar[3], Praveen Shukla[4]

[123]Assistant Professor, Department Of CSE J D College of Engineering & Management, Nagpur

[4]Research Scholar, Department Of CSE J D College of Engineering & Management, Nagpur

ABSTRACT

Password authentication is a frequently used authentication method that relies on secure password storage. Proposing a framework for secure password storage that can be readily integrated into existing authentication systems and is designed to be password-safe. When a client receives a bare password, it is hashed using a cryptographic hash function first (e.g., SHA-256). After then, the hashed password is turned into a negative password for further use. Finally, a symmetric-key technique is used to encrypt the obtained negative password into an Encrypted Negative Password (abbreviated as "ENP") (e.g., AES). The use of multi-iteration encryption may be used to enhance security even more. ENP passwords are tough to crack because of the cryptographic hash function and the symmetric encryption. After then, the decrypted negative password is re-encrypted with the RSA technique to further enhance its security.

KEYWORDS: Encrypted Negative Password, Symmetric key algorithm, hashed password

1. INTRODUCTION

Analysis and comparison of rule quality shows that the ENP can withstand operation table attacks and provide superior positive identification protection in the face of lexicon attacks. Despite the fact that ENP does not include any new components (such as salt), it could still withstand precomputation attacks. For the first time, a password may be protected using only the plain password by combining the cryptographic hash function with the negative password and the symmetric-key algorithm. The current system uses the simplest method out of all of the others. The simple affirmative identification is encrypted and stored in the information.. This technique is extremely vulnerable, and obtaining the password is a simple matter of launching an attack. For the most part, the hashing mechanism, which uses algorithms like the Secure Hash Algorithm or Message Digest, is still in use today to protect passwords. With this method, you get extra protection, and you don't get the password itself, just a "hash" based on the password. However, the hashed value from a rainbow table or a lookup table attack can yield the raw password. As a result, the Encrypted Negative Password System has been implemented. There has been a significant rise in the number of online services, and password authentication has become the most used method of authentication because it is both inexpensive and easy to implement..

Literature Survey

Theory on passwords has fallen behind practise, where huge providers deploy back-end

ISSN PRINT 2319 1775 Online 2320 7876

smarts to survive with faulty technology. As long as the goal is not impenetrable security but minimising harm at an acceptable cost, passwords will continue to be a helpful signal. Theories of password strength, user behaviour, and password-composition policies that work well in theory are often unsupported by evidence of reduced harm in practise and have even been directly contradicted by empirical observation in some cases. Passwords offer numerous examples of this kind of divergence. Large Web services, on the other hand, seem to be able to get by with less-than-secure passwords, thanks in part to clever back-end technology. [2] Industry's experience with data-driven engineering has led to this important but unnoticed innovation. The greatest difficulty we have today is ensuring the safety of our computers and our data. The system or information should only be accessible to those who are authorised to do so. Authentication is a prerequisite for authorization. Several methods of authentication are at our disposal for this purpose. The password method is the most widely used since it is so simple. A password protects a computer or piece of information so that only people with the proper permissions have access to it. Textual passwords, often known as alphanumeric passwords, are the most common type of password. Text passwords, on the other hand, can easily cracked using a variety of attack methods. Graphic passwords were developed to protect against these flaws. Images (pictures) are used as passwords instead of text in this method. Psychology also shows that visuals are more easily retained by humans than text. Graphical passwords are easy to remember and hard to guess because of this. As a result, almost all graphical passwords are vulnerable to shoulder surfing attacks. Mobile devices such as smartphones, PDAs, iPods, and iPhones can all benefit from it. In today's world, the password mechanism [3] is commonly used to authenticate users. This work makes three contributions as a result of the strategy we propose. For starters, we'll use probability-threshold graphs to gauge the strength of passwords. The second option is to use statistical language modelling approaches to improve password security. New challenges (such as normalisation) arise when modelling passwords, and a wide design space for password models, encompassing both wholestring model and template-based model, are also identified in this paper Third, a comprehensive investigation of many password models has yielded a number of discoveries, which have been presented here. Even though PCFGW has been widely regarded to be the state-of-the-art and commonly employed for password research, we show that whole-string Markov models outperform it in the studies.Mr. Rudresh Gurav , Ms. Leena Dabhade, To increase password security, online authentication systems have started to enforce stricter password policies. We introduce a new metric called Coverage to quantify the correlation between passwords and personal information. Personal-PCFG cracks passwords much faster than PCFG and makes online attacks much more likely to succeed. We examine the use of simple distortion functions that are chosen by users to mitigate unwanted correlation between personal information and passwords. To increase password security, online authentication systems have started to enforce stricter password policies. Password re-generation method is available in this system.

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.

ISSN PRINT 2319 1775 Online 2320 7876

 Journal Volume 10, Iss 9, Sep 2021

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

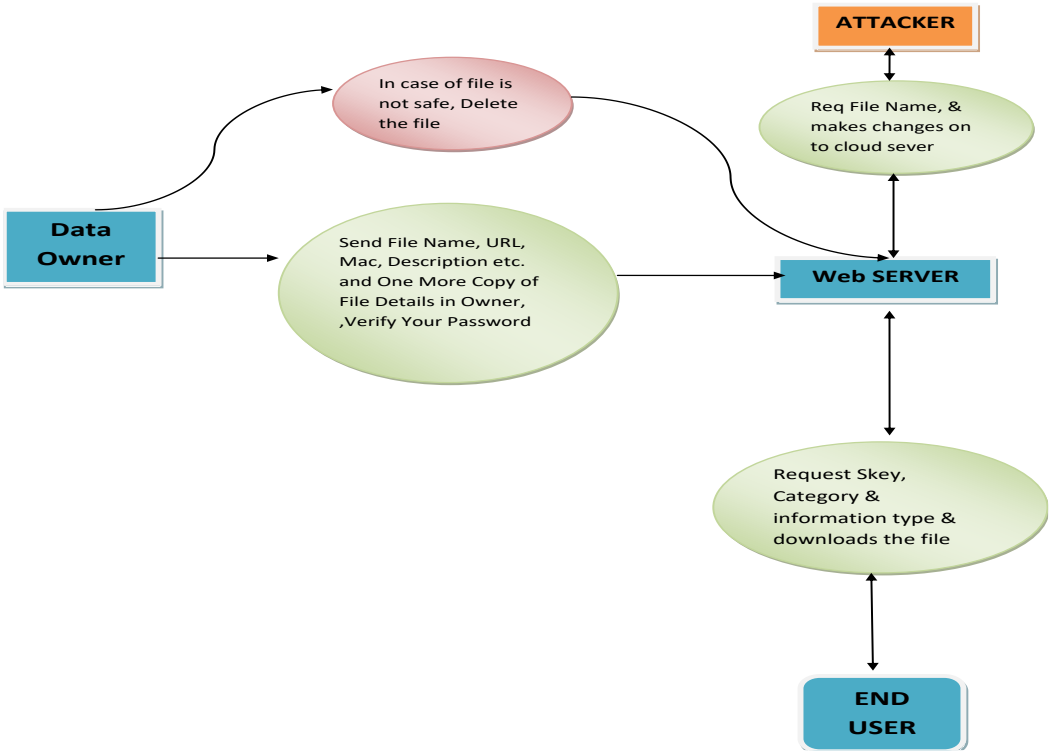

Fig 1: Working Flow

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

IJFANS International Journal of Food And Nutritional Sciences Official Publication of International Association of Food and Nutrition Scientists

ISSN PRINT 2319 1775 Online 2320 7876

 Journal Volume 10, Iss 9, Sep 2021

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.

2. RESULTS AND DISCUSSION

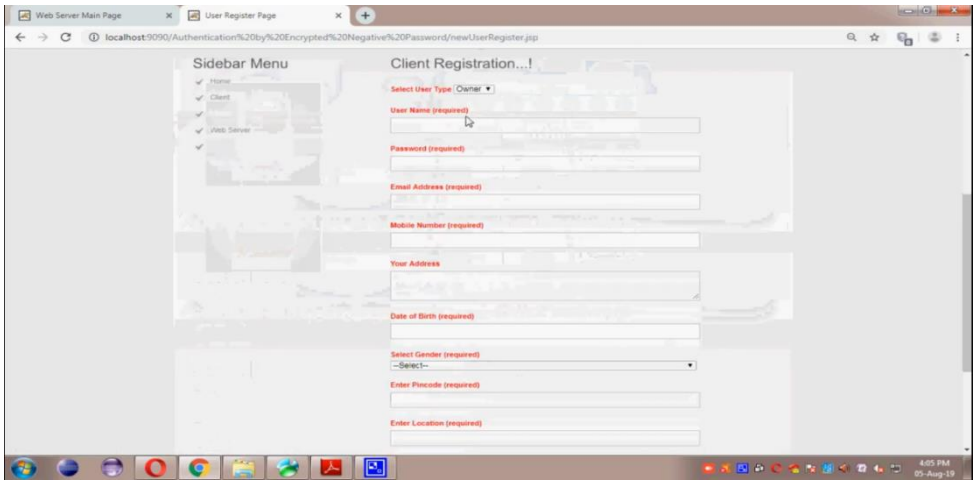

Fig 2: Registration

IJFANS International Journal of Food And Nutritional Sciences
Official Publication of International Association of Food and Nutrition Scientists

ISSN PRINT 2319 1775 Online 2320 7876

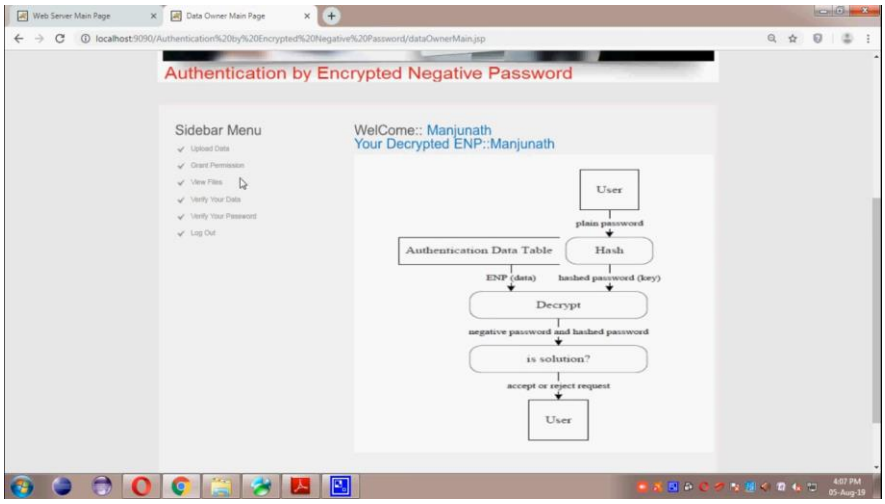

Fig 3: Home Page

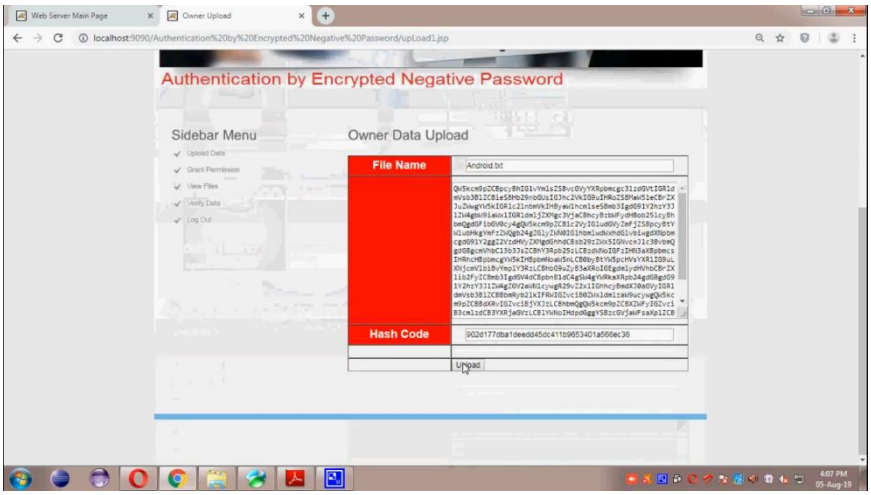

Fig 4: Data Upload Page

3. CONCLUSION

In this paper, we proposed a password protection scheme called ENP, and presented a password authentication framework based on the ENP. In our framework, the entries in the authentication data table are ENPs. In the end, we analyzed and compared the attack complexity of hashed password, salted password, key stretching and the ENP. The results show that the ENP could resist lookup table attack and provide stronger password protection under dictionary attack. It is worth mentioning that the ENP does not need extra elements (e.g., salt) while resisting lookup table attack.

Future Work

In the future, other NDB generation algorithms will be studied and introduced to the ENP to further improve password security.Furthermore, other techniques, such as multi–factor authentication and challenge–response authentication.

ISSN PRINT 2319 1775 Online 2320 7876

 Journal Volume 10, Iss 9, Sep 2021

4. 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

ISSN PRINT 2319 1775 Online 2320 7876

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.

Author's Profiles

Mr. Ravichand Kopila completed his M.Tech in Computer Science from Acharya Nagarjuna University. He has published more than 10 papers in UGC Journals. He has got more than a Decade of experience in various engineering colleges. Currently he is working as an Associate Professor in CSE department at VISVODAYA ENGINEERING COLLEGE, Kavali, Nellore (DT). His areas of interest include Cloud Computing, Computer Network, Programming Language.

SHAIK FARIDA Pursuing B.Tech With Specialization Of Computer Science and Engineering in VISVODAYA ENGINEERING COLLEGE KAVALI

ISSN PRINT 2319 1775 Online 2320 7876

GANGI VENKATA JYOTSHNA Pursuing B.Tech With Specialization Of Computer Science and Engineering in VISVODAYA ENGINEERING COLLEGE KAVAL

MADHAVARPU KARTHIK Pursuing B.Tech With Specialization Of Computer Science and Engineering in VISVODAYA ENGINEERING COLLEGE KAVALI

SIMHADRI MADHU VENKAT Pursuing B.Tech With Specialization Of Computer Science and Engineering in VISVODAYA ENGINEERING COLLEGE KAVALI