SJIF Impact Factor 2021: 8.013| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 6 | Issue: 5 | May 2021 - Peer Reviewed Journal

AUTHENTICATION BY ENCRYPTED NEGATIVE PASSWORD

Haseeb Ur Rahman[1], Mohd Asghar[2], Mohd Abdul Salman[3,]

*[*1*2*3]Affiliated to Osmania University, Information Technology, ISL engineering college, Hyderabad, Telangana, India.*

(Sheena Mohammed, Department of Information Technology, ISL engineering college, Hyderabad, Telangana, India.)

ABSTRACT

Secure password storage is a vital aspect in systems based on password authentication, which is most widely used authentication technique, despite some security flaws. In this paper, we propose a password authentication framework that is designed for secure password storage and could be easily integrated into existing authentication systems. In our framework, first, the received plain password from a client is hashed through a cryptographic hash function (e.g., SHA-256). The hashed password is converted into a negative password. Finally, the negative password is encrypted into an encrypted negative password (ENP) using a symmetric-key algorithm (e.g., AES), and multi-iteration encryption could be employed to further improve security. The cryptographic hash function and symmetric encryption make it difficult to crack passwords from ENPs. Moreover, there are lots of corresponding ENPs for a given plain password, which makes precomputation attacks (e.g., lookup table attack) infeasible. The algorithm complexity analyses and shows 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 introduce extra elements; besides, the ENP could still resist precomputation attacks. Most importantly, the ENP is the first password protection scheme that combines the cryptographic hash function, the negative password, and the symmetric-key algorithm, without the need for additional information except the plain password.

KEYWORDS: *Plain parole, Cryptographic hash function, Encrypted negative parole, symmetric-key algorithm.*

I. INTRODUCTION

Owing to the development of the Internet, a vast number of online services have emerged, in which password authentication is the most widely used authentication technique, for it is available at a low cost and easy to deploy [1], [2]. Hence, password security always attracts great interest from academia and industry [3]. Despite great research achievements on password security, passwords are still cracked since users' careless behaviors [4]. For instance, many users often select weak passwords [5], [6]; they tend to reuse same passwords in different systems [7]-[10]; they usually set their passwords using familiar vocabulary for its convenience to remember [11], [12]. In addition, system problems may cause password compromises. It is very difficult to obtain passwords from high security systems. On the one hand, stealing authentication data tables (containing usernames and passwords) in high security systems is difficult. On the other hand, when carrying out an online guessing attack, there is usually a limit to the number of login attempts [13]. However, passwords may be leaked from weak systems [14]. Vulnerabilities are constantly being discovered, and not all systems could be timely patched to resist attacks, which gives adversaries an opportunity to illegally access weak systems [15]. In fact, some old systems are more vulnerable due to their lack of maintenance. Finally, since passwords are often reused, adversaries may log into high security systems through cracked passwords from systems of low security.

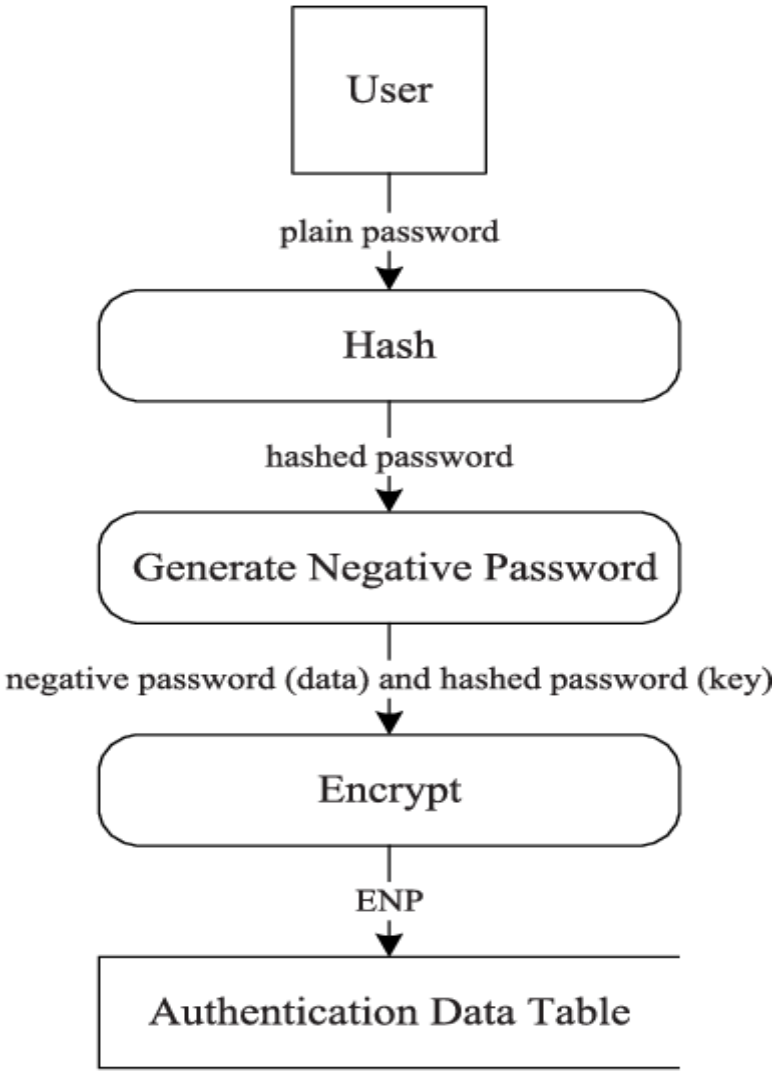
II. PROPOSED METHODOLOGY

To protect passwords in associate degree authentication knowledge table, the system designer should 1st choose a cryptological hash

SJIF Impact Factor 2021: 8.013| ISI I.F.Value:1.24 | DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 6 | Issue: 5 | May 2021 - Peer Reviewed Journal

perform and a symmetric-key formula, wherever the condition that has to be glad is that the dimensions of the hash price of the chosen cryptological hash perform is adequate to the key size of the chosen symmetric-key formula. For convenience, some matches of cryptological hash functions and symmetric-key algorithms. additionally, cryptological hash functions and symmetric-key algorithms that don't seem to be listed here might even be utilized in the ENP, that adequately indicates the pliability of our framework. The planned framework relies on the ENP; therefore, for higher understanding, the information flow sheet of the generation procedure of the ENP.

III. MODELING AND ANALYSIS



IV. RESULTS AND DISCUSSION

Data Owner during this module, {the knowledge|the info|the information} owner uploads their data within the net server. For the protection purpose the information owner encrypts the information file then store within the net. The information owner will have capable of manipulating the encrypted record. {the knowledge the info the information} owner can send Meta data to Audit net. In audit net raw or information data is offered for auditing and knowledge integrity checking purpose. Knowledge owner can produce associate degree user additionally the} knowledge owner will set the access permission.

Data Auditing and Verification the information owner can even audit the information integrity within the corresponding net for validatory whether or not the information is safe or not mistreatment digital sign and net uniform resource locator. If the information isn't safe then he can delete the information and re transfer the information to the corresponding net server.

SJIF Impact Factor 2021: 8.013| ISI I.F.Value:1.24 | DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 6 | Issue: 5 | May 2021 - Peer Reviewed Journal

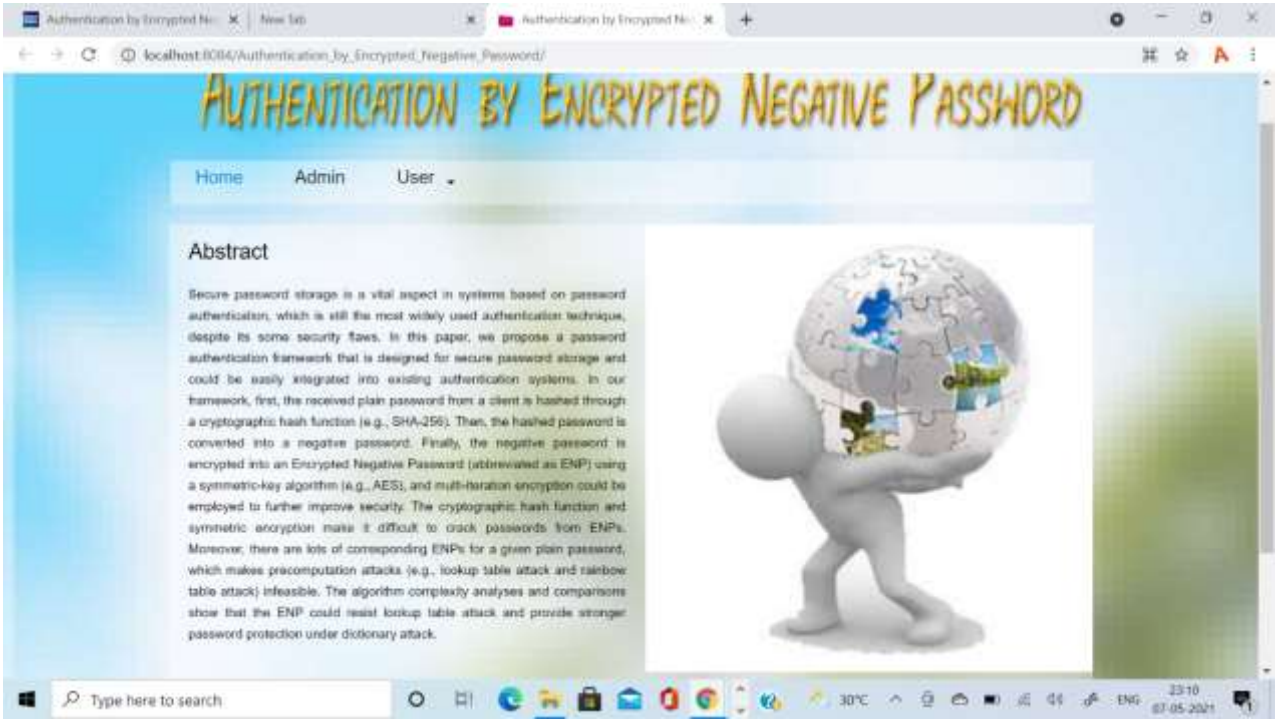


Fig 1.0: Home page.

Web Server the online server is accountable for knowledge storage associate degreed file authorization for an user. The information file are hold on with their tags like file name, secret key, digital sign, and owner name. the information file are causing supported the privileges. If the privilege is correct then the information are sent to the corresponding user and conjointly can check the file name, user name and secret key. If all area unit true then it'll send to the corresponding user or he are captured as aggressor. the online server {can conjointly|also can|can even|may also|may} act as aggressor to switch the information which is able to be auditing by the audit net and also read All Encrypted Negative parole, read All aggressor, read All parole Attackers.

Data Consumer (End User) the information shopper is nothing however the top user WHO can request and gets file contents response from the corresponding net servers. If the file name and secret key, access permission is correct then the top is obtaining the file response from the online {or else| alternatively| as associate degree alternative |instead}he are thought of as an aggressor and conjointly he are blocked in corresponding net. If he desires to access the file once block he desires to United Nations block from the online and conjointly verifies parole. aggressor is one WHO is group action the online file by adding malicious knowledge to the corresponding net. they will be at intervals an online or from outside the online. If aggressor is from within the online then those attackers area unit referred to as internal attackers. If the aggressor is from outside the online then those attackers area unit referred to as external attackers.

Aggressor aggressor is one WHO is group action the online file by adding malicious knowledge to the corresponding net. They will be at intervals an online or from outside the online. If aggressor is from within the online then those attackers area unit referred to as as internal attackers. If the aggressor is from outside the online then those attackers area unit referred to as external attackers.

SJIF Impact Factor 2021: 8.013| ISI I.F.Value:1.24 | DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 6 | Issue: 5 | May 2021 - Peer Reviewed Journal

Fig 2.0: Admin login page.

Fig 3.0: User registration page.

SJIF Impact Factor 2021: 8.013| ISI I.F.Value:1.24 | DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 6 | Issue: 5 | May 2021 - Peer Reviewed Journal

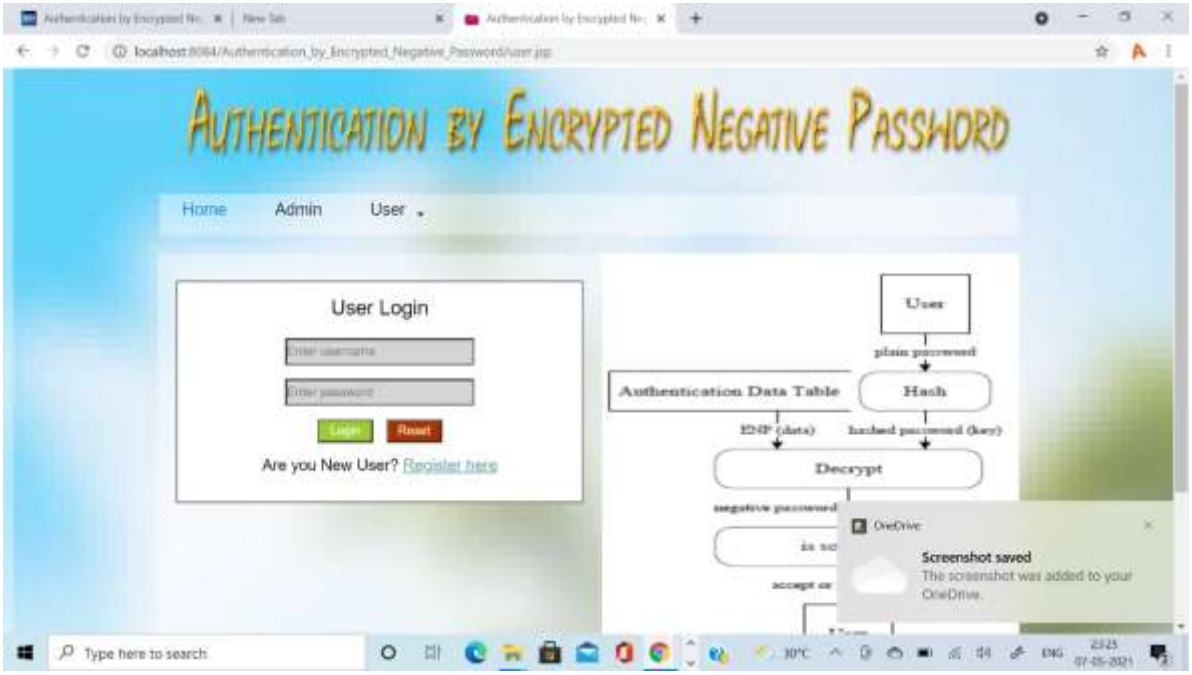


Fig 4.0: User login page

V. CONCLUSION

In this paper, we tend to planned a parole protection theme referred to as ENP, and conferred a parole authentication framework supported the ENP. In our USER Plain parole Hash Hashed parole Generate negative parole write Authentication knowledge table International Journal of Engineering analysis & Technology (IJERT) ISSN: 2278-0181 printed by, www.ijert.org RTICCT - 2020 Conference Proceedings Volume eight, Issue twelve Special Issue - 2020 nineteen framework, the entries within the authentication knowledge table area unit ENPs. In the end, we tend to analyzed and compared the attack complexness of hashed parole, salt-cured parole, key stretching and also the ENP. The results show that the ENP might resist operation table attack and supply stronger parole protection underneath lexicon attack. It's price mentioning that the ENP doesn't want further components (e.g., salt) whereas resisting operation table attack.

VI. 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 password models," 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. International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Published by, www.ijert.org RTICCT - 2020 Conference Proceedings Volume 8, Issue 12 Special Issue - 2020 20.*