International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-6, April 2020

Strong Authentication using Encrypted Negative Password

V. Priyankaselvi, R. Sivakami

Abstract*: *Passwords are mostly employed in every place within the world. Nowadays maintaining password is extremely difficult. Because Passwords could also be leaked from weak systems. passwords that are given by a human is easy to identified and cracked. Initially password given by a user's often select weak passwords and it can be reused. Unauthorized person may enter into the login process and they hacked a Password very easily. Passwords are usually in the kind of hashed passwords. During this work it develops a Secured Smart lock using Strong Authentication. it's a raspberry pi connected to the Wi-Fi, a camera, a key pad system and a lock system. the house owner can give access to the guest by IoT. He can even send the One-time password to the guest mobile to enter into the house. The owner can view the one that is before of the door using the camera.

Keywords- Authentication, IoT, Password, Smart lock

I. INTRODUCTION

A. Maintain Password Security

Passwords are principally utilized in each digital system. Maintaining password security is highly efficient in today's world. Maintaining watchword security resulted in an exceedingly mixture of safe and insecure systems. Maintain a secure watchword may be a drawback of ever-increasing importance. With the rise in on-line services, the number of credentials per person security.

B. Authentication of Password

specific high-profile cases like arcanum security has been compromised and a number of the reasons why this happened. By review things, can detail the implementation of negative authentication for the authentication of the arcanum. completely different approaches that will be tried and each will have some blessings and disadvantages. this could enable you to higher perceive its potential blessings. Finally, it explained the analysis, with some recommendations on the thanks to increase the protection of arcanum security.Arcanum authentication is that the foremost usually used authentication technique, for it's accessible at an occasional price. As an instance, several users usually choose weak arcanum they need a bent to utilize same passwords in many systems.

Revised Manuscript Received on April 30, 2020.
***** Correspondence Author
V. Priyankaselvi*, Computer Science and Engineering, Sona College of Technology, Salem, India. Email: priyankavellaiswamy@gmail.com
Dr. R. Sivakami, Computer Science and Engineering, Sona College of Technology, Salem, India. Email: sivakamir@sonatech.ac.in

The users sometimes set their passwords victimization straightforward identification.

C. VULNERABILITIES

Resources such as processor and storage have become additional and abundant. A number of the trends generalized of extrajudicial persons, may get access to info on vulnerabilities from vulnerability databases. Use of the vulnerability's info are simply hacked by the users. Moreover, some powerful attack tools love hash cat, Rainbow Crack and John the liquidator give a range of functions. Hash algorithms raises the next demand for secure positive identification storage.

D. SECURITY SYSTEM

Attacks are usually identified by the precomputation of lookup table attack. It contains a password that are reused and cannot be changed in a short time does not have a security. Then the authentication data table will obtain from a low security and unsafe systems.

The plain passwords are searched by matching the hashed passwords in a key and an authentication table. Finally, the unauthorized person enters into the high-level security-based systems by using the usernames and passwords. If a user login or enter in the low security system the data may be hacked and the unauthorized person can view the data or the information that are provided in the data table.

II LITERATURE SURVEY

PAPERS CONTRIBUTED TO PROBLEM FORMULATION

A. oPass: User Authentication protocol Resistant

Text countersign is most well-liked various types of authentication used by the user for the convenience of the function to work easily on web. However, human based passwords are simple to taken and there is a chance to attack a various vulnerable threat. At the start of any of the password users typically choose a password which can be easily identified. Consequence for reusing the passwords of the habitual countersigns may be destroyed by the hackers. Then typewriting of countersigns in untrusted computers suffers password stealer threat. Associate in Nursing someone is to Launch many countersigns the malware attacks.

B. Smart card – based authentication protocol for password

Authentication used in password is typically maintained in a large system that managed the remote access to pc networks.

Thus, on list variety of the protection and management issues that occur in ancient watchword authentication protocols, analysis has targeted on good card-based watchword authentication. Throughout this paper, they show that the improved identification authentication theme planned by Xu-Zhu-Feng is prone to internal and impersonation attacks. The authors planned associate improvement of their answer with a replacement economical robust identification authentication protocol, demonstrate that the new protocol satisfies the wants of robust identification authentication and is a lot of economical.

C. The shoulder surfing Resistant Graphical password verification

Nowadays laptop equally as data security is that the foremost necessary challenge. Approved users ought to access the system or data. By comparing with the arcanum technique the passwords mostly used is a straightforward Technique. Arcanum provide the details of the information is typically used by those who have permission often to read or access them. Ancient arcanum technique might be a matter password that is Associate in Nursing alphanumeric password. However, the matter arcanum method are simply cracked in various types of attack.

D. Imperfect Authentication Password

Theory on passwords has lagged behind apply, wherever sizable quantity of suppliers uses back-end smarts to manage with imperfect technology. oversimplified models of user and offender behaviours have LED to the analysis community to emphasize the wrong threats. Authentication is also a classification downside amenable to machine learning, with signals in addition to the word offered to massive internet services. Passwords continue as a helpful signal for the long-term, wherever the goal can't offer security however it reduces the damage at the appropriate value.

E. Enhancing Privacy through Negative Representations of Data

The paper introduces the conception of an NDB, among that a set of records decibels is delineated by its complement set. All the records do not gift in decibel are delineated itself is not expressly hold on. once introducing the conception, it regards concerning the feasibleness of such a theme and its potential for enhancing privacy. information consisting of n, l-bit records are typically delineated negatively victimization solely O(ln) records. Membership queries for decibel are typically processed against the negative illustration in time is no worse than a linear in its size. Reconstructing the information delineated by a negative database given as input.NP-hard downside calculates the time quality as a performance based on the sizes of the negative representations of data.

F. Protection of Data Privacy based on Hard -to-Reverse Negative Databases

A set of data components are typically depicted in the method of complement set containing the negative information. Weather that does not appear to be gift in dB are depicted is not expressly hold on. The content of the paper contains the negative information of Negative Database illustration theme for saving the negative image. It completely was projected by a habitual using of a set of Negative Database to view one Database and every record in dB is allotted separate NDB. The advantage of this technique is manufacturing the negative databases to observe. The Reverse Negative Databases is observed that the tough to urge database for the related privacy enhancing applications that are provided and used.

III RESEARCH ISSUES

PASSWORD PROTECTION TECHNIQUES

A. Hashed based Password

The best Technique of storing password is directly store a comprehensible password. This method detects a drag that after obtain the datas of all passwords are immediately compromised. For a convenient and the safe arcanum the author proposed a hash password employing hash function based on a cryptographic method is more efficient to use the method directly from a hashed password to recover a plain password. The authentication system provided the security using the hashing password method and, in the database and it is used to save only a hashed password.

Hashed password provides a precomputing table employed with the attacks such as a lookup table and a rainbow table which are used is sufficiently large. Therefore, the unauthorized users could obtain the next success rate of avoiding the hacking of the passwords.

B. Salted Password

The computational attacks are controlled by using the common method to be used by the user is the salted password. In this technique the random data of the hashed function from a cryptographic hash method is mixed with a comprehensible. Salted password sometimes randomly generated by a system based on the key values and the given password.The hash values that are used by a plain password will differ according to the password. While a user enters a weak password, the Encrypted Negative Password is more efficient and it doesn't ask the requirements for any elements which are given by the user password.

C. Key Stretching

By avoiding a dictionary attack by Key stretching method is used to converts a weak password into the enhanced passwords. Key stretching method will increase the time and cost which is required for all password given by the user. In order to that the ability of fighting for the rise of the dictionary attack. Within an Encrypted Negative Password that is proposed during key stretching will help to improve a security using multi-iteration encryption is employed to further improve password security under dictionary attack.

D. Negative Database

In a Negative Database a positive Database is stored and it is described as U= f0. It consists of the set of n number of bit sequences and m entries. For every entry of the Negative Database contains the symbols '0','1' and '*'.'0' can match to the number of bits 0 and it is similar for the symbol '1'.

But '*' match to the bit either 0 or 1. The positions 0 and 1 are known as specified positions whereas * are known as unspecified positions.

IV.PROPOSED SYSTEM

THEORETICAL BACKGROUND

In a proposed system a protection is given for a password in a name called as Encrypted Negative Password is which is depend upon a Negative Database.

It also presents in a password verification, symmetric key encryption method and cryptographic hash technique that is depend upon the Encrypted Negative Password present in a proposed system.

The mostly and large used applications such as Negative Database is used to provide more security to the password.

Symmetric coding has a major advantage and also typical for parole protection. as a result of the key key's typically that are shown in an encrypted password and hold on at a side of the verification knowledge table.

If the verification table password that is encrypted by a password given by an owner in a database table is compared with the password that encrypted by a new user recently type a password is same then the lock will open and it is not a same password it sent an alert message to the owner. Thus, these passwords are directly compromised.

we tend to provide a high-level security for the password known as Encrypted Negative Password. To improve the security two levels of encrypted technique such as ENP1 and ENP2 is generated to give a best password security verification.

METHODOLOGY

In a proposed system positive identification method is used for the password to be secured in a high level comparing to the existing algorithms.

The method which is used in a proposed system is very simple. In our work, at first received plain positive identification is hashed through a cryptographical hash operate.

At that point the hashed positive identification is regenerate as an encrypted password. The encrypted negative password converts into an Encrypted Negative Password identification by the symmetric algorithm key method and multi-iteration coding can be used for providing further security for the password.

ADVANTAGES

The techniques of cryptography hash function and bilateral encoding create troublesome to break a Password from Encrypted Negative Password.

Even though an immeasurable and countersign, that make a pre-computation attacks such as operation table and rainbow table are unfeasible.

From the analysis of the difficulties Encrypted Negative Password may resist operation table attack and also makes stronger countersign avoidance.

DESIGN

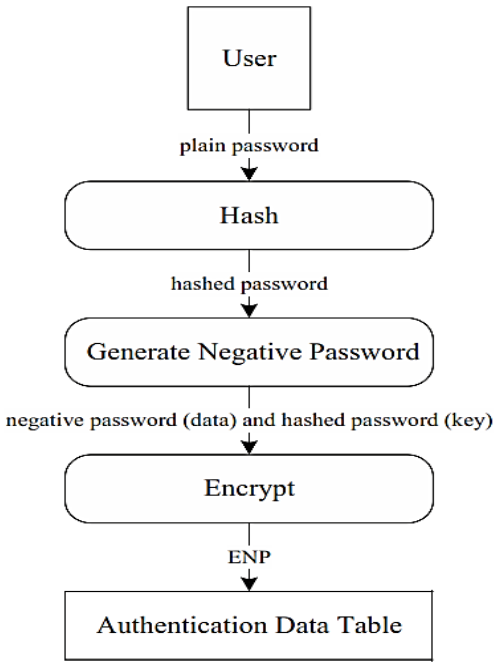

Fig. 3.1 Generation procedure of the ENP.

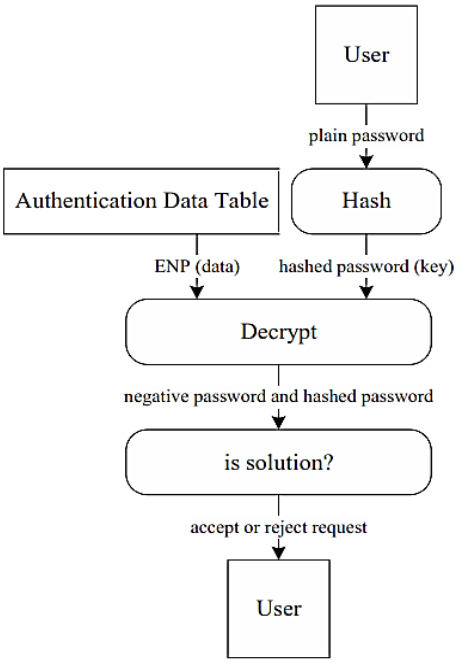

Fig. 3.2 Verification procedure of the ENP.

A. IMPLEMENTATION

In ENPI, we tend to use the prefix rule with permutation to get negative passwords that is Negative database. It consists of the Hashing Technique such as Secured Hash Algorithm.

a. Hashing

SHA-256 can be one of a function in SHA-2 cryptographical Hash functions. Secured hashed algorithm in a method of unidirectional hash is generated from any piece of information. However, the data cannot be generated from the hash. In easy words,

Secured Hash Algorithm-256 in every cryptographic hash method has a length 256 bits. It is Keyless Hash function and it associates with the Magnetic Detection Code.

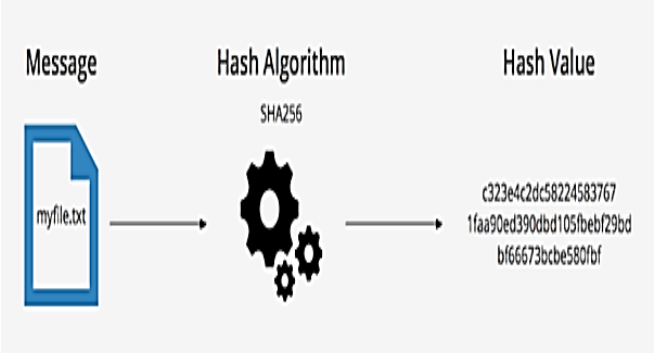

Fig 3.3 Hash Algorithm

The SHA-256 algorithmic rule is kind of SHA-1 format. SHA-256, have the cushiony & splitted into the blocks of 512-bits. According to the size of the variants size of the output, message, rounds, blocks and internal size varies.

b. AES Features

The features of AES have n bit of plain text and it has a pre-round transformation it will go as many rounds according to the number of bits. After that the key is expanded according to the round keys that is already a standard number of rounds and Key size.

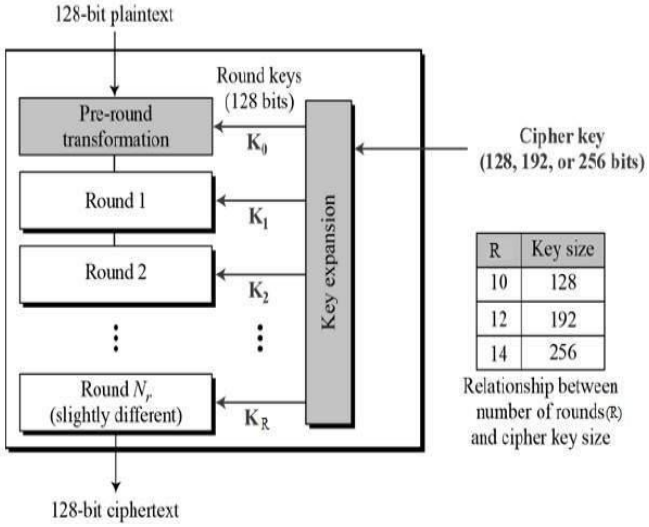

Fig 3.4 AES Design

c. AES Transformation

The AES method transforms by shifting a rows and a columns.Then the encrypted key is supported by the number of substitutions based on the size of the key.

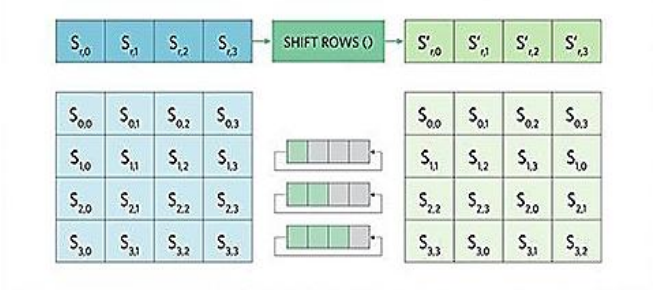

Fig 3.5 AES Transformation

RESULT

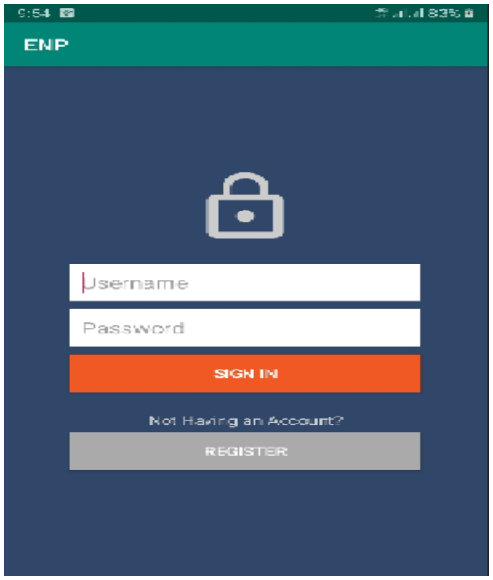

Fig A1.1 User Login

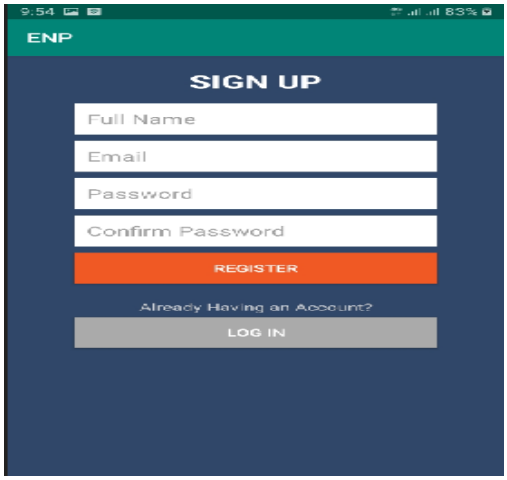

Fig A1.2 Registration Details

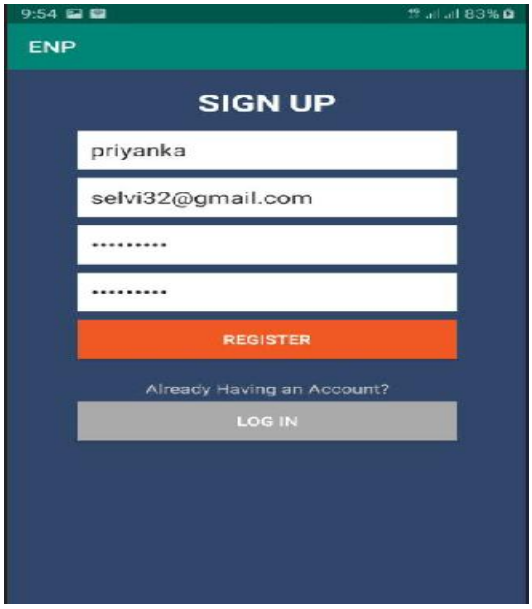

Fig A1.3 Sign Up details

Fig A1.4 Encrypted Password

II. CONCLUSION

Security should be engaged during a very continuous cycle of self-reformation. sadly, as has been mentioned, several organizations fail to implement even the foremost basic measures. Today, there is not any word security system that takes advantage of hashing, seasoning and stretching to protect its passwords. corporations and user's alike ought to push code vendors to provide easier to implement security in their systems. Most directors can have enough work to worry concerning which they require their ROI to come as shortly as potential. Users are a lot of inclined to implement secure policies, even once it's troublesome to verify that they are truly doing it.

REFERENCES

1. J. Bonneau, C. Herley, P.C.van oorschot, and F. Stajano," Password and the evolution of imperfect authentication," Communications of 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 ACM, vol.42, no.12, pp.40-46, Dec.1999
5. E.H Spafford, "Opass: Preventing Weak password choices," Computers and 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. Florencia 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. Komaduri, A.L. Durity, P.S. Huh, M.L. Mazurek, 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. H. M. Sun, 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
10. 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
11. P. Oechslin, "Making a faster cryptanalytic time- memory trade-off," in proceedings of Advances in cryptology – CRYPTO 2003. Springer Berlin Heidelberg, pp. 617-630
12. F. Esponda, "Negative representations of Information," Ph.D. dissertation, University of New Mexico, Albuquerque, NM, USA, 2005
13. F. Esponda, E. S. Ackley, S. Forrest, and P. Helman, "Online negative databases," in proceedings of Artificial Immune Systems. Springer Berlin Heidelberg, 2004, pp. 175-188
14. J. Kelsey, B. Schneier, C. Hall, and D. Wagner, "Secure applications of low-entropy keys," in proceedings of Information Security, Springer Berlin Heidelberg, 1998, pp. 121-134
15. D. Zhao, W. Luo, R. Liu, and L. Yue, "A fine grained algorithm for generating hard to reverse negative databases," in proceedings of 2015 International Workshop on Artificial Immune Systems, Jul. 2015, pp. 1-8
16. D. Zhao and W. Luo, "One-time password authentication scheme based on the negative database," Engineering Applications of Artificial Intelligence, vol. 62, pp. 396-404, 2017
17. J. Bringer and H. Chabanne, "Negative databases for biometric data," in proceedings of the 12th ACM Workshop on Multimedia and Security, ACM, 2010, pp. 55-62
18. J. Liang and X. Lai, "Improved collision attack oh hash function MD5," Journal of Computer Science and Technology, vol. 22, no. 1, pp. 79-87, Jan. 2007
19. Y. Sasaki and K. Aoki, "Finding preimages in full MD5 faster than exhaustive search," in proceedings of Advances in Cryptology-EUROCRYPT 2009, Springer Berlin Heidelberg, 2009, pp. 134-152
20. "Hashcat, "https://hashcat.net/hashcat/

AUTHORS PROFILE

PRIYANKASELVI. V, Research scholar in Sona College.