International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 6, September-October 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Encrypted Negative Password using for Authentication

Priya K P[1], Dr. Lakshmi J. V. N[2]

[1]MCA Student of Information Security Management Service, [2]Associate Professor,
[1,2]Department of Computer Application, Jain Deemed-To-Be University, Bangalore, Karnataka, India

ABSTRACT

Password authentication is one of most likely used authentication techniques. Secure password storage is the most difficult process. In this paper, we propose a password confirmations structure that is intended for secure password storage and could be effectively coordinated into existing authentication systems. In this project, first we receive the plain text from the user then hashed through a cryptographic function. The next step, hashed password is converted into a negative password. Finally, the negative password is encrypted into an Encrypted Negative Password using encryption algorithm. Challenge–response authentication and multi-factor authentication could be employed to further improve security.

KEYWORDS: *Encrypted Negative Password, Algorithm, Blowfish, hash password, encryption*

How to cite this paper: Priya K P | Dr. Lakshmi J. V. N "Encrypted Negative Password using for Authentication" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-6, October 2020, pp.1597-1599, URL: www.ijtsrd.com/papers/ijtsrd35711.pdf

IJTSRD35711

1. INTRODUCTION

Now day's cyber-offense is most common, in that password cracking is one of the attacks. For instance, many user takes week password according to their familiar vocabulary and uses the same password for different system. The attacker uses many ways to get the credentials such as guess the password, or shoulder surfing, and other password cracking tool is used to steel the sensitive data. To overcome this problem we should use strongly hashed encrypted password. The combination of hash function and encryption work make it is hard to split passwords from ENPs. The analysis and comparison of algorithm show that the ENP cloud oppose lookup table assault and give stronger protection of a password under dictionary assault. Here we take two steps to make a strong password, first hashing the password then encrypt the password.

2. Existing system

The aim of the paper is enhancing the security. However, password is leaked from the week system. Some old system are more vulnerable due to their lack of maintenance and algorithm limitations. The hashing and encryption method leads to lookup table attack and dictionary attack. The older ENPs uses hashing and encryption algorithm without need of any additional information except the plain password. And also in the existing system uses the hashing algorithm such as MD5 and SHA1 to 256. The encryption algorithm AES and RSA.[1],[2] The algorithm analysis shows that these algorithms as its own drawbacks to overcome this problem hashing algorithm PBKDF2 and encryption algorithm Blowfish is use to improve the security. And also using salt function will provide stronger protection to the password.

3. Proposed system

The combination of hash function and symmetric encryption, make it is difficult to split passwords from ENP system. The algorithm analysis and comparison show that the ENP provides the more security to the password system. In this system using the additional information to the password that is add salt value to the plain password it is more difficult to crack the password system. And also implement the Multi-iteration encryption provides more security to the system.

A. Methodology

The proposed framework includes two phases: the registration section and authentication section. Once adopting our framework to safeguard passwords in associate authentication information table, the system designer should initial choose a cryptographic hash function and a symmetric-key algorithm, where the condition that has to be satisfied is the size of the hash value of the chosen cryptographic hash function is capable the key size of the chosen symmetric key algorithm.

Registration phase

1. User enters the plain text such as user name and password.

2. The system checks the user name exist in the database or not.
3. Then received password is hashed through hashing algorithm such as PBKDF2 withHMAC-SHA1.
4. Hashed password converted into negative password using NDB algorithm.

5. Encrypt the negative password using symmetric encryption algorithm such as Blowfish algorithm.
6. Finally, store the encrypted password in the authentication table.

Authentication phase

1. If existing user, the Username and password transmitted to server.
2. Verify the username and password ,if existing the user name,
3. Search the ENP from the authentication table.
4. ENP is then decrypted it will get the hash value of the plain text.
5. If the hash value matches user can login. Architecture The below figure shows a general diagram the activities

System Architecture Diagram

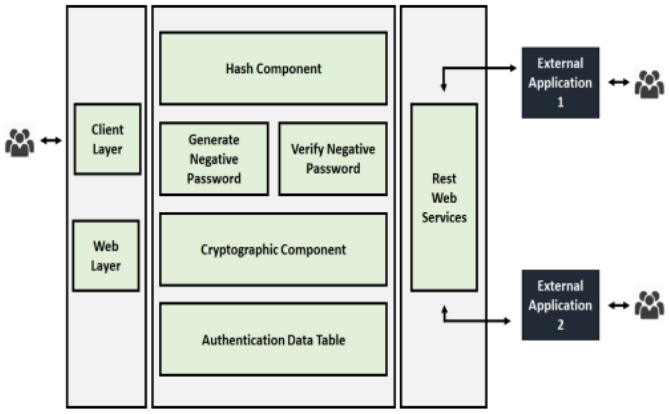

Fig.1: Block Diagram of ENP

B. Algorithms

PBKDF2- This is one in the PBE algorithm. It applies a pseudorandom function like hash based authentication code (HMAC) to the input text together with the salt value and repeat the processes accurately and over to produce a derived key which might be used as a cryptographic key in the subsequent operation.

The strength of the PBKDF2 is makes it more durable for somebody to determine your master password by making repeated guesses in a brute forces attack. For giving better opposition against brute force attacks, PBKDF2 presents CPU-intensive operations. These tasks rely upon an iterated pseudorandom work (PRF) which aides input values to a derived key. The most significant properties to guarantee is that the iterated pseudorandom function is cycle free. The PBKDF2 includes a 5input parameters. Pseudorandom function, original password, sequence of bits, number of iteration, specify the derived key length. [13]

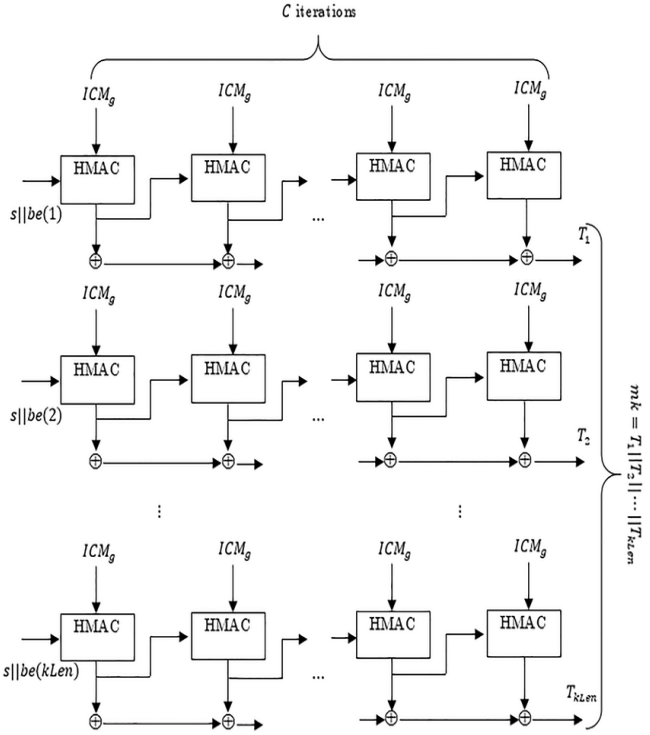

Fig.2: PBKDF2 Algorism

DK= PBKDF2 (PRF, Password, Salt, C, DKlen).[13]

Derived key DK → U1 = F (password, salt, c, dkIen)

F (password, salt, c, I) = U1 ^ U2 ^……..^ UC-1

Where

- U1 = PRF(p,s,c,1)
- U2 = PRF(p,s,c,2)
- ..
- Uc = PRF(p,s,c,n-1)

Each single square Ti - i.e., Ti = Function (p, s, c, i) - is computed as Ti = U1 ⊕ U2 ⊕ ... ⊕ Uc

BLOWFISH-Drop-in replacement for DES and IDEA algorithm. Blowfish is a symmetric encryption algorithm, it uses one key for encryption and the same key is used for decryption. The algorithm analysis shows that blow fish algorithm is Faster Encryption and decryption time. And it uses less memory (5KB). Blowfish records the highest average entropy per byte of encryption, this is the achievement of new security aspect. Easily modified for different security levels. [4][14] This algorithm contains feaster structure, and size of the Plain text 64 bits. Blowfish has a variable key length up to maximize of 448 long, making it both flexible and secure. This algorithm contains 16 rounds to produce the cipher text.

Working

The working of blowfish is divide the plain text into left and right respectively, and perform the XOR operations on the left part in original password with using sub key divided from original plain text. The XOR output apply to the function, then function output XOR to the right side plain text. Swap the output each other, the same procedure is repeated for 16 rounds after 16th round directly add the sub keys to produce the chipper text.

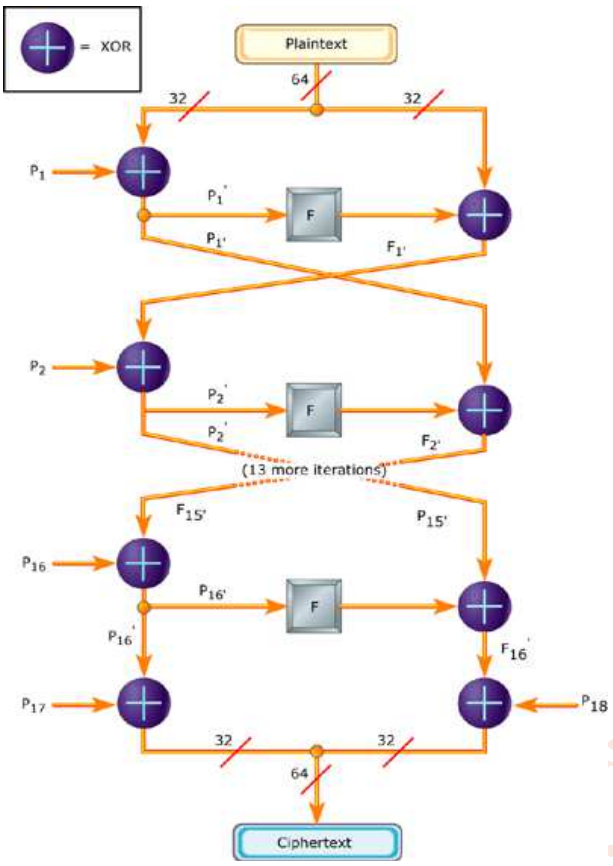

Fig.3: Blowfish Algorithm

Function value

Function f divided into 4 S-boxes. The function isolates a 32-bit input into four bytes and utilizations those as indices into an S-array. The lookup results are then gathered and XORed single unit to create the output.

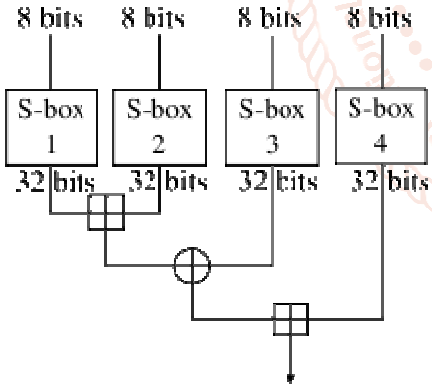

Fig.4: Graphic portrayal of F

Algorithm

- Divide 64-bits into two 32 bits(L,R)
- For i=1 to 16
  - XL = XL XOR Pi
  - XR = F(XL) XOR XR
  - Swap XL and XR
- Swap XL and XR(16 Rounds)
- XR = XR XOR 17
- XL = XL XOR P18
- Concatenate XL and XR

C. Advantages

Stronger security algorithm that provides resistance to vary reasonably attacks as well as dictionary attacks and look-up table attack. No further burden on programmers for configuring additional parameters. And also Easy and convenient to use. This is light weight efficient password protection scheme and easier to integrate this with existing systems. It provides a robust security against various sorts of attack. To provide an efficient interface access to the clients to access the portal. And deploy the project over the cloud in order that it are often accessed from various geographical location from any device.

4. Conclusion

Thus this encrypted negative word may be used for securing the password and conjointly the web pages. This ENP system prevents the rainbow table assault and also the look up assault and secures the passwords. The password used is safe and nobody will ever attempt to break the password. Rather than simply hashing we are converting the hash value into negative values and encrypting. So throughout during verification also thus we check whether it's the solution or not but do not know the actual password. In the future, various NDB generation algorithms will be considered and acquainted with the ENP to improve e password security. Furthermore, different techniques, like multi–factor authentication and challenge–response authentication, are going to be introduced into our secret authentication framework.

References

[1] Authentication by Encrypted Negative Paaword for an Intuitive Stock Management System. K.Subramanian, V.Sreyas, M.Nikitha and S.Arathi. 2019, SSRG Intranatinal Journal of computer Science and Engineering(SSRG-IJCSE).

[2] Encrypted Negative Password Using RSA Algorithm. Salwa P.B, Nice Mathew. 2019, International Research Journal of Engineering and Technology(IRJET).

[3] ieeexplore.ieee.org.

[4] A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention. Mohammed Nazeh Abdul Wahid, Abdulrahman Ali, Babak Esparham and Mohamed Marwan. 2018, Journal of Computer Science Applications and information technology,.

[5] Priyadarshini Patil, Prashant Narayan, Narayan D.G., Meena S.M. A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish. 2016.

[6] dspace.calstate.edu › bitstream › handle › ChidriLaxmi_Project2019.

[7] Authentication by Encrypted Negative Password. Luo, Wenjian. 2018, IEEE.

[8] Comparison of Encryption Algorithms: AES, Blowfish and Twofish for Security of Wireless Networks. Ghosh, Archisman. 2020, International Research Journal of Engineering and Technology (IRJET) , p. 4.

[9] Wikipedia. en.wikipedia.org › wiki › Password.

[10] RSA Algorithm using modified subset sum cryptosytem. Sonal S, Prasanth S, Rvi Shankar D. s.l. : 2nd international confrence on computer and communication technology, 2011.

[11] Alarge scale stydy of web password habits. D.Florencio andC .Herly. s.l. : 16th international confrence on world wide web, 2017. ACM.

[12] Semanticscholar. www.semanticscholar.org › paper › Authentication-by-Encrypted-Negative-....

[13] wikipedia. en.wikipedia.org › wiki › PBKDF2.

[14] www.embedded.com › ... › Encrypting data with the Blowfish algorithm.