IJCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Vol.-7, Special Issue-15, May 2019 E-ISSN: 2347-2693

Design and Implementation of Encrypted Negative Password

Manasa N[1*], Preethi P[2], Rakshitha R[3], Jyothi V[4], Lakshmikantha S[5]

[1,2,3,4,5]Department of Computer Science, East West Institute of Technology, Bengaluru, India

DOI: https://doi.org/10.26438/ijcse/v7si15.111115 | Available online at: www.ijcseonline.org

Abstract- Secure password storage is the essential feature in system based on password verification, which is most broadly used verification technique, despite its some security weakness. In this paper, a password authentication scheme that is designed for secure password storage and could be easily consolidated into present authentication systems. In this framework the client enters the plain password which is hashed through the cryptographic hash function such as SHA-256. This hash function isthen converted into negative password. Finally using a symmetric-key algorithm such as Advanced Encryption Standard the negative password is encrypted into an ENP(Encrypted Negative Password).So this method makes it difficult for the intruder to crack the password. ENP method overcomes pre computation attacks.ENP does not provide extra elements such as salt which is one of useful advantage.ENP is the first password protection scheme which integrates cryptographic hash function, the negative password and the symmetric-key algorithm in a successful way.

Keywords**:** Authentication, negative database, symmetric key algorithm**.**

I. INTRODUCTION

Many user studies and survey have confirmed that people can recall graphical password more reliably than text-based password over a long period of time. This seems to be the main advantage of graphical passwords. Although some research exists in the field but there is still no concrete evidence to prove whether graphical password in general is more or less secure than text-based password. The many researchers had put there efforts to make it more secure and easy to use by developing different mechanisms. But most of the existing methods have shown some significant drawbacks, therefore, they are not widely acceptable. The question of less implementation of image based authentication has to be answered on a case by case basis, depending on specific algorithms and implementations.

On contrast, pure recall is retrieval without external cues to aid memory. Using recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage, for example, remembering a textual password that one has not written down. Pure recall is a harder memory task than recognition. Between pure recall and pure recognition there is a different form of recollection: cued recall.

The difference is that this technique uses the hash function SHA-1, which produces a 20 byte output. This makes the authentication secure and requires less memory. However, an image file still occupies more space than text even after hashing. The authors suggested a possible future improvement by providing the persistent storage and this could be deployed on the Internet, cell phones and PDA's. However, this method still requires users to memorize the alphanumeric code for each pass-object variant. For example, if there are 4 pictures each with 4 variants, then each user has to memorize 16 codes. Although the pass-objects provide some cues for recalling the codes, it is still quite inconvenient. Hong et al. later extended this approach to allow user to assign their own codes to pass object variants. And shows the log-in screen of this graphical password scheme. However, this method still forces user to memorize many text strings and therefore suffer from the many drawbacks of text-based passwords follows. Although the preliminary user studies have shown some promising results for the Pass face technique, the effectiveness of this method is still uncertain.

Paid to the development of the internet, a huge number of online services have come out ,in which password verification uses the authentication method and this authentication technique is available at low cost. The password security always attracts great interest from the academia and industry. Without affecting the research achievements on security still the passwords are attacked by the attacker because of user giving the weak password or by repeating the same passwords. The plain passwords are sent to password list and later sent to the authentication data table from low security password list. Then the plain passwords are searched in the look up table, if the password are matched in the authentication data table and key in the look up table then the attacker can easily login through user name and password and could steal sensitive information. To overcome the look up table attack the corresponding hashed password is determined. By the corresponding hashed password the look up table could be quickly constructed and its results is in high success rate. Generally Password protection include hashed password, salted password and the key stretching. Apart from general password protection introduced a password protection scheme called Encrypted Negative Password it is based on the Negative Database.

II.RELATED WORK

A. Password Protection Strategies

1.Hashed Password:- Storing plain password is the ordinary scheme, in which the opponent can obtain the authentication data table so the passwords are compromised which is its main drawback. As the cryptographic hash function is infeasible to recover plain password this scheme is best suited. The cryptographic Hash function rapidly matches data of arbitrary size to fixed size sequence of bits. In this technique only hash password are stored in the authentication system. hash password scheme cannot withstand rainbow table and lookup table attack. In many of the application system passwords are recommended to be stored in the form of hash format.

2.Salted Password:-Salted password technique is used to withstand pre-computation task. In this technique the series of plain password and a salt are hashed through a function

3.Key Stretching:-To withstand dictionary attack, key stretching was proposed which converts weak passwords to secure password. Key stretching technique is more secure against brute-force attack by increasing space and time resources. Key stretching uses extra elements such as salt, in contrast ENP does not introduce extra element.

B. Negative Database

Negative Database stores the compression of the compliment of a positive database denoted as NDB. denotes the universal set of n-bit sequences; denotes an n-bit some of NDB concepts are shown, NDB carry three symbols in each entry such as 0,1,*. '0' symbol the bit '0' and '1' matches the bit '1' ,'*' matches either 0&1 these '0' or '1' is known as specified position &'*' is known as unspecified position. In an NDB, a series of bits is protected by one entry, series of bits are corresponded by the symbols at the specified position. If every entry in the (U-DB) is protected by an NDB, then the NDB is complete otherwise incomplete. The DB is transfigured from the NDB with only one entry is known as Single NDB or else known as Multiple NDB.

There are two kinds of NDB generation algorithm: 1) Single NDBs 2) Multiple NDBs under certain condition these generation algorithm are generated among NDB, few are hard-to-reverse and others are easy-to-reverse, here we hire two easy-to-reverse computes single NDB generation algorithm to generate negative password. NDB has been used in several fields as a form of negative representation of details, such as biometric recognition, authentication and information hiding.

To save the real authentication data table, NDB was used as an additional protection layer and also used to save the biometric data while bearing powerful recognition. One-time password protection authentication scheme was proposed based on NDB over the authentication method, difficulty of reversing the NDB by the protected passwords. By the cryptographic hash function and symmetric encryption passwords are protected. The authentication is based on the comparison of hash value of the plain password from a client and hashed password corresponding to some ENP on the server.

III.METHODOLOGY

The below figure shows a general block diagram describing the activities performed by this project.

The entire architecture has been implemented in nine modules which we will see in high level design and low level design in later chapters.

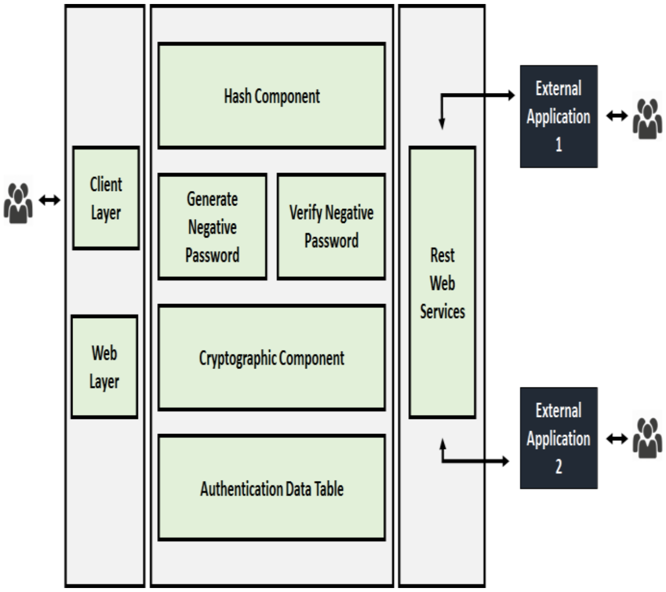

Fig. 1

Registration phase

Ontheclientside,auserentershis/herusernameandpassword.Then,theusernameandplainpasswordaretransmittedtotheserverthroughasecurechannel;Ifthereceivedusernameexistsintheauthenticationdatatable,“Theusernamealreadyexists!”isreturned,whichmeansthattheserverhasrejectedtheregistrationrequest,andtheregistrationphaseisterminated;otherwise,gotoStep(3);

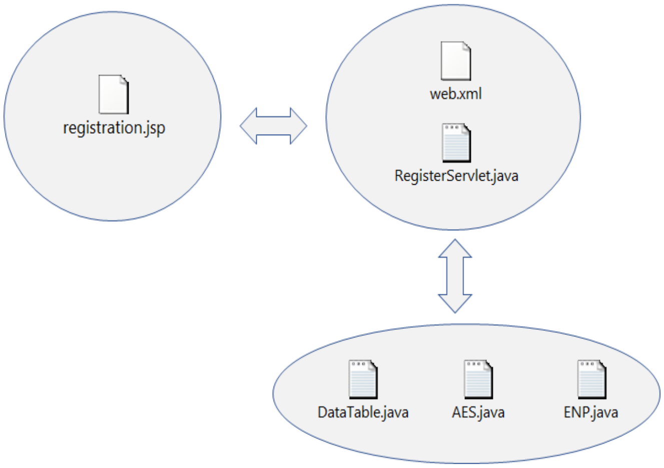

Fig. 2

The received password is hashed using the selected cryptographic hash function;The hashed password is converted into a negative password using an NDB generation algorithm

The negative password is encrypted to an ENP using the selected symmetric-key algorithm, where the key is the hash value of the plain password. Here, as an additional option, multi-iteration encryption could be used to further enhance passwords;
The username and the resulting ENP are stored in the authentication data table and “Registration success” is returned, which means that the server has accepted the registration request

Authentication phase

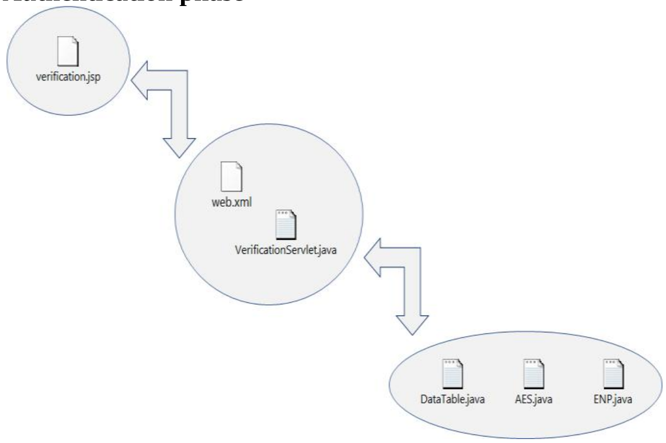

Fig. 3

On the client side, a user enters his/her username and password. Then, the username and plain password are transmitted to the server through a secure channel;
If the received username does not exist in the authentication data table, then “Incorrect username or password!” is returned, which means that the server has rejected the authentication request, and the authentication phase is terminated; otherwise, go to Step (3);
Search the authentication data table for the ENP corresponding to the received username;
The ENP is decrypted (one or more times according to the encryption setting in the registration phase) using the selected symmetric-key algorithm, where the key is the hash value of the plain password; thus, the negative password is obtained;
If the hash value of the received password is not the solution of the negative password then “Incorrect username or password!” is returned, which means that the server has rejected the authentication request, and the authentication phase is terminated; otherwise, “Authentication success” is returned, which means that the server has accepted the authentication request

ENP-as-a-Service

This portal enables the owner of the product to share the solution we have proposed to the external applications. The user just have to add a new client by entering the client’s email ID. The portal will then generate the Client Identifier and the unique PIN and sends it across an email to the client. The client will also get the API details which has to be invoked to consume the web services we are exposing. The client identifier and the client PIN are mandatory to be included in each client request.

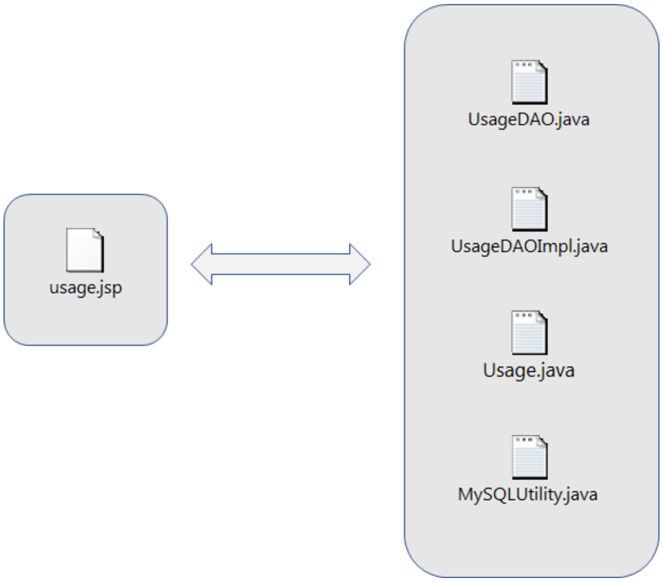

Fig. 4

Basically, two APIs are been exposed to the external clients

- Registration Service
- Verification Service

These APIs are exposed as a RESTFul web services.

REST stands for REpresentational State Transfer. REST is web standards based architecture and uses HTTP

Protocol. It revolves around resource where every component is a resource and a resource is accessed by a common interface using HTTP standard methods. REST was first introduced by Roy Fielding in 2000.In REST architecture, a REST Server simply provides access to resources and REST client accesses and modifies the resources. Here each resource is identified by URIs/ global IDs. REST uses various representation to represent a resource like text, JSON, XML. JSON is the most popular one.

A web service is a collection of open protocols and standards used for exchanging data between applications or systems. Software applications written in various programming languages and running on various platforms can use web services to exchange data over computer networks like the Internet in a manner similar to inter-process communication on a single computer. This interoperability (e.g., between Java and Python, or Windows and Linux applications) is due to the use of open standards. Web services based on REST Architecture are known as RESTful web services. These webservices uses HTTP methods to implement the concept of REST architecture. A RESTful web service usually defines a URI, Uniform Resource Identifier a service, provides resource representation such as JSON and set of HTTP Methods.

Usage Statistics

This portal enables the users of the product to get access to the usage statistics of the clients on the APIs they have shared with them. Fundamentally, each and every clients request access through the RESTFul webservice will be logged into the database.

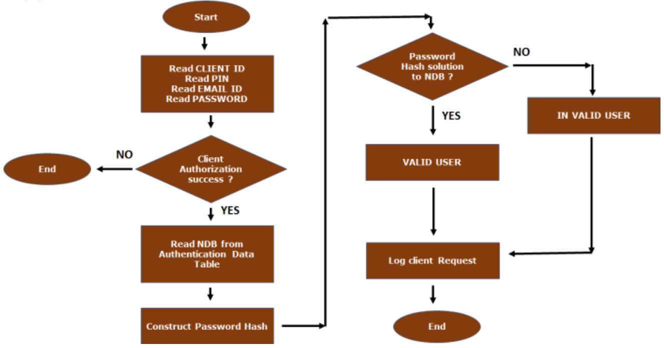

Fig. 5

The owner of the product will then be shown with a cumulative report of the numbers of times each APIs have been consumed by each client. This report is useful especially when the owner of the product wants to charge the clients over pay-as-you-go model.,

Generation Algorithm

Input: A password String ‘str’

```
Step 1: Compute the Hash code of the input String ‘str’ using SHA256 Algorithm
        hashStr← sha256(str)
Step 2: Convert the ‘hashStr’ into binary format
        binaryStr←strToBinary(hashStr)
Step 3: Compute the Random permutation of ‘binaryStr’
        permutedBits←randomPermutation(binaryStr)
Step 4:
m ←permutedBits.length
ndb[] ← empty[m]
for  i← 0 to m with step size of 1
        x[] ← CREATESYMBOLS(m);
        for j ← 0 to i with step size of 1
                x[j] ←permutedBits.charAt(j);
        x ←invertPermutation(x)
        ndb[i] ← x

result[][] ← empty[m][m]
for i← 0 to m with step size of 1
        result[i] ←AES.encrypt(ndb[i])
return result
```

Verification Algorithm

Input: A password String ‘str’ and a negative database ‘ndb’

```
Step 1: Compute the Hash code of the input String ‘str’ using SHA256 Algorithm
        hashStr← sha256(str)
Step 2: Convert the ‘hashStr’ into binary format
        binaryStr←strToBinary(hashStr)
Step 3:
        m ←binaryStr.length
        decryptedNDB← empty[m][m]
        k ← 0
        for i← 0 to m with step size of 1
                decryptedNDB[k][i] ←AES.decrypt(ndb[i])
                k++;

Step 4:
for i← 0 to m with step size of 1
        if (NUMBEROFSP(ndb[i])  != i)
                return false;
Step 5:
X[] ← empty[m]
for i← 0 to m with step size of 1
        index ←INDEXOFSP(ndb[i])
        x[index] ←ndb[i][index]
        for j ← i+1 to m with step size of 1
                ndb[j][index] = ‘*’

if (hash == x)      return true
else return false
```

IV. Conclusion and Future Scope

Stronger security algorithm which provides resistance to various kind of attacks including dictionary attacks and look-up table attack .No extra burden on programmers for configuring more parameters and it is simple and convenient to use

A scheme for password security is known as ENP, the authentication of password structure is dependent on ENP, the data given for the table are ENP. Later the attack has been examined and estimated by salted password, key stretching, ENP ,hashed password. Therefore the ENP provide us with secure password protection downward the dictionary attack. For a better password security in addition with ENP another NDB generation algorithm can be introduced.

ACKNOWLEDGEMENT

We would like to thank our principal Dr.KChennakes hava luand head of the department DR. Arun Biradar, East West Institute of Technology, Computer Science and Engineeringf or supporting us to carry out our project with clear guidance from Assistant Professor Mr. Lakshmikantha S.

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.

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

[14] 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.

[15] 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.

[16] R. Song, “Advanced smart card based password authentication protocol,” Computer Standards & Interfaces, vol. 32, no. 5, pp. 321–325, 2010.

[17] M. C. Ah Kioon, Z. S. Wang, and S. Deb Das, “Security analysis of MD5 algorithm in password storage,” in Proceedings of Instruments, Measurement, Electronics and Information Engineering. Trans Tech Publications, Oct. 2013, pp. 2706–2711.

[18] P. Oechslin, “Making a faster cryptanalytic time-memory trade-off,” in Proceedings of Advances in Cryptology - CRYPTO 2003. Springer Berlin Heidelberg, 2003, pp. 617–630.

[19] S. Noel, M. Elder, S. Jajodia, P. Kalapa, S. O’Hare, and K. Prole, “Advances in topological vulnerability analysis,” in Proceedings of 2009 Cybersecurity Applications Technology Conference for Homeland Security, Mar. 2009, pp. 124–129.

AUTHORS PROFILE

Ms. Manasa N is pursuing her 8 semester B.E in Computer science and engineering at East West Institute of Technology,Bengaluru,India. Her area of interest includes Network Security.

Ms. Preethi P is pursuing her 8 semester B.E in Computer science and engineering at East West Institute of Technology,Bengaluru,India. Her area of interest includes Network Security.

Ms. Rakshitha R is pursuing her 8 semester B.E in Computer science and engineering at East West Institute of Technology,Bengaluru,India. Her area of interest includes Network Security.

Ms. Jyothi V is pursuing her 8 semester B.E in Computer science and engineering at East West Institute of Technology,Bengaluru,India. Her area of interest includes Network Security.

Mr. Lakshmikantha S got M.Tech degree in Computer Science, Bengaluru, India. He is currently working as Associate Professor in the Department of CSE,EWIT. His area of interest includes Network Security.