iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** IV **Month of publication:** April 2021

DOI: https://doi.org/10.22214/ijraset.2021.33897

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue IV Apr 2021- Available at www.ijraset.com

Authentication by Encrypted Negative Password using SHA-256 and RSA Algorithm

Mayuri Jadhav[1], Rinku Shewale[2], Jhanvi Chaudhary[3]
[1, 2, 3]*Department of Computer Engineering, Bharati Vidyapeepth's College Of Engineering For Women, Pune, Maharashtra, India*

Abstract: ***Secure password storage is an important feature in systems based on password authentication, which is still the most widely used authentication method, despite some security flaws. In this project, we propose a password authentication framework designed to keep passwords secure and can be easily integrated into existing authentication systems. In our framework, for the first time, a clear password obtained from a client quickly with a cryptographic hash function (e.g., SHA-256). After that, the hashed password is changed to the negative password. Finally, the negative password is encrypted in the Encrypted Negative Password (abbreviated as ENP) using a corresponding key algorithm (e.g., AES), and finally, the encrypted password is encrypted and encrypted using the RSA algorithm to improve password security.***

Keywords: ***Authentication, cryptographic function, symmetric-key algorithm, Salted password, Hashed password, Key Stretching, OTP.***

I. INTRODUCTION

These days there are many online services popping up that require a secure password and one of the strongest and most widely used password verification methods. It is available at low cost. And because of the negligent behavior of users, passwords are easily broken, which is why the password authentication system is growing .The standard password protection systems include passwords, salted passwords and key extensions. In this paper, a password protection program called Encrypted Negative Password (abbreviated as ENP) is proposed, based on cryptographic hash and equivalent encryption, and a password verification framework.

A. Objective

The purpose of this paper is to increase password security. When you make a guess attack online, there is a limit to the number of login attempts. To increase password security, online authentication systems have begun enforcing stricter password policies. In this project we propose to design and implement secure one-time password system (OTP) to provide a better way to enforce a set of strict policies, finally, the encrypted password is encrypted and the RSA algorithm is used to improve password security.

B. Scope

By obtaining a password online sites can offer security and protection against hacking passwords. Passwords in the authentication table are delivered in the form of quick passwords. Other powerful attack tools, such as hash cat, Rainbow Crack and John the Ripper, provide functions, such as multiple hash algorithms, multiple attack models, multiple operating systems, and multiple platforms, which require much-needed secure password storage. In these cases, attacks are often performed as opponents before calculating the check table, where the keys are the hash values of the items in the password list containing frequently used passwords, and the records shown corresponding to the specific passwords in the password list.

II. RELATED WORK

A. Hashed Password

The simplest scheme to store passwords is to directly store plain passwords. However this scheme presents a problem that once adversaries obtain the authentication data table, all passwords are immediately compromised. To safely store passwords, a common scheme is to hash passwords using a cryptographic hash function, because it is infeasible to directly recover plain passwords from hashed passwords.

B. Salted Password

Password hashing is a key step in protecting your users from backend, but it is not a mistake because it hashes in a consistent way. This means that it is predictable and can be predicted by a dictionary attack or a rainbow table attack. Salting is the act of adding a random string to a password before performing a hashing function.

C. Key Stretching

Salting is the act of adding a random string to a password before performing a hashing function.

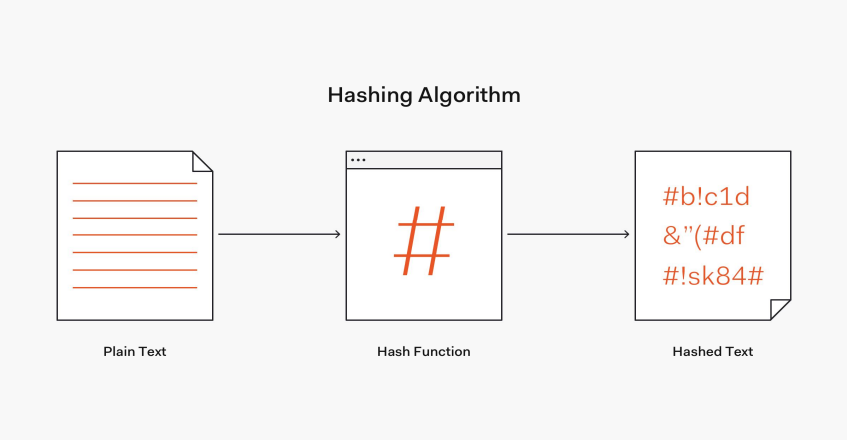


Fig -1: Hashing Algorithm

D. Negative Password

The creation of the negative password is that the plain password is converted into the ASCII value and then converted into binary values of 0's and 1's. Then we split the values as two bit pairs and there are 4 forms:

00->0
01->1
10->*
11->*

For e.g.: "00101101" it's denoted as "0**1".

III. PROPOSED SYSTEM ARCHITECTURE

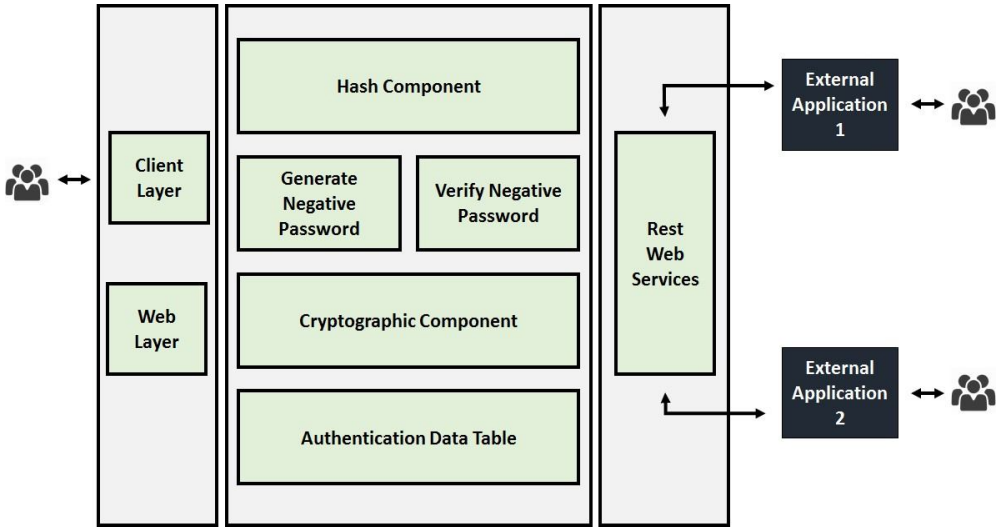


Fig -2: System Architecture

A. *Registration Phase*

On the client side, a client enters his/her username and password. At that point, the username and plain password are transmitted to the worker through a secure channel.If the received username exists in the authentication data table, "The username already exists!" is returned, which means that the worker has rejected the registration demand, and the registration phase is terminated; otherwise, go to Step(C).The received password is hashed utilizing the selected cryptographic hash function; The hashed password is converted into a negative password utilizing an NDB generation algorithm. The negative password is encrypted to an ENP utilizing the selected symmetrickey algorithm, where the key is the hash value of the plain password. Here, as an additional option, multi-iteration encryption could be utilized to further enhance passwords.The username and the subsequent ENP are stored in the authentication data table and "Registration success" is returned, which means that the worker has accepted the registration demand.

B. *Authentication Phase*

On the client side, a client enters his/her username and password. At that point, the username and plain password are transmitted to the worker through a secure channel. On the off chance that the received username does not exist in the authentication data table, "Incorrect username or password!" is returned, which means that the worker has rejected the authentication demand, and the authentication phase is terminated otherwise, go to Step (C), 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) utilizing the selected symmetric-key algorithm, where the key is the hash value of the plain password; in this way, 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 worker has rejected the authentication demand, and the authentication phase is terminated, otherwise, "Authentication success" is returned, which means that the worker has accepted the authentication demand.

C. *ENP-as-a-Service*

This site empowers the item proprietor to share the arrangement we have proposed with outer applications. The client ought to just add another customer by entering the customer's email ID. The site will create a customer identifier with an extraordinary Stick and send you an email to the customer. Customer identifier and customer PIN are needed to be remembered for every customer demand. Fundamentally, two APIs are revealed to an outside customer:

1) Registration Service
2) Verification Service

IV. LITERATURE SURVEY

Later on, other NDB generation algorithms will be examined and introduced to the ENP to further improve password security. Furthermore, other techniques, such as multi–factor authentication and challenge–response authentication, will be introduced into our password authentication framework [1].

The work characterizes a multi-factor authentication model in case the application supports multiple authentication factors. The core of the proposed model is hazard based authentication. Results of simulations of some key scenarios often utilized in practice are also presented [2].

Security is a major issue when utilizing web services. Double-factor authentication is most utilized at this time to protect client's account. One example of double factor authentication is One Time Password (OTP). OTP is a password that is valid for only one login session. In this research OTP generated from plaintext which is a combination of username, hand phone's number and access time [3].

In this paper, the enhanced secure hash algorithm is implemented on web portals to guarantee the improvement of security from possible attacks. The enhanced algorithm introduces the following features from the original algorithm of SHA-1:

Selection of primitive functions and constant is utilized. Instead of equally disseminating the primitive functions of SHA-1, the selection will depend on Q15 value. The constant utilized for each round will depend on Q0 value.

Expanded hashed message. SHA-1 message output is composed of 160 pieces. The enhanced secure hash algorithm is expanded to 512-bits hash message.

Additional register blocks. Initially, SHA-1 contains 5 registers (A, B, C, D and E). Since the expanded SHA-1 requires 512 pieces. The registers are also expanded to 8 blocks (A, B, C, D, E, F, G and H). From 32 x 5 = 160 pieces, to 64 x 8 = 512 pieces.

Inclusion of salt algorithm. Utilizing slope cipher, salt algorithm is included on the enhanced hash function to assure that no collision may occur for large record of client accounts. [4]

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue IV Apr 2021- Available at www.ijraset.com

A. Encryption Module

Encryption function is part of the core of the framework, before encryption the primary thing is detecting the USB interface, we should stop the operation if there is no USB security key. At that point, the PIN requires authentication security key code, the wrong type will bring about the suspension. Encryption, the framework can be partitioned into two parts operations, as part of the security key to complete, including the security of key internal random number generator to generate the session key, at that point key in the RSA algorithm for encryption processing motor session key: Ek (K1) = Mk, and then send K1, Mk to the computer; the second part completed by the computer, symmetric algorithm is achieved by the code, choose 128-bit AES, encryption keys are generated by the security key K1, EK1 (T) = MT, the final task is connect the MT that is the encrypted documents and the encrypted key Mk to create a new record a cipher text M.

B. Decryption Module

Decryption function is part of the core of the framework before the decryption, we should also check the security keys and the verification PIN code, otherwise, the operation finished. In the decryption, the key decryption of the key should be done inside the security key , aim to guarantee the private key never leave the security enters in order to prevent malicious programs to steal. While the document is encrypted on your computer to complete, so improving the efficiency of declassified documents. Decryption process is as follows: First, read MK from the cipher text M, MK is sent to the security key, by the RSA algorithm processing motor which in the USB security key to decrypt the session key K1, DK (MK) = K1, obtained K1 will be sent to the computer, the computer will decrypt Mp, DK1 (MT) = T, P to plain text, and need to restore the record type of the plaintext [5]

C. RSA Algorithm

The RSA algorithm contains the following -

The RSA algorithm is a popular adjective in a restricted field in addition to numbers that include key numbers. The numbers utilized in this way are large enough to make it difficult to solve. There are two sets of enters in this algorithm: private key and public key steps to work on RSA algorithm –

1) *Step 1:* Generate the RSA modulus The first process starts with the selection of two main numbers, p and q, and counts their product N, as indicated - N=p*q
2) *Step 2:* Determined Number (e) Think of a number as a found number that should be greater than 1 and less than (p-1) and (q-1). The main condition will be that there should be no standard feature of (p-1) and (q-1) other than 1
3) *Step 3:* Public key The specified numbers n and e form the key to South African society and are made public.
4) *Step 4:* Private Key The secret key d is calculated from the numbers p, q and e. The mathematical relationship between numbers is as follows - ed = 1 mod (p-1) (q-1)

D. Encryption Formula

Think of a sender who sends this explicit text to a person with a public key (n, e). Encrypting a clear text message in the given context, use the following syntax -

C = Pe mod n

E. Decryption Formula

The writing process for translation is very straightforward and incorporates computational analytics in a systematic way. If you think that recipient C has a secret key d, the output modulus will be calculated as -

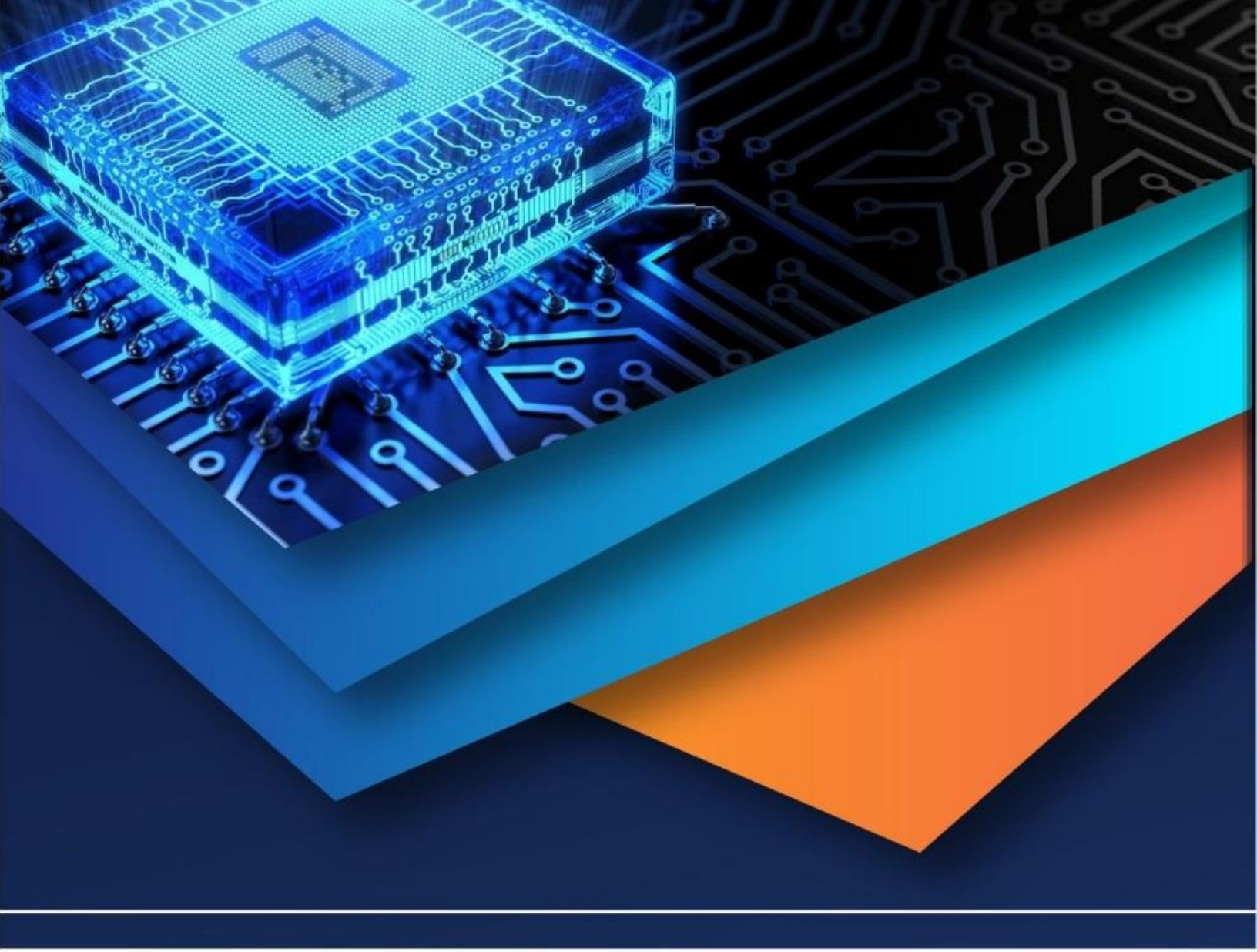
Plaintext = mod for Cd n

V. CONCLUSIONS

In this project, we have proposed a password protection program called ENP, and introduced an ENP-based password verification framework. In our framework, the sections in the authentication table are ENPs. Finally, we analyzed and compared the seriousness of the attacks of the hashed password, the salty password, the key extension and the ENP. The outcomes show that the ENP can withstand the attack of the check table and provide strong password protection under dictionary attacks. It is fair to say that the ENP does not require additional substances (e.g., salt) while opposing the invasion table.

REFERENCES

[1] Authentication by Encrypted Negative Password Wenjian Luo, Yamin Hu, Hao Jiang, Junteng Wang IEEE Transactions on Information Forensics and Security Year: 2019 | Volume: 14, Issue: 1 | Journal Article | Publisher: IEEE Cited by: Papers (8)
[2] Multi-Factor Authentication Modeling Libor Dostálek 2019 9th International Conference on Advanced Computer Information Technologies (ACIT) Year: 2019 | Conference Paper | Publisher: IEEE
[3] One Time Password (OTP) Based on Advanced Encrypted Standard (AES) and Linear Congenital Generator(LCG) Imamah 2018 Electrical Power, Electronics, Communications, Controls and Informatics Seminar (EECCIS) Year: 2018 | Conference Paper | Publisher: IEEE
[4] Implementation of Enhanced Secure Hash Algorithm Towards a Secured Web Portal Froilan E. De Guzman; Bobby D. Gerardo; Ruji P. Medina 2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS) Year: 2019 | Conference Paper | Publisher: IEEE
[5] Study of file encryption and decryption system using security key Gang Hu 2010 2nd International Conference on Computer Engineering and Technology Year: 2010 | Volume: 7 | Conference Paper | Publisher: IEEE



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY