IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 8, Issue 8, August 2020

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

9940 572 462 | 6381 907 438 | ijircce@gmail.com | www.ijircce.com

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 8, August 2020 ||

Authentication by Encrypted Negative Password

Saranya E, Ponmangai G.

Assistant Professor, Department of Computer Science and Engineering, Sri Eshwar College of Engineering, Coimbatore, India.

B.E, Department of Computer Science and Engineering, Sri Eshwar College of Engineering, Coimbatore, India

ABSTRACT: Secure secret phase stockpilling is an indispensable angle in frameworks in light of secret word verification,which is as yet the most broadly utilized verification strategy,in spite of some security blemishes. Here I propose a secret word verification system that is intended for secure secret phase stockpiling and could be effectively incorporated into existing confirmation frameworks.

KEYWORDS: Secure secret phase stockpilling, verification

I.INTRODUCTION

In this paper, I proposed a password Authentication that is been designed for secure password storage and could be easily integrated into existing authentication system. Here we first receive the plain password from a client and that is hashed through cryptographic hash function (SHA-256).Then the hashed password is converted into a negative password.Finally the negative password is been encrypted using AES and multi-Iteration encryption could be employed to further improve security.

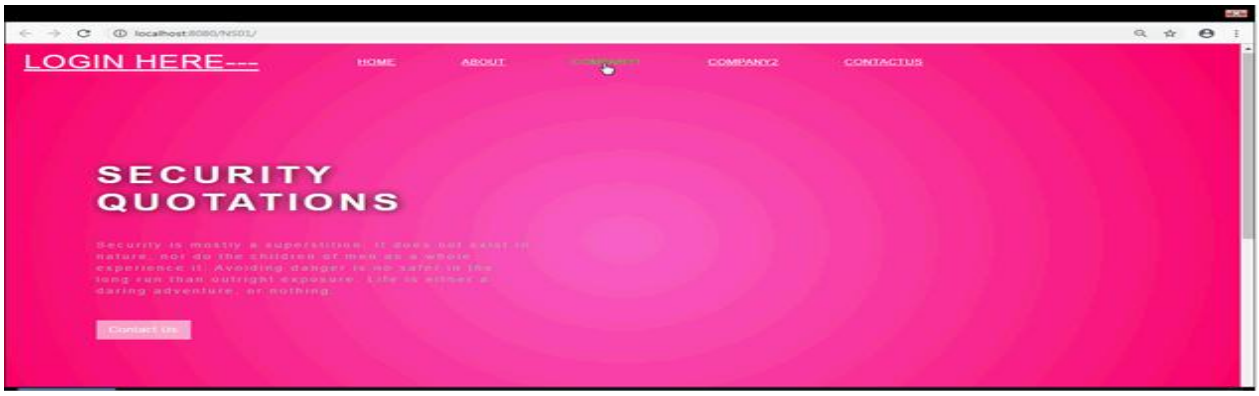

Fig.1: Home page

II. GOALS AND MOTIVATION

- To develop a web app for a portal within a organization and Secure the data in the portal with the negative encrypted password.
- Legally sharing the requirements with the other organisation by sending the key to check in to their requirement as per our approval.

III. PROPOSED SYSTEM

A. Registration Phase

The registration phase is divided into six steps. (1) 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.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 8, August 2020 ||

(2) If the received username exists in the authentication data table, ―The username already exists!‖ is returned, which means that the server has rejected the registration request, and the registration phase is terminated; otherwise, go to Step (3).

(3) The received password is hashed using the selected cryptographic hash function.

(4) The hashed password is converted into a negative password using an NDB generation algorithm (i.e., Algorithm A.1 or Algorithm A.2 in the Appendix).

(5) 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.

(6) 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.

B. Authentication Phase

The authentication phase is divided into five steps. (1) 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.

(2) 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).

(3) Search the authentication data table for the ENP corresponding to the received username.

(4) 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.

(5) If the hash value of the received password is not the solution of the negative password (verified by Algorithm 1 or Algorithm 2), 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.

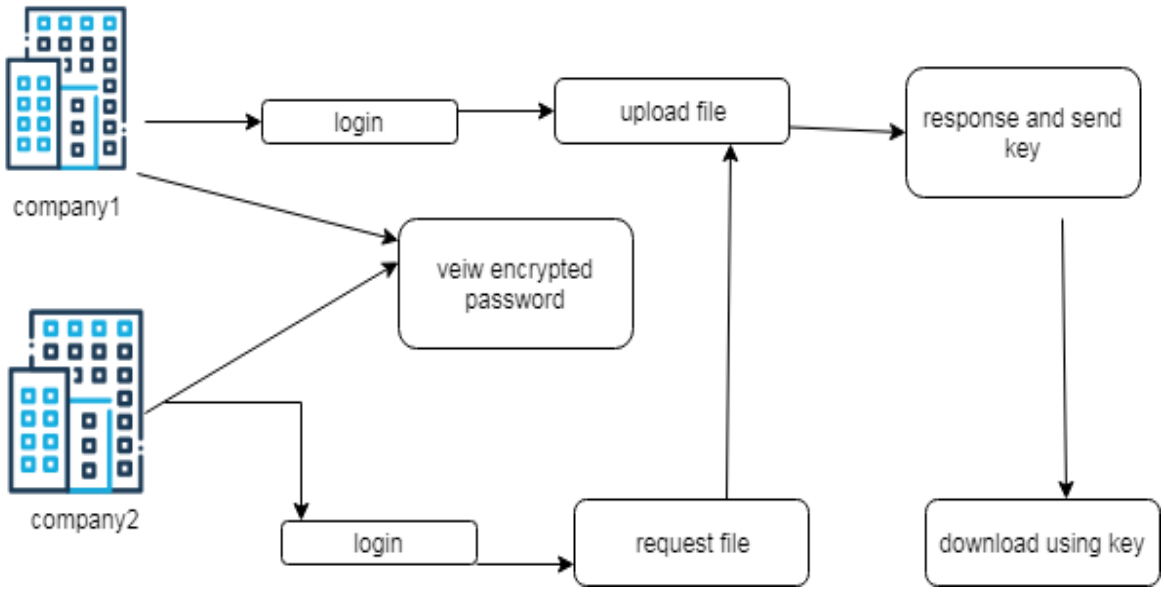

Fig no:2 Process of uploading and Downloading.

IV.EXISTING SYSTEM

S. Boonkrong proposed dynamic salt generation and placement are used to improve password security.

But here the salt is a random string that is dependent on the original password .consequently it could resist look up table attack. It could not defend against dictionsry attack and also introduces an extra element.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 8, August 2020 ||

V. PROPOSED SYSTEM

In this paper,a password protection scheme called Encrypted Negative Password is proposed, which is based on NDB cryptographic hash function and symmetric encryption, and a password authentication framework based on ENP is presented.we analyze and compare the attack complexity of hashed password,key stretching and ENP. It provides stronger password protection under dictionary attack.

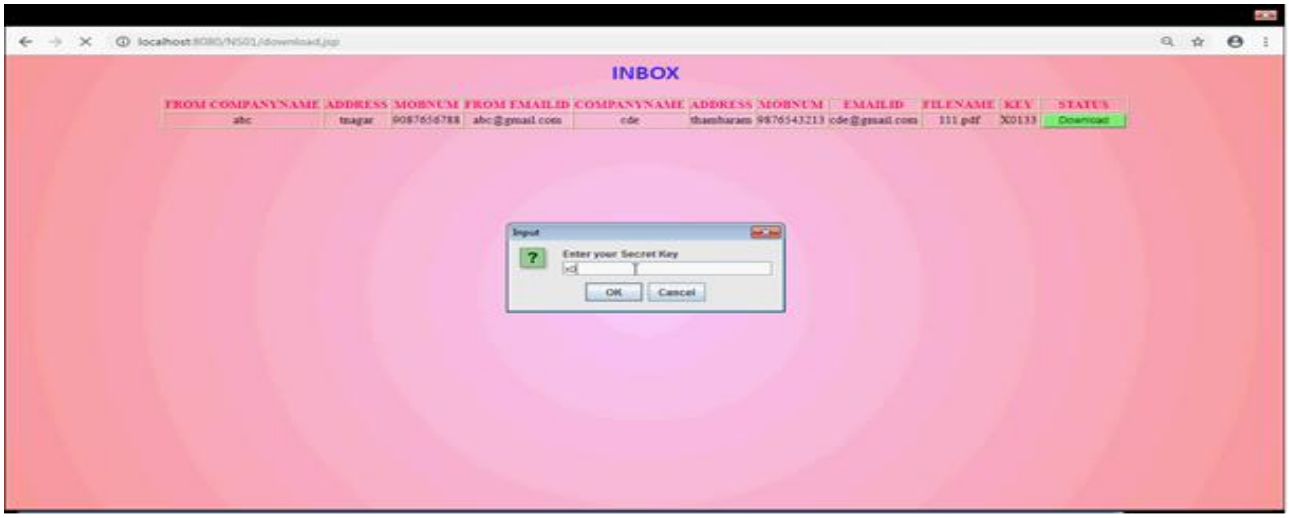

Fig no 3:SAMPLE PAGE TO DOWNLOAD A FILE

V1.RESULT AND DISCUSSION

This paper finally gives security for the customers who register into the portal and provide a safe and secure transfer of files .when an organization wants to access a file in a authorized manner , first he will be able to view the files in an encrypted format .Then he requests the file which he needs to access .Once the request is sent the other organisation will be notified about that request. so he can accept or reject the request based on his intention. once he accepts the request a key will be sent to the user and he will be getting a accepted notification .If he clicks download option he will be asked to enter the key value .Finally the file will be downloaded .

VII.ACKNOWLEDGEMENT

I am glad to thank .M.S. E.Saranya for guiding about the strong Password – only Authenticated key exchange. .We extend our sincere thanks to E.Saranya who have helped us in availing the required technology in developing the Authentiction portal.

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 resis-tant 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] 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.
[5] 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.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 8, August 2020 ||

[6] 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.

INNO SPACE

SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details