International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN: 2456-172X | Vol. 2, No. 2, June - August, 2017 | Pages 136-141

AUTHENTICATION BY ENCRYPTED NEGATIVE PASSWORD

G.KEERTHANA[1], K.PUSHPAVALLI[2]

Department of Information Technology, Agni College Of Technology, Chennai.

Abstract- Secure secret phrase stockpiling 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 its some security blemishes. In this paper, we propose a secret word verification system that is intended for secure secret word stockpiling and could be effectively incorporated into existing confirmation frameworks. In our structure, first, they got plain secret phrase from a customer is worked out a cryptographic hash work. At that point, the hashed secret phrase is changed over into a negative secret key. At long last, the negative secret key is scrambled into an Encrypted Negative Password utilizing a symmetric-key calculation (e.g., AES),and multi-cycle encryption could be utilized to further improve security. The cryptographic hash work and symmetric encryption make it hard to break passwords from ENPs. Also, there are loads of comparing ENPs for a given plain secret key, which makes precipitation assaults infeasible. The calculation intricacy investigations and examinations demonstrate that the ENP could oppose query table assault and give more grounded secret key insurance under word reference assault. It is value referencing that the ENP does not present additional components (e.g., salt); other than this, the ENP could at present oppose precomputation assaults. In particular, the ENP is the primary secret Key securities conspire that consolidates the cryptographic hash work, the negative secret word and the symmetric-key calculation, without the requirement for extra data with the exception of the plain secret phrase.

1.INTRODUCTION

Secure secret phrase stockpiling 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 its some security blemishes. In this paper, we propose a secret word verification system that is intended for secure secret word stockpiling and could be effectively incorporated into existing confirmation frameworks. In our structure, first, they got plain secret phrase from a customer is worked out a cryptographic hash work. At that point, the hashed secret phrase is changed over into a negative secret key. At long last, the negative secret key is scrambled into an Encrypted Negative Password utilizing a symmetric-key calculation (e.g., AES),and multi-cycle encryption could be utilized to further improve security. The cryptographic hash work and symmetric encryption make it hard to break passwords from ENPs. Also, there are loads of comparing ENPs for a given plain secret key, which makes precipitation assaults infeasible. The calculation intricacy investigations and examinations demonstrate that the ENP could oppose query table assault and give more grounded secret key insurance under word reference assault. It is value referencing that the ENP does not present additional components (e.g., salt); other than this, the ENP could at present oppose precomputation assaults. In particular, the ENP is the primary secret Key securities conspire that consolidates the cryptographic hash work, the negative secret

word and the symmetric-key calculation, without the requirement for extra data with the exception of the plain secret phrase.

2. EXISTING SYSTEM

In existing framework, secure secret phrase stockpiling is an imperative viewpoint in frameworks in light of secret word confirmation, which is as yet the most generally utilized verification system, in spite of its some security imperfections.

2.1 OSVDB Technique

The Open Sourced Vulnerability Database was a free and publicly released weakness database The objective of the task was to give precise, point by point, current, and impartial specialized data on security vulnerabilities. The task advanced more noteworthy and progressively open cooperation among organizations and people.

2.1.1 Drawbacks

- Not as User-Friendly as Commercial Software.
- Lack of extensive tech support.

3.PROPOSED SYSTEM

It depends on the polynomial duty for distributed computing, which can understand the certainty of database records in the cloud. Also, the proposed plan can bolster open undeniable nature in that all customers in the framework can confirm the database.

3.1 Encrypt Technique

A password protection scheme called Encrypted Negative Password is proposed, which is based on the Negative Database, cryptographic hash function and symmetric encryption, and a password authentication framework based on the ENP is presented.

3.1.1 Advantages

The advantages of our techniques are analyzing and comparing the attack complexity of our scheme with that of typical password storage schemes under lookup table attack and dictionary attack

4. SYSTEM ARCHITECTURE

System architecture (Fig 1)is the conceptual model that defines the structure, behavior, and more views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system. A system architecture can consist of system components and the sub-systems developed, that will work together to implement the overall system. There have been efforts to formalize languages to describe system architecture; collectively these are called architecture description languages (ADL)

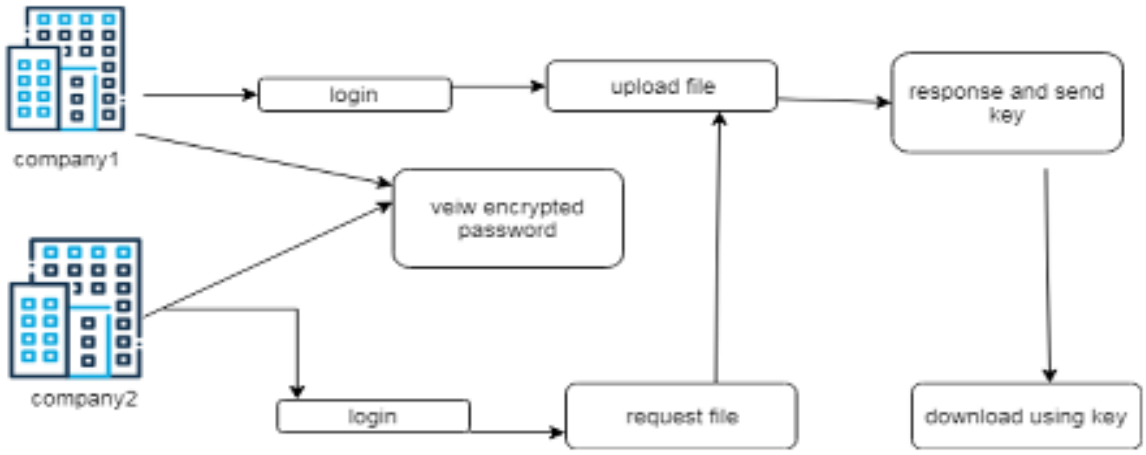

Fig 1 System Architecture

5.IMPLEMENTATION

5.1 User Interface Design:

. This is the first module(Fig 2) of our project. The important role for the user is to move login window to user window. This module has created for the security purpose. In this login page we have to enter login user id and password. It will check username and password is match or not (valid user id and valid password). Ifwe enter any invalid username or password we can't enter into login window to user window it will shows error message. So we are preventing from unauthorized user entering into the login window to user window. It will provide a good security for our project. So server contain user id and password server also check the authentication of the user. It well improves the security and preventing from unauthorized user enters into the network. In our project we are using JSP for creating design. Here we validate the login user and server authentication.

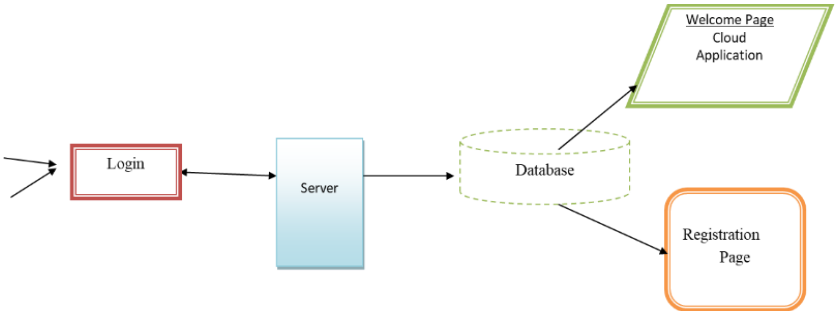

Fig 2 User Interface Design

5.2 Views Encrypted Password

In this part registered user (Fig 3)will view the encrypted passwords from the database stored. After registration from the each company or users they will view their encrypted passwords.

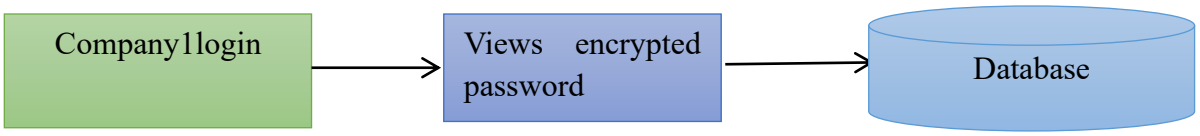

Fig 3 Views Encrypted Password

5.3 Upload file from company

In this module(Fig 4) , after logging in company have to upload some files i.e. to be pdf or a text file. The uploaded file gets encrypted and stored in the database. With that also that hacker cant able to access files.

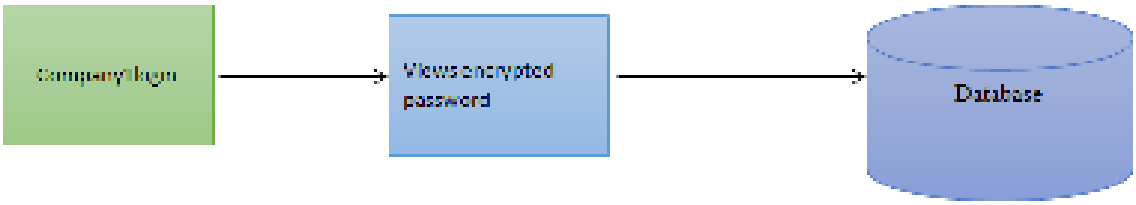

Fig 4 Upload file from company

5.4 Company2 views uploaded file:

In another side(Fig 5), company2 login and view the files uploaded by other

Fig 5 Company2 views uploaded file

company. They can only view the name of the file. They cannot get or download file directly.

5.5 Request for some file:

Here Company2(Fig 6) request for some files uploaded by the company1. Directly they can click on request button it will be sent to the company1 as a notification.

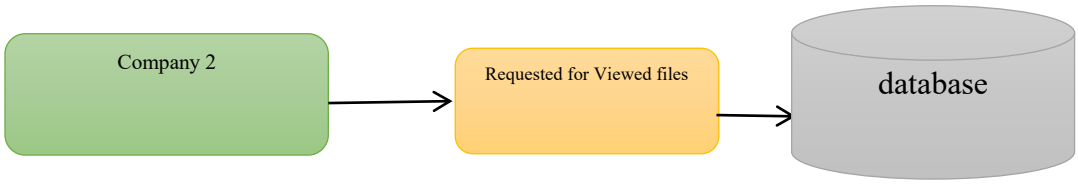

Fig 6 Request for some file

5.6 Company1 accepts with sending Key:

Company1 receives notification after getting log in. here there will be the request sent by other company. If they accepts means, key will be generated for download the file. The key will be sent to the requested company for downloading file with acceptance notification. Otherwise it will be rejected.

5.7 Company2 downloads file using Key:

Here the acceptance notification(Fig 7) will be received with the key. When he downloads the file it asks for entering the key. If it is matched it will be downloaded.

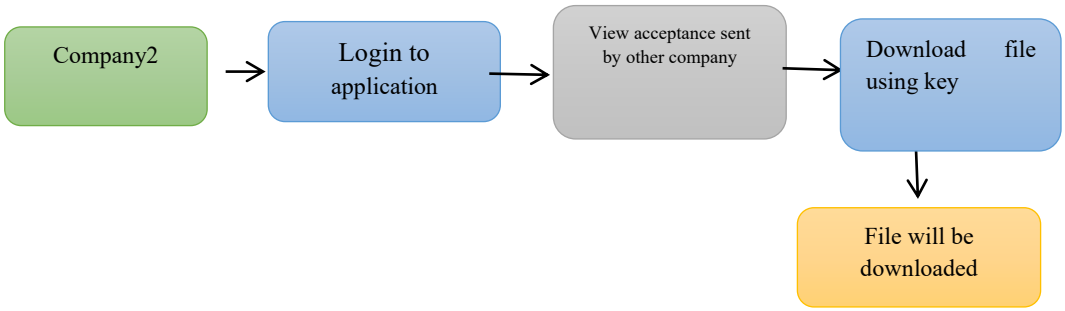

Fig 7 Company2 downloads file using Key

6. Conclusion

In this paper, we proposed a secret phrase assurance conspire called ENP, and exhibited a secret key confirmation structure dependent on the ENP. In our system, the passages in the validation information table are ENPs. At last, weexamined what's more, looked at the assault multifaceted nature of hashed secret phrase, salted secret key, key extending and the ENP. The outcomes show that the ENP could oppose query table assault and give more grounded secret key security under word reference assault. It is worth referencing that the ENP needn't bother with additional components (e.g., salt) while opposing query table assault.

7. Future Enhancement

In the future, other NDB generation algorithms will be studied 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.The NDB is a new security technique that is inspired by biological immune systems and has a wide range of applications. Symmetric encryption is usually deemed inappropriate for password protection.In database security, a negative database is a database that extras characteristics that can't be connected with a particular entry. A negative database is a kind of database that contains immense proportion of data including mirroring data.

References:

a) *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.*

b) *M. A. S. Gokhale and V. S. Waghmare, ―The shoulder surfing resis-tant graphical password authentication technique,‖ Procedia ComputerScience, vol. 79, pp. 490–498, 2016.*

c) *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.*

d) *A. Adams and M. A. Sasse, —Users are not the enemy,‖ Communications of the ACM, vol. 42, no. 12, pp. 40–46, Dec. 1999.*

e) *E. H. Spafford, —Opus: Preventing weak password choices,‖ Computers & Security, vol. 11, no. 3, pp. 273–278, 1992.*

f) *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.*

g) *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.*

h) *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.*

i) *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.*

j) *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.*