ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 11, Issue, 03, pp.1910-1912, March, 2019

DOI: https://doi.org/10.24941/ijcr.34620.03.2019

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

RESEARCH ARTICLE

PREVENTION OF BRUTEFORCE ATTACK USING MULTIPLE SECURITY TECHNIQUES

Vishal Kushwaha, Archit Maniyath and *Himatkumar Purohit

Department of Information Technology, Padmabhushan Vasantdada Patil Pratishthan's College of Engineering, Mumbai, India

ARTICLE INFO

Article History:
Received 16th December, 2018
Received in revised form
23rd January, 2019
Accepted 27th February, 2019
Published online 31st March, 2019

Key Words:
Honey encryption, steganography, Brute force attack.

ABSTRACT

Most dominant password storage method, store passwords directly in the databases and are mainly prone to brute force attack. Similar to password, storing data directly in the database on the server is another common thing to do. We have proposed the use of honey encryption as an algorithm to limit the possibilities of a password to get hacked. We have considered generating password based on password and other data. We then encrypt the generated password before storing them in the database. Further we have considered applying steganography techniques to hide the data behind multimedia content before storing them directly into the database on the server. We will define certain functions that will allow any user to generate passwords and consequently hide them behind some multimedia content. We will also compress the data before storing it on the server to make storage efficient system.

***Citation: Vishal Kushwaha, Archit Maniyath and Himatkumar Purohit,* 2019.** "Prevention of bruteforce attack using multiple security techniques", *International Journal of Current Research*, 11, (03), 1910-1912.

INTRODUCTION

The simplest form of user authentication available to us particularly on the Web is the password based authentication protocol, and the data is stored directly on the server. However these techniques are vulnerable to many attacks such as shoulder-surfing, key-loggers, brute force attacks etc. Any hacker can crack these passwords and eventually get access to the data stored in the database. To limit the chances of getting the correct password and thereby increasing the confidentiality of the data in database store, functions for generating and encrypting the passwords will be developed. Honey encryption (HE) provides flexibility and helps in avoiding attacks such as brute force attack .As different data is provided to the special function for creating unique passwords. Steganography helps in hiding data behind multimedia content so that even if the data gets into the hands of the attacker, he/she would still have difficulty comprehending what the data is. She/he cannot get the correct information unless and until they perform reverse steganography on the multimedia content. Data hiding along with encryption may very well be the next big thing and it is complemented by compressing the data to make the process efficient.

Literature survey

Schemes based on Honey Encyption: Ari Jules et al. (2014) proposed an encryption system, known as Honey Encryption in 2014, which is an encryption technique which limits the brute force attack too much. Honey encryption according to the author is used to generate honey words and provides plausible data to the attackers for incorrect passwords. In this the user inputs the password. Through a function multiple random seeds and passwords are generated, a password and seed combination list (i.e. List 1) is formed along with another list (i.e. List 2) consisting of seeds and passwords. Whenever a user provides any password a seed is immediately fetched from List 1 (This is where the passwords and seeds are present), this seed is then used to fetch the messages stored by the user. When no password is found in List 1, then a prompt will appear saying "Password doesn't match". Whereas when a password match is found in List 1 then the messages can be retrieved. The stored password is a cipher text which is obtained by performing XOR operation on plain text and seed.

Following are the limitations of Honey Encryption system

- Remembering Password structure is sometime difficult.
- Password typography can be difficult for users.
- XOR operation is not much secure and can be easily decrypted by offline and online attacks.

Baby Shamini et *al.* (2017) studied that passwords are the credentials users think that protects their sensitive information from outside world. In fact this is one of the weakest forms of security. There are many ways in which an attacker can get hold of your personal information one of which is sending multiple requests to the server which the system cannot handle

***Corresponding author:* Himatkumar Purohit**
Department Of Information Technology, Padmabhushan Vasantdada Patil Pratishthan's College of Engineering, Mumbai, India.

and the system fails or crashes which makes it impossible for the original user to login to its account and access its data. This type of attack strategy is called DDOS i.e. Distributed Denial of Service and this is detected when the system crashes due to overload. So, to detect or catch the attacker they created a shopping website where security is provided on passwords. During registration process all the honey words and passwords from users are stored inside the server. Then this password is stored into the database or server in another format or encrypted format using AES algorithm. The magic happens when the attacker tries to login with the set of honey words for several times then it is redirected to a dummy page which is created to mislead the attacker in thinking that he/she has logged in successfully. The dummy webpage will display purchase successful to make believe the attacker that he has succeeded in his quest. The trick to identifying the attacker lies in these steps. The attacker will fill in the address and number details while making the payment requirements which will then be stored into another database which will be mailed to original user's alternative mail id. Then finally the hackers IP address are blocked from accessing again.

Schemes based on Steganography: Islam *et al.* (2016) studied the differences between steganography and Cryptography. Both of which protect the data from unauthorized user but have completely different approaches. Cryptography encrypts the data however steganography does no such thing rather it hides the data behind a multimedia file or content. They further saw the parameters that differentiate one steganography method from another. These parameters include Security, Payload Capacity and Robustness. Steganography techniques exploit the weaknesses of the HVS. The most common steganography techniques uses LSB bit for hiding data however the researchers decided to use the more unconventional MSB bits. It involved comparing the data bit with the difference between bit no. 5 and bit no. 6. If the difference is not equal to the data bit then we traverse bit no. 5. Using MSB bits for steganography proved to be quite efficient as it provided much higher PSNR value and a lower payload value.

Proposed SystemL: Passwords are common way of authentication used on web. Passwords are stored directly on the database directly or after encryption. Stored passwords are generally the combination of lowercase, uppercase, numbers and special characters which provide more security. But these are prone to various attacks like the famous brute force attack. So new schemes are required to overcome issues faced by existing schemes and provide more security. In similar way data are stored directly on the database or some encryption are performed on the data. But after encryption also it is prone to various attacks like brute force attack. So new schemes are required to overcome issues faced by existing schemes and to make database storage more efficient. Every scheme has some pros and cons, our scheme too has some pros and cons. The advantage of our scheme is to provide strong security to users password and data. Another advantage of our scheme is that it provides resistance to attacks such as dictionary and brute-force attacks and also provides efficient storage system. There are few limitations of our scheme such as it requires high computational power and time then existing schemes, as password generation and encryption, data encryption and hiding operations are performed which makes the system more complex. The scheme we have proposed which includes combination of Honey Encryption and AES for password and AES and Steganography for data. User provides a password and data to upload, based on the password multiple random passwords are generated and encrypted while the data is encrypted and steganography is performed with zip based data compression.

System Module

Random password: These are passwords which no one knows and are generated with the function combining password with user data during registration process.

Random Password= (Password + User data) x Encrypt part

Password: This is the dynamic part of the random password, which is provided by the user and some string modifications are performed to get plausible password.

User data: It is the static part of the random password. It is the data provided by user during registration process which is used to combine with password.

Encrypt part: It is a static part of the random password. It uses AES encryption scheme to encrypt the generated random password and the correct password.

Data processed: This is the processed data obtained by processing the data by combining encryption and data hiding schemes.

Data Processed = Data x Encrypt part x Data compression x Data hiding part

Data: It is the data which may be any multimedia content user want to upload.

Encrypt part: It is a static part in data processed, where the data is encrypted using AES.

Data compression: It is a static part in data processed, where the encrypted data is compressed and the compression ratio varies based on the data.

Data hiding part: It is a process in which the encrypted data is hidden behind multimedia content before data upload.

Methodology: The proposed scheme of our project is derived after keen analysis of password storage schemes introduced over course of time. Also, we deploy a scheme of password storage and a scheme of data storage.

Registration Phase. This phase involves following steps

- The User is asked to provide basic details such as email, DOB, First name, Last name, Password which is a combination of lowercase, uppercase, number and special character.

Example: ABCabc@123

- The User provided password is then used to generate random passwords similar to correct password using some combination of password with DOB.

Example: password: ABCabc@123, generated password: aBcAbC@123

- The output list is then encrypted using AES encryption and again stored in list.
- The cipher text of passwords are then stored in database in a shuffled order.

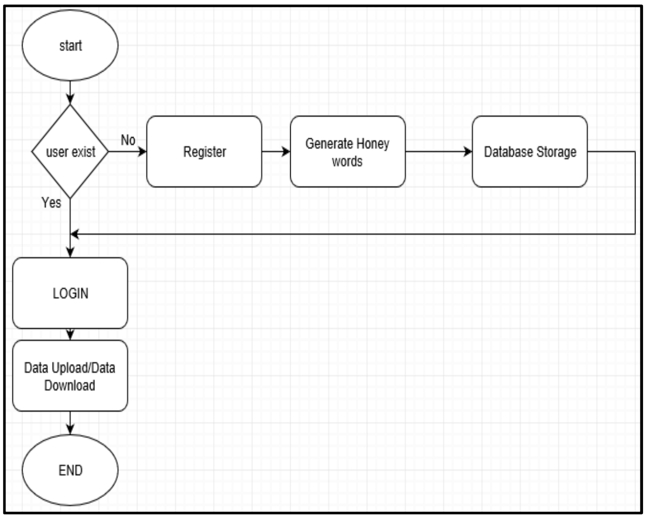

Figure 1. Flow Chart of User Process

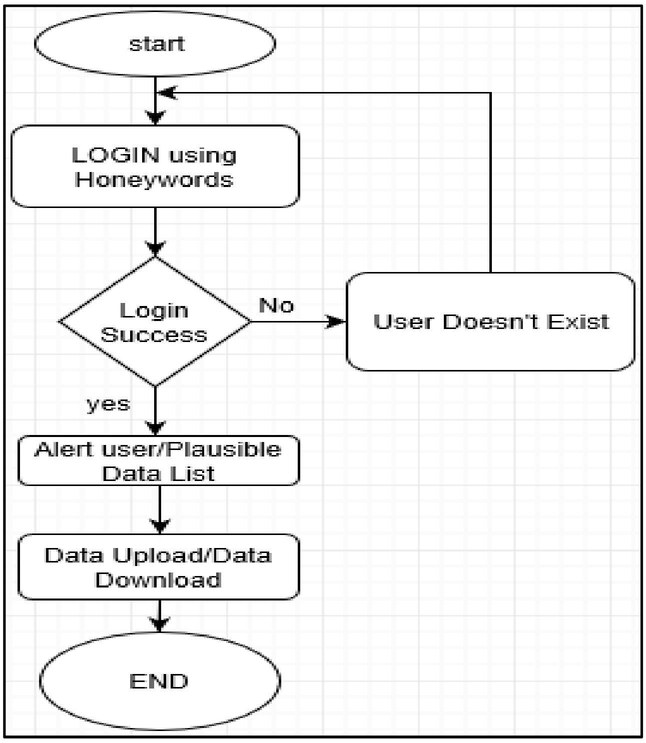

Figure 2. Flow Chart of Attacker process

Data Storage Phase. This phase involves following steps

- The user password is used for AES encryption process on data.
- The encrypted data is compressed under zip data compression schemes.
- The compressed data is processed through steganography scheme that hides the data behind multimedia content.
- The final process is that the processed data is uploaded on database and a reference is stored with password in database.

Data Access Phase. This phase involves following steps

- During Login stage, the user/attacker has to provide username and password.
- This username stored in database is accessed and password is matched with the list of passwords.
- If the user password and password from list matches then data's associated with passwords are displayed and if no password matches then a prompt displaying "wrong credentials" is prompted.
- After login occurs a list of data is available which when downloaded then the reverse steganography provides a compressed data which on decompression provides an encrypted data on which decryption is done using password provided by user during login.

Conclusion

To provide security we could either use cryptography or steganography. But we have proposed a system that provides security at various layers. Layer 1 involves Encryption (Honey + AES), Layer 2 involves Compression and Layer 3 involves Steganography (MSB bits).In the proposed system, the steganography method uses MSB image steganography technique to transfer data securely. This system can be further extended to provide better security, by using more secure steganography techniques like video steganography, Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT).

REFERENCES

Ari Juels, 2014. Thomas Ristenpart, "Honey Encryption: Encryption beyond the Brute-Force Barrier", in IEEE Security & Privacy, pp. 59-62.

Baby Shamini, P., Dhivya, E., Jayasree, S., Pavithra and Lakshmi, " Detection and avoidance of attacker using honey words in purchase portal", 2017 Third International Conference on Science Technology Engineering & Management (ICONSTEM).

Ammad Ul Islam, Faiza Khalid, Mohsin Shah, Zakir Khan, Toqeer Mahmood, Adnan Khan and Muhammad Naeem, "An improved image steganography technique based on MSB using bit differencing" in 2016. *Sixth International Conference on Innovative Computing Technology (INTECH).*

****