Encrypted Negative Password Using ELGAMAL

A Sandeep Kumar Reddy[1], K V H N Vishnuvardhan[2]
[1]*PG Student, Dept of CSE, Indira Institute of Technology & Sciences, Markapur*
[2]*Asst.Professor, Dept of CSE, Indira Institute of Technology & Sciences, Markapur*

Abstract **- Secure password storage is a in systems major fact based on password authentication, which has been widely used in authentication technique. Proposing a password authentication framework that is designed for secure password storage and it can be easily integrated into existing authentication systems. First, the received plain password from a client side is hashed using a cryptographic hash function. Then, hashed password is converted into a negative password. Finally, the received negative password is encrypted into an Encrypted Negative Password (abbreviated as ENP) using a symmetric-key algorithm. Using multi-iteration encryption could be employed to further improve security. Both the cryptographic hash function and symmetric encryption make it difficult to crack passwords from ENPs. The Elgamal is a asymmetric encryption algorithm that uses a pair of public key and a private key to encrypt and decrypt messages when communicating. Most importantly, the ENP is the first password protection scheme that combines the cryptographic hash function, the negative database, and the Elgamal Algorithm. This Encrypted Negative Password system still can resist the precomputation attacks. Thus, by securing the cloud servers with negative password system, all these vulnerabilities can be reduced**

Index Terms **- Cloud, Elgmal, Negative Passwords, Security.**

I.INTRODUCTION

By the large development of the Internet, a huge number of online services have emerged, which password authentication is the most widely used authentication technique, for it is available at a low cost. Password security always attracts great interest from academia and industry. Because of careless behavior of the users password has been cracked, hence password authentication technique has been increasing. For instance, many of the users select weak passwords so that it can be reuse same passwords in different systems. Because they set their password according to their familiar vocabulary. It is very difficult to obtain passwords from high security systems. On the other side stealing authentication data tables (containing usernames and passwords) in high security systems is difficult. The aim of the project is to enhance password security. When carrying an online guessing attack, there is a limit to the number of login attempts. However, passwords can be leaked from weak systems. Some old systems are more vulnerable due to their lack of maintenance. The passwords are often reused, adversaries may log into high security systems through cracked passwords from low security systems. There are lots of corresponding ENPs for a given plain password, which makes attacks (e.g., lookup table attack and rainbow table attack infeasible. The complexity analyses of algorithm and comparisons show that the ENP could resist lookup table attack and provide stronger password protection under dictionary attack. It is mentioning that the ENP does not introduce extra elements (e.g. salt). Most importantly, the ENP is the first password protection scheme that combines the cryptographic hash function, the negative password and the asymmetric-key algorithm without the need of any for additional information except the plain password. The key certificates have been used to authenticate the user's key pair. Finally, the received encrypted negative password is again encrypted using the Elgamal algorithm to improve the security of the password.

II. LITERATURE SURVEY

A. Typical Password Protection Schemes Some of the password protection schemes are hashed password, salted password and key stretching.

1) Hashed Password: The simple way to store passwords is to directly store plain passwords. However, this scheme presents a problem that once adversaries has been obtain the authentication data table, all passwords are immediately compromised. To store safely hash passwords using a cryptographic

hash function, because it is infeasible to recover plain passwords from hashed passwords. The cryptographic hash function maps the data of arbitrary size to a fixed-size sequence of bits. In the authentication system that using the hashed password scheme, only hashed passwords are stored. However, hashed passwords do not resist lookup table attack. Rainbow table attack is more practical for its space-time trade off. Processor resources and storage resources are becoming richer, so the precomputed tables used in the above two attacks become large, so that adversaries obtain a higher success rate of cracking hashed passwords. 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. The cryptographic hash function quickly maps data of arbitrary size to a fixed-size sequence of bits. In the authentication system using the hashed password scheme, only hashed passwords are stored. However, hashed passwords cannot resist lookup table attack. Furthermore, rainbow table attack is more practical for its space-time trade off. Processor resources and storage resources are becoming richer, which makes the precomputed tables used in the above two attacks sufficiently large, so that adversaries could obtain a higher success rate of cracking hashed passwords.

2) Salted Password:

To resist precomputation attacks, the most common scheme is salted password. In this scheme, the concatenation of a plain password and a random data (called salt) is hashed through a cryptographic hash function. The salt is usually generated at random, which ensures that the hash values of the same plain passwords are almost always different. The greater the size of the salt is, the higher the password security is. However, under dictionary attack, salted passwords are still weak. Note that compared with salted password, the ENP proposed in this project guarantees the diversity of passwords without the need for extra elements (e.g., salt).

3) Key Stretching:

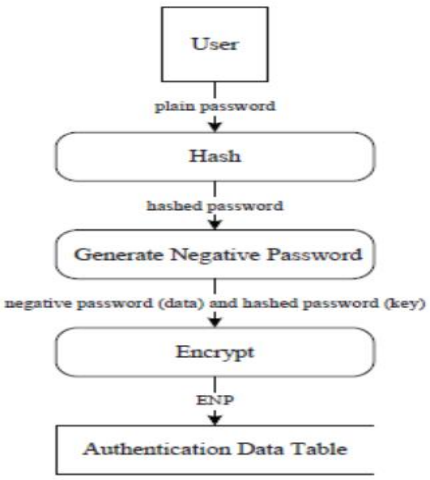
To resist dictionary attack, key stretching, which converts weak passwords to enhanced passwords, was proposed. Key stretching could increase the time cost required to every password attempt, so that the power of defending against dictionary attack is increased. In the ENP proposed in this project, like key stretching, multi-iteration encryption is used to further improve password security under dictionary attack, and compared with key stretching, the ENP does not introduce extra elements (e.g., salt)

III. APPLICATIONS

By securing the password the online sites can provide security and protected from the cracking password. Passwords in the authentication data table presented in the form of hashed passwords. Processor resources and storage resources are becoming more and more abundant, so that the hashed passwords cannot resist precomputation attacks, such as rainbow table attack and lookup table attack. Moreover, they download and use attack tools without the need of any professional security knowledge. Some 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 grand higher demand for secure password storage. In these situations, attacks are usually carried such as adversaries pre compute a lookup table, where the keys are the hash values of elements in a password list which contains frequent used passwords, and the records displayed are corresponding plain passwords in the password list. From the low security system generate an authentication data table. Finally, they search for the plain passwords in the lookup table with corresponding matching hashed passwords in the authentication data table and the keys in the lookup table. Then, by log into higher security systems through cracked usernames and passwords, they could steal more sensitive information of users. One of the main advantages that above lookup table attack is that the corresponding hashed password is determined for a given plain password. So that the lookup table could be quickly constructed, and the size of the lookup table could be large, which result in high success rate of cracking hashed passwords.

IV. PROPOSED SYSTEM

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 their 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.



Architecture Explanation

The proposed framework includes two phases: the registration phase and authentication phase. When adopting our framework to protect passwords in an authentication data table, the system designer must first select a cryptographic hash function and a symmetric-key algorithm, where the condition that must be satisfied is that the size of the hash value of the selected cryptographic hash function is equal to the key size of the selected symmetric-key algorithm. For convenience, some matches of cryptographic hash functions and symmetric-key algorithms are given. In addition, cryptographic hash functions and symmetric-key algorithms that are not listed here could also be used in the ENP, which adequately indicates the flexibility of our framework. The proposed framework is based on the ENP; hence, for better understanding, the data flow diagram of the generation procedure of the ENP is shown in Fig. 4.11, and the data flow diagram of the verification procedure of the ENP is shown in Fig. 1.

In Existing system Hashed Passwords with Symmetric Encryption security is provided. However, this scheme presents a problem that once adversaries obtain the authentication data table, all passwords are immediately compromised. The cryptographic hash function quickly maps data of arbitrary size to a fixed-size sequence of bits. In the authentication system using the hashed password scheme, only hashed passwords are stored. However, hashed passwords cannot resist lookup table attack. Furthermore, rainbow table attack is more practical for its space-time tradeoff.

Disadvantages

- Symmetric cryptosystems have a problem of key transportation.
- The secret key is to be transmitted to the receiving system before the actual message is to be transmitted.
- System is not secured due to lack of improved dynamic Key-Hashed Message Authentication Code function (abbreviated as d-HMAC).
- Password protection scheme called Encrypted Negative Password is absent.

PROPOSED SYSTEM

In the proposed system, a password protection scheme called Encrypted Negative Password (abbreviated as ENP) is proposed, which is based on the Negative Database (abbreviated as NDB), cryptographic hash function and asymmetric encryption, and a password authentication framework based on the ENP is presented. The NDB is a new security technique that is inspired by biological immune systems and has a wide range of applications. Asymmetric encryption is usually deemed inappropriate for password protection. To summarize, the main contributions of this project are as follows: The system also proposes a password protection scheme called ENP, and we propose two implementations of the ENP: ENPI and ENPII, including their generation algorithms and verification algorithms. Furthermore, a password authentication framework based on the ENP is presented. The system analyzes and compares the attack complexity of hashed password, salted password, key stretching and the ENP. The results show that the ENP could resist lookup table attack without the need for extra elements and provide

Advantages

- Proposed Asymmetric key uses a pair of public and private keys.
- The primary advantage of asymmetric cryptography is increased security: the private keys do not ever need to be transmitted or revealed to anyone.
- Can provide digital signatures that can be repudiated
- The system more powerful password scheme by dynamic salt generation and placement are used to improve password security.

Application Modules

Client Module

1. 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 exists in the authentication data table, “The username already exists!” is displayed, which means that the server has rejected the registration, and the registration phase is terminated; otherwise, go to Step (3);
3. Then the received password is hashed using the selected cryptographic hash function
4. The received password is hashed using the selected cryptographic hash function.
5. The hashed password is converted into a negative password using an NDB generation algorithm.
6. The negative password is encrypted to an ENP using the selected asymmetric-key algorithm, where the key is the hash value of the plain password. Here, as an
7. Additional option, multi-iteration encryption could be used to further enhance passwords.
8. 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 Module

The authentication phase is divided into five steps.

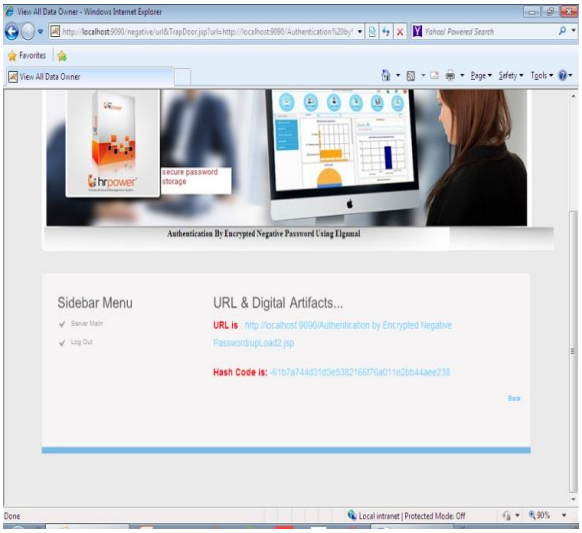
1. On the client side, a user enters his/her username and password. Then, the username and plain password are transmitted to the server through a secure channel.
2. If the received username does not exist in the authentication data table, then “Incorrect username or password!” is returned, which means 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 asymmetric-key algorithm, where the key is the hash value of the plain password; thus, the negative Password is obtained

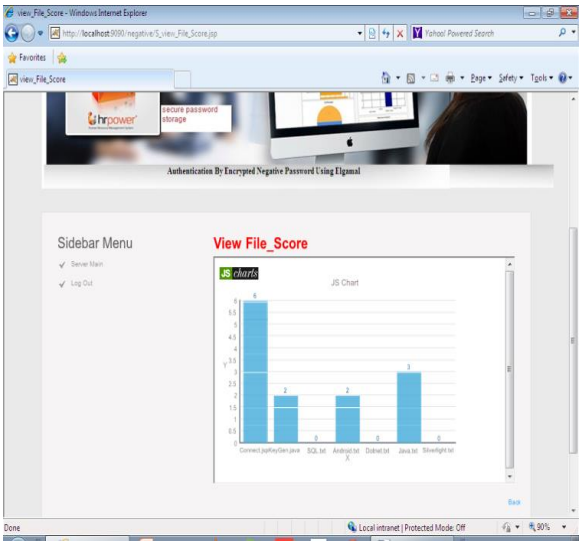
Authenticated Negative Passwords Using ELGAMAL Module

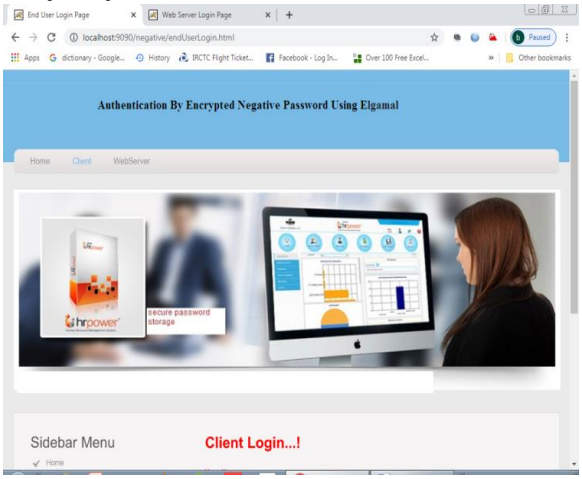
This module provides user to secure their passwords using hash function, the asymmetric-key Elgamal algorithm. The cryptographic hash function converts plain passwords to hashed passwords; the fixed length property of resulting hashed passwords offers convenience for the subsequent encryption, since the length requirement for the secret keys (private and public) in the asymmetric key algorithm; and other properties (such as avalanche effect and collision resistance) are also crucial factors of employing the cryptographic hash function

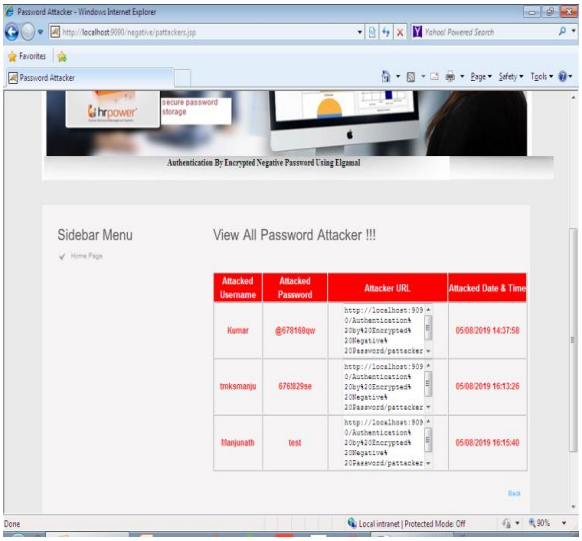
V.RESULTS

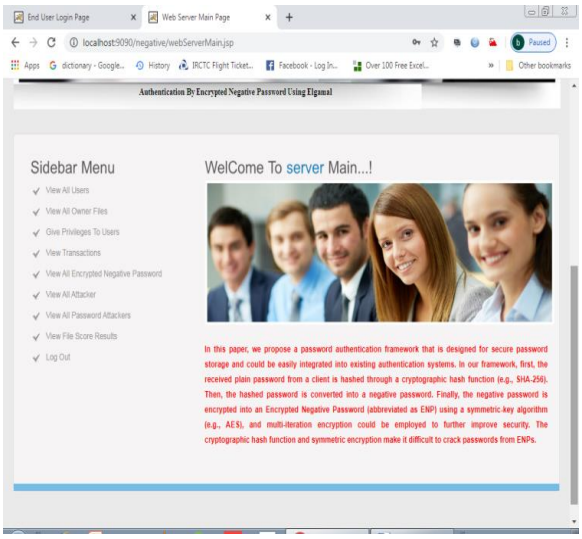
A set of experiments carried out on stress analysis data obtained from internet sources. The performance evaluation of the system is performing using this dataset. The screenshots of various phases of stress analysis system are as follows

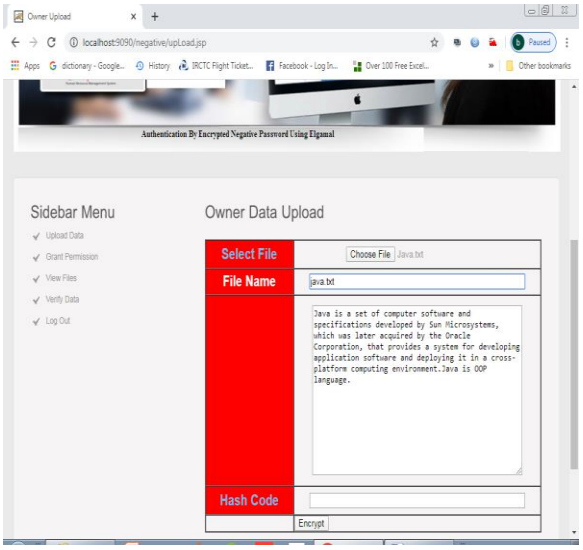


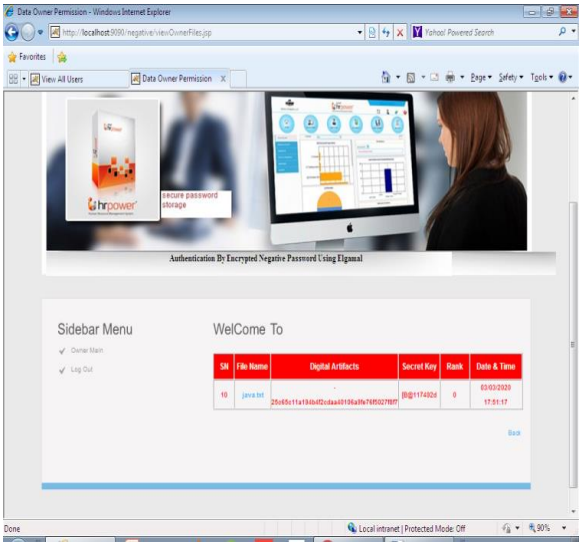












VI.CONCLUSION

In this paper, we proposed a password protection scheme called ENP, and presented a password authentication framework based on the ENP. In our framework, the entries in the authentication data table are ENPs. In the end, we analyzed and compared the attack complexity of hashed password, salted password, key stretching and the ENP. The results show that the ENP could resist lookup table attack and provide stronger password protection under dictionary attack. It is worth mentioning that the ENP does not need extra elements (e.g., salt) while resisting lookup table attack. 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.

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. Kala pa, 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