Authentication using Encrypted Negative Password

Dr. T Shyam Prasad, Sai Vamshi Kondapaka, Neha Reddy Lega, Anish Chandra K

1 Assistant Professor - Department of Computer Science and Engineering ,2 IV year Department of Computer Science And Engineering ,3 IV year Department of Computer Science And Engineering, 4 IV year Department of Computer Science And Engineering

Anurag University, Ghatkesar, Hyderabad, India

1[shyamprasadcse@anurag.edu.in](mailto:shyamprasadcse@anurag.edu.in) , 2[20eg105356@anurag.edu.in](mailto:20eg105356@anurag.edu.in), 3[20eg105358@anurag.edu.in](mailto:20eg105358@anurag.edu.in) 4.[20eg105355@anurag.edu.in](mailto:20eg105355@anurag.edu.in).

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Abstract** - This abstract introduces Encrypted Negative Password Authentication (ENPA) as an innovative approach to address these challenges. ENPA enhances security by minimizing the exposure of sensitive information. Even in the event of a data breach, adversaries gain no advantage as the negative passwords are never stored in a recoverable format. Additionally, incorporating encryption and hashing techniques mitigates risks associated with common attacks such as rainbow table attacks.

**Index Terms** – Encrypted Negative Password(ENP), Encrypted Negative Password Authentication (ENPA) ,Secured Hashing Algorithm(SHA), Message Digest 5(MD5), Advanced Encryption Standard(AES), Negative Database(NDB)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# **Introduction**

Password security is a topic that garners attention from both industry circles. Despite the advancements, in password security research passwords continue to be compromised due to users negligent actions. For example many individuals opt for passwords tend to use the password across multiple platforms and often choose easily memorable words, for their passwords. Furthermore system vulnerabilities can lead to password breaches. Acquiring passwords from secure systems poses challenges as stealing authentication data tables containing user credentials is no task. Additionally online guessing attacks are usually limited in the number of login attempts allowed. However weaker systems may expose passwords to leaks. With discoveries of vulnerabilities and not all systems being promptly updated against threats cyber adversaries find openings to illicitly access systems. Lastly the practice of password reuse can enable attackers to infiltrate high security systems using compromised passwords from platforms.

**I.I.BACKGROUND**

Password storage schemes are fundamental components of authentication systems, responsible for securely storing and managing user passwords. The evolution of password storage schemes has been driven by the need to address security vulnerabilities and adapt to emerging threats in the ever-changing landscape of cybersecurity.

Different Types of Password Storage Methods:

* Plaintext Storage: This is the most basic and least secure method where passwords are stored as-is, without any encryption or hashing. In this method, passwords are easily readable if attackers gain unauthorized access to the storage system.
* Cryptographic Hashing: Passwords are hashed using cryptographic algorithms such as MD5, SHA-1, SHA-256, etc. The hash function converts passwords into fixed-length hash values, making it computationally infeasible to reverse-engineer the original password from the hash.
* Salted Hashing: In this method, a unique random value (salt) is added to each password before hashing. Salting prevents identical passwords from producing the same hash, making it more difficult for attackers to use precomputed tables (rainbow tables) for password cracking.
* Key Stretching: Key stretching techniques, such as PBKDF2 (Password-Based Key Derivation Function 2), bcrypt, and scrypt, introduce computational overhead by repeatedly applying a hashing function to the password. This slows down the password hashing process, making it more time-consuming for attackers to crack passwords.
* ENP: ENP (Encrypted Negative Password) is a pioneering approach to authentication that prioritizes user privacy and security. Users create passwords that are then converted into negative passwords. The system encrypts and securely stores hashed versions of these passwords on the server, enhancing resilience against common attacks. With ENP, users can enjoy a streamlined and secure authentication experience while minimizing the risk of unauthorized access to their accounts.

Password storage space systems are essential parts of verification systems in charge of safely keeping along with taking care of customer passwords. The advancement of password storage space systems has actually been driven by the demand to attend to protection susceptabilities coupled with adjust to arising hazards in the ever-changing landscape of cybersecurity.

Various Kinds of Password Storage Methods:

* Plain Storage: This is one of the most standard along with the very least protected approach where passwords are saved unedited, without any file encryption or hashing. In this approach, passwords are conveniently legible if aggressors get unapproved accessibility to the storage space system.

* Cryptographic Hashing: Passwords are hashed making use of cryptographic formulas such as MD5, SHA-1, SHA-256 and so on. The hash feature transforms passwords right into fixed-length hash worths making it computationally unwise to reverse-engineer the initial password from the hash.

* Salted Hashing: In this technique an one-of-a-kind approximate worth (salt) is contributed to each password prior to hashing. Salting avoids similar passwords from creating the very same hash making it harder for assaulters to utilize precomputed tables (bow tables) for password splitting.

* Secret Stretching: Key extending methods such as PBKDF2 (Password-Based Key Derivation Function 2), bcrypt plus scrypt present computational expenses by consistently using a hashing feature to the password. This decreases the password hashing procedure making it even more lengthy for assaulters to fracture passwords.

* ENP: ENP (Encrypted Negative Password) is an introducing method to verification that focuses on individual personal privacy together with protection. Customers produce passwords that are after that exchanged adverse passwords. The system secures along with safely shops hashed variations of these passwords on the web server, boosting durability versus typical strikes. With ENP customers can take pleasure in a structured as well as safe and secure verification experience while lessening the threat of unapproved accessibility to their accounts.

# **Literature survey**

# **II.I  Concerns and Security for Hashing Passwords**

**Authors, Year : Jonathan Herrera; Md Liakat Ali**, 2019.

The aim of this paper is to discuss current concerns with hashing and propose a new system level approach that will add an extra layer of security for storing passwords. The greatest security threat is bad security practices. One sees with some of the greatest hacks, resulting in some of the greatest losses, it was because of bad security practices. It is important to have security for passwords that are designed to last many years once implemented.

**II.II.** **Salty Secret: Let us secretly salt the secret**

**Authors, Year :** E M Wasifur Rahman Chowdhury , M Saifur Rahman, A. B. M. Alim Al Islam, Mohammad Sohel Rahman , 2017.

Using password is, perhaps, still the most versatile method of securing secret and confidential information, even though several recent studies have pointed out possibility of breaching it. A general trend of having different passwords for several user accounts of the same user (such as multiple email accounts, multiple social networking accounts, etc.) can barely overcome the possibility as users mostly prefer retaining similarity among own passwords, which results in the possibility of breaching almost all passwords once only one password gets breached. Consequently, several research studies attempted to strengthen passwords. However, none of the studies is yet to get wide popularity for not being able to achieve a delicate balance between strength of password and user friendliness. To achieve this goal, we present a new password based authentication system in this paper. The proposed system is based on intermixing between a fixed text (conventional part of a password) and a free random text (newly added) at different pre-defined indices having different per-defined lengths. The addition of the free random text adds an additional level of difficulty in breaching the password. We present different variants of our proposed system along with their possible attack models. We demonstrate strength of our proposed system through rigorous analytical formulation and numerical simulation. Besides, we confirm achieving a delicate balance between strength of the password and user friendliness through performing real user evaluation.

**II.III.** **On the Economics of Offline Password Cracking**

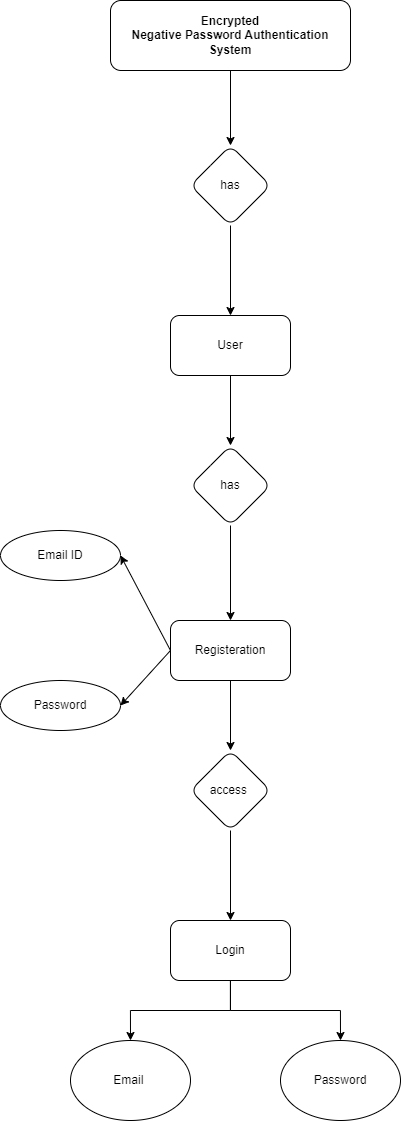
**Authors, Year:** Jeremiah Blocki, Ben Harsha, Samson Zhou, 2020.

We develop an economic model of an offline password cracker which allows us to make quantitative predictions about the fraction of accounts that a rational password attacker would crack in the event of an authentication server breach. We apply our economic model to analyze recent massive password breaches at Yahoo!, Dropbox, LastPass and AshleyMadison. All four organizations were using key-stretching to protect user passwords. In fact, LastPass' use of PBKDF2-SHA256 with 105 hash iterations exceeds 2017 NIST minimum recommendation by an order of magnitude. Nevertheless, our analysis paints a bleak picture: the adopted key-stretching levels provide insufficient protection for user passwords.

# **Encrypted Negative Password**

Encrypted Negative Password is the password storage scheme that we are focusing on in this paper. Like key stretching, it gives high security against lookup table attacks and dictionary attacks. The Encrypted Negative Password (ENP) storage mechanism is a novel approach to securely store user passwords while prioritizing privacy and security.

* The system consists of two main modules: Registration and Login/Authentication. In the Registration module, users are required to input their Email ID and a chosen password. The system then proceeds to hash the received plain password using a cryptographic hash function and converts it into a negative password through a Negative Database (NDB) generation algorithm. The negative password is encrypted using the AES algorithm, and the user's email, hashed password, negative password, and encrypted password are securely stored in the database.
* For the Login/Authentication module, users need to provide their Email ID and password. Upon entering, the system checks the existence of the username in the authentication data table. If found, it retrieves the corresponding Encrypted Negative Password (ENP) and decrypts it using the AES algorithm. The negative password is then obtained through decryption, completing the authentication process.



**III.I. Modules and their Description**

The system comprises 1 major module with their sub-modules as follows:

**Module:**

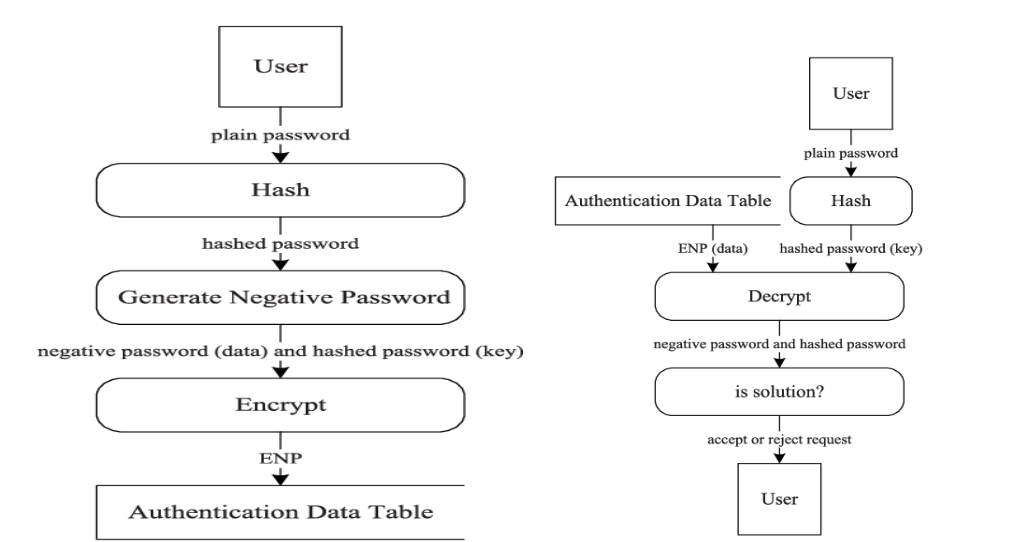
1. **Registration:**

* The user will have to enter their Email ID.
* They can enter a password.
* Hash the received plain password using a selected cryptographic hash function.
* Convert the hashed password into a negative password using an NDB (Negative Database) generation algorithm.
* Encrypt the negative password using an AES algorithm.
* Store the user's email, hashed password, negative password, and encrypted password in the database.

**2. Login/Authentication:**

* To log in, the user will have to enter their Email ID and password.
* If the username exists, search the authentication data table for the Encrypted Negative Password (ENP) corresponding to the received username.
* Decrypt the ENP using the AES algorithm.
* Obtain the negative password by decrypting the ENP.

**Concept Tree:**



**III.II Parameter Formulas:**

**1. Hashing Formula:** HashedPassword= HashFunction(Password+Salt).

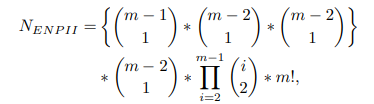
**2.Encryption Formula:** EncryptedData= EncryptionAlgo(Data, EncryptionKey)

**3. Negative Authentication Criteria:** Define conditions like FailedAttempts > Threshold or SuspiciousBehaviour == True

**4. Monitoring Criteria:** Define criteria for triggering alerts, such as Multiple\_Failed\_Logins or Unsusual\_Access\_Pattern.

**5. Key Management:** KeyRotationPeriod= Interval for changing encryption/decryption keys.

**6. Number of ENP Generated:** The number of ENPs converted from a plain password is calculated by



**7.** **Performances of ENP** : The time complexity of the generation of ENP is O(m2 ), and the time complexity of the verification of ENP is also O(m2 ), where m is the length of the hashed password. Since the length of the hashed passwords in the ENP is smaller, the generation and verification of the ENP are efficient.

**III.III. Features/Advantages of ENP:**

The major advantages of the proposed system in this paper are as mentioned below:

* Enhanced Security:

Utilizes cryptographic hash functions to securely store and protect user passwords in the authentication database.

Incorporates negative authentication criteria to detect and prevent unauthorized access attempts, enhancing security against various attacks such as brute force and dictionary attacks.

Employs symmetric-key encryption to ensure the confidentiality and integrity of authentication data during transmission between the client and server, mitigating the risk of eavesdropping attacks.

* Usability:

Maintains a user-friendly interface, allowing users to securely authenticate with their passwords without significant additional complexity.

Provides a seamless registration and login process, minimizing friction for users while ensuring robust security measures are in place.

Offers flexibility in handling authentication attempts, allowing users to authenticate securely from various devices and locations.

* Scalability:

Designed to scale effectively to accommodate a growing user base and increasing authentication demands.

Utilizes efficient cryptographic techniques and authentication mechanisms to ensure optimal performance even under high load conditions.

* Flexibility:

Adaptable to different authentication requirements and security policies, allowing organizations to customize authentication parameters based on their specific needs.

Integrates seamlessly with existing authentication systems and infrastructures, enabling organizations to leverage their current investments while enhancing security measures.

* Resilience Against Attacks:

Provides resilience against common password-based attacks such as brute force, dictionary, and rainbow table attacks through the use of cryptographic hash functions and negative authentication criteria.

Enables proactive detection and mitigation of suspicious activities through continuous monitoring and evaluation of negative authentication criteria.

* Compliance and Regulatory Alignment:

Helps organizations align with regulatory requirements and industry best practices related to password security and data protection.

Facilitates compliance with standards such as GDPR (General Data Protection Regulation), HIPAA (Health Insurance Portability and Accountability Act), and PCI DSS (Payment Card Industry Data Security Standard).

* User Trust and Confidence:

Enhances user trust and confidence in the authentication system by implementing robust security measures and safeguarding user credentials against unauthorized access.

Demonstrates a commitment to protecting user privacy and confidentiality, fostering positive user experiences and long-term user relationships.

* Future-Proofing:

Positions organizations for future advancements in authentication technology and evolving cybersecurity threats by adopting a forward-thinking approach to password security.

Provides a foundation for integrating additional authentication factors and advanced security features to address emerging threats and enhance overall security posture.

# **COMPARISONS**

**IV.I.** Comparison of Existing Strategies for Problem solving:

|  |  |  |  |
| --- | --- | --- | --- |
| Sl.No | Strategies | Advantages | Disadvantages |
| 1. | Text-based passwords | Easy to implement, Cost-effective, flexible for users, Most-Popular method. | Security Concerns, User behavior, Password Management. |
| 2. | Biometric Authentication | High security, Difficult to forge. | Cost, Privacy concerns, Spoofing risks. |
| 3. | Time-Based One-Time Password (TOTP) | Dynamic Security codes, cost-effective | Time-dependent, Device-dependent, Potential for Interception. |
| 4. | Token-based Authentication | Difficult to replicate, Multiple Authentication factors. | Cost, Token loss, Logistics. |
| 5. | Graphical Password Authentication | Memory recall, Resistance to keyloggers, Customization. | Limited security, Shoulder surfing, Usability issues, limited adaptation. |
| 6. | Multi-Factor Authentication (MFA) | Enhanced security, Strong User verification, Reduced risk of unauthorized access | Complexity, Usability, Cost of Implementation, Dependency on device, Integration challenges. |

**IV.II.** Comparison of Existing Method from selected Strategies (Text- Based Password storage methods) :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sl.No | Author | Strategies | Advantages | Disadvantages |
| 1. | [Jonathan Herrera](https://ieeexplore.ieee.org/author/37086944928); [Md Liakat Ali](https://ieeexplore.ieee.org/author/37085649038) | Hashed-Password | Easy to use and implement. One-way transformation, Consistency. | Brute-force attacks, dependency on hash algorithm entirely, collision vulnerabilities, Dictionary attacks. |
| 2. | [E M Wasifur Rahman Chowdhury](https://ieeexplore.ieee.org/author/37086161596); [M Saifur Rahman](https://ieeexplore.ieee.org/author/37089215860); [A. B. M. Alim Al Islam](https://ieeexplore.ieee.org/author/38061107100); [M Sohel Rahman](https://ieeexplore.ieee.org/author/37089215860) | Salted-Password | Unique hash values, Randomization, Scalability. | Implementation complexity, Storage overhead, Incompatibility, Salt visibility, Increased Computation time. |
| 3. | [Jeremiah Blocki](https://ieeexplore.ieee.org/author/37947782900); [Benjamin Harsha](https://ieeexplore.ieee.org/author/37086420588); [Samson Zhou](https://ieeexplore.ieee.org/author/37085995887) | Key-Streching | Resistant to brute-force attacks, Customizable iterations. | Increased computational overhead, Resource intensiveness, Potential DOS attacks, bad user experience. |
| 4. | [Laurentius Kuncoro Probo Saputra](https://ieeexplore.ieee.org/author/37087467848); [Willy Sudiarto Raharjo](https://ieeexplore.ieee.org/author/37087472715) | Password-Based Key Derivation Function (PBKDF2) | Customizable iterations, Supported by wide range of programming languages. | Susceptible to brute-force attacks using GPU acceleration due to its simple structure. |
| 5. | Wenjian Luo, Yamin Hu, Hao Jiang, and Junteng Wang | Encrypted Negative Password  (ENP) | Resistance to Lookup table attack, resistance to dictionary attack, User friendly experience with secure password storage. | Complexity compared to other methods. |

# **CONCLUSION**

In final thought "Encrypted Negative Password Authentication System" stands for a considerable development in password safety offering a durable plus efficient service to reduce the susceptabilities related to typical password-based verification techniques. With the combination of cryptographic hash features unfavorable verification requirements along with symmetric-key security ENP attends to crucial obstacles in verification while improving safety and security plus functionality.

Among the key benefits of ENP is its capacity to offer improved safety procedures without giving up functionality. By safely hashing passwords and integrating unfavorable verification requirements ENP successfully safeguards versus usual password-based strikes such as strength plus thesaurus assaults. Additionally using symmetric-key security makes certain the privacy together with stability of verification information securing versus eavesdropping as well as interception.

Furthermore, ENP supplies versatility and also scalability allowing companies to customize verification criteria to satisfy their certain protection needs as well as fit expanding customer bases. Its versatility to existing verification systems as well as regulative conformity criteria even more improves its attract companies looking for to improve their cybersecurity position while sticking to sector laws.

By growing individual trust fund as well as self-confidence with the execution of durable protection actions ENP advertises favorable customer experiences as well as lasting customer partnerships. Companies taking on ENP show a dedication to shielding customer personal privacy together with discretion straightening with progressing cybersecurity finest techniques as well as regulative needs.

Finally ENP stands for a transformative strategy to password safety and security, supplying companies a detailed remedy to reinforce verification systems together with shield delicate details from harmful stars. With its mix of durable safety steps, functionality coupled with scalability ENP arises as a keystone of contemporary cybersecurity, encouraging companies to guard their electronic possessions as well as keep individual count on an ever-changing risk landscape.

**VI. 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.

[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. Kalapa, 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.

[20] International Journal of Trend in Scientific Research and Development (IJTSRD) Volume 4 Issue 6, September-October 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470 @ IJTSRD | Unique Paper ID – IJTSRD35711 | Volume – 4 | Issue – 6 | September-October 2020 Page 1597 Encrypted Negative Password using for Authentication Priya K P1, Dr. Lakshmi J. V. N2

[21] Authentication by Encrypted Negative Password Wenjian Luo, Senior Member, IEEE, Yamin Hu, Hao Jiang, and Junteng Wang Citation information: DOI 10.1109/TIFS.2018.2844854, IEEE Transactions on Information Forensics and Security