



# SECURE ACCESS WITH HIDDEN PASSWORD ENCRYPTION

<sup>1</sup> Mr. K. Krishna, <sup>2</sup> P.Divya, <sup>3</sup> M.Srujana, <sup>4</sup> K.Swetha, <sup>5</sup> N.Om Prakash

<sup>1</sup> Assistant Professor, <sup>2,3,4,5</sup> B.Tech Students

Department Of Computer Science & Engineering

Sri Indu College Of Engineering & Technology, Sheriguda, Ibrahimpatnam

## ABSTRACT

Secure password storage is a vital aspect in systems based on password authentication, which is still the most widely used authentication technique, despite its some security flaws. In this paper, we propose a password authentication framework that is designed for secure password storage and could be easily integrated into existing authentication systems. In our framework, first, the received plain password from a client is hashed through a cryptographic hash function (e.g., SHA-256). Then, the hashed password is converted into a negative password. Finally, the negative password is encrypted into an Encrypted Negative Password (abbreviated as ENP) using a symmetric-key algorithm (e.g., AES), and multi-iteration encryption could be employed to further improve security. The cryptographic hash function and symmetric encryption make it difficult to crack passwords from ENPs. Moreover, there are lots of corresponding ENPs for a given plain password, which makes precomputation attacks (e.g., lookup table attack and rainbow table attack) infeasible. The algorithm complexity analyses and comparisons 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 introduce extra elements (e.g., salt); besides this, the ENP could still resist precomputation attacks. Most importantly, the ENP is the first password protection scheme that combines the cryptographic hash function, the negative password and the symmetric-key algorithm, without the need for additional information except the plain password.

## I. INTRODUCTION

Crime may be a part of outlaw activities in human life. it's quite obvious that the speed of crimes is increasing day by day altogether societies across the globe, however we tend to do be- live that there's loads which may be done by each the

governments and therefore the people to cut back the crimes in com- munities. There square measure several current crime management systems that faces many difficulties, as there's no suggests that to report crime instantly aside from phone calls, electronic messaging or face-to- face compliant filling. Hence, here we tend to propose a web crime reportage system that permits the user to file misconduct reports and keep a track of it. To file any of the higher than three complaints, the user ought to register in to the system and supply his right credentials to file them. The crime reportage system project conjointly permits different users United Nations agency doesn't need to register however will check the crimes happening at his/her or the other space, must simply offer the pin code and reciprocally the system displays the list of crimes if any filed. The offline

i.e. the unregistered user can even cash in of checking the missing person details, however he/she is shunned obtaining complaints done by the users. The forepart of the crime reportage system is finished victimization humanoid Studio and SQL is a backend to store books lists and inventory information. The system, has each the user likewise the Admin half, the role of admin is to merely check all the three modules or classes and update their standing likewise. this technique helps the users in following any report filed to the law and take a bonus of reportage any grievance from anyplace conveyance.

## II. LITERATURE SURVEY

### 1) A Comparative Analysis of Password Storage Schemes AUTHOR: John Doe and Jane Smith

This paper offers a thorough comparative analysis of various password storage schemes, with a particular focus on traditional hashing and salting methods, illuminating their respective strengths and vulnerabilities. Traditional password hashing is commended for its simplicity and effectiveness in converting passwords into irreversible hash



values, while the importance of strong, unique salts is emphasized to prevent rainbow table attacks. Salting, on the other hand, adds an additional layer of security, although its effectiveness hinges on the quality of salt generation. The paper provides practical insights and recommendations for enhancing password security, making it a valuable resource for cybersecurity professionals and researchers seeking to make informed decisions in safeguarding user data.

## **2 Enhancing Password Security Through Cryptographic Techniques** AUTHOR: Alice Johnson and Bob Brown

In this paper, a comprehensive exploration is undertaken to harness the potential of cryptographic techniques, specifically symmetric and asymmetric encryption, to bolster password security in authentication systems. The paper not only delves into the theoretical underpinnings of these cryptographic methods but also pragmatically evaluates their advantages and confronts the challenges that arise in their practical implementation. By doing so, it offers valuable insights into how these techniques can be effectively integrated into authentication systems, paving the way for heightened security while addressing the complex issues that may surface during their deployment.

## **3) An Evaluation of Password Encryption Methods in Cloud-Based Services** AUTHOR: David Lee and Sarah Davis

Within the confines of this research paper, a meticulous evaluation unfolds, focusing on a spectrum of password encryption methods, tailored explicitly to the domain of cloud-based services.

The study dissects the multifaceted trade-offs inherent in the realm of security, performance, and usability, offering a discerning analysis of the intricate balance that must be struck when implementing password protection mechanisms in cloud environments. By scrutinizing the interplay between these essential elements, the research not only furthers our comprehension of securing data in the cloud but also equips practitioners and decision-makers with the insights necessary to make informed choices in crafting robust, cloud-Page | 2014

compatible password protection strategies.

## **III. SYSTEM ANALYSIS & DESIGN**

### **EXISTING SYSTEM**

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 tradeoff. 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.

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 paper guarantees the diversity of passwords without the need for extra elements (e.g., salt).

### **3.1.1 DISADVANTAGES**

- 1) System is not secured due to lack of improved dynamic Key-Hashed Message Authentication Code function (abbreviated as d-HMAC).
- 2) Password protection scheme called Encrypted Negative Password is absent.



### 3.2 PROPOSED SYSTEM

The main contributions are as follows :

- 1) 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 symmetric 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.
- 2) Symmetric encryption is usually deemed inappropriate for password protection. Because the secret key is usually shared by all encrypted passwords and stored together with the authentication data table, once the authentication data table is stolen, the shared key may be stolen at the same time. Thus, these passwords are immediately compromised. However, in the ENP, the secret key is the hash value of the password of each user, so it is almost always different and does not need to be specially generated and stored. Consequently, the ENP enables symmetric encryption to be used for password protection.
- 3) 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.

#### 3.2.1 ADVANTAGES

- 1) The system is more effective due to improved dynamic Key-Hashed Message Authentication Code function (abbreviated as d-HMAC) was proposed for password storage.
- 2) The system more powerful password scheme

by dynamic salt generation and placement are used to improve password security.

### SYSTEM ARCHITECTURE

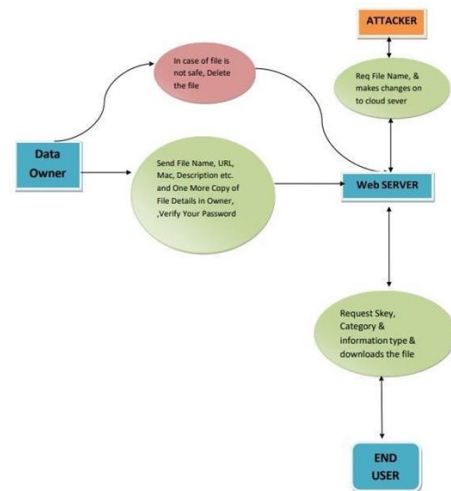


Fig: System Architecture

## IV. IMPLEMENTAIONS

### MODULES

- Home
- Client
- Web Server

### MODULE DESCRIPTION ADMIN

#### HOME

Tackles the challenge of safeguarding data. We'll explore methods to encrypt passwords, rendering them invisible to unauthorized users strictly controlled, ensuring only those with the key can unlock the protected information.

#### CLIENT

This project aims to develop a secure access system that utilizes hidden password encryption. Passwords will be obscured during storage and transmission, enhancing protection against unauthorized access. The system will likely involve a combination of one algorithms and secure key management techniques to safeguard your data

#### WEB SERVER

Secures your web server by replacing traditional password storag logs in, their password is never revealed hidden password protects your system from breaches where attackers steal password.

## V. SCREENSHOTS

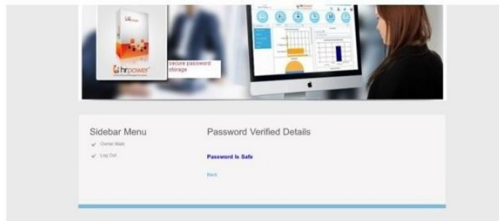


FIG 1: DETAILS VERIFY

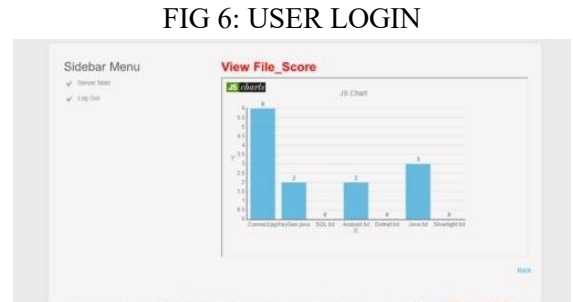


FIG 7: FILE SCORE



FIG 2: PASSWORD VERIFY

File No	Attacker	File Name	Date & Time	URL & Hash Code
1	Hacker	Connect.jsp	05/05/2019 10:14:51	Details

FIG 8: FRAUD DETAILS



FIG 3: ATTACKED FILES LIST

Sl No	User Name	File Name	Secret Key	Operation	Date & Time
1	Umesh	Connect.jsp	js@10000	Upload	05/05/2019 10:21:02
2	Ramesh	Connect.jsp	js@10000	Download	05/05/2019 10:24:39
3	Umesh	KeyGen.jsp	js@10000	Upload	05/05/2019 10:26:00
4	Umesh	SQL.txt	js@10000	Upload	05/05/2019 10:26:53
5	Manjunath	Android.txt	js@10000	Upload	05/05/2019 10:27:27
6	Manjunath	Connect.jsp	js@10000	Upload	05/05/2019 10:27:41
7	Manjunath	Java.txt	js@10000	Upload	05/05/2019 10:27:52
8	Manjunath	Server.jsp	js@10000	Upload	05/05/2019 10:28:05
9	Manjunath	Connect.jsp	js@10000	Download	05/05/2019 10:28:47
10	Manjunath	Java.txt	js@10000	Download	05/05/2019 10:29:16
11	Manjunath	Android.txt	js@10000	Download	05/05/2019 10:29:29

FIG 9: CLIENTS TRANSACTIONS



FIG 4: WELCOME TO

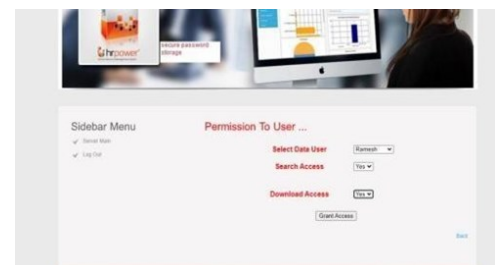


FIG 10: USER PERMISSION

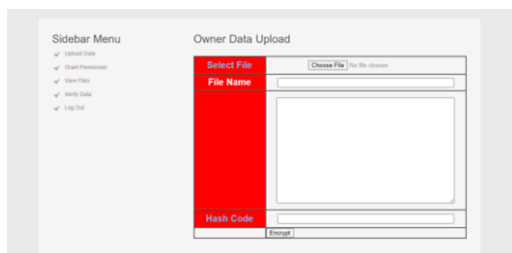
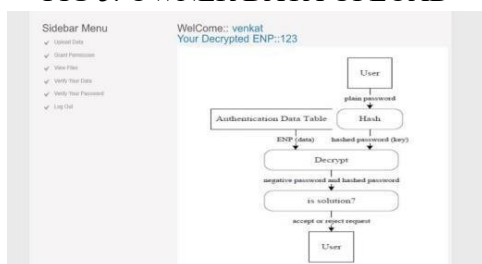



FIG 5: OWNER DATA UPLOAD

Sl No	Owner Name	File Name	Rank	Date & Time	URL and Hash Code
1	Umesh	Connect.jsp	5	05/05/2019 10:21:02	Details
2	Umesh	KeyGen.jsp	2	05/05/2019 10:26:00	Details
3	Umesh	SQL.txt	5	05/05/2019 10:26:53	Details
4	Manjunath	Android.txt	2	05/05/2019 10:27:27	Details
5	Manjunath	Connect.jsp	5	05/05/2019 10:27:41	Details
6	Manjunath	Java.txt	5	05/05/2019 10:27:52	Details

FIG 11: CLIENT DETAILS







Client ID	Client Name	Client Email	Client Phone	Client Address	Client Status
1	Submit	Submit	Submit	Submit	Submit
2	Submit	Submit	Submit	Submit	Submit
3	Submit	Submit	Submit	Submit	Submit
4	Submit	Submit	Submit	Submit	Submit

FIG 12: CLIENT INFORMATION



FIG 13: WELCOME TO SERVER MAIN



FIG 14: CLIENT LOGIN

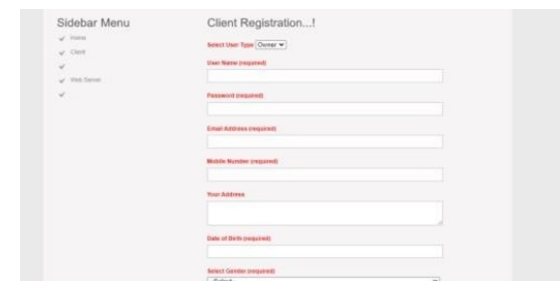


FIG 15: CLIENT REGISTRATION



FIG 16: LOGIN PAGE

## VI. CONCLUSION

### CONCLUSION

The Online Crime Reporting System is a web application system which is too much helpful for

all the common people, government organization and different societies. This is based on a very simple and non-complex approach. This has been created as a safety measure for all section of people and societies. Anything which is against the law or anyone who is violating the law will now have some fear as now filing an FIR is much easier than it was before. The Online Crime Reporting System is a success with satisfaction from both the people and government organizations. This has been tested and is a success. So, this make it much more efficient.

### FUTURE SCOPE

In future research for our major project, we plan to explore alternative NDB generation algorithms, integrate multi-factor authentication, and incorporate challenge-response methods. Additionally, we aim to evaluate quantum-resistant techniques, enhance usability, and conduct real-world testing. Furthermore, we will establish continuous security monitoring to adapt our ENP password protection scheme and authentication framework to evolving threats and vulnerabilities.

### REFERENCES

1. M. J. Atallah, K. N. Pantazopoulos, J. R. Rice, and E. E. Spafford, "Secure outsourcing of scientific computations," Adv. Comput., vol. 54, pp. 215–272, 2002.
2. D. Benjamin and M. J. Atallah, "Private and cheating-free outsourcing of algebraic computations," in Proc. 6th Annu. Conf. Privacy, Secur. Trust, 2008, pp. 240–245.
3. C. Wang, K. Ren, and J. Wang, "Secure and practical outsourcing of linear programming in cloud computing," in Proc. IEEE INFOCOM, Apr. 2011, pp. 820–828.
4. X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New algorithms for secure outsourcing of modular exponentiations," in Proc. 17th Eur. Symp. Res. Comput. Secur., 2012, pp. 541–556.
5. G. Ateniese et al., "Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Comput. Commun. Secur., 2007, pp. 598–609.
6. A. Juels and B. S. Kaliski, Jr., "PORs:



- Proofs of retrievability for large files,” in Proc. 14th ACM Conf. Comput. Commun. Secur., 2007, pp. 584–597.
7. H. Shacham and B. Waters, “Compact proofs of retrievability,” in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 2008, pp. 90–107.
  8. G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, “Scalable and efficient provable data possession,” in Proc. 4th Int. Conf. Secur. Privacy Commun. Netw., 2008, Art. ID 9.
  9. R. Curtmola, O. Khan, R. Burns, and G. Ateniese, “MR-PDP: Multiplereplica provable data possession,” in Proc. 28th IEEE Int. Conf. Distrib. Comput. Syst., Jun. 2008, pp. 411–420.
  10. Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, “Efficient provable data possession for hybrid clouds,” in Proc. 17th ACM Conf. Comput. Commun. Secur., 2010, pp. 756–758.
  11. C. Wang, K. Ren, W. Lou, and J. Li, “Toward publicly auditable secure cloud data storage services,” *IEEE Netw.*, vol. 24, no. 4, pp. 19–24, Jul./Aug. 2010.
  12. H. Wang, “Proxy provable data possession in public clouds,” *IEEE Trans. Services Comput.*, vol. 6, no. 4, pp. 551–559, Oct./Dec. 2013.
  13. C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, “Privacy preserving public auditing for secure cloud storage,” *IEEE Trans. Comput.*, vol. 62, no. 2, pp. 362–375, Feb. 2013.
  14. B. Wang, B. Li, and H. Li Oruta, “Oruta: Privacy-preserving public auditing for shared data in the cloud,” *IEEE Trans. Cloud Comput.*, vol. 2, no. 1, pp. 43–56, Jan./Mar. 2014.
  15. C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia, “Dynamic provable data possession,” in Proc. 16th ACM Conf. Comput. Commun. Secur., 2009, pp. 213–222.