Enhanced Text-Based Graphical Password Using Cryptographic Salt and Hash Technique

Preethika S
Research Scholar, PG and Research Department, Quaid-E-Millath Government College for Women (Autonomous), Chennai, India

Velmayil G
Assistant Professor, PG and Research Department, Quaid-E-Millath Government College for Women (Autonomous), Chennai, India

ABSTRACT

Textual password is most typical methodology used for password authentication. The Username and Password authentication is an important part of today's internet application technology that normally controls access to restricted resources. Several authentications methods are bestowed. However users are acquainted with textual password method. Textual passwords are vulnerable to various attacks like eavesdropping, dictionary, SQL injection, brute force, denial of service attacks, shoulder surfing and key loggers. To overcome from these attacks several authentication systems like biometric authentications, token based authentications, graphical based authentications are used. These existing methods are nothighly secure, economical enough and have high failure rate. This paper consolidates the utilization of plain content accreditations that are cryptographically hashed at runtime with text based graphical login accreditations. The objective is to dependably ensure access to a client account not withstanding when such record is under attack while in the meantime guaranteeing helpful and secure login encounter by real clients. This framework approved by utilizing the tools like Microsoft Visual Studio, SQL Server and Mat lab.

Keywords

Hashed password, graphical password, SQL Injection attacks, cryptographic salt and password protection.

1. INTRODUCTION

Client validation is an essential part in most computer security. It gives the thought to get to control is client responsibility. Though there are various sorts of client confirmation frameworks, alphanumeric username and passwords is the preeminent basic kind of client verification. They are adaptable and easy to execute and utilize.

Alphanumeric passwords are needed to satisfy two contradictory necessities. They should be effectively recalled by a client, while they must be difficult to figure by faker. Users are known to decide on easily guessable and/or short text passwords that are a simple target of dictionary and brute-forced attacks. Imposing a powerful password policy generally results in an opposite effect, as a user might resort to write down his or her difficult to remember passwords on sticky notes exposing them to direct stealing.

A graphical password is simpler than a text-based password for many folks to recollect. Graphical passwords might offer higher security than text-based passwords as a result of many people, in an attempt to memorize text-based passwords, use plain words. A dictionary search will usually hit on a password and allow a hacker to achieve entry into a system in seconds. However if a series of selectable images is employed on successive screen pages, and if there are several images on every page, a hacker should strive each attainable combination at random.

Applications, such as, MasterCard information, customer demographics, client orders, consumer preferences, etc., use the database to store the data. Consequently, databases became enticing and very lucrative targets for hackers to hack. SQL Injections happen when a developer accepts user input that is directly placed into a SQL Statement and doesn't properly validate and separate out dangerous characters. This may enable an attacker to alter SQL statements passed to the database as parameters and enable her to not only steal data from your database, but also modify and erase it.

To address these issues analysts have propelled a few procedures running from protective coding best practices to computerized systems for recognition and avoidance of these types of assaults. The utilization of graphical passwords has been introduced by researchers to take care of the issues of attacks like online password guessing, dictionary, brute force, SQL Injection etc., on login form which is in infant stage. This exploration overcomes from these issues and enhance the security of the framework by make use of the graphical password, cryptography salt and hash method.

2. RELATED WORK

Shaukat Ali, et.al (2009) [10], proposed a way that prevents the client data from the SQL Injection attack by utilizing the Hashing Techniques. It stores the user subtle elements with the hash esteem for each username and secret key inside the back end. When user login with username and secret word, it creates the hash esteem and contrast it and the backend. Despite the fact that hash systems give a considerable measure of points of interest it has a few issues with executing the great strategy.

Sangita Roy, et.al (2011) [8], proposed a SQL Injection vulnerable scanner that is quick, light-weight and has a low false positive rate. These scanners demonstrate as a viable instrument to find the vulnerabilities in a web application and in addition to test the productivity of counter assault components. In the last some portion proposed a security instrument to counter SQL Injection Attacks. The security philosophy depends on the outline of a channel for the HTTP asks for send by customers or clients and search for assault marks.

M.Kameswara Rao, et.al (2012) [3],proposed a text based shoulder surfing resistant graphical password scheme, PPC. To login the framework, the user needs to blend his text password to create a few pass-pairs, and follow four predefined guidelines to get his session password on the login screen. Be that as it may, the login procedure of PPC is excessively muddled and monotonous.

Yi-Lun Chen, et.al (2013) [15], the text based shoulder surfing resistant graphical password plan is enhanced by utilizing colour. In the enrolment stage, user has to pick one colour and set his textual password. In login stage, framework shows circle which is partitioned into 8 segments what's more, every part has diverse hues. Every one of the character is put arbitrarily in these segments. User needs to pivot the segment till all characters come into beforehand picked colour. Be that as it may, characters are not obviously discernible and programmer can figure the colour.

Tivkaa, M.L., et.al (2015) [14], proposed a confirmation arrangement that addresses the issue of SQL injection and online password guessing attack on login frame as actualized utilizing the web applications. This framework contains two login stages and the client can get to just if both the login succeeds. The one login is text based and the other login is graphical based so the client needs to recollect both sort of secret key to login every time so the client may mistook for the passwords. The user needs patience to login due to two login stage.

3. PROPOSED SYSTEM

In the enhanced text-based graphical password using cryptographic salt and hash technique, we will portray a straightforward and effective graphical password in view of text, concatenating the cryptographic salt and lastly hash the password. The password letters in order utilized as a part of the proposed conspire contains 64 characters, including 26 capitalized letters, 26 lowercase letters, 10 digits and 2 symbols "." and "/".

Table 1 show the new parameters introduced in this system.

Table 1: Comparing the Existing and Proposed System

Method	**Graphical Password**	**Graphical Password + Salt**	**Graphical Password + Salt + Hash**
Existing	Yes	No	No
Proposed	Yes	Yes	Yes

The proposed system includes two stages, the registration stage and the login stage, which can be portrayed as in the accompanying. In registration phase, the individual subtle elements of the user are put away in the database. This is accomplished by actualizing the framework in the Microsoft Visual Studio and stores the information into the database SQL Server. In login stage, the user login into the framework to get to the account.

Registration Phase

In registration phase, the user demand to enter the username and textual password alongside the individual subtle elements. Then after login happen through graphical password. The textual password is then stored in the database alongside the cryptographic salt which creates a string arbitrarily using the RNG Crypto Service Provider. At that point the password and the cryptographic salt linked and scramble the content using the hash technique SHA512. This hashed password is put away in the database. The sampleset of two-hundred records are registered into this enhanced text-based graphical password using cryptographic salt and hash technique.

Login Phase

The user request to login the framework, and the framework shows a hover made out of 8 similarly estimated sectors. The colors of the curves of the 8 segment are distinctive, and every segment is recognized by the color of its curve. At first, 64 characters are put averagely and haphazardly among these divisions. All the showed characters can be at the same time pivoted into either the adjoining part clockwise by tapping the "clockwise" catch once or the neighbouring division counter clockwise by tapping the "anticlockwise" catch once, and the turn operations can likewise be performed by looking over the mouse wheel. The login screen of the proposed plan can be delineated by an illustration appeared in Figure 1.

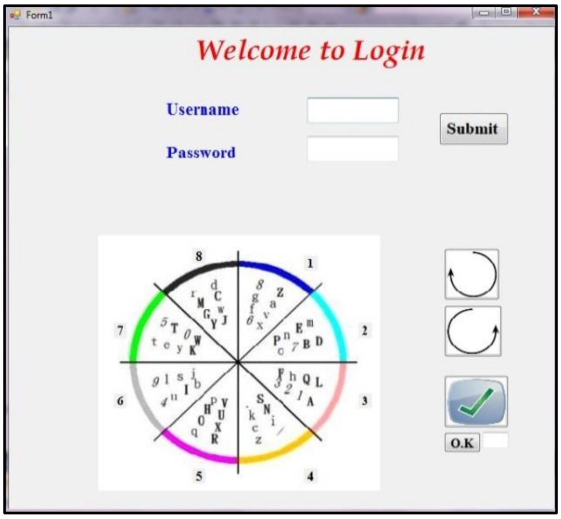
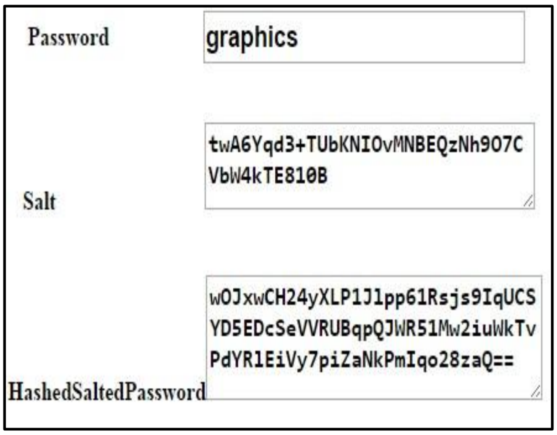


Figure 1: Login Screen of Enhanced text-based graphical p0061ssword using cryptographic salt and hash technique

The login screen of proposed system is shown in Fig 1, in that theuser enters the username and then selects the characters of password which is enlisted during registration using the circle by rotating it in both clockwise button and anticlockwise button.



Password graphics

Salt twA6Yqd3+TUbKNIOvMNBEQzNh9O7CVbW4kTE810B

HashedSaltedPassword wOJxwCH24yXLP1J1pp61Rsjs9IqUCSYD5EDcSeVVRUBqpQJWR51Mw2iuWkTvPdYR1EiVy7piZaNkPmIqo28zaQ==

Figure 2: View of Salt and Hashed Salted Password

The view of generating the cryptographic salt for entered textual password “graphics” and the hashed password is displayed in Figure 2.

The registered passwords are assessed by make use of the attacks and the outcome is shown in figures of Results and Discussions segment.

4. METHODOLOGY

In this enhanced text-based graphical password using cryptographic salt and hash technique, we tend to deliver a secure authentication system by strengthening the graphical password in two layers.

It produces the salt esteem for every user password and keep inside the database. At that point it figures the hash estimations of Salt and Password and stores into the database. This hash method keeps the illegitimate user to execute the SQL Injection attack into the framework. Furthermore it makes hard to handle the dictionary attack and brute force attack as a result of the password length.

Once a user needs to login into database using username and password, it recover the information from database on each event.

The user has to follow the steps to login into the proposed system.

Algorithm

Step1: User request to enter the username.

Step2: The login phase displays the circle which is equally partitioned into 8 sectors. Each sector contains the uppercase letters, lowercase letters, digits and symbols. The circle contains the total of 64 characters. Step3: The graphical password is made to rotate the circle towards clockwise and anti- clockwise.

Step4: Password confirmation is carried out.

Step5: Cryptographic salt is generated randomly for each password while registering.

Step6: The cryptographic salt for the entered password is retrieved from the database.

Step7: To intensify the security the password is encrypted.

Step8: The hashed password is then compared with the database which is stored during registration, every time when the user login.

Step9: If the password matched with the database then the user can login into the account.

Step10: Account is blocked when login fails for three consecutive times.

Step11:Related information is imparted through registered email.

5. RESULTS AND DISCUSSIONS

The examination of the enhanced text-based graphical password using cryptographic salt and hash technique system is done in this area on premise of ease of use and security. The proposed system has been evaluated in terms of space length, attacks, accidental logins and usability.

5.1 Password Space

The enhanced text-based graphical password using cryptographic salt and hash technique system has character set of 64 characters, these characters are equally and randomly divided among 8 sectors and password length L is in between 8<L<20. Therefore total number of all possible passwords with length L is 8 * 64L. . Therefore, password space of proposed scheme is given by,

$$\sum_{L=8}^{20} 8 \ * 64L \approx 1.008 \text{ x } 10^{30} \qquad (1)$$

The password length tried so far by researchers is 15 characters (8<L<15). The proposed system holds the length of the password up to 20 (8<L<20) characters which provides space for key enforcement and increase the number of probability of password combinations by 5 factorial which is a tough factor for attacker in trials.

5.2 Accidental Logins

The probability of passwords accurately reacting to Ki is 8/64 i.e. 1/8. The achievement probability of accidental login with the password with length L, denote by P_{al} (L),

$$P_{al}(L) = \left(\frac{1}{8}\right)^{L} \qquad (2)$$

Example: If L=12, then

$$P_{al}(12) = \left(\frac{1}{8}\right)^{12} \approx 9.31 \text{ x } 10^{-10}$$

This method keeps up the standard identical with other methods by not allowing more accidental logins.

5.3 Entropy of Password

Password entropy depends on the character set utilized which is expansible by utilizing lowercase, capitalized, numbers and additionally images and also password length. Password entropy predicts how troublesome a given password is split through guessing, brute force cracking, dictionary attacks or other normal methods.

The entropy is calculated for the registered passwords and the system generated salted hashed password is screened in Figure 3.

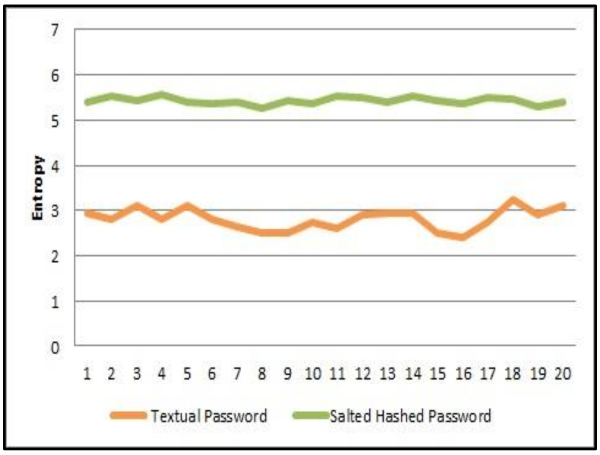


Figure 3: Entropy of Passwords

The result depicts the password in multiples of ten and its corresponding entropy of registered password with high rate proving efficiency over existing traditional authentication system.

5.4 Breaking Time

Breaking time of the passwords is calculated to identify the strength using the online password crack tool.Table 2 shows the breaking time of the textual password and the salted hashed password in hours.

Table 2: Breaking Time of Passwords in Hours

Passwords	Textual Password (hours)	Salted Hashed Password (hours)
Technology45@	86	1665774
sharon20	20	1675445
anirisha@Naz	58	1630237
Chocolates	40	1689849
system20admin	34	1665914
sara@tara45D	90	175835
56shan$R	62	169029
$ruthi25	53	148947
Mughil11$	78	167332
kayal10	18	169019

Textual password is effortlessly weaker than the salted hashed password furthermore it shows that the salted hashed password is fortified than the textual password.

The average breaking time of the passwords are shown in Figure 4.

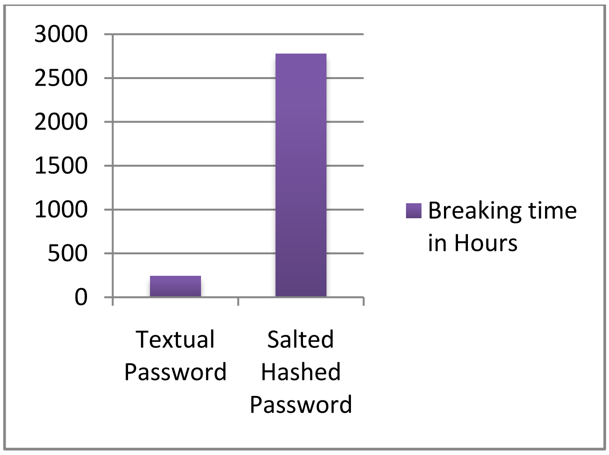


Figure 4: The breaking time of password in hours

An enhanced text-based graphical password using cryptographic salt and hash technique system is hard to break than the existing traditional authentication system even after long hours.

Research proves that when the attacker tries to break for the longer time, then the aggressor is tired of the procedure and stops the attacks. This infers that long breaking time will lead to less attack.

5.5 Attacks Handled

Attacks like brute force, dictionary, SQL injection, guessing are evaluated to discover the strength and quality of the system. Registered passwords and the system generated Salted hashed password are validated on various attacks using Matlab and presented in Figure 5.

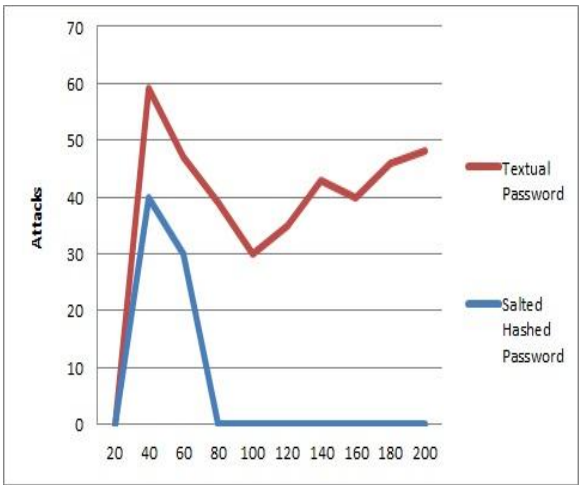


Figure 5: Password Attacks

The Salted Hashed Password has a few attacks when compared with the textual password. Henceforth this system withstand on different attacks.

5.6 Usability

As most users know about textual passwords, it is generally less demanding for the user to discover characters than symbols on the login screen. What's more, since the system shows the capitalized letters, the lower case letters, the 10 digits and the symbols "." and "/", in three diverse typefaces on the login screen, the user can without much of a stretch and proficiently discover his pass-characters. What's more, the operation of the proposed plan is basic and simple to take in the user just needs to pivot the divisions to login the system.

6. CONCLUSION

In this enhanced text-based graphical password using cryptographic salt and hash technique system, we have proposed a graphical password in which the user can without much of a stretch and proficiently complete the login handle without agonizing over attacks like shoulder surfing, dictionary, brute force, SQL injection etc.

The operation of the proposed plan is easy and simple to learn for user acquainted with textual passwords. The password length of twenty characters is accomplished at no other time. The cryptographic salt is concatenated with the password that prevents the system from the dictionary and brute force attacks. The hash technique secures the system from the SQL Injection attack by executing the illegal queries.

This system is enhanced to resists on any attacks and secures the system from the hackers. The user can undoubtedly and productively to login the system without utilizing any physical or on-screen keyboard. At long last, we have dissected the resistances of the proposed plan to shoulder surfing and inadvertent login.

7. FUTURE WORK

The proposed effect will be upgraded by the twofold security and block the illegitimate user to access the system. Once password protection is ensured, the system will be extended to detect, avoid and prevent SQL injection queries. At present algorithm is developed to execute from the server side,which can be implemented on the client side as well. Scalability of algorithm will be concentrated from the network perspective to improve the performance.

8. REFERENCES

[1] Diksha G. Kumar , Madhumita Chatterjee, “Detection block model for sql injection attacks”, I.J. Computer Network and Information Security, 2014, 11, 56-63.

[2] Kanchan Choudhary, Anuj Kumar Singh, Rashmi Gupta, “A modified scheme for preventing web application against sql injection attack”, International Journal of Computer Applications (0975 – 8887) Volume 141 – No.10, May 2016.

[3] M.Kameswara Rao, Sushma Yalamanchili,” Novel shoulder-surfing resistant authentication schemes using text-graphical passwords”, International Journal of Information & Network Security (IJINS) Vol.1, No.3, August 2012, pp. 163-170 ISSN: 2089-3299.

[4] Manjunath G , Satheesh K , Saranyadevi C,Nithya M,” Text-Based Shoulder Surfing Resistant Graphical Password Scheme”, International Journal of Computer Science and Information Technologies, Vol. 5 (2), 2014, 2277-2280.

[5] Mary Cindy Ah Kioon, ZhaoShun Wang and Shubra Deb Das, “Security analysis of md5 algorithm in password storage”, Atlantis Press, Paris, France, 2013.

[6] Ms. Vidya Vijayan, Ms. Josna P Joy, Mrs. Suchithra M S,” A review on password cracking strategies”, IJRCCT, 2014.

[7] P. Sriramya and R. A. Karthika, “Providing password security by salted password hashing using bcrypt algorithm”, ARPN Journal of Engineering and Applied Sciences, VOL. 10, NO. 13, JULY 2015.

[8] Sangita Roy, Avinash Kumar Singh and Ashok Singh Sairam , ”Detecting and defeating SQL injection attacks”, International Journal of Information and Electronics Engineering, Vol. 1 , No. 1 , July 2011.

[9] Saurabh Saoji, Swapnali Bhadale, Harshada Wagh, “Textual graphical password scheme against shoulder surfing attack”, International Journal of Engineering and Computer Science ISSN: 2319-7242, Volume 4 Issue 3 March 2015, Page No. 10988-10991.

[10] Shaukat Ali, Azhar Rauf, and Huma Javed, "SQLIPA: An authentication mechanism against sql injection", European Journal of Scientific Research, Volume 38, No. 4, 2009.

[11] Sruthy Manmadhan and Manesh, “A method of detecting sql injection attack to secure web applications”, International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.6, November 2012.

[12] Surya Pratap Singh, Upendra Nath Tripathi, Manish Mishra, “Detection and prevention of sql injection attack using hashing technique”, IJMCTR, Volume 2, Issue 9, Sep 2014.

[13] T.S.Thangavel and K.S.Rangasamy, " Provable secured hash password authentication”, International Journal of Computer Applications (0975 – 8887), 2010, Volume 1 – No. 19.

[14] Tivkaa, M.L., Choji, D. N., Agaji, I., Atsa‟am, D., “An enhanced password-username authentication system using cryptographic hashing and recognition based graphical password”, IOSR-JCE, Volume 8, Issue 4, Ver-1, Jul-Aug. 2016.

[15] Yi-Lun Chen, Wei-Chi Ku, Yu-Chang Yeh, and Dun-Min Liao,” A Simple text-based shoulder surfing resistant graphical password scheme”, IEEE 2nd International Symposium on Next-Generation Electronics (ISNE) - February 25-26, Kaohsiung , Taiwan.