RESEARCH ARTICLE OPEN ACCESS

Prevention of SQL Injection with Two Fold Secured Authenticated System using Text Based Graphical Password

Dr. Velmayil G[1], Preethika S[2]

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

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

Abstract:

Textual password is the most typical methodology used for password authentication. 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. Several authentication systems like biometric authentications, token based authentications and graphical based authentications are used to overcome these attacks. Existing methods are insecure, have high failure rate and not enough to meet out economically. Graphical passwords are also vulnerable to shoulder surfing. None of the recall-based based techniques are considered should-surfing resistant. At this point, only a few recognition-based techniques are designed to resist shoulder-surfing which open up the need for a research solution. This paper proposes the prevention of SQL injection with two-fold secured authenticated system using text based graphical password. It consolidates the utilization of plain content accreditations that are cryptographically hashed at runtime with text based graphical login accreditations. The two factor authentication of formula password is implemented to enhance the authentication system. The passwords are stored in different database to secure from the hackers. 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 is accomplished by blocking the illegitimate user as black list once login failed consecutive three times.

Keywords — **SQL injection, cryptographic salt, hash, attacks, graphical password, two factor authentication.**

I. INTRODUCTION

Various sorts of client confirmation frameworks are in practice. Alphanumeric username and passwords is the preeminent basic kind of client verification. Alphanumeric is a term encompassing all the letters in a given language set as well as the numerals. In some usages, the alphanumeric character set may include upper and lower case letters, punctuation marks, and symbols (example: @, &, and *). The mishmash of letters and numerals used for texting abbreviations is sometimes referred to as alphanumeric. Alphanumeric characters are used to strengthen the password.

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.

Applications, such as, Credit/Debit Card 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 Statementand 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.

This paper explains the exploration overcomes from these issues and enhance the security of the framework by making use of the graphical password, cryptography salt, hash method and formula password.

II. RELATED WORK

Tivkaa, M.L., et.al (2016), proposed a confirmation arrangement that addresses the problem of SQL injection and on-line password guesswork attack on login frame as actual utilizing the web applications. This framework contains two login stages and also the client will get into simply if both the login succeeds. The one login is text based and the alternative login is graphical based therefore the consumer has to recall each kind of secret key to login on every occasion therefore the consumer mistook for the passwords. The user wants patience to login due to two login stage.

SaurabhSaoji, et.al (2015), proposed textual graphical password scheme against shoulder surfing attack using color combination. The user chooses one color as his pass color from eight colors given by the system. In account details user can enter the ten digit card number. The account number and textual password are going to be automatically generated by the system. This technique indeed of security since the user wants the ten digit card number to come up with the textual password anytime to login to the system. Just in case of loss of card number the user cannot access their account.

T. Rajesh and et.al (2014), proposed a password management system using cryptographic salt generated for each username and password. Additionally generate the online concern username / password using ASCII code for the registered password. It finds the ASCII code of every character of the username/password. This approach fails as a result of repetition of username and password might ends up in generating identical ASCII code.

Sangita Roy, et.al (2011), proposed a SQL Injection vulnerable scanner that's fast, light-weight and contains a low false positive rate. These scanners demonstrate as a viable instrument to seek out the vulnerabilities in an exceedingly internet application and additionally to check the productivity of counter assault elements. Within the last some portion proposed a security instrument to counter SQL Injection Attacks. The protection philosophy depends on the outline of the channel for the HTTP asks for send by customers or clients and look for assault marks.

III. PROPOSED METHODOLOGY

In proposed methodology two phases of authentication are implemented to secure the authentication system from various attacks. Two-factor authentication provides an additional layer of security and makes it harder for attackers to gain access to a person's devices and online accounts, because knowing the victim's password alone is not enough to pass the authentication check. Two-factor authentication has long been used to control access to sensitive systems and data, and online services are increasingly introducing it to prevent their user's data from being accessed by hackers who have stolen a password database or used phishing campaigns to obtain user's passwords.

The registration phase and the login phase of proposed authentication system can be portrayed as in the accompanying. In registration phase, the individual subtle elements of the user are stores 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 phase, two stages of user's login to get into the framework to get to their account. Two phases of proposed authenticated system:

1. Registration phase
2. Login Phase
   - Graphical Based Password
   - Formula Based Password

A. Registration Phase

Registration phase in proposed authenticated system used to create the account in the authentication system. The user demands to enter the username and textual password alongside the individual subtle elements in registration phase. In this proposed system when the user enters the 'submit' button, the user data stores in different databases. Cryptographic salt generated for each user password when the user creates their account by using RNG Crypto Service Provider. In a very typical setting, the salt and also the password are concatenated and processed with a SHA 512 cryptographic hash function, and the resulting output is stored in databases. The sample set of one-hundred and fifty records are registered into this authenticated system using text-based graphical password.

B. Login Phase

Once user created their account in the registration phase, can access their account using the login phase. This proposed authentication system use two-factor authentication to authorize the user. Standard security procedures only requiring a simple username and password which has become increasingly easy for criminals to gain access to a user's private data such as personal and financial details and then use that information to commit fraudulent acts.

In login phase there are two stages to access the user account. The user login to the system using text-based graphical password in first stage and formula based password in second stage.

1) **Stage I - Graphical Password*:***

Graphical passwords are more prone to shoulder surfing attacks as compared to textual passwords. To beat the weakness of text as well as graphical passwords we propose an authentication system referred to as prevention of SQL Injection with two folds Secured authenticated System using Text-Based Graphical password which is a combined approach of text as well as graphical passwords. The scheme is user friendly. It supports client-server environment and its main advantage is it's resistant to brute force attack, shoulder surfing.

The user requests to login the system, and the system displays a circle composed of eight equally sized sectors. The colors of the arcs of the eight sectors are completely different, and every sector is known by the color of its arc. Initially, seventy two characters are placed averagely and indiscriminately among these sectors. All the displayed characters will be at the same time revolved into either the adjacent sector clockwise by clicking the "clockwise" button once or the adjacent sector anti-clockwise by clicking the "anti-clockwise" button once.

The 72 characters are in two typefaces and four colors to identify the characters. Therein the 26 upper case letters (A-Z) are in bold typeface and blue in color, the 26 lower case letters (a-z) are in italic typeface and red in color, the 10 digits are in bold and orange in color and the ten symbols (. / ! @ # $ % ^ & *) are in bold

typeface and maroon in color. Additionally, the button for rotating clockwise, the button for rotating anti-clockwise, the "Submit" button, and the "Signin" button are displayed on the login screen. All the displayed characters will be simultaneously rotated into either the adjacent sector clockwise or the adjacent sector anti-clockwise.

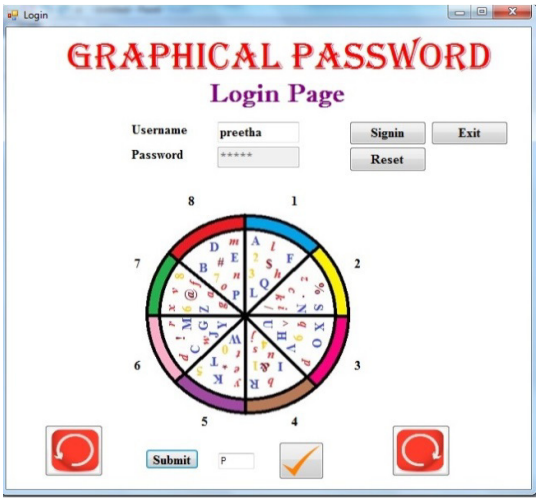

Figure 1: Screenshot of Login Phase – Stage I

In figure1, the screenshot of login phase of stage-1 of proposed authenticated system is shown. The users are request to enter the username and password using the graphical image which is depicted in the screenshot. This graphical image can be rotated both clockwise and anticlockwise using the buttons. Each character in the password should be selected through the button and the submit button used to send each character to the password text area. Finally signin button move the user to the second level of authentication.

*2) **Stage II - Formula Password:***

A In this proposed authentication system the two-factor authentication is implemented to secure the system from the intruders. When the user successfully logged into the first stage of authentication (graphical password authentication) then the legitimate user are moved to the second stage of authentication (formula password authentication). In the stage-2 of login phase, the formula is used to validate the authorized user to access their account.

The user requests to selects a character from each panel of three panels of alphabets while creating their account in registration phase. Then the formula created using the addition operation, example A+B+C. This formula is stored in the database2 along with the user subtle.

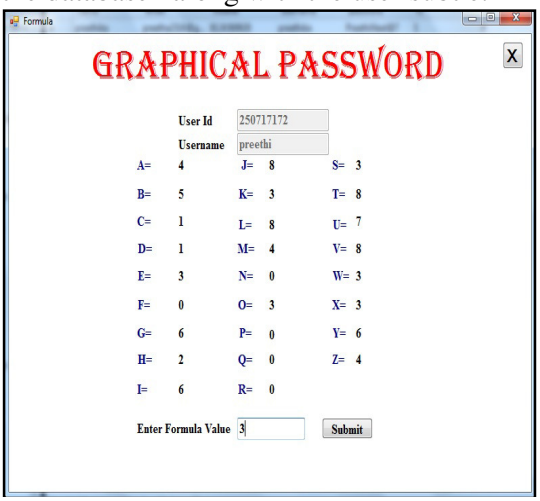

Figure 2: Screenshot of Login Phase – Stage II

In figure 2, the screenshot of second stage of login phase is shown. The random values are generated for each alphabet (A-Z) and the user request to enter the value of the registered formula in the textbox and selects the submit button to proceed the process. Once the user authorized, they can access their account. Else the user listed under black list and blocked their account.

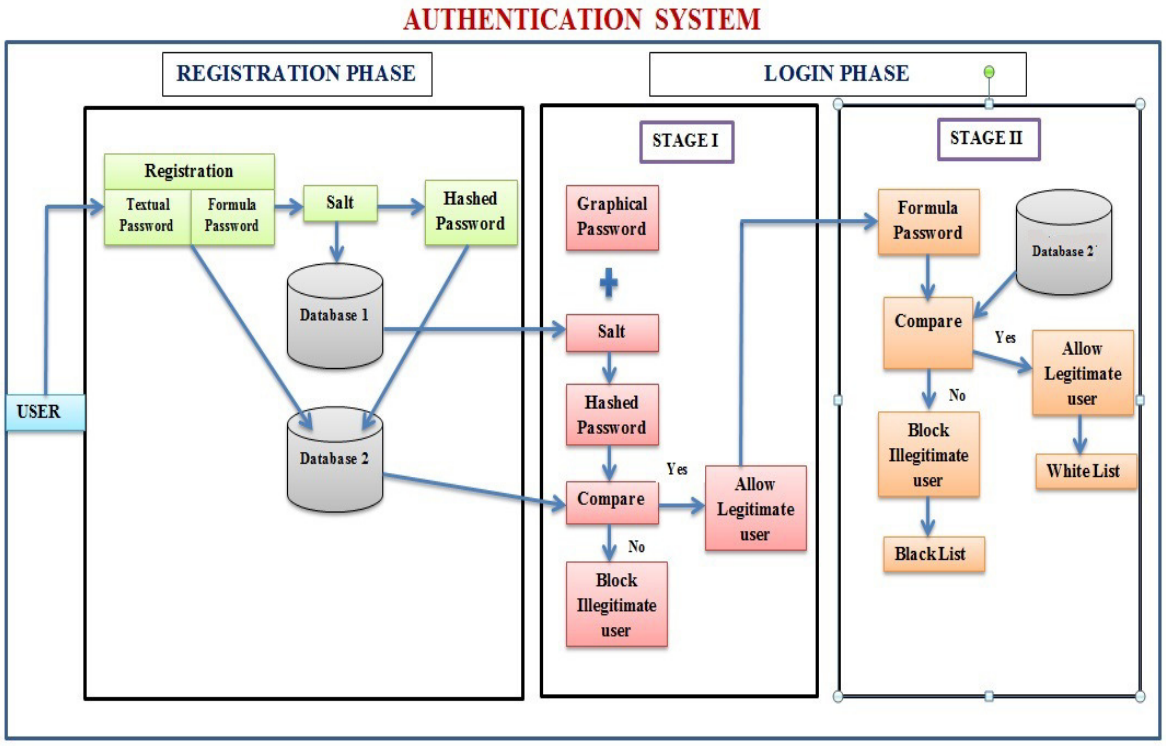

Figure 3: Block Diagram of Prevention of SQL Injection with Two Fold Secured Authentication System using Text Based Graphical Password.

In figure 3, the block diagram of proposed authenticated system is shown. The proposed system consists of two phases to authorize the user to access the account. This is achieved by imposing the cryptographic salt and hash technique.

The user has to move both stages successfully to access their account. In this proposed authenticated system two different databases are used to store the user details. In database1 the username and password along with salt are stored. Database2 stores the user subtle along with hash value. Once a user needs to login into this authenticated system using username and password, it recover the information from database on each event.

TABLE I
EXISTING VS. PROPOSED AUTHENTICATED SYSTEM

Method	**G P**	**G P + Salt**	**G P + Salt + Hash**	**G P + Salt + Hash + F P**
Existing	Yes	No	No	No
Proposed	Yes	Yes	Yes	Yes

In table 1, the existing methodology is compared with the proposed authenticated system. In prevention of SQL injection with two folds authenticated system using text-based graphical password the new parameters are introduced which is not found in the existing system. The cryptographic salt and hash technique with the graphical password (GP) and formula password (FP) are introduced in this proposed authenticated system.

IV. ALGORITHM

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

Step 1: User request to enter the username.

Step 2: The login phase of first stage displays the circle which is equally partitioned into 8 sectors. Each sector contains the uppercase letters, lowercase letters, digits and special characters. The circle contains the total of 72 characters.

Step 3: The graphical password is made to rotate the circle towards clockwise and anti-clockwise.

Step 4: Password confirmation is carried out.

Step 5: Cryptographic salt is generated randomly for each password while registering.

Step 6: The cryptographic salt for the entered password is retrieved from the database.

Step 7: To intensify the security the password is encrypted.

Step 8: The hashed password is then compared with the database which is stored during registration, every time when the user login.

Step 9: If the password matched with the database then the user can move next stage of authentication.

Step 10:In second stage of authentication user enters the value of the formula password which registered.

Step 11:If the calculated value of formula password matched with the database then the user can login into the account.

Step12: Account is blocked when login fails f0or three consecutive times.

Step 13:Blocked users are listed under Black list as illegitimate user and the White list as legitimate user.

This algorithm explains the working principles of the proposed authentication system.

V. RESULTS AND DISCUSSIONS

The proposed methodology needs to be verified for correctness and security based on the parameters. The various metrics are used to verify the proposed methodology. The authenticity and integrity of the authentication system need to be measured based on the password strength, length, complexity, unpredictability, key combination and breaking time. Each should be scrutinized using methods and tools for the authenticity.

a. Password Length

Lengthy passwords are often associated with an increase in password entropy, which basically is the measure of how much uncertainty there is in a key. Increase in password length leads to increase in the average amount of time necessary for successful attacks.

TABLE III
SAMPLE PASSWORDS AND LENGTH

PASSWORD	LENGTH
Mothi@sand11	12
Sanjana2006$	12
Srinivasan%99	13
Rajeshwari2017@	15
Banuparagathi23%	16
$ruth!B@huley@n<3	17

In this proposed authentication system the password is mandatory to fulfil the minimum length of twelve characters and the maximum length of twenty characters. The problems of short password or familiar password are overcome by implementing the cryptographic salt and hash technique. Salted password contains 40 characters and the hashed password contains 88 characters in the combination of alphabets, numbers and special characters and it also increase the complexity of the passwords.

b. Complexity

Complexity is often seen as an important aspect of a secure password. The password gets into the complexity when it had a combination of characters the following categories:

- Uppercase letters (A through Z)

- Lowercase letters (a through z)
- Base 10 digits (0 through 9)
- Non-alphanumeric characters (, . ! @ # $ % ^ & *)

In this proposed authentication system, the password should contain characters with the combinations of uppercase, lowercase, digits and special characters. This is implemented by using the validation controls in the proposed authentication system. This password complexity enhances the proposed authentication system and also prevents the authentication system from dictionary and brute force attacks.

c. Password Strength- Entropy

Password entropy predicts how difficult a given password would be to crack through guessing, brute force cracking, dictionary attacks or other common methods. An increase in entropy is seen as directly proportional to password strength. It's usually expressed in terms of bits. Entropy is calculated using the Formula 1 to find the strength of the password and how it is difficult to crack. In this paper the following formula is used to calculate the entropy for the sample of 150 dataset.

L*log C2 **(Formula 1)**

Where L - Length of Password

C - Character Set

TABLE IIIII
SAMPLE DATASET WITH ENTROPY

S.No	Password	L	C	Entropy
1	Mothi@sand11	12	72	74.03910002
2	VidathGFPreethika22$	20	72	123.3985
3	Sanjana2006$	12	72	74.03910002
4	K!shoReShank@r90	16	72	98.71880002
5	Srinivasan%99	13	72	80.20902502
6	Mic15.05.1999	13	72	80.20902502
7	Jesus&04.1999	13	72	80.20902502
8	Anandhimani^10	14	72	86.37895002
9	jaYannarun&30	13	72	80.20902502
10	Devishree$00	12	72	74.03910002

Sample of 10 data from the 150 data set is depicted in table 3. The table contains the password, length of the password, character set and the entropy value of each password. In proposed authentication system the minimum length of password is 12 and the maximum length of password is 20. The entropy column clearly proves that the increase in entropy value is direct proportional to the password strength. It prevents the authentication system from brute force attacks and also dictionary attack.

Password entropy predicts how difficult a given password would be to crack through guessing, brute force cracking, dictionary attacks. From this figure 4 the values of entropy increased when the length of the password increased. It illustrates that long password have high entropy value than the short password. When the entropy value is high then it is to be the strong password.

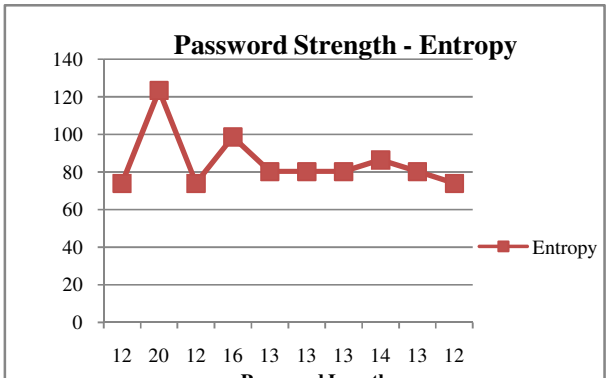

Figure 4: Entropy of Sample Passwords

Minimum and Maximum entropy of proposed character set of 26, 52,62 and 72 are tabulated in table 4.

TABLE IVV
MINIMUM AND MAXIMUM ENTROPY FOR CHARACTER SET

Entropy	Uppercase (26) or Lowercase (26)	Uppercase (26) + Lowercase (26)	Uppercase (26) + Lowercase (26) + Digits (10)	Uppercase (26) + Lowercase (26) + Digits (10) + Special Characters (10)
	26	52	62	72
Min (Len-12)	56.4052766	68.4052766	71.4503557	74.0391000
Max (Len-20)	94.0087943	114.008794	119.083926	123.3985

Entropy value of minimum length of 12 characters and the maximum length of 20 characters with various character set are tabulated in table 4. If password contains only uppercase or lowercase characters then the character set is 26. The character set is 52 when the password contains both the lowercase and uppercase characters. Or if password contains the uppercase, lowercase and digits then the character set is 62. And if character set is 72 then the password contain all the characters with uppercase, lowercase, digits and special characters.

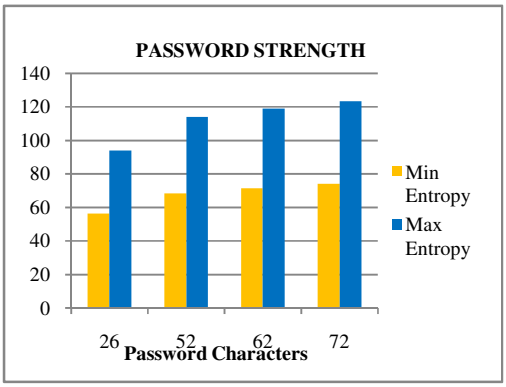

Figure 5: Minimum and Maximum Entropy

Minimum and maximum entropy of various character set are depicted in figure 5. This illustrates that the increase in character set have high entropy value than the others. This proposed authentication system implemented the character set of 72 characters. Result shows the minimum entropy of the length of 12 characters password with the character set as 72 and the maximum

entropy of the length of 20 characters password with the character set as 72 which is higher than other character sets.

D. Key Combination

The possible combinations of the password are calculated to find the strength of the password and computing time of cracking password. If the password has more key combination then the cracking time is high. The key combination is calculated using the following formula 6.2.

Combination = CL (Formula 2)

Where C – Character Set

L – Password length

In Table 5, the key combination of proposed authentication system is shown. This table illustrates that increase in length of the password will increase the possible combinations. When the key combination is high then the breaking time of the password also increase. This prevents the proposed authentication system from dictionary attack and brute force attack. The probability of identifying the key combination became highly complex and becomes hard to detect. Time consuming which makes the attacker gives up.

TABLE V
KEY COMBINATION

Password Length (L)	Possible combinations (C^L)
12 characters	1.94084E+22
20 characters	1.40168E+37
40 characters	1.96472E+74
88 characters	2.79E+163

d. Breaking Time

Breaking time of the passwords is calculated to identify the strength using the formula. Table 6 shows the breaking time of existing and the proposed methodology in hours.

TABLE VI
BREAKING TIME

METHODOLOGY	BREAKING TIME (HOURS)
Existing	5.1633E+23
Proposed – Salt	9.27783E+61
Proposed – Hash	1.3165E+151

Breaking time of average time of the password length from 12 to 20 of both existing methodology and proposed methodology are shown in table 6. The result depicts that proposed authentication system (salt and hash) takes 9.27783E+61 and 1.3165E+151 times to crack the password than the existing methodology 5.1633E+23 times. Thus the proposed authentication system is secured than the existing authentication system and also it prevents from the brute force attack and dictionary attack. The hacker terminates the process of hacking the password when it takes more time. Thus the proposed authentication system is secured from attacks since the breaking time is higher than the existing methodology.

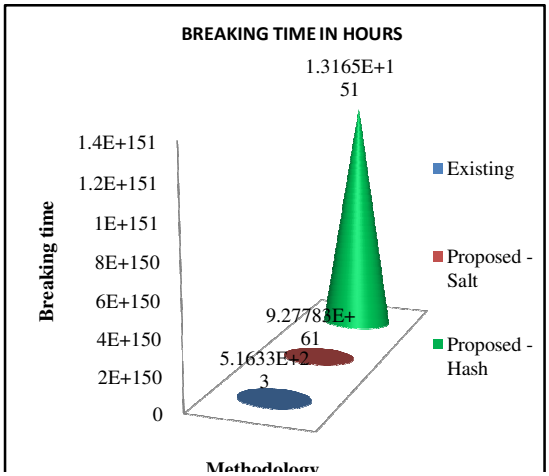

Figure 6: Breaking time in Hours

The proposed authentication system implements cryptographic salt and hash technique to enhance the authentication system and to prevent the system from various attacks. From Figure 6, the proposed authentication system took more time to break the password than the existing methodology. The hacker drops the process of hacking the password when the breaking time increases. This tends to secure the authentication system from the various attacks.

e. Attacks Handled

The attacker breaks into the system by proving to the application that is known and valid user, the attacker gains access to whatever privileges the administrator assigned that user. This means that if the attacker manages to enter as a normal user might have limited access to only view some important information. The following attacks are handled in the proposed methodology.

- Guessing Attacks
- Brute Force Attacks
- Dictionary Attacks
- Shoulder Surfing Attack
- SQL Injection

In proposed authentication system the cryptographic salt value and hash value are generated. This prohibit the SQL injection since when the password mismatched it terminate the process and exit from the system when it fails to login for three consecutive times. Graphical image is used to login to the proposed authentication system. Special character "=" is not initialized. Due to this the hacker fails to inject the malicious codes listed above.

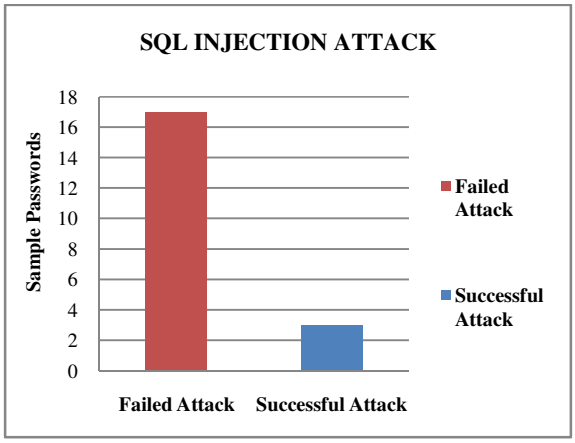

Figure 7: Breaking time in Hours

In Figure 7, the SQL injection attacks performed for sample of 20 datasets from 150. In proposed authentication system the cryptographic salt and hash technique are generated to prevent the execution of malicious code in the authentication system. And also two factor authentication of formula authentication is implemented in this proposed authentication system. The hashed password is compared to find the legitimate user to access the authentication system. This Figure depicts that the proposed authentication system have high failure rate of performing SQL injection attack than the existing methodology.

VI. CONCLUSION AND FUTURE SCOPE

The proposed authentication system implements a secured authentication system using the graphical passwords will secure the authenticated system from illegitimate user and hackers. This securing the system with two folds security by implementing the two stages of login to access the account, the applying of formula authentication in second phase to secure the authenticated system from unauthorized persons to

access data. Detection of brute force attacks and dictionary attacks is achieved by imposing the lengthy password and improves the complexity of the password. In this proposed authenticated system the password should be minimum of 12 characters and maximum of 20 characters. And each password must be in the combination of uppercase, lowercase, digits and special characters which gives the complexity (Detecting the password strength by satisfying the three primary factors like length, complexity and unpredictability of passwords), and also avoiding the password shoulder surfing attack by the use of the graphical image to enter the password instead of using the keyboard.

Proposed authentication system implements a cryptographic salt and Hash Technique using the RNG Crypto Service Provider and SHA 512, and also by blocking the user who failed to access their account and identify the of legitimate and ill-legitimate users using white list and black list to prevent the SQL injection. The users who accessed their account are listed under white list. Others who failed to login into the system are listed as black list. This research concludes that the SQL injection is prevented by using the text based graphical password and also block the illegitimate user to login to the account by blocking their account when it exceeds the three failed logins.

In future Simple formula used in this methodology which will be more complex in future. Algorithm is developed to execute from the server side, which can be implemented on the client side as well.

REFERENCES

1. *Diksha G. Kumar , MadhumitaChatterjee , "Detection block model for sql injection attacks" , I.J. Computer Network and Information Security, 2014, 11, 56-63.*

2. *KanchanChoudhary, 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.KameswaraRao, SushmaYalamanchili," 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 , SaranyadeviC,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. *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.*

7. *SaurabhSaoji, SwapnaliBhadale, HarshadaWagh, "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.*

8. *Shaukat Ali, AzharRauf, and HumaJaved, "SQLIPA: An authentication mechanism against sql injection", European Journal of Scientific Research, Volume 38, No. 4, 2009.*

9. *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.*

10. *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.*