Journal for Research in Applied Sciences and Biotechnology

www.jrasb.com

ISSN: 2583-4053

Volume-2 Issue-1 || February 2023 || PP. 134-141

https://doi.org/10.55544/jrasb.2.1.18

Highly Secure and Easy to Remember Password-Based Authentication Approach

Sayed Elham Sadat[1], Hedayatullah Lodin[2] and Nazak Ahmadzai[3]

[1]Assistant Professor, Computer Science Faculty, Department of Information Technology, Kabul Education University, Kabul, AFGHANISTAN.

[2]Assistant Professor, Computer Science Faculty, Department of Information Systems, Kabul University, Kabul, AFGHANISTAN.

[3]Education Faculty, Department of Computer Science, Paktia University, Gardiz City, Paktia, AFGHANISTAN.

[1]Corresponding Author: sayed.elham@kuk.ac.in

www.jrasb.com || Vol. 2 No. 1 (2023): February Issue

Received: 13-01-2023	**Revised:** 03-02-2023	**Accepted:** 13-02-2023

ABSTRACT

Everyone connected and using the Internet is concerned regarding the security and also the privacy of their sensitive information available on the Internet. As authentication is the fundamental part of security, there are different authentication mechanisms through which the systems can be secured. The password-based authentication mechanism is a cheap and easy method for enforcing authentication in the systems for many years. The weakest aspect in password security is human, as they choose weak and easy to guess passwords or a highly secure and complex password which might be difficult to remember and recover the password. On the other hand, Dictionary and Brute force attacks are widely used to compromise the passwords of the users over the Internet. In this paper, a password generation system is proposed which generates a password based on the user's input like, time and location data. The system generates a password that is highly secure, easy to remember, easy to recover, and can effectively defend against Brute force and dictionary attacks. The generated passwords have been checked in three online password checkers, which verifies that the system is generating highly secure and crack resistant passwords. The system is implemented using PHP scripting language with a user-friendly environment.

Keywords- attacks, brute force attack, complex password, dictionary attack, password, password generator, password recovery, secure password, strength checker.

I. INTRODUCTION

Password-based authentication mechanism is the key to security, it is used to secure the accounts and other personal data from unauthorized access. Password authentication is the cheapest mechanism in order to authenticate a system. Passwords are the most vulnerable part of a system in a network. Mostly the passwords created by the users are personal information such as names and telephone numbers, the users are selecting this information as their password because they can easily remember them, and sometimes they use one same password for many applications and websites, because it would be difficult for them to remember too many passwords. These passwords are easy to guess and easy to crack by a hacker. On the other hand, strong passwords are difficult to crack but not easy to remember. An intruder can perform different attacks in order to steal the password of a user. The attacker can take the advantage as the users used common, easy to guess, and short words as their passwords, they will be able to perform dictionary attacks to steal the passwords.

Using strong passwords is one of the main parts of password policies which should be strictly followed while creating a password for a system. A strong password should have both upper case and lower-case

ISSN: 2583-4053

Volume-2 Issue-1 || February 2023 || PP. 134-141

https://doi.org/10.55544/jrasb.2.1.18

letters, digits, punctuations and the length of the password should be more than 8 characters. The desired password should be easy to remember so that it should not be needed to write it down somewhere.

According to the Verizon 2017 Data Breach Investigation Report, 81% of the data breaches in the systems are caused due to that hacker had stolen and/or the users used a weak password. [1].

Dictionary attacks attempt to defeat password protected system by systematically entering each word in a dictionary as a password. This attack is mostly successful because many users are using ordinary and common words that are easily available in dictionary. The limitation of dictionary attack is that they are not effective with the systems in which multiple word passwords and also in the systems in which random permutations of lowercase and uppers case letters combine with numerals and special characters are used.

On the other hand, Brute force attacks, in which the attacker tries every combination of numbers, letters, and also special characters until the password is discovered is an another most common type vulnerability for password-based authentication systems. This attack is carried out with the help of scripts or bots which target a website login page. The main difference between other cracking methods and brute force is that it does not use intellectual strategy, they simply try different combinations of characters until the prefect combination which matches the correct password is achieved. The main advantage of brute force attack is that it is simple to perform. Every password-based authentication system can be cracked with the help of brute force attack. Accordingly, the amount of time taken by a brute force attack to crack a system password is an effective metric for determining a system security level. As Brute force attack, may have to run through every possible combination of the letters, numbers and special characters before achieving the desired password, that makes the brute force attack very slow. The slowness is respectively related to the number of characters in the targeted string. As an example, a four characters password takes longer time as compared to three characters password and relatively, a five characters password takes longer time than four characters password to crack and achieve the desired goal. If the target is adequately long and having different characters combinations, it could take days, months, years or even decades to crack using the brute force attack.

In this paper, the human factor problems with the text-based password authentication is investigated and proposed a usable solution to these problems by focusing on both types of attacks: Brute force and Dictionary attack. Finally, a user-friendly, automated, and robust system is proposed which generate password based on user input, time, and location data (Longitude and latitude) which is provided by the user. The generated passwords are highly secure, easy to remember, and easy to recover. As the user is able to regenerate the password by providing the same data.

II. DESIRABLE CHARACTERISTICS OF PASSWORDS

The following are the desirable characteristics of passwords, which should be considered while choosing a password.

A. Reasonable Length

The password length is an important factor in password security, as the length of the passwords are increasing, the strength and challenges for cracking the password are increasing. Therefore, 12 characters or more passwords are recommended.

B. Mixed Symbols, Numbers, and Caps

Another characteristic of a strong password is that it should include numbers and symbols, more diverse character, many complex passwords, this characteristic will decrease the chances of successful brute force attack.

C. Substitutions

Some alphabet letters and some numbers can be substituted with some special characters, like “@” for “a”, “!” for “i”, “$” for s, and etc. This will increase the complexity of the password.

D. Easy to Remember

The chosen passwords should be easy to remember, as there are third-party methods available for resetting the passwords, but still there are some chances that those parties could also be compromised. Therefore, the password chosen should have the feature which can easily remember. Forgetting the password and resetting it, will waste your and system administrator time.

E. Not Easy to Guess

Short, common, and easy to guess words and numbers, and also words available in dictionary should not be included in the password. As the dictionary attack will be used to compromise the password.

F. Password Change

The user should change, currently using password after using it for some time, because when the password strength is not enough, within a specific amount of time, a brute force attack can compromise the target password, therefore, the passwords should be changed after a specific time.

G. No Password Save in Browser

The browsers should not be allowed to save any type of password, as the browsers are easily hacked and the information can be directly taken from it.

III. MOTIVATION AND OBJECTIVE

Every person using different online services or connected to those services are concerned with the

ISSN: 2583-4053

Volume-2 Issue-1 || February 2023 || PP. 134-141

https://doi.org/10.55544/jrasb.2.1.18

security and also the privacy of their personal information from attackers. As the new tools are developed in order to protect the security of the users, the new techniques are also rapidly developed to break the security. User authentication is one of the ways in order to provide security for the users and systems.

Password-based authentication mechanism is a cheap and easy method for enforcing the authentication in the systems for many years. the weakest aspect in password security is human, as they choose weak and easy to guess passwords which do not follow the proper password policies or they may select some password as the will be difficult to remember, to recall the password, they will try to write it in a notebook, sticky, or save it in their devices which can be easily compromised later.

The objective of this paper is to design user-friendly online password generation system, which will effectively address the two mostly occurred, dictionary and brute force cracking attacks on password, and also the problem with remembering and recovering the password. The proposed system will generate highly secure and strong password based on the information provided by the user, which will be easy to remember and easy to recover.

IV. RELATED WORK

One of the most common reasons that the hackers can easily access the protected systems is having a weak and insecure authentication system. Simple and common password, which can be easily guessed can enable them to gain access to the system. Having a password that is difficult to guess makes it prohibitively very difficult to a common hacker to break into a system. The most difficult the password, the lower the likelihood that a system will be a victim.

Based on the semantic transformation of a given password Yang et al. [2] proposed a password enhancement method that can analyze the semantic structure of the password in an effective manner. And the experiment was conducted on publicly available real-world passwords data sets. And according to that experiment, the system can effectively reduce the guesses.

Different open-source applications can be used by organizations in order to improve compliance with the password policies and also ensure a better quality of passwords. A study of two open-source tools that are easily customizable was conducted by Frenz [3]. One of the tools is used to generate secure random passwords, and the other tool is based on exemplify technique which ensures password quality and compliance. According to the hypothesis discussed regarding the easy customizable open-source password generation and also password complexity checking tools can effectively improve the security of the systems.

Accordingly, AES encryption process of passwords which are in transmission and storage can be improved by a method introduced by Liu et al. [4]. Which is based on adding the random number as a key in order to encrypt the password. RSA transmission encryption method is being introduced, and also compared both RSA and AES encryption methods. Their experiment shows that as compared to RSA, advanced AES is much faster and secure.

According to Tsokkies et al. [5] the bad password construction strategies should be taken care while designing educational activity tools. Relatively, they have designed a tool that can complement awareness and also training efforts to the users that such relevant passwords can be generated, therefore they need to avoid them and help them to select strong passwords. The proposed tool is identifying information from users in regards to their family, interest, and also allowing user to add their desired filed as well, relatively, the tool present list of categories of specific construction strategies. In the end, based on users selected password length, list of potential passwords will be generated to the user, and can search for the specific password that the user was considering is included in the list.

The theory of human ecological memory in order to explain the cost of accounts passwords to the users was introduced by Zhao et al. [6]. An experiment on 304 users was performed, in which they proved that the security benefits of modifying high-value account are greater, whenever the users are modifying a single account. Modifying accounts with password reuse in case of modifying multiple accounts can cause greater security for the user. Their experiments show that whenever the users are modifying accounts, including personal information will increase the password strength and also minimize the memory cost. They evaluated the memory cost of user passwords from ecological memory and also password strength aspects. They have proposed a model that quantitively explains when the users manage multiple accounts at the same time and also relatively achieve a higher security level.

PassGen tool is enable to generate passwords with the help of semantic annotation using context-free grammars. With the help of context-free grammar, the system can make an infinite set of strings and objects. In the proposed system, the user will specify their interest for example music or movies, phrases form the interest will be combined with most three digits and one special character to generate a strong memorable password. [7]

Dynamic password providing idea which is based on user's knowledge on the depicted picture was introduced by Basharzad et al. [8] in which the proposed approach is cable to resolve the short comes of the biometric authentication mechanism. Their method authenticates the users based on selected points on a picture. They claimed that their idea is capable to reduce

ISSN: 2583-4053

Volume-2 Issue-1 || February 2023 || PP. 134-141

https://doi.org/10.55544/jrasb.2.1.18

the cracking and forgetting issues with the password system.

A new improved approach to generate and manage passwords was presented by Billa et al. [9] in their approach there is no need to store the password anywhere, instead, it will only save the three parameters which are set by the user in order to identify them in the local storage of the device where the system is installed. In their method, multiple hashed parameters are used to generate a password, which will be used as the password of the system where the user wants to register. The problem of memorizing multiple passwords was solved by proposing to use three parameters in which the two parameters will remain constant for all systems. The proposed system is implemented using an android application called PassMan.

A password generator scheme was introduced and analyzed by Maqbali et al. [10], with the name of AutoPass. Their scheme resolves different issues available in previous systems with the help of new techniques. With the help of mentioned system, the users can generate passwords with features like forced password change, and password meeting the site-specific requirements. AutoPass allows the cross-platform working procedure.

online authentication mechanism called combinedPWD was proposed by Zheng et al. [11], which insert different separators into the password in order to increase the strength of existing password authentication system. The mechanism allows the users to insert spaces (separators) anywhere in the password while registering their account, the website will record the number of spaces in every gap. If the password entered is wrong, or if the password is correct but the number of spaces are wrong, the user will not be authenticated. According to the authors, the proposed mechanism can avoid brute force and also dictionary attacks effectively. For keylogger attack, a 2-dimensional mechanism is also proposed.

A strong virtual password authentication mechanism consists of rules like minimum and maximum password limit, passwords should be consisting of numbers, symbols and letters, was proposed by Rahiem et al. [12]. They claimed that, those rules can significantly increase the cracking time of passwords to nine centuries, which is the result of Kaspersky lab secure password measurement. Two algorithms were introduced, one for character generation of virtual password. The second for login process, in which the real password from the database will be converted to virtual password with the help of replacing each character of real password with the characters generated in first process.

Attempt-based password system in which there is three passwords for first three attempts and then repetition occurs was proposed by Khan et al. [13]. Accordingly, the user will be remembering only one password rather than multiple passwords approach. For example, the user needs to remember only password for the third attempt. The two other passwords for first and second attempts are just a fragment of the third attempt password. For a successful login, the user needs to know only two things. The correct password and number of the attempt. If in the first attempt, the entered password is correct, then there is no need to enter the passwords for the two next attempts. Accordingly, the hacker needs to know the above mentioned two things to crack the system password. Therefore, the efforts to crack o break the password will be bounded to only three times. The proposed system can defend the brute force attack effectively.

On the other hand, multi-level authentication techniques, in which the user is strictly authenticated in multiple levels in order to access a system is a good option for having a highly secure authentication mechanism. Dinesha et al. [14] proposed a multi-level authentication system specifically for cloud services, in which the system generates the password and concatenate the password at multiple levels. The users will be authenticated only when the password authentication is successful in all the previous levels. The proposed system architecture is consisting of two entities, one who provides the could services and the another one is authenticated client organizations who access the could. The multiple level of authentication is organized as: first level authentication – where the organizational level password authentication is done, which is authentication for cloud vendor. Second level authentication- where the team level authentication is done, which authenticates the particular team for access the could services. Likewise, there can be more than two authentication levels. Finally, the last level is the user-level password authentication.

An integrated secure mechanism with the help of PHP and MySQL functions to reset the user passwords which will improve the security for resetting passwords was presented by Huang [15]. The password reset mechanism, rest the password by integrating the front-end and back-end information. They claimed that, with the help of this method, the unnecessary access to the database will be reduced. Which will prevent attacks on the database.

A survey was conducted by Maqbali et al. [16] on recovery emails sent from the top 50 websites on the internet. They have investigated the structure, content, and design issues in both security and also usability aspects. Consequently, the techniques which are used for recovering the passwords and vibration in the contents of emails are also investigated. Finally, a number of recommendations were formulated to have best password recovery email which will maximize both, security and usability.

Journal for Research in Applied Sciences and Biotechnology

www.jrasb.com

ISSN: 2583-4053

Volume-2 Issue-1 || February 2023 || PP. 134-141

https://doi.org/10.55544/jrasb.2.1.18

V. PROPOSED WORK

Our objective is to develop an application which generate password based on user input data which are easy to them to remember. The inputs will vary for every individual, so the password will be too difficult to compromise.

An efficient algorithm is proposed which generate password based on user input like time, and location data (Longitude and latitude). The password generated in using this algorithm is highly secure, easy to remember, and easy to recover. The user is able to regenerate the password by providing the same data.

A. Algorithm

In the methodology, at first, the user provides his/her name, any desired city name, and a time which can be the time of generating the password or any other desired time. when the user is selecting a city, the system will take the first two digits of its longitude and latitude data in order to generate the password. Combinedly (name + latitude + longitude + time) will form a password for the user which is will be highly secure, easy to remember, and easy to recover. Now the user only needs to remember the location (name of the city) and time in order to recover the forgotten password.

By just entering its own name, city name, and time, the user will be able to recover the old password generated by the system. the users will be asking to change the city after an interval of time, in order to avoid the hackers to know about the city name. By combining the city and time data with the user name, it would be difficult to the hacker to guess and crack the password.

Algorithm - 1 Password Generation based on User's Input (Location Data)

Require: Name, city name, time
1: **Begin**
2: *input_data* ← name, city name and time
3: *special_chars* ← {$, @, |, 0, !, #}
4: *alphabets* ← {s, a, l, o, I, h}
5: *special_chars2* ← {*, +, -, ^, !, ?, #, ~, @, !, >, <, &, _, |, \, %}
6: *name* = user input name
7: *city* ← user input city name
8: *time* ← concatenate hour with minute and add ":" in between
9: *lat* ← whole number of latitude(*city*) from database
10: *lng* ← whole number of longitude (*city*) from database
11: *final_password* ← capitalize first and last character of (*name*)
12: *final_password* ← *final_password*.replace(*alphabets, special_chars*)
13: *final_password* ← append "@" and *lat,long* at the end of *final_password*
14: *final_password* ← append "-" and *time* at the end of *final_password*
15: *L* = len(*final_password*)
16: **If L < 8 then**
17: *final_password* ← append (8-L) number of *special_chars2*
18: **print** *final_password*
19: **End if**
20: **End**

In the above Algorithm, the term "name" shows the user's name provided to the system, "city" is the name of the city which user chose and "time" is the hour and minutes that the user selected. According to Algorithm 1 line 8, Hour and Minutes of the selected time will be combined, and ":" character will be added in between them.

A database is used in this system, in which the data about the world countries, their cities and latitude and longitude information of cities are stored. In Algorithm 1 lines 9 – 10 The system will extract the whole number of the latitude and longitude information of the selected city form database. For example, the latitude and longitude for "Kabul" city is ("Latitude: 34.5167", "longitude: 69.1833") so, the system will extract the data as ("Latitude: 34", "longitude: 69"), and this information will be combined with the name provide by the user in order to generate a password. Afterward, based on line 11 of Algorithm 1, the first and last character of name input will be capitalized.

Subsequently, the system will append and replace some letters of the text which is located in final_password with some special characters according to their physical similarity in line 12 of Algorithm 2. For example, in the world "swati" the letter "s" will be replaced with "$", the letter "a" will be replaced with "@" and the letter "i" will be replaced with "!".

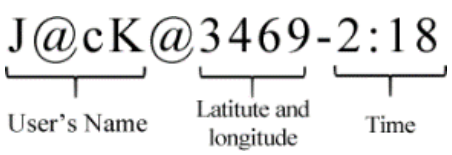
Finally, the system will generate the password by appending ("@", "lat", "lng", "-" ,"time") with the final_password. In Algorithm 1 these steps are covered in lines 13 – 14.

The following is a password generated by Algorithm 1:

User Input:

- Name: jack
- City: Kabul
- Time: 2:18

System Output:



Journal for Research in Applied Sciences and Biotechnology

www.jrasb.com

ISSN: 2583-4053

Volume-2 Issue-1 || February 2023 || PP. 134-141

https://doi.org/10.55544/jrasb.2.1.18

VI. FEATURES OF THE PROPOSED SYSTEM

A. Easy to Remember Passwords

The system is generating passwords based on user's input, those inputs are familiar to the users and easy to remember. The generated passwords are totally random and harsh like some other online password generators. On the other hand, the systems are designed with a user friendly and easy to use interfaces which enables anyone to use it easily.

B. Handling Uncertain Inputs

The systems are capable to find and resolve the issues with uncertain or ambiguous inputs. According to algorithm 1, in which the user is asked to enter his/her name, select a city and a time, if the user provides data that are combinedly less than 8 characters which do not satisfy the password policy [39], the systems will add some special characters to the password which will full fill the required policy regarding the length of a password, algorithm 1 lines 16 – 19.

C. User Safety

As the system is based on run-time methodology, neither they save nor they keep a log of any input provided by the user. In Algorithm 1, the user is providing, first name, city and time, based on which the password will be generated. later on, by remembering only city and time, the user will be able to recover the forgotten password easily.

D. Cracking Attack Resistant

In the proposed system, two mostly common cracking attacked which targets passwords in a system is taken into consideration. The generated passwords are highly resistant against different password cracking attacks, especially Brute force, and Dictionary, the defensive and attacking mechanisms for both types of attacks is explained below.

1) Resistant Against Brute Force Attack:

In Brute force attacks, the attacker tries every combination of numbers, letters, and also special characters until the password is discovered. As Brute force attack, may have to run through every possible combination of the letters, numbers and special characters before achieving the desired password, that makes the brute force attack very slow. The slowness is respectively related to the number of characters in the targeted string. As the short passwords take less time to crack, accordingly, the target is adequately long and having different character combinations, it could take days, months, years or even centuries to crack using the brute force attack. In the proposed system, the generated passwords are having different types of special characters along with capital and small letters and numbers with a minimum length of 8 characters.

2) Resistant Against Dictionary Attack:

Dictionary attacks attempt to defeat password protected systems by systematically entering each word in a dictionary as a password. This attack is mostly successful because many users are using ordinary and common words that are easily available in the dictionary. The dictionary attack is successful when there is one name or a word, or sometimes when there are composite words like ("Love you", "text book"). Accordingly, the proposed system is effectively defending this attack, because there is no chance that the systems will use only single composite name or word in the password as in proposed system the name provided by the users is combined with the location and time data along with special characters, which can defend against dictionary attack.

VII. EXPERIMENTAL RESULTS

In order to perform experiment, a total of ten passwords from ten unique inputs are generated. Accordingly, the strength and crackability of all generated passwords are tested on three popular online password checkers named "Kaspersky Password Checker" [17], "Thycotic Password Strength Checker" [18] and "Cryptool Password Meter" [19].

The "Kaspersky Password Checker" is checking the strength of the password by performing different types of brute force attack which a person can execute using a personal or a home computer. Using this tool, the results for 10 passwords generated, is showing that the minimum time for cracking a generated password from sample inputs, is 55 centuries and the maximum time for cracking a generated password is 10000+ centuries, using brute force attack. This proves that the proposed system is generating highly secure passwords which can effectively defend brute force attack.

The "Thycotic Password Strength Checker" is checking the password strength of a given password against brute force and dictionary attacks. Using this tool, the results is showing that the minimum time for cracking a generated password from sample inputs, is 15 billion years and the maximum time for cracking a generated password is 16 quadrillion years, using brute force and dictionary attacks, which proves that the proposed system 2 is generating highly secure and almost impossible to crack passwords.

The Cryptool Password Meter is checking the strength of a given password in 5 different password checkers, estimators, and password managers like, KeePass, Mozilla, PGP, zxcvbn, Stutz' PS. It shows the rating of a password in percentage from all mentioned tools. And also calculate the total of all results achieved. Using this tool, the results is showing that the lowest rating in percentage, is 75% and the highest rating in percentage is 87% which proves that the proposed

ISSN: 2583-4053

Volume-2 Issue-1 || February 2023 || PP. 134-141

https://doi.org/10.55544/jrasb.2.1.18

system 2 is generating highly secure passwords. The below figure shows the experiment results of Cryptool Password Meter for the proposed system.

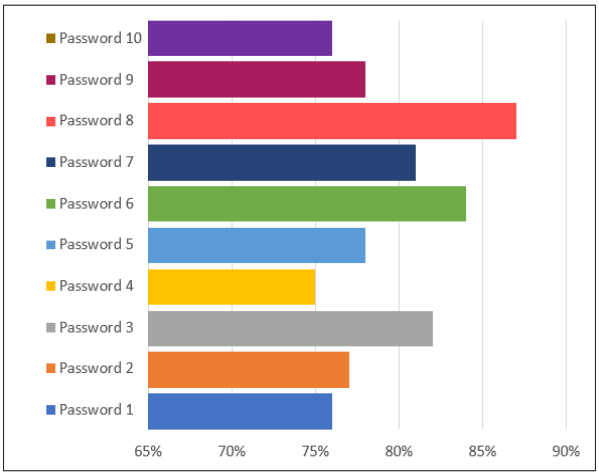


Figure 1: Cryptool Password Meter Result

VIII. CONCLUSION

Authentication is the fundamental part of security, Password-based authentication mechanism is an easy method for enforcing the authentication in the systems. The human factors are causing the security of password-based authentication to be compromised. The proposed system in this paper is generating password based on user's input. The password is generated based on user input, time, and location data. The generated passwords were highly secure, easy to remember, and the method for recovering the forgotten password was efficient and easy. As the user is able to regenerate the password by providing the same data.

The generated passwords have been checked in three online password checkers, the results from all three online password checkers indicate that algorithm is generating highly secure passwords, which are crack resistant, and many centuries are required to crack the passwords.

As there are three main factors in authentication, which are: "Something you know", "Something you have", and "Something you are". According to these factors, the proposed system in this dissertation covers the "Something you know" section of the authentication mechanism. As future work, the proposed systems in this dissertation can be extended by adding voice recognition parameter in the password generation process, which will cover "Something you are". Since password-based authentication is the cheapest authentication mechanism, on the other hand, biometric is a costly authentication mechanism, therefore, the sound recognition parameter is a good option for including it in the password generation process, as almost most of the devices are equipped with sound capturing hardware. This will increase the security and usability, in addition, the generated passwords will be much more personalized and easier to recover.

REFERENCES

[1] Verizon, "2017 Data Breach Investigations Report," Verizon, United States, 2017.

[2] D. He, X. Yang, B. Zhou, Y. Wu, Y. Cheng and N. Guizani, "Password Enhancement Based on Semantic Transformation," *IEEE Network* , vol. 34, no. 1, pp. 116 - 121, 2019.

[3] C. M. Frenz, "Improving Organizational Password Policy Compliance via Open Source Tools," in *2011 IEEE World Congress on Services*, USA, 2011.

[4] Y. Liu, W. Zhang, X. Peng, Y. Liu, S. Zheng, T. Wei and L. Wang, "Design of password encryption model based on AES algorithm," in *2019 IEEE 1st International Conference on Civil Aviation Safety and Information Technology (ICCASIT)*, China, 2019.

[5] P. Tsokkis and E. Stavrou, "A password generator tool to increase users' awareness on bad password construction strategies," in *2018 International Symposium on Networks, Computers and Communications (ISNCC)*, Italy, 2018.

[6] Y. Zhao, W. Li, Z. Zhang and P. Wang, "Password Expiration Strategy: A Perspective of Ecological Memory," in *2019 IEEE Fifth International Conference on Big Data Computing Service and Applications (BigDataService)*, 2019.

[7] A. Ade-Ibijola and B. Ogbuokiri, "Syntactic Generation of Memorable Passwords," in *2019 International Multidisciplinary Information Technology and Engineering Conference (IMITEC)*, South Africa, 2020.

[8] S. N. Basharzad and M. Fazeli, "Knowledge based dynamic password," in *2017 IEEE 4th International Conference on Knowledge-Based Engineering and Innovation (KBEI)*, Iran, 2017.

[9] J. B. Billa, A. Nawar, M. M. H. Shakil and A. K. Das, "PassMan: A New Approach of Password Generation and Management without Storing," in *Conference: 2019 7th International Conference on Smart Computing & Communications (ICSCC)*, 2019.

[10] F. A. Maqbali and C. J. Mitchell, "AutoPass: An automatic password generator," in *2017 International Carnahan Conference on Security Technology (ICCST)*, Spain, 2017.

[11] W. Zheng and C. Jia, "CombinedPWD: A New Password Authentication Mechanism Using Separators Between Keystrokes," in *2017 13th International Conference on Computational Intelligence and Security (CIS)*, China, 2017.

[12] M. Z. F. Rahiemy, P. Sukarno and E. M. Jadied, "Hardening the Virtual Password Authentication Scheme," in *2018 6th International Conference on*

ISSN: 2583-4053

Volume-2 Issue-1 || February 2023 || PP. 134-141

https://doi.org/10.55544/jrasb.2.1.18

Information and Communication Technology (ICoICT), Indonesia, 2018.

[13] S. Khan and F. Khan, "Attempt based password," in *2016 13th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, Pakistan, 2016.

[14] H. A. Dinesha and V. K. Agrawal, "Multi-level authentication technique for accessing cloud services," in *2012*, India, 2012 International Conference on Computing, Communication and Applications.

[15] C.-Y. Huang, "An Integrated Mechanism for Resetting Passwords in Web," in *The 2017 International Conference on Computational Science and Computational Intelligence (CSCI'17), At Las Vegas, NV, USA.*, USA, 2017.

[16] F. A. Maqbali and C. J. Mitchell, "Email-based Password Recovery - Risking or Rescuing Users?," in *2018 International Carnahan Conference on Security Technology (ICCST)*, Canada, 2018.

[17] "Kaspersky Password Checker," Kaspersky, [Online]. Available: https://password.kaspersky.com/.

[18] Thycotic Password Strength Checker," Thycotic , [Online]. Available: https://thycotic.com/resources/password-strength-checker/.

[19] "Cryptool Password Meter," Cryptool Password Meter, [Online]. Available: https://www.cryptool.org/en/cto-highlights/passwordmeter.