International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-4, February 2020

User Authentication and Password Protection using an Algorithm ACR

Patlolla Aravind Reddy, Pakkireddy Harsha Chandan Reddy

Abstract*: In general, every web or android based application required security for login. So for that we have to encrypt the password while signup itself,these encrypting the password there are many algorithm but by trail and error method or by using some attacks(man in middle attack etc..,) we can know the password, so in order to reduce attacks we came up with new algorithm to protect the password. Even after getting the password where many of the applications like banking , messaging application uses OTP process. These OTP could also be stolen easily (although it is difficult to do so) but still. So to over come this we came up with modified OTP process that decreases the time and it will be difficult to stole. So here we first we will encrypt the password using algorithm ACR and when user want lo login we go with the modified OTP process.

***Keywords* : security, encyption, OTP, man in middle attack.**

I. INTRODUCTION

The user authentication is an essential requirement for the current protected web-based applications now a days. The common ways for authentication is through passwords, face or fingerprint and ID cards based which are normally accustomed limit access to a variety of systems[1].

Now a days password encrpyion plays a major role in securing the user details. This password encrption can be done in many ways, every application in real world use password encrytion storage in different ways. One application may use hashing processes and other may use any algorithms on their own according to their satisfactory and complexity. User authentication should have the following password should be easy to remember, user authentication protocol should be executed quickly and easily and the password should be secured [2].

In this paper, when user sign up the password will be encrypted and then encrypted password will be stored in the database. In these encryption we considor an array, where the array consits of all letters and symbols. Now encryption is done using this array and space value. user authentication is verifing whether the user using his own credentials(correct credentials).To overcome this we came up with modified OTP. When the user try to login, first he enters the userid, then he get the message regarding OTP format.

Revised Manuscript Received on February 28, 2020.
***** Correspondence Author
Patlolla Aravind Reddy*, School of Information Technology and Engineering, Vellore Institute of Technology, Vellore.
Pakkireddy Harsha chandan Reddy, School of Information Technology and Engineering, Vellore Institute of Technology, Vellore.

Then the password from database is feteched and decrypted and compared with the user password and it allows if credentials matches.

While consolidating letters and numbers muddled passwords does to some degree assaults and postpones aggressors from trading off records, it isn't easy to use. Researcher and industries have proposed many other alternatives to solve this problem such as OTP (One Time Password) and grid unlock pattern [3].Previously, attackers have undermined numerous single direction and single factor user authentication schemes by creating phishing websites similar in appearance to legitimate websites and then spreading these websites via emails, DNS poisoning, Tabnabbing, content injection or Browshing[4].Chunling CHEN in 2016[5] has proposed mutual authentication scheme that be suitable for RFID based on both lightweight and security. XUE-GUANG WANG in 2006[6] has proposed modified remote user authentication scheme. ShipraKumari in 2014[7] has proposed remote user authentication scheme which is based on the tangent theorem of circle. Nilay Ylldmm in 2015[8] has proposed biometric identification features to mobile devices to increase their security features.

II. PROBLEM FLOW

Firstly user need to sign up, in this process the password will be encrypted and saved in database. so that middle person who are dealing with database works can not view password. If user already exist he can directly skip signup. After submitting the registration page it will be redirected to Login page which contains a field where user need to submit User Id. Based on User Id , here undergoes two processes.

1) Password is fetched from database
2) Phone number is fetched from database

Password that is fetched is decrypted to undergo validation OTP(Random Generation) will be send to registered phone number including format of password entry which is decided randomly.(eg XXXXOTP or OTPXXXX).If message is XXXXOTP the password field should contain password followed by OTP(concated). If message is OTPXXXX the password field should conatin OTP followed by password.
Finally, Validation is done to authorize the user.

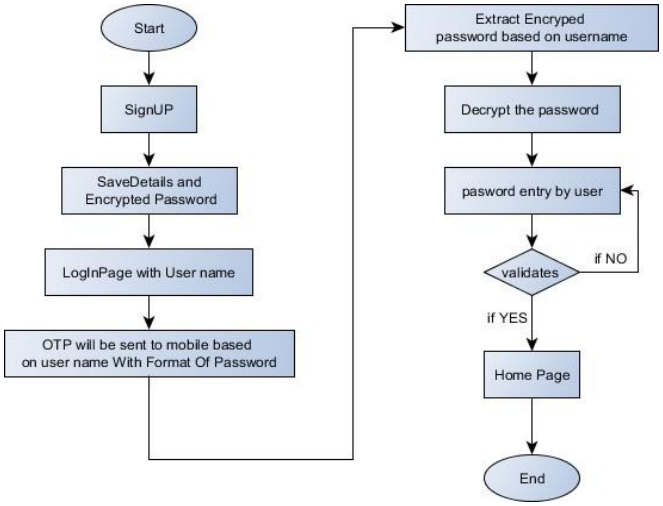


Fig 1 . Overall Process

This process is done using

i. Netbeans to create a sample application
ii. Wampp server as Database
iii. Text local website to send OTP in message format.

III. ENCRYPTION PROCESS FOR ACR

i. The password given by the user will be saved in database in encrypted manner. A huge set of characters will be intialized in an array.
ii. Initially a space value will be generated.
iii. Each two characters of the password will be inserted with randomly generated characters acoording to the sapce value.
iv. Now the total number of characters will serve as a base value or a key. Each character present in the password will be multiplied with base value.
v. Now the multiplied value will be divided into two factors and the index charcter will be fetched from array using the two factors .
vi. Now the character before multiplication will be repled with those two characters (i.e factors)and this process will be repeated for whole password.
vii. Now the index charcater of the base value will be appended to the modified password and it is saved in the database.

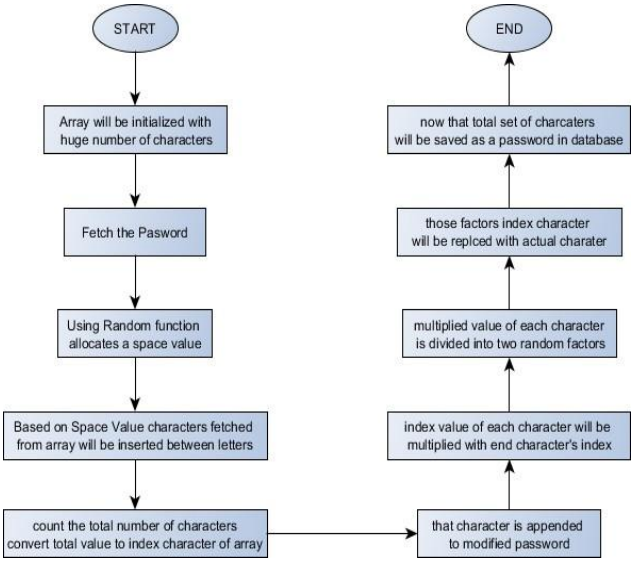


Fig 2 . Architecture for Encryption of ACR

IV. DECRYPTION PROCESS FOR ACR

i. The password that is saved in the database will be fetched The same array used in encryption is used here.
ii. Array index value of last character present in password will be fetched.
iii. Now two consecutive character of paasword will be multiplied (index values are taken from array)
iv. Now the multiplied value will be divided with the base value
v. The output value is used to fetch the characater from the array which is replaced with those two characters.
vi. Finally the last character will be deleted from the string(i.e Base value will be deleted)

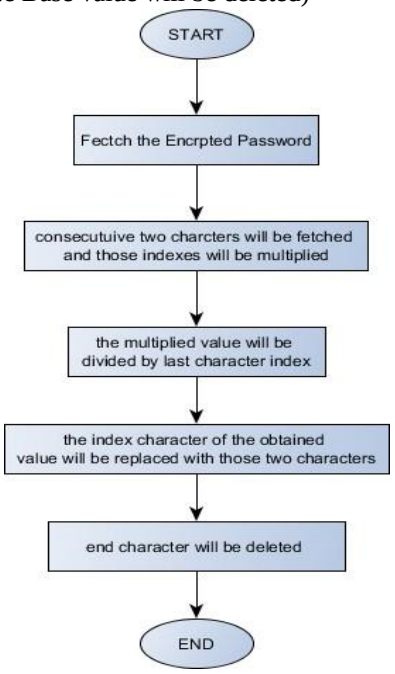


Fig 3 . Architecture for Decryption of ACR

V. STEPS INVOLVED IN THIS PROCESS

Step -1: Registration phase

User has to signup first, while submitting the signup form the password will be encrypted and stored in the database.

Fig 4. Registration phase

International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-4, February 2020

Below Fig 5 show's how encrypted data look in the database.

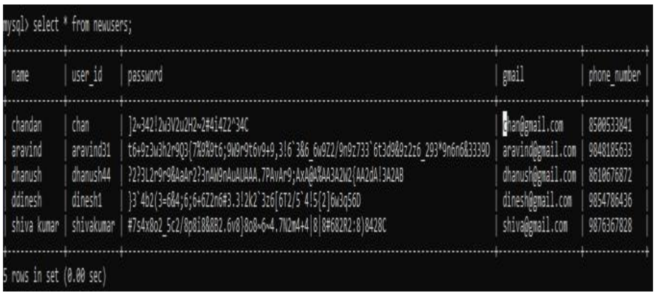


Fig 5 . Few Sample Database values

Step -2:Login Page

After the registration, when the user try to login first he has to submit User id. Then user get the OTP, the OTP will be in form of OTPXXXX or XXXXOTP.

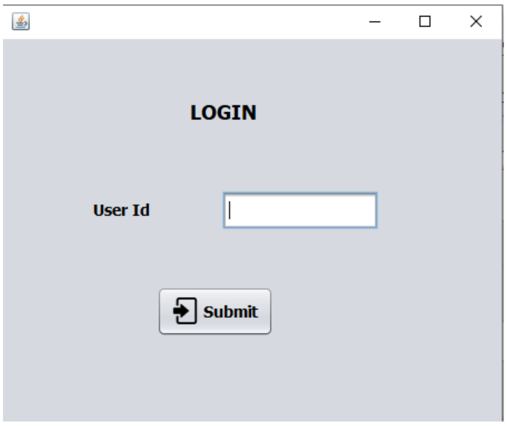


Fig 6.Login Page

Step -3:OTP Received to mobile with format

i. If the OTP is like "OTPXXXX" then user password will be OTP folloed by Password.

ii. If the OTP is like "XXXXOTP" then user password will be password followed by OTP.

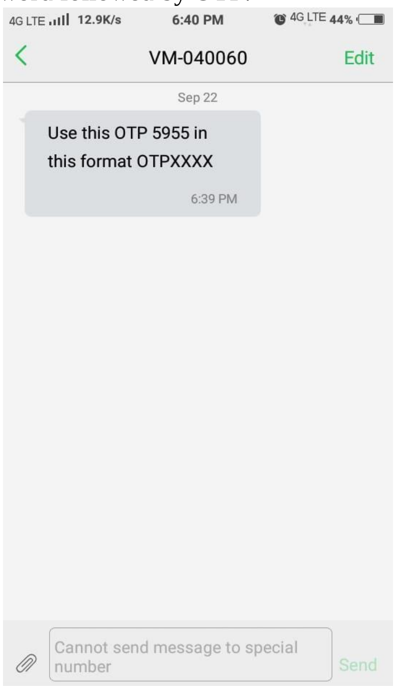


Fig 7. OTP received to mobile

Step -4:Entering the password

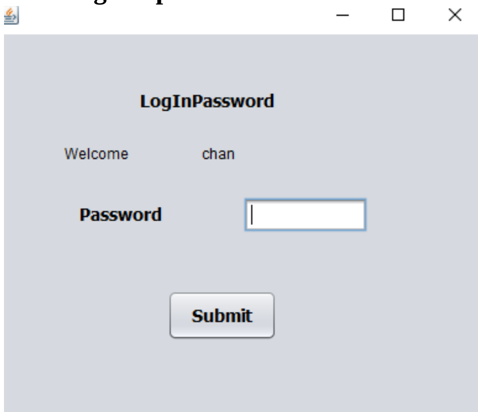
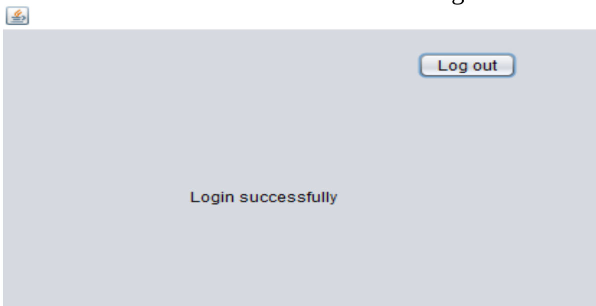


Fig 8.Password section

If the correct credentials are entered we will get



The array used for encryption and decryption

String option[]= {"$","1","2","3","4","5","6","7","8","9","0","A","B","C","D","E","F","G","H","I","J","K","L","M","N","O","P","Q","R","S","T","U","V","W","X","Y","Z","@","a","b","c","d","e","f","g","h","i","j","k","l","m","n","o","p","q","r","s","t","u","v","w","x","y","z","#","*","!","%","^","&","(",")","_","-","+","=","~","?","/","[","]","{","}","|","`",":",";",",",".","<"
};

VI. RESULT AND DISCUSSION

To implement the ACR algorithm we have used Netbeans (java) and mysql for the database few inputs and outputs are mention below.

S. no	Password	Space value (random)	Encrypted password	Total length of password
1	ara@210	2	7a^7z7?5&7[7a7u7,7@7`3s272S7R271y7z3Y27B	40
2	chan@95	4	(4u7j7z377z5z5K2v7(2a7l4z3a7,7n7z5u7z5b7@7C7(2=7+7K37175(4K3757D	64

3	virat@20	4	v8,8w2~2<8i8}4o2j8,8.5.5.8*8N2~4:8i4=8j8~6_6N2.7s2+4l8#6]4u482y4^6o4o8c28D	74
4	shashi_12	3	`6_3{3=3{5}9)9(9t6~9)9%9`6f9{8:9{5+9n6z7&6&6p9<9{8z7z5+933t6/3f9929C	68

The space value is chosen randomly, so password length varies every time. For example if we take password as "ara@210" the length of password is seven and space value(random number) is 2.Now in between two characters two random values(based on space value) from array will be selected and placed then the password size is 19. Then each character is divided into two character,now length becomes 38 and in password we insert space value and length of the password as this data will be used for the decryption of the password.

VII. CONCLUSION

The proposed ACR algorithm will improve the security for the login authentication. As we used randam space value, as password size increases the encrypted size also increases which results to providing more security to the password. In this paper we proposed random OTP process which protect from the attacks. As the OTP and Password concatination will be in two ways which will be randomly given to user, according to that the password varies every time user login and every time user login the password will be different as we add OTP to the password.

REFERENCES

1. SHAN, C. P., LOON, W. H., WIN, L. K., DIN, D., & SEAK, S. C. (2019, April). Automated Login Method Selection in a Multi-modal Authentication System: Login Method Selection based on User Behavior. In 2019 IEEE 9th Symposium on Computer Applications & Industrial Electronics (ISCAIE) (pp. 120-124). IEEE.
2. Bandyopadhyay, S. K., Bhattacharyya, D., & Das, P. (2008, April). User authentication by secured graphical password implementation. In 2008 7th Asia-Pacific Symposium on Information and Telecommunication Technologies (pp. 7-12). IEEE.
3. A. Sethi, O. Manzoor, and T. Sethi, User Authentication on Mobile Devices, Cigital, Dulles, VA, USA, 2012.
4. Varshney, G., Misra, M., & Atrey, P. (2017, October). A new secure authentication scheme for web login using BLE smart devices. In 2017 11th IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID) (pp. 95-98). IEEE.
5. Chen, C., Wang, Y., Yu, H., & Qiang, X. H. (2016, October). The RFID mutual authentication scheme based on ECC and OTP authentication. In 2016 IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB) (pp. 1-4). IEEE.
6. Wang, X. G., & Chai,i Z. C. (2006, August). Two secure remote user authentication schemes using smart cards. In 2006 International Conference on Machine Learning and Cybernetics (pp. 2653-2658). IEEE.
7. Kumari, S., & Om, H. (2014, August). Remote login password authentication scheme using tangent theorem on circle in a multi-server environment. In 2014 First International Conference on Networks & Soft Computing (ICNSC2014) (pp. 76-80). IEEE.
8. Yıldırım, N., & Varol, A. (2015, May). Android based mobile application development for web login authentication using fingerprint recognition feature. In 2015 23nd Signal Processing and Communications Applications Conference (SIU) (pp. 2662-2665). IEEE.
9. Varshney, G., Misra, M., & Atrey, P. (2017, October). A new secure authentication scheme for web login using BLE smart devices. In 2017 11th IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID) (pp. 95-98). IEEE.
10. Liu, J., Sun, J., & Li, T. (2005, November). An enhanced remote login authentication with smart card. In IEEE Workshop on Signal Processing Systems Design and Implementation, 2005. (pp. 229-232). IEEE.

AUTHORS PROFILE

Patlolla Aravind Reddy is currently pursuing his 4 th. Year M.Tech (S.E) in Vellore Institute of Technology, Vellore.

Pakkireddy Harsha Chandan Reddy is currently pursuing his 4 th. Year M.Tech (S.E) in Vellore Institute of Technology, Vellore.