IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

SECURE LOGIN USING ONE TIMEAUTHENTICATION PASSWORD SYSTEM

DR.K.GOWSIC[1],K.MANOJEKUMAR[2],R.MITHUNRAJ[3],K.PRAVIN[4], R.SANJAYKUMAR[5]
1 ASSOCIATE PROFESSOR 2,3,4,5 UG STUDENT,
DEPARTMENTOFCOMPUTERENGINEERING

MAHENDRA ENGINEERING COLLEGE NAMAKKAL

Abstract - *With the rapid evolution of the wireless communication technology, user authentication is important in order to ensure the security of the wireless communication technology. Password play an important role in the process of authentication. In the process of authentication, the password enter by the user will be transmitted along the traffic to the authentication server in order to allow the server to grant access to the* ***authorized*** *user. The attackers will use the chance to attempt to sniff others person password in order to perform some illegal activities by using other's identity to keep them safe from trouble. Due to the issues, there are many solutions has been proposed to improve the security of wireless communication technology. In this paper, the previously proposed solution will be used to enhance the security of the system. The solution adopted is the one time password, hashing and two-factor authentication. There also a new solution will be added by using the special character to help to save more data. The objective of the system outcome is to enhance the current login authentication system. It provides solutions for making password breaking more difficult as well as convinces users to choose and set hard-to-break passwords.*

*Keywords:*One-time password, Network security, password reuse, password stealing, etc.

I. INTRODUCTION

The Password is cannot be theft or stolen by anyone be causing of we using a new method of login type. In our login page need some criteria when the user login they need to give username .

It will generate some special character and send to our email and then user need to enter the password with they received special character.

Then only it enter to the account if we enter wrong then it wont login to your account. Every time we login to our account it will generate a special character.

According to Plagiary(2014), there is 47% of the American adults account been hacked in that year. Their personal information is exposed by the hackers. Due to the problem exists, there are more people no longer trust that password will be able to protect their online account. According to Suleiman(2017), some of the attackers will sell the email account that is been hacked to others to gain profit.

1. ProbemStatement

Authentication is an activity to authenticate the person credential that wishes to perform the activity. In the process of authentication, the password enter by the user will be transmitted along the traffic to the authentication server in order to allow the server to grant access to the authorized user. When the password is transmitted, the attackers will try to sniff into the network to obtain data that include the user's password. Currently, there is rainbow table which able to trace the password with the hash algorithm to obtain the user's password. Once the password is succeeded to be decrypted, the attackers can use the user credential to do something illegal such as fraud others which will cause the user lost in credit.

It is important to protect our own account because our credit is priceless. It is hard to trace the attackers in the cyber world. The secure login system is needed to ensure the cyber safety. Therefore, this project would like to provide alternative ways to log in to a system because current login system is not secure enough.

2. Objectives

- The main objective is to implement a secure login authentication system with utilizing with two-factor authentications. By using the concept two-factor authentication could help to increase the strength of the login system. The attacker will need to pass through the next barrier of defence to success to login. This system will help to enhance the login authentication system.
- Next objective is to ensure login password will not be transmitted over the network. As compared to the previous solution, the password is just encrypted, but the attackers might succeed to decode the data and retrieve the password. So in order to prevent this happens, the password with the random key will need to be hash before the sender sends the password to the server. It is important to secure the password of the user.
- Apart from that, the third objective will be to generate the one time password offline. This will help in perform the login procedure if there is a limited connection of wi-fi or mobile signal is weak. It will help the user who lives in the countryside which has a weak phone signal

II. RESOURCES REQUIRED

✓ Hardware Requirement

- 1TB HDD
- 8GB Ram
- Laptop or PC

✓ Software Requirement

- ASP. Net: For all frontend logic.
- C# : For all connection logic .
- HTML : For all the layout designing.
- CSS : For interfacing and designing the pages.
- JavaScript : For developing all client side requirements.
- MySQL : For database we are using MySQL, can use any version of MySQL.
- Microsoft Visual Base : For Frontend development.

III.PROPOSEDSYSTEM

Due to the importance to secure the password, I had implemented an enhanced version of the login authentication from the existing proposed solution. Under the existing system, the password whether it is encrypted or hashed, it still exists in the network traffic to reach the service. Once the attackers get the encrypted or hashed password, the attacker will have the chance to succeed to discover the algorithm to retrieve back the plain text.

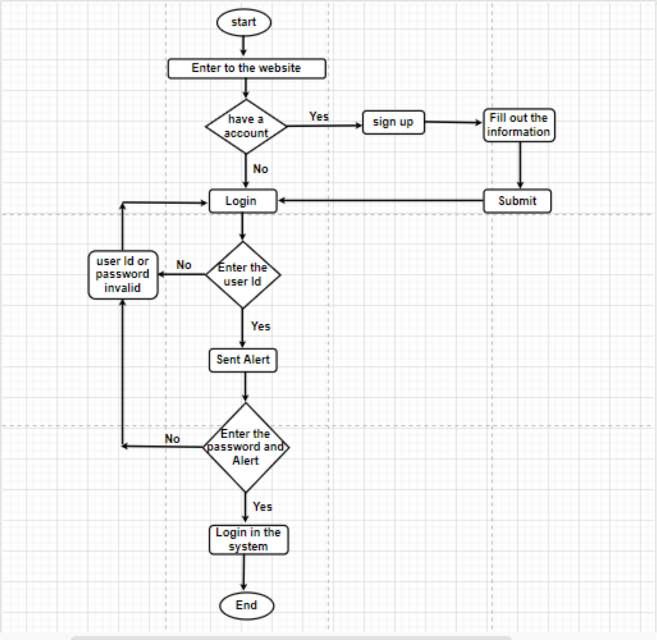

Figure.SystemArchitecture

The proposed solution to enhance the security of login authentication system by implementing the new system. In the new system to be proposed, it will help to enhance the password security. The system will help to ensure the password will not be transmitted along the traffic. Therefore, this project would like to provide alternative ways for login to a system by using special character as the random key when the user attempts to log in. By using this method, attackers will be hard to decrypt the password since they will need to generate a huge rainbow table if the random key is long enough.

IV. EXISTING SYSTEM

Authentication is a process to access to login account and accessing the service provided by the system or server using the password. It also has an alternative way to authenticate the user which is using biometric authentication by using fingerprint or iris recognition. However, human has the tendency to create easily remember password which it will lead to a problem. By definition, authentication is the use of one or more mechanisms to confirm that you are the authenticated user. Once the identity of the human or machine is validated, access is granted. There are existing acknowledged three authentication factors are things the user know, things the user have and biometric authentication. Biometric-based authentication is a good way to authenticate the user but it is expensive and raises some privacy concern. One Time Passwords (OTP) offers a promising alternative for two-factor authentication systems. A one-time password is a password that is valid for only one login session or transaction, on a computer system or other digital device

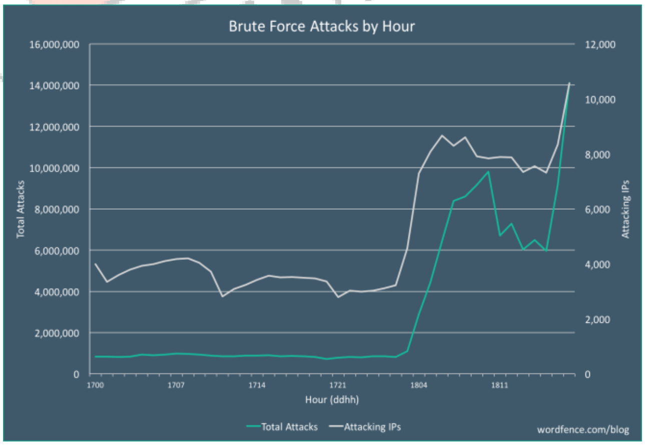

Figure.Password Attack per Hour

V. CONCLUSIONS

The project has achieved a huge success to mitigate with the rainbow table attack where the attackers will need to generate a huge rainbow table to exploit the system. A huge rainbow table will require a lot of time to be generated. Apart from that, the system also uses the 2 factor authentication where it requires the actual password and OTP to grant success to the system. Next, one of the huge success where will be the OTP can be generated without connection to internet which helps to prevent the attackers to able to retrieve the actual password from the network flow. There is some problem faced when implementing the system where there is the shortage of time to complete and improve the system. One of the major problem faced is when the laptop to act as the server of the system is having some faulty. The faulty cause spends of time and money to be fixed where time is wasted for the period of fixing.

VI. ACKNOWLEDGME T

I would like to express my sincere thanks and appreciation to my supervisors, Dr. GanMing Lee who has given me this bright opportunity to engage to implement SecureLogin Authentication System project. It is my first step to establish a career in networksecurity field. A million thanks to you.

Finally, I must say thanks to my parents and my family for their love, support andcontinuous encouragement throughout the course.

VII. REFERENCES

[1] M.Wu, S. Garfinkel, and R. Miller, “Secure web authentication with mobile phones,” in DIMACS Workshop Usable Privacy Security Software, Citeseer, 2004.

[2] B. Parno, C. Kuo, and A. Perrig, “Phoolproof phishing prevention,” Financial Cryptography Data Security, pp. 1–19, 2006.

[3] Kritika Shrivastava, ShwetaManda, Prof. P.S. Chavan,Prof.T.B.Patil,“Conceptualmodelforproficientautomated AttendanceSystembasedonfaceRecognitionandGenderclassificationusingHar-Cascade,LBPHalgorithmalongwithLDAmodel”,InternationalJournalofAppliedEngineeringResearchISSN09734562,Volume13,Number10pp.8075-8080©ResearchIndia Publications,2018

[4] Deepan.P1, Raja Vignesh.R2, Venkateswaran.S3, “faceRecognitionbasedAutomatedAttendanceManagementSystemusingHybridClassifier”,InternationalResearchJournalofEngineeringandTechnology (IRJET) e-ISSN: 2395-0056, vol.4 Issue: 5,p-ISSN:2395-0072, May2017.

[5] Subarna,B.Viswanathan,“RealtimeFacialexpression recognition based on deep convolutionalspatialneuralnetworks”,D.M.International

[6] Conference on Emerging Trends and Innovations inEngineeringandTechnologicalResearch,ICETIE TR8529105,2018.

[7] R. Dhamija, J. D. Tygar, and M. Hearst, “Why phishing works,” in CHI’06: Proc. SIGCHI Conf. Human Factors Computing Systems, New York, 2006, pp. 581–590, ACM.

[8] J. McCune, A. Perrig, and M. Reiter, “Bump in the ether: A framework for securing sensitive user input,” in USENIX Annu. Tech. Conf., 2006, pp. 185–198.

[9] M. Mannan and P. van Oorschot, “Using a personal device to strengthen password authentication from an untrusted computer,” Financial Cryptography Data Security, pp. 88–103, 2007.

[10] N. Provos, D. Mcnamee, P. Mavrommatis, K. Wang, and N. Modadugu, “The ghost in the browser: Analysis of web-based malware,” in Proc. 1st Conf. Workshop Hot Topics in Understanding Botnets, Berkeley, CA, 2007.

[11] S. Garriss, R. Cáceres, S. Berger, R. Sailer, L. van Doorn, and X. Zhang, “Trustworthy and personalized computing on public kiosks,” in Proc. 6th Int. Conf.

[12] Hung-Min Sun, Yao-Hsin Chen, and Yue-Hsun Lin (2012), “oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks,” IEEE transactions on information forensics and security, Vol. 7, No.2.

[13] Hung-Min Sun, Yao-Hsin Chen, and Yue- Hsun Lin (2012), “oPass: A User Authentication Protocol Resistant to information forensics and security, Vol. 7, No.2.