Volume 9, Issue 06, June 2024 ISSN (online): 2456-0006

International Journal of Science Technology Management and Research

Available online at: www.ijstmr.com

A Review of E-Authentication Systems

Divya Morker
MSC (Computer Science)
Indira College, Malegaon

Prof. G. B. Hiray
MSC (Computer Science)
Indira College, Malegaon

Abstract-: ***The rapid advancement of wireless communication technology underscores the critical need for user authentication to safeguard its security. Passwords are pivotal in this authentication process, wherein user-entered passwords are transmitted alongside traffic to an authentication server, enabling access for authorized users. Exploiting this process, attackers endeavor to intercept passwords to perpetrate illicit activities under false identities. Consequently, numerous solutions have been proposed to fortify wireless communication security, including the utilization of one-time passwords, hashing, and two-factor authentication. Additionally, this paper proposes integrating QR codes to augment data storage capacity. The overarching goal of these enhancements is to bolster the existing login authentication system, making password breaches more challenging and encouraging users to adopt stronger passwords.***

Keywords-: ***Authentication, QR, OTP,***

I. INTRODUCTION

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. According to Pagliery(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 Sulleyman(2017), some of the attackers will sell the email account that is been hacked to others to gain profit. 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.

II. LITERATURE SURVEY

Authentication is an activity to authenticate the person credential that wishes to perform the activity. If the credential is matched, the process is completed and the user will be granted for the access. Generally, the user will need to provide their password to begin using a service of the system. According to Rouse (2014), user authentication authorizes human-to-machine interactions in operating systems and applications as well as both wired and wireless networks to enable access to networked and Internet connected systems, applications and resources.

In their investigation of password evolution, Bonneau (2015) state that: The password is added to the sharing operating system in 1960s. However, the problem arose very quick due to the leakage of the unencrypted password master file. When reaching 1970s, the password started to be stored in the hashed form. In 1979, the hashed password was improved with the salting. With the mid-1990s introduce of the World Wide Web, the password is secure using the public-key cryptography via secure sockets layer (SSL) client certificates. The password is then started to link to the email and two-factor authentication is introduced.

In the early of 2010s, the smartphone starts to be widely used. The reason for the implementation is also because of the free smartphone applications to act as a second factor based on the emerging time-based-one time-pad (TOTP) standard. TOTP is an algorithm that computes a one-time password from a shared secret key and the current time. There are also services provided by sending codes via short message service (SMS) as a backup authentication mechanism.

In their investigation of password evolution, Denso (2016) state that: Quick Response (QR) code was created by 1994 in Japan. It is named after quick response because of the high-speed reading. QR code is an evolution of the barcodes. The evolution occurs due to the limitation of the barcodes which only can hold 20 alphanumeric characters. The project is then carried out by Masahiro Hara and his development team for 1 year and a half. The outcome of the QR code is a huge success due to it can store 7,000 numerals with the additional capability to code Kanji characters was finally created. With the current technology, the QR code is scanned can help to redirect to a website or coupon.5. Ensuring privacy and data protection is paramount in developing bank attrition systems. Secure login

systems and data encryption are essential features. According to a report by the Federal Trade Commission (2020), implementing robust security measures is crucial for maintaining customer trust and compliance with regulatory requirements.

III. SYSTEM ARCHITECTURE

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.
In the 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.
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 QR code 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. Under the proposed system, the user will key in the username then the password will be obtained. The server will generate a random key with 40 characters in the form of QR code. The phone will then scan the QR code to obtain the random key. The password will then combines the random key and hash. The server will retrieve the password from the database then combine the random key and hash it. Both of these hash value generated will take the first 6 character as the OTP. Once it is both matches, the login is success.

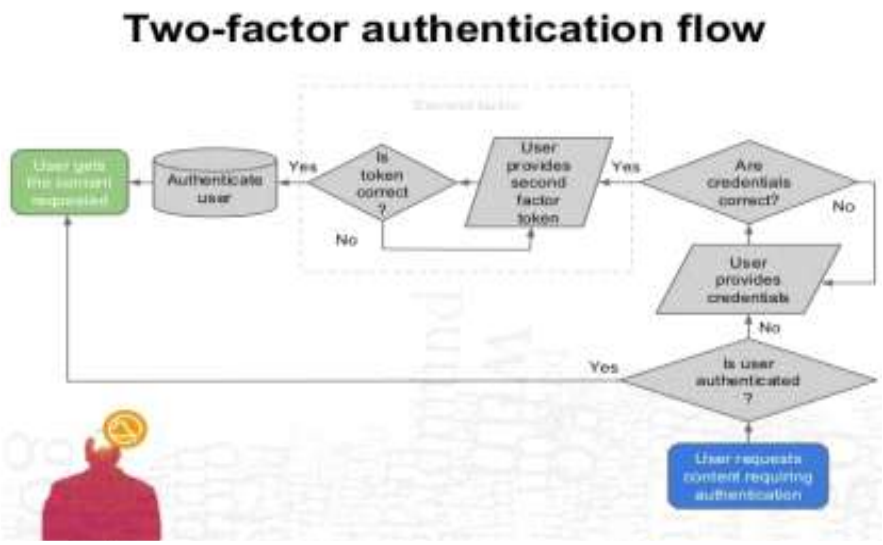

Figure 1. System two factor authentication flow

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.

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. The OTP authentication main idea is to provide infinite factors and create different password every time during user logging in to improve the security of the system. The OTP authentication system is implemented by two main mechanisms. The first mechanism is the challenge-response mode. The system will generate a challenge to the user when the user is logging in. The OTP is generated by combining user keyed in the password and challenge generate by the system. The user will need to key in the OTP to log in successfully. The next mechanism is time synchronization. This mechanism will use the user login time to generate the random number. The user can generate the password combining his passphrase. OTP also only valid for a short period of time only

CONCLUSION

Implementing the system encounters various challenges, particularly when time constraints hinder thorough system development. A significant issue arises when the designated laptop acting as the system's server experiences malfunctions, requiring time and financial resources for repair, thereby delaying progress. To enhance the system, synchronization of OTP with time can be implemented,

generating OTP by selecting random characters from the hashed password. Additionally, improving the login system entails enforcing password criteria, mandating a minimum length of 8 characters and a combination of upper and lower case letters, numbers, and symbols.

REFERENCE

1. "Design and Implementation of Two-factor Authentication Using OTP and QR Code" by R. Suganya and R. Deepa, International Journal of Engineering and Technology, 2018.
2. "A New Two-Factor Authentication Scheme Using QR-Code and One-Time Password for Secure Internet Services" by J.-S. Yoon, K.-B. Kim, and Y.-H. Kim, Journal of Information Processing Systems, 2018.
3. "A Two-Factor Authentication System Using QR Code and One-Time Password" by H. Kim and M. Yoon, International Journal of Engineering and Technology, 2017.
4. Milton K. (n.d.), Can a Hacker Bypass Encryption? , Available from:http://itstillworks.com/can-hacker-bypass-encryption-2996.html(Accessed: 18 November 2017).
5. Vaithyasubramanian, S., Christy, A. and Saravanan, D. (2015) 'Two Factor Authentications for Secured Login in Support of Effective Information Preservation', 10(5), pp. 2053–2056. Available from: http://www.arpnjournals.com/jeas/research_papers/rp_2015/jeas_0315_1713.pdf (Accessed: 18 November 2017).