International Journal For Technological Research In Engineering
Volume 6, Issue 8, April-2019 *ISSN (Online): 2347 - 4718*

USER AUTHENTICATION CONCEPT: A COMPLETE REVIEW

Harvans Lal[1], Dinesh Kumar[2], R.K.Vyas[3]
[1]M.Tech Scolar,[2,3]Asst. Professor
[1,2] Shekhawati Institute of Engineering and Technology, Sikar,
[3]Shekhawati Engineering College, Dundlod.

Abstract: In order to secure any system, the first and foremost requirement is the proper security mechanism. This paper reviews the concept of the user authentication, drawback of improper user authentication as well as the paper explores the innovative concept and works in the field of the user authentication.
Keywords: User Authentication, Game Based Authentication.

I. INTRODUCTION

With the regularly expanding number of administrations accessible on the web, clients are required to verify themselves ordinarily consistently. Various verification components with various qualities and shortcomings have been proposed and sent relying upon the setting of utilization, which lie under three noteworthy classes: learning based (e.g., passwords); token-based (e.g., charge cards); and biometric-based (e.g., unique finger impression), and their blends. Information based validation is as of now the most widely recognized methodology for getting entrance control in online administrations [1], with security going about as an agreement between the supplier and the client, with the supplier overseeing the terms (e.g., conveyed confirmation approach) and the client having no state

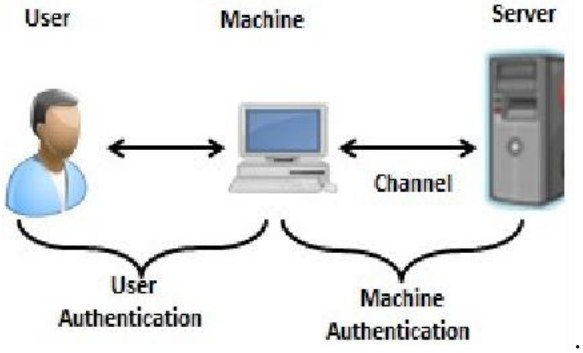

Fig 1 User Authentication

The previously mentioned practice raises convenience issues because of expanded retaining necessities, given that the clients discover challenges to recollect their passwords and are typically not willing to comprehend the security issues raised in light of the fact that validation is an auxiliary objective for them [1].

Learning based verification systems incorporate utilization of a remembered mystery for confirmation which can be either an alphanumeric password, an individual distinguishing proof number (PIN) or a graphical mystery. Alphanumeric passwords are ending up less usable because of the expanding number of accessible administrations that require confirmation, joined with severe password arrangements [1].

Memorability is a noteworthy issue driving clients in defying essential security guidelines, for example, utilizing exceptionally straightforward passwords, thinking of them down or reusing similar passwords for various administrations. Wide utilization of touch-screen gadgets has presented another test for alphanumeric passwords, since studies have demonstrated that composing on virtual consoles is slower and harder than on physical consoles [1]. To defeat this issue, graphical validation systems have been proposed. These can be characterized under two noteworthy classifications: the review based by illustration or distinguishing areas on a picture, and the acknowledgment based by perceiving a lot of pictures among a standard set. Security issues are brought up for this situation since the confirmation key pool is restricted contrasted with alphanumeric passwords. [1]

II. SECURITY THREATS

Security concerns both the clients and the specialist co-ops for various reasons and utilizing secure validation components is of significant significance for both, as assailants might target either side. Assaults on the client side lie under the catch assaults class, where the objective of the assailant is to take the confirmation key and access the administration. These incorporate shoulder surfing, i.e., utilizing perception procedures to get the confirmation key; social building, i.e., utilizing social control of the client to persuade them to disclose private data, for example, phishing; malware, i.e., utilizing noxious programming to assemble touchy data and on contact screen gadget smirch assaults with aggressors expecting to recognize the password design. [2]

Fig 2. Security Attacks

Then again, server side assaults which lie under the speculating assaults class, where the objective of the aggressor is to figure the confirmation key by attempting surmises over and again, the outcomes of a fruitful assault would influence a large number of clients and would affect the supplier's believability. Speculating assaults can be additionally isolated in internet think about where the aggressor cooperates legitimately with the administration and disconnected think about where the assailant has accessed obvious content, for example, cryptographic hashes [3] which can be utilized to confirm surmises. Suppliers shield the clients and the administrations from internet speculating assaults by presenting components, for example, CAPTCHA [3], restricting the quantity of endeavors for fruitful login and deferring the reaction time after progressive mistaken suppositions. Disconnected assaults are more diligently to manage since the aggressor does not have time constraint other than the computational intensity of the gadget used to make the speculated verification key rundown. Animal power assault is a broadly utilized disconnected assault otherwise called comprehensive key inquiry which involves efficiently testing every conceivable password until the right one is found. For client picked passwords, inquiry advancements have been proposed, for example, lexicon assaults and astute beast compel [3].

III. LITERATURE SURVEY

The various works is done to apply the better user authentication in order to restrict the unauthorized access. In the below section we have discuses , the same.

Y.Zhu et. al 2018 proposed Multi-fAcet Password Scheme (MAPS) for the purpose of mobile authentication. The approach makes use of the information form the multiple facets and minimum movements are required to generate the password which have the greater strength as compared to the 4 digit pin and the 8 characters based alphanumeric passwords.

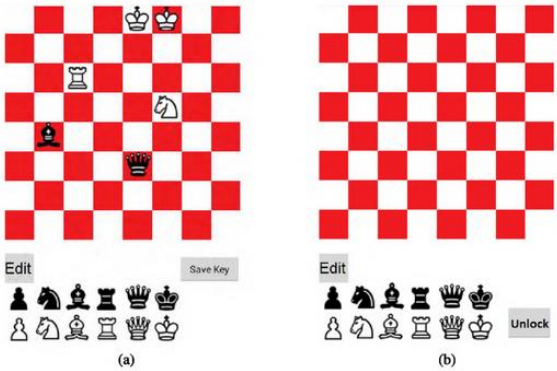

Fig 3. Multi-fAcet Password Scheme

M. H. Zak et. al 2017 proposed a pattern based password , the concept is used to generate the password using the location in the grid and together with that it also generate the dummy password in order to misguide the attackers. The users in order to validate the password or access the system will have to recognize the pattern and have to reenter it when entering or accessing the system.

Pooja M. Shelke , also proposed the 3D password scheme which make the password pattern by the movement of the chess pieces , the password contains the combination of the alphabets , digits on the basis of the piece moved and the position. The pattern form are easy to recognized as per the movement of the pieces.

Fig 4. 3 D Password

IV. PROPOSED SCHEME

As seeing the necessity of the proper authentication scheme, the work we are proposing in the dissertation which we are planning to do is also based on the proper authentication of the user. In order to make the process more interative the chess game is form the basis of creating the password for the user authentication. In this we are using the four player chess for forming the password pattern. The process starts with the entering of the password length by the user, which form the basis for the chances. In the each chance the player have to move the piece in the chess board. The pattern is forms by analyzing the piece moves; position moved and also accompany it with some special character to increase the password strength. The proper result analysis with the implementation will be proposed in the next paper of our research work as we have to yet implement it.

V. CONCLUSION

User authentication plays an important role in the security. If the proper user authentication scheme is implemented then the security can be raised to the higher level. The paper reviews the concept of user authentication as well as we have discussed the innovative works of other authors and also discusses the work we are going to propose.

REFERENCES

[1] Christina Katsini,Marios Belk,Christos Fidas,Nikolaos Avouris,George Samaras,"Security and Usability in Knowledge-based User Authentication: A Review",PCI,2016

[2] Belk, M., Germanakos, P., Fidas, C., & Samaras, G. 2013. Studying the effect of human cognition on user authentication tasks. In International Conference on User Modeling, Adaptation, and Personalization. Springer Berlin Heidelberg, 102-113.

[3] De Carné de Carnavalet, X., and Mannan, M. From very weak to very strong: Analyzing password-strength meters. In Network and Distributed System

Security Symposium , 2014.
[4] Y. Zhu et al., "CMAPS: A Chess-Based Multi-Facet Password Scheme for Mobile Devices," in IEEE Access, vol. 6, pp. 54795-54810, 2018.
[5] M. H. Zaki, A. Husain, M. S. Umar and M. H. Khan, "Secure pattern-key based password authentication scheme," 2017 International Conference on Multimedia, Signal Processing and Communication Technologies (IMPACT), Aligarh, 2017, pp. 171-174.
[6] Pooja M. Shelke , F. M. Shelke Mr. B. G. Pund, "Advance Authentication Technique: 3D Password", IJRITCC ,June 2016.

