Secure Authentication and Data Sharing approach using the Four player Chess Based Password

[1]Jitendra Kumar Katariya,[2]Gajendra Shrimal
[1]M.Tech Research Scholar , [2]Asst. Professor ,
[1,2] Department of Computer Science and Engineering
Jagannath University, Jaipur ,Rajasthan ,India.

Abstract : Security is of most extreme significant in each part of the data transmission. In the time of Information innovation, it is happening to more significance. The most widely recognized utilization of securing the significant data is by utilizing password. Be that as it may, the typical content passwords are recognizable and can be effectively split utilizing the savage power assault. In our proposed work, we have picked a novel plan of password age, which have its principle premise chess. The game based password is produced by putting away the developments of the game parts.

***Index Terms* – Game Based Password, Security, Authentication.**

I. INTRODUCTION

An approval part (or system) is a way for you to exhibit that you're allowed to get to something. Passwords have been the default strategy for approval for whatever time span that most of us have expected to exhibit to a PC that we're allowed to get to it. Regardless, passwords are not using any and all means the main affirmation segment.

Something you know: Examples of this are your incredible old mystery state, bank card PIN or a protected word when the alert association calls your home; these are for the most part occasions of using something you know to approve yourself.[1]

Something you have: Examples are a swipe card to get to a sheltered zone, a code sent to your cellphone as a segment of a login method (to exhibit you have your cellphone) or a SecureID token that gives a consistently changing code you need to enter to get entrance – all are something you have that can be used to check yourself.

Something you are: This is the spot biometric security comes in. To get to our information center we have to put our pointer on a unique finger impression scanner in the wake of swiping a card. But on the off chance that you take someone's pointer you won't presumably get to our information center, paying little respect to whether you've stolen a genuine swipe card. Other biometric structures consolidate retinal scopes (the veins at the back of the eye) and iris channels (the concealed bit of the eye).

Various characteristics used for check: a few distinct properties that you once in a while watch used for approval are:

- Some place you are. For instance at a physical area prepared to get snail mail.
- Something you can do. For instance decisively recreate an imprint.
- Something you appear. For instance a neurological quality that can be inspected by a MRI.
- Somebody you know. For instance that can be endorsed by a casual network chart or chain of trust.

Most of us believe them to be a weight – something you have to suffer to have the alternative to use an organization you need access to. In this article we will explain how PC systems have created in the way they process your mystery key, how present day online applications do approval and why it's basic to pick a strong mystery state. When you wrap up this you should have a working learning of hashing counts, how mystery expression part works and what "strong mystery state" genuinely infers.

In the start of PCs and unified PCs, passwords were secured in a database as plain substance. When you expected to sign-in, a gatekeeper application would approach you for your mystery word. It would take whatever you made in and beware of the remote possibility that it was proportionate to whatever it had secured in the database and accepting veritable, you were permitted get to.[2]

As the Internet created and created, malignant software engineers started expanding unapproved access to systems. When they were in, they would rapidly download the plain-content mystery state database and have minute access to all customers passwords. Architects and systems chiefs expected to come up with a response for this issue and the game plan they thought of was 'mystery word hashing'.

Consider a hashing count as a machine. In one end you input any substance or matched information. Out the far edge you get a number that is a certain length – lets state 32 digits long in our model. The information you feed in can be any size, from a few bytes to various terrabytes or greater. Despite what information you feed in, you get a 32 digit number (in this model) curiously addresses the information. What is surprising about a hashing count machine is that if you feed something unclear in you get the identical 32 digit number. In case you feed in War and Peace, you get a number. If you copy the book verbatim and feed in a similar substance, you get a comparable number. In case you change a lone character in the novel, you will get an absolutely special number. [2]

Hashing estimations differ in the way they work and the most conspicuous qualification is the length of the number each one discharges.

MD5 which is incredibly outstanding discharges 128 parallel digits.

SHA2 discharges 256 bits (or twofold digits)..

II. RELATED WORK

Pooja M. Shelke,F. M. Shelke,Mr. B. G. Pund [1] Providing more noteworthy security to any structure requires giving any confirmation system to that structure. There are various affirmation systems, for instance, printed password, graphical password, etc. Nevertheless, these frameworks have some limitation and hindrance like they can without quite a bit of a stretch hacked or part by using various gadgets. One of the instruments is creature control computation. Thusly, to overcome the impediments of existing approval technique, another improved affirmation framework is proposed. This technique is multi-password and multifaceted approval system as it unites diverse check methods, for instance, printed password, and graphical password, etc. Most indispensable bit of 3d password arrangement is thought of 3d virtual condition. This approval Strategy is additionally created than some different plans as we can join existing plans. Similarly this Strategy is hard to break and easy to use.

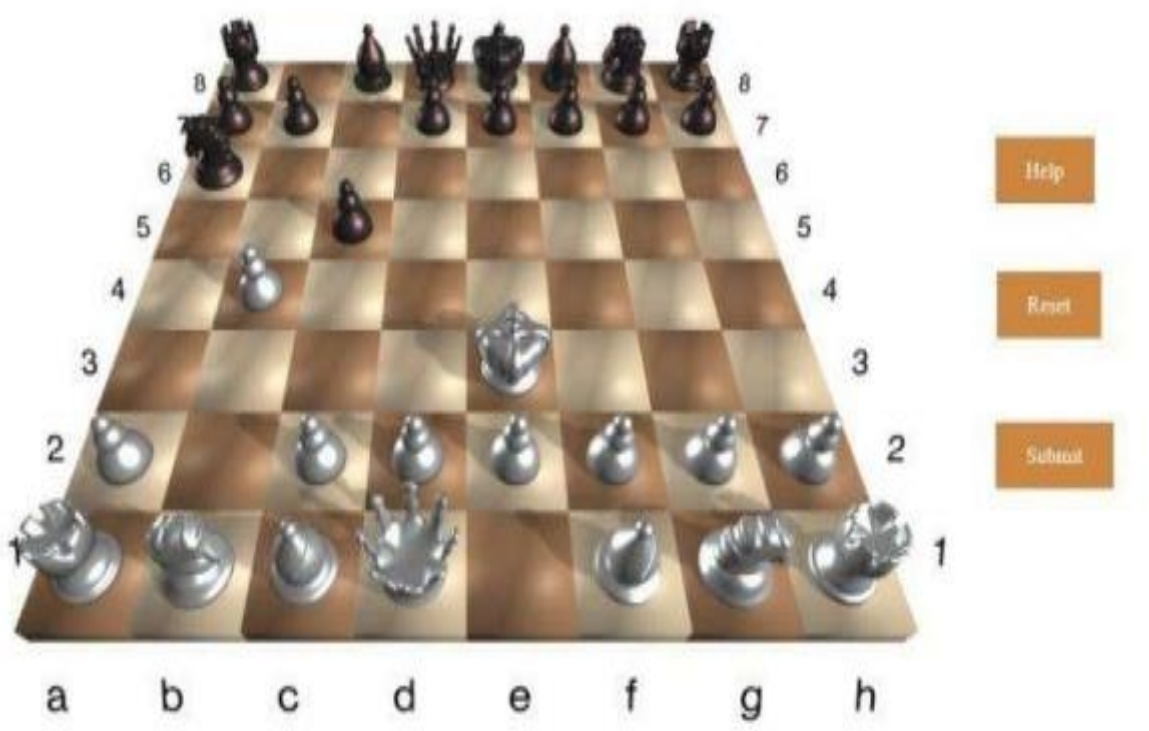

Fig. 1 chess 3d password creation

In this paper creators rout these obstructions using the 3D Password arrangement. 3D password is a multifaceted check plot which joins existing affirmation methods into 3D Virtual Environment. This condition contains diverse virtual articles. The customer investigates through this condition and speaks with the things. The mix and game plan of the customer correspondences in the earth shapes the 3D Password. Thusly this paper instructs concerning our examination about 3D password and how to construct 3d password.

ArashHabibiLashkari et al [2] investigate the idea concerning Shoulder aquatics snare in graphical puzzle word attestation. information and PC security is strengthened, everything considered, by passwords that square measure the quality some bit of the affirmation system. the premier extensively discovered PC accreditation framework is to utilize character set username and riddle key that has mammoth weights. a conceivable downside of graphical riddle word plans is that they're feebler against shoulder aquatics than regular alphanumerical substance passwords. Precisely once clients input their passwords in AN open spot, they'll be in risk of assailants taking their puzzle word. AN assailant will get a puzzle articulation by direct data or by record the individual's confirmation session. this can be induced as shoulder-surfing and could be a superb risk, of exceptional concern though confirming in open spots. Passwords have totally unique obliging properties in like way as clearing legacy relationship; so authorscan imagine their utilization for an all-encompassing opportunity to arrive back. Disastrously, today'sstandard strategies for riddle key learning square measure subject to blend of ambushes reliant on recognition, from pleasant spying (bear surfing), to progressively surprising techniques.

Shoulder-surfing strike happens once using direct perception frameworks, for example, watching somebody's shoulder, to encourage passwords, PINs and diverse troublesome individual learning. conjointly as once a customer enters information using a console, mouse, contact screen or any ordinary information contraption, a malevolent onlooker could little question get the customer's puzzle word limits.

Sandeep Kumar Pandey [3] gives information about Chess Game as a Tool for Authentication Scheme. First stage for information security is affirmation and the standard stage for approval is memorability of password and principles that will be used for check reason. The most by and large used arrangement is printed plan. At any rate the strong password of literary arrangement is hard to

hold and ordinary passwords are frail against various assaults. Therefore, graphical approval plot has been proposed as an elective plan, prodded particularly by the manner in which that individuals can remember pictures better than content. In any case, these are vulnerable against shoulder surfing assault. To vanquish this issue various structure based approval plans has been proposed. Regardless, either these arrangement's shoulder surfing safe property isn't strong or these have various awesome principles, which are hard to hold. Along these lines, to overcome these issues we propose a confirmation plot which depends on chess game. Since this arrangement contains only two rules of chess, in this manner easy to recall.

This approval plans contains three phases: Registration, Login and Verification. In enlistment organize, customer needs to show his/her customer name and Password. The base length of password should be 7. In login arrange, an interface of network (10×10 or 12×12) will be appeared, through which customer need to make his session password by using certain standard of chess game (for instance Diocesan Rule and Rook rule). The affirmation stage will check the password of customer and grant him/her to get to their record. The two bits of chess, whose guidelines used in this real activity plot, are Bishop and Rook. In chess, the pastor can move any number of squares corner to corner. Additionally, Rook can move any number of squares along any position or record, or can move any number of square vertically or on a level plane. I called it Rook rule. Therefore this arrangement contains only two rules and no extra mapping is required for shoulder surfing hindrance or shrouded cameras.

SahanaR.Gadagkar et al [4] gives about Authentication is a basic factor of security. There are various approval methodology open, for example, Textual Passwords, Graphical Passwords, Biometric Identification, etc anyway each of these, independently having a few disservices. To vanquish the confinements of the present approval technique, another improved confirmation plot is introduced, for instance 3D Password. This technique can be consolidated with existing verification strategies and therefore it will in general be called.

III. PROPOSED WORK

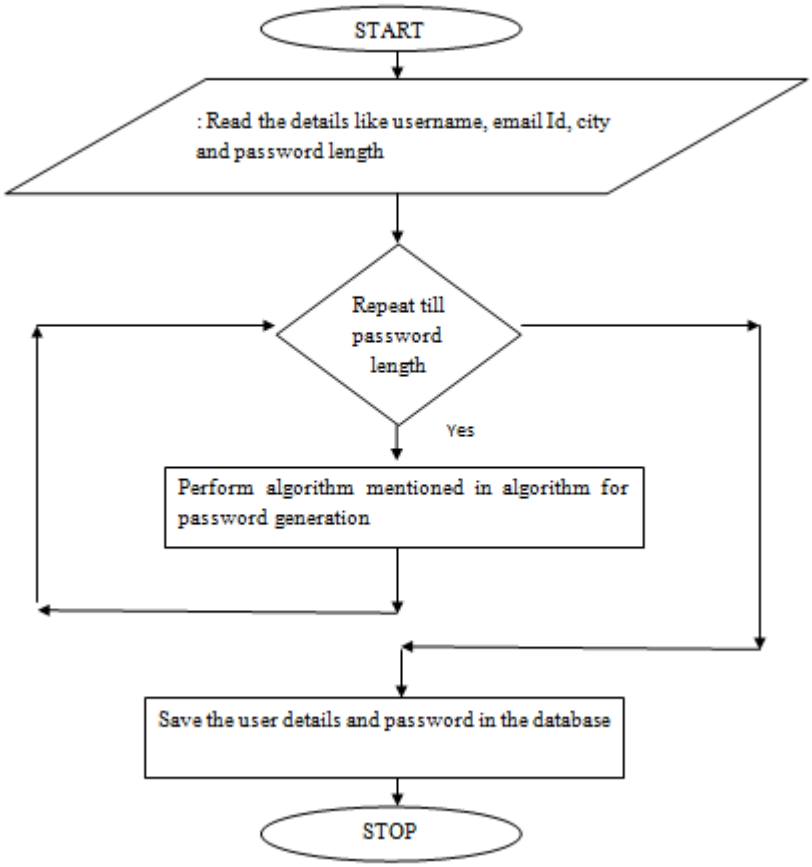

Fig 2. Flowchart for Proposed Work

The algorithms which is as follows,

Step 1: Read Chances

Step 2: Repeat For I : 1 to Chances Step 1 By 1 :

Step 3: Check the Player chance

Step 4: Receive Input for Player Movement

Step 5: Validate the Movement on basis of chess rules of Diamond Ring chess

Step 6: Form the password which constitute player-chess unit-from position-to position

[End of For Loop]

Step 7: Store Generated Password

IV. Result Analysis

The OTP which is generated using the algorithm is tested on various tool online and results are comparatively better than the previous works.

Table 1. Result Analysis

Test Key	Website/Tool	Result
Pt_PAWN_43_55_!_gs_PAWN_69_68_@_ yt_FREZ_102_90_#_bs_KING_76_77_$	Password Meter	Very Strong
Pt_PAWN_43_55_!_gs_PAWN_69_68_@_ yt_FREZ_102_90_#_bs_KING_76_77_$	Password Checker	Excellent Strength
Pt_PAWN_43_55_!_gs_PAWN_69_68_@_ yt_FREZ_102_90_#_bs_KING_76_77_$	Cryptool2	Entropy 4.22 Strength 225 Very Strong

IV. Conclusion

Secure Login is key to progress to the any of the application. The exposition idea isn't just cutting edge yet additionally gives us the idea of how the 100% security can be accomplished. In the thesis the protected idea of utilizing the Game put together password which is based with respect to the one of a kind idea of Diamond Ring Chess , having the various developments when contrasted with the typical chess, improves the security as well as diminish the odds of the hacking or breaking the password. And furthermore by approving the quality of the created key or password against the password approving destinations, unmistakably to break the password requires a great deal of time and in this manner secure.

References

[1]. Pooja M. Shelke,F. M. Shelke,Mr. B. G. Pund ,"Advance Authentication Technique: 3D Password", *International Journal on Recent and Innovation Trends in Computing and Communication*, Volume 4,Issue 6,pp 632-635,June 2016.

[2]. ArashHabibiLashkari,Dr. Omar Bin Zakaria,SamanehFarmand and Dr. RosliSaleh, "Shoulder Surfing attack in graphical passwordauthentication ," *International Journal of Computer Science and Information Security*, pp 145-154,Vol. 6, June 2009

[3]. Sandeep Kumar Pandey , "Chess Game As A Tool For Authentication Scheme," *International Journal of Scientific Research Engineering & Technology (IJSRET)*,pp 076-083,Vol. 2, July 2012

[4]. SahanaR.Gadagkar, AdityaPawaskar and Mrs. Ranjeeta B. Pandhare, "3d Password Authentication for WebSecurity, "*International Conference on Recent Innovations in Engineering and Management* ,pp 82-86 , March 2016.

[5]. J. Cui, X. Zhang, J. Gao and N. Cao, "A Security and Efficiency Authentication Scheme Based on Human-Memorable Password," *IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), Guangzhou,China*, pp. 293-296,July 2017.

[6]. W. LinLin, W. YuNu, W. YaJie and C. Guoqiang, "Research on the Surakarta chess game program based on unity 3D," *29th Chinese Control and Decision Conference (CCDC), Chongqing, China*, pp. 7671-7674,May 2017.

[7]. Nicholas MicallefandNalinAsankaGamagedaraArachchilage"Changing users' security behaviour towards security questions: A game based learning approach," *IEEE Military Communications and Information Systems Conference (MilCIS), Canberra*, pp. 1-6,November 2017.

[8]. S. Bader and N. E. B. Amara, "Design of a 3D Virtual World to Implement a Logical Access Control Mechanism Based on Fingerprints," *IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA),*pp 1239-1246,November 2017

[9]. Anjali Arora, Priyanka and Saibal Kumar Pal, "A Survey of Cryptanalytic Attacks on Lightweight Block Ciphers,"International Journal of Computer Science and Information Technology & Security (IJCSITS) ,pp 472-481 ,Volume 2, April 2012.