

SECURE PASSWORD GENERATION USING THE DIAMOND RING CHESS

Harvans Lal¹, Dinesh Kumar², R.K.Vyas³

¹M.Tech Scholar, ^{2,3}Assistant Professor

^{1,2}Shekhawati Institute of Engineering and Technology, Sikar, ³Shekhawati Engineering College, Dundlod.

Abstract : Security is of utmost important in every aspect of the information transmission. In the age of Information technology, it is becoming of more importance. The most common use of protecting the important information is by making use of password. In our proposed work, we have chosen a novel scheme of password generation, which have its main basis chess. The game based password is generated by storing the movements of the game components.

In this paper will make use of the Four-player diamond ring chess to generate the password used for sharing the photos. The password generation process in the Four-player diamond ring chess is more secure as compared to the two player chess as the more number of players involved and the more number of combinations can be used in the generation process. The proposed approach based on the Four player chess with 19 objects in each side in total of $19 \times 4 = 76$ different objects which can be moved.

Index Terms – Chess Based, Entropy, Security, password, cryptography.

I. INTRODUCTION

Cryptography is the arrangement or approach of passing on inside watching destructive substances .It is a used as a touch of a few fields: data security and [1] affirmation, and find the opportunity to control. The essential inspiration driving Cryptography is encoding the messages and changing their hugeness, not their world. Cryptography is utilized as a bit of different areas portrayals: ATM cards, PC passwords [1], on-line shopping, stock exchanging, e-keeping money. Cryptography is the technique to change over the text message (Plain text) into coded plot (cipher) by Sender and send it to Receiver who changes over (unscramble) the message into extraordinary text setup (Plain text) in the wake of enduring it so as to confirm it from getting lost or hurt. Cryptography has been climbed as essential contraction for information transmission. A plan of figuring's of cryptography has been considered [2].

With enigma key cryptography, a particular key is used for both encryption and interpreting. As showed up in Figure 2, the sender uses the key (or some game plan of rules) to encode the plaintext and sends the figure substance to the gatherer. The recipient applies a for all intents and purposes indistinguishable key (or control set) to unscramble the message and recover the plaintext. A solitary key is used for as far as possible; bewilder key cryptography is in like manner called symmetric encryption..

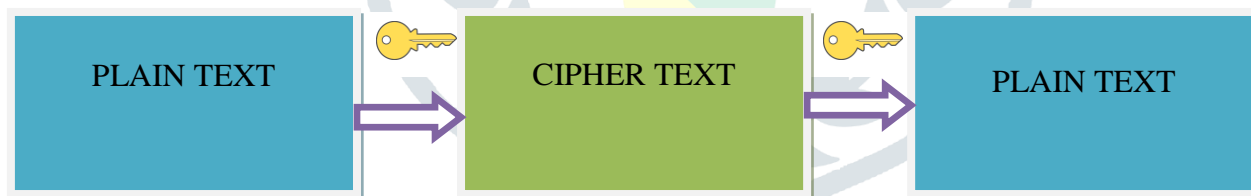


Fig 1 Secret key Cryptography.

SKC uses same problem key for both encryption and unscrambling Secret key cryptography plans are everything seen as sorted out as being either stream ciphers or square ciphers. Stream ciphers handle a solitary piece (byte or PC word) promptly and execute a type of data part so the key is continually advancing. A piece cipher is shown in light of the manner in which that the plan encodes one square of data at some irregular minute using an identical key on each square. With everything considered, the proportional plaintext piece will reliably scramble to an essentially indistinguishable cipher text while using a commensurate key in a square cipher at any rate the comparable plaintext will encode to different cipher text in a stream cipher [3].

Stream ciphers are of different sorts at any rate two authenticities saying here. Self-synchronizing stream ciphers figure each piece in the key stream as a piece of the past n bits in the key stream. It is named "self-synchronizing" in light of the way in which that the unscrambling procedure can stay synchronized with the encryption approach just by knowing how far into the n -bit key stream it is. One issue is goof spread; a scattered piece in transmission will achieve n reshaped bits at the getting side. Synchronous stream ciphers pass on the key stream in a way free of the message stream yet by using a basically indistinguishable key stream time work at sender and recipient. While stream ciphers don't build transmission mishandles, they are, by their tendency, uncommon with the target that the key stream will at long last repeat.

Public Key Cryptography

Symmetric-key cryptosystems use a comparative key for encryption and unscrambling of a message, in any case a message or storing up of messages may have a substitute key than others. A gigantic inconvenience of symmetric ciphers is the key affiliation fundamental to use them securely. Each conspicuous match of giving gatherings must, ideally, share a substitute key, and conceivably each cipher text exchanged like way [4][5]. The proportion of keys required extensions as the square of the proportion of structure people, which quickly requires complex key affiliation plans to keep them all straight and question. The trouble of securely setting up an enigma key between two giving get-togethers, when an ensured channel does not starting at now exist between them, other than demonstrates a chicken-and-egg issue which is a huge even disliked hindrance for cryptography customers in this present reality[4].

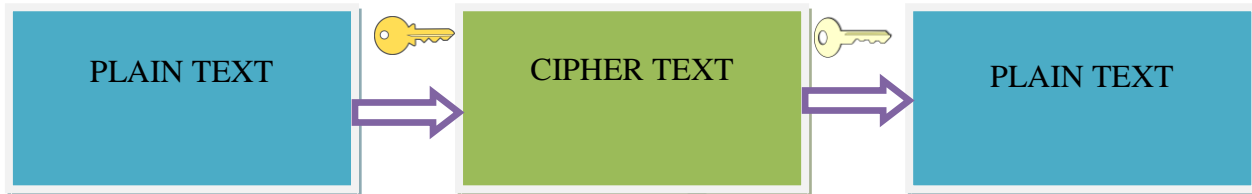


Fig 2 Public Cryptography with Different Key.

In open cryptography two distinctive keys—open and private—are made. These two keys are phenomenal at any rate dependent on each other. In open key cryptosystems, the open key may be uninhibitedly scattered, while its arranged private key must stay mystery. In an open key encryption system, the open key is used for encryption, while the private or enigma key is used for unraveling..

II. RELATED WORK

Pooja M. Shelke, F. M. Shelke, Mr. B. G. Pund [6] Providing more prominent security to any structure requires giving any check methodology to that system. There are various affirmation systems, for instance, textual password, graphical password, etc. In any case, these frameworks have some imperative and impediment like they can without quite a bit of a stretch hacked or part by using various gadgets. One of the instruments is creature control estimation. Thusly, to overcome the drawbacks of existing approval strategy, another improved affirmation framework is proposed. This approach is multi-password and multifaceted approval system as it combines diverse check techniques, for instance, textual password, graphical password, etc. Most imperative 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. In like manner this Strategy is hard to break and easy to use.

In this paper creators rout these obstructions using the 3D Password arrangement. 3D password is a multifaceted check plot which joins existing affirmation techniques 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 communications in the earth shapes the 3D Password. Thusly this paper teaches concerning our examination about 3D password and how to assemble 3d password.

ArashHabibiLashkari et al [7] examine the thought concerning Shoulder Surfing attack in graphical password check. Information and PC security is reinforced, as it were, by passwords which are the standard some bit of the affirmation technique. The most comprehensively seen PC affirmation procedure is to utilize alphanumerical username and password which has huge disadvantages. To crush the vulnerabilities of standard strategies, visual or graphical password plans have been made as possible elective reactions for text-based course of action. A potential drawback of graphical password plans is that they are more weak against shoulder surfing than ordinary alphanumerical text passwords. Precisely when clients input their passwords in an open spot, they might be in danger of attackers taking their password. An attacker can get a password by direct wisdom or by record the individual's check session. This is suggested as shoulder-surfing and is a known risk, of unprecedented concern while confirming in open spots.

Passwords have various supportive properties additionally as across the board legacy association; in this way creators can anticipate their use for quite a while to come. Tragically, the present standard procedures for password input are liable to collection of attacks based on discernment, from easygoing spying (bear surfing), to progressively stunning systems.

Shoulder-surfing attack happens while using direct perception frameworks, for instance, examining somebody's shoulder, to get passwords, PINs and other delicate individual information. Similarly as when a customer enters data using a keyboard, mouse, contact screen or any conventional information device, a vindictive observer may almost certainly acquire the customer's password capabilities.

Sandeep Kumar Pandey [8] gives information about Chess Game as a Tool for Authentication Scheme. First stage for information security is affirmation and the guideline arrange for approval is memorability of password and fundamentals that will be used for check reason. The most for the most part used arrangement is textual arrangement. In any case the strong password of textual arrangement is hard to hold and normal passwords are frail against various attacks. Therefore, graphical approval plot has been proposed as an elective game plan, prodded particularly by the manner in which that individuals can remember pictures

better than text. In any case, these are unprotected against shoulder surfing attack. To vanquish this issue various system based approval plans has been proposed. Regardless, either these arrangement's shoulder surfing safe property isn't strong or these have various awesome standards, which are hard to hold. Consequently, to crush these issues we propose a confirmation plot which is based on chess game. Since this arrangement contains only two rules of chess, therefore easy to recall.

This approval schemes contains three phase: Registration, Login and Verification. In enlistment arrange, customer needs to display 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 license him/her to get to their record. The two bits of chess, whose rules used in this authentic cation plot, are Bishop and Rook. In chess, the priest 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 dimension plane. I called it Rook rule. Accordingly this arrangement contains only two rules and no extra mapping is required for shoulder surfing impediment or concealed cameras.

III. PROPOSED WORK

In our methodology we have proposed the novel plan for the password confirmation and secure photograph sharing. In this we have made the password conspire, when we have displayed a framework based chess for four players, where the password is created by the development of the players in the game. Because of the quantity of various developments and association of the move number of players the created password will be progressively strengthful and hard to break.

In our approach we have proposed the novel scheme for the password authentication and secure photo sharing. In this we have created the password scheme, when we have presented grid based chess for four players, where the password is generated according to the movement of the players in the game. Due to the number of different movements and involvement of the move number of players the generated password will be more strength and difficult to crack.

Algorithm for Password Generation

Stage 1: Read Chances

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

Stage 3: Check the Player possibility

Stage 4: Receive Input for Player Movement

Stage 5: Validate the Movement on premise of chess standards of Diamond Ring chess

Stage 6: Form the password which comprise player-chessunit-fromposition-toposition

[End of For Loop]

Stage 7: Store Generated Password.

1. Movement to Chess units in Four Player chess:

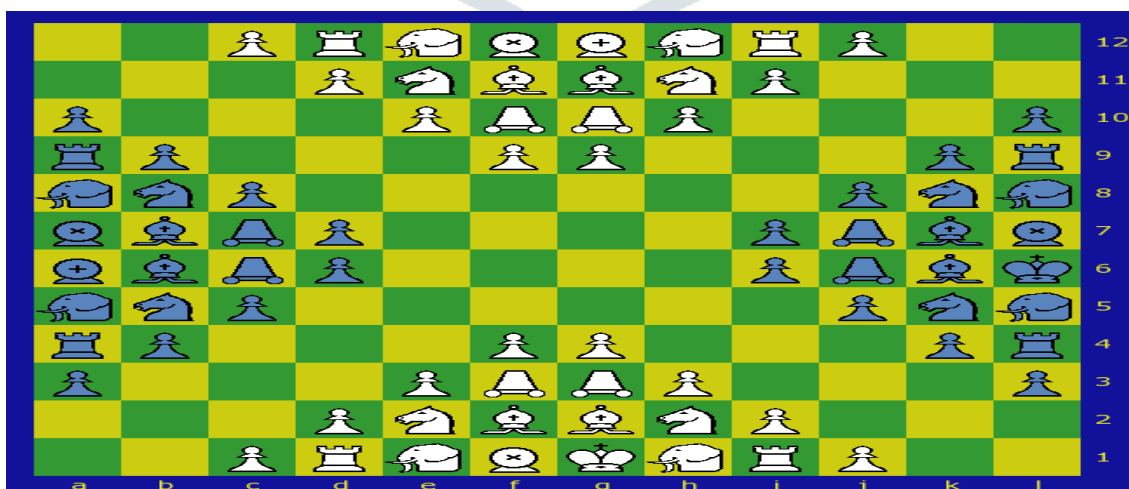











Fig 3 Four Player Chess

TABLE 1 MOVEMENT OF PLAYERS IN 4 PLAYER CHESS

	The KING moves one phase in any of the 8 extended direction, and must be kept out of Check.
	The FERZ moves one phase corner to corner. It also procures its 4R put as a central piece, addressing the celebrated guide that its name infers.
	The WAZIR, twofold of the Ferz, moves one phase symmetrically. Like the Ferz it is a central piece.
	The ELEPHANT moving accurately two squares in any of the 4 slanting headings. The structure used as a piece of this variety is a bouncing one, and the for the most part square may be unfilled or had. It secures its 4R put as a symmetric piece flanking the central ones.
	The BISHOP, twofold of the Rook, ascensions to 11 squares (to thwart invalid moves) slantingly through release squares. It obtains its Courier put as a symmetric piece flanking the central ones.
	The KNIGHT makes any 2:1 bounce, and in this variety can't be blocked. It obtains its 4R put as the typical detachment symmetric piece from the central ones.
	The ROOK trips to 11 squares (to deflect invalid moves) symmetrically through fumes squares. It gets its 4R put as a farthest symmetric piece from the central ones.
	The DABBABA moves unequivocally two squares in any of the 4 symmetrical headings. The structure used as a piece of this variety is a hopping one, and the for the most part square may be void or had. It procures its Courier Kamil/Ash Taranga put as a farthest symmetric piece from the central ones.
	The PAWN propels one phase symmetrically beside while getting, which it finishes one phase slantingly forward.

2. Registration Process in Dissertation

In the dissertation work, in order to work out the file sharing, the users have to first perform the generation process. Without registration no user is allowed to share the files on the server.

In order to perform the registration, user has to click on the “New User Registration Here” option on the home screen. And the algorithm for the registration process is mentioned below.

➤ Algorithm for Registration process

In order to register the new user for the system, we will follow the following steps,

Step 1: Click on the “New User Registration Here” Button.

Step 2: Read the details concerned with the user registration like username, emailed , city etc.. , the important thing is the password length which will determine the number of chances the users get to create the password.

Step 3: Perform the algorithm mentions in section 3.5.1 to generate the password.

Step 4: The details of the user and password generated is saved in the database.

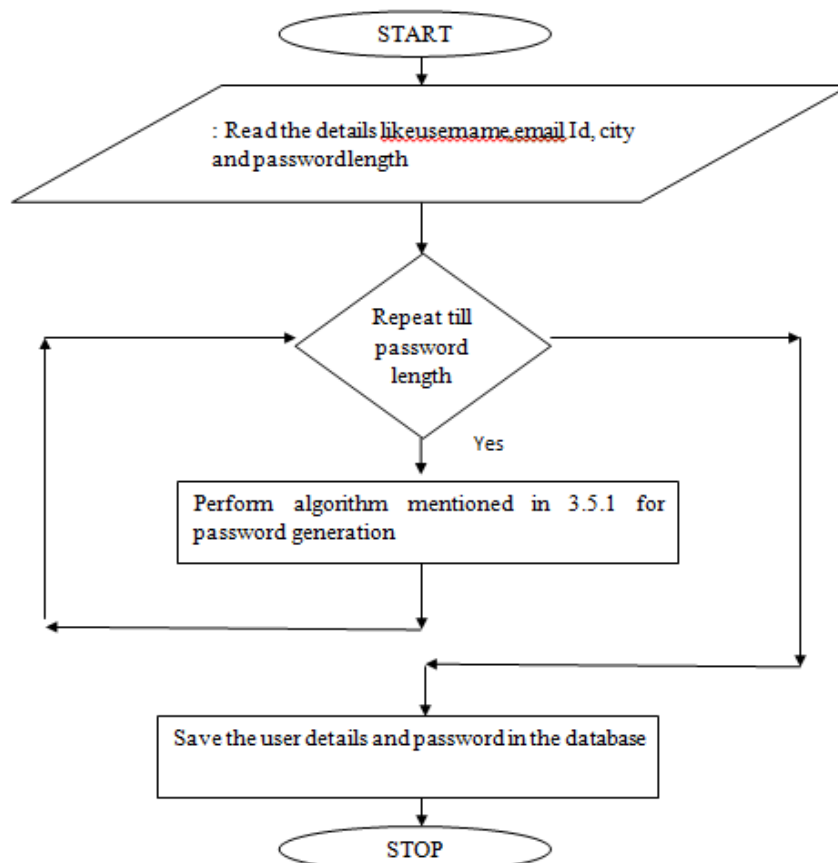


Fig 4: Flow Chat of Proposed Algorithm

IV. IMPLEMENTATION AND RESULT ANALYSIS

After the registration process , Diamond Ring based chess is presented and will required to enter the sequential moves from player 1, player 2 and so on.

The movement of the players will form the password like player_position1_position2.

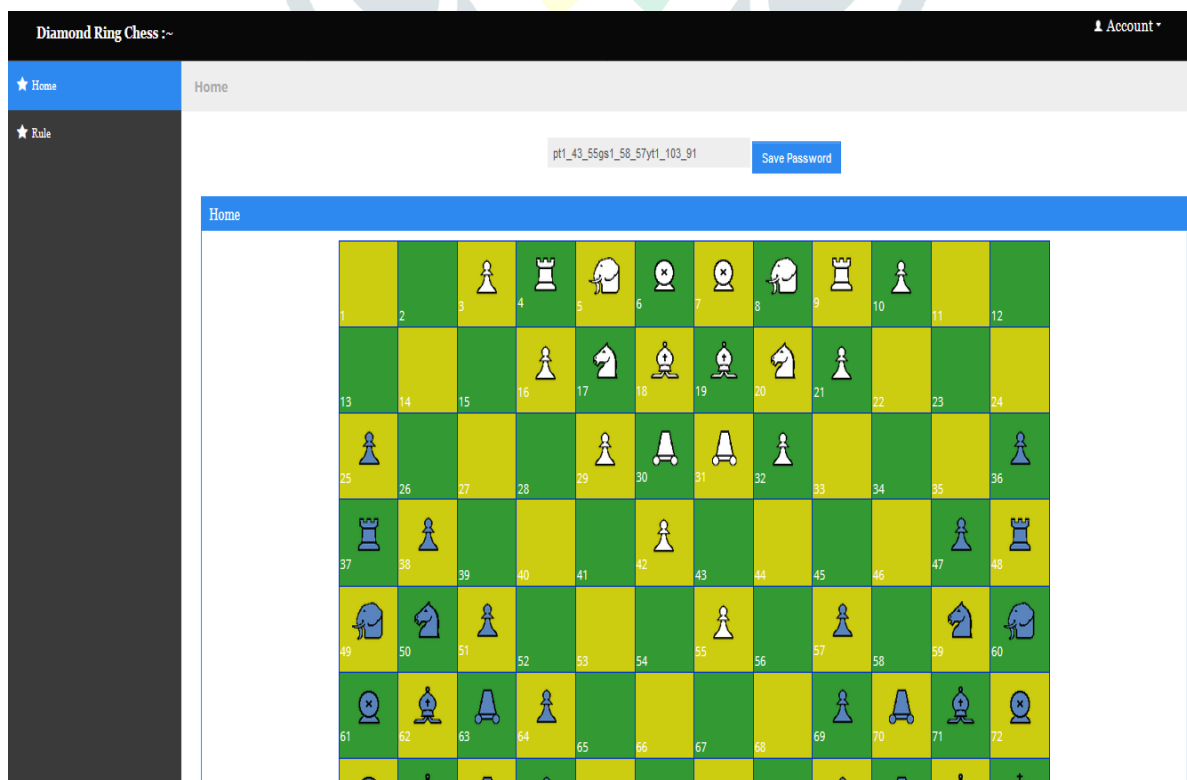


Fig. 5 Password Creation Form

Example of such password is ,

pt1_PAWN_42_54_!gs1_PAWN_69_68_@yt1_PAWN_103_91_#bs1_PAWN_76_77_%pt1_PAWN_43_55_!

The result of the strength of the password pattern generated is analyzed using the various tools online and some of the tools results we have mentioned in the table 1.

Table 2. TEST RESULT ANALYSIS TABLE PROPOSED WORK

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

Table 3. Comparative Analysis

Test Key	Website/Tool	Result
r1bqkbnr/pp1ppppp/n7/2p5/1P6/4K3/PPPPPPPP/RNBQ1BNR	Cryptool2	Entropy 3.8 Strength 168 Very Strong

V. Comparative Study

TABLE 4 COMPARATIVE ANALYSIS

Approach Basis	The base paper is based on the approach of the two player chess, based on the normal chess which is played and contains 64 block movements of the 32 total objects.	The proposed approach based on the Four player chess with 19 objects in each side in total of $19*4=76$ different objects which can be moved.
Password Strength	The Password string which is generated is like r1bqkbnr/pp1ppppp/n7/2p5/1P6/4K3/PPPPPP/RNBQ1BNR which contains the sequence of the repeated characters susceptible to the brute force attack.	The password string generated is like pt1_43_55gs1_69_68yt1_102_90bs1_76_77 which contains the combination of the different characters which is hard to crack and the entropy which counts the password strength is 3.84 is such string which is very strong.

VI. CONCLUSION

Secure Login is key to success to the any of the application. The dissertation concept is not only futuristic but also gives us the concept of how the 100% security can be achieved. In the dissertation the secure concept of using the Game based password which is based on the unique concept of Diamond Ring Chess , having the different movements as compared to the normal chess, not only enhances the security but also lessen the chances of the hacking or cracking the password. And also by validating the strength of the generated key or password against the password validating sites, it is clear that to break the password requires a lot of time and thus secure.

In the thesis, the security connected relies upon the photograph which is being given as a contribution by perusing the regarded document, later on work, the utilization of camera can be incorporated to tap the ongoing picture that can be utilized for the approval work and furthermore can incorporate the figure print to cross approve the client and will likewise prefer to work of the voice based passwords.

REFERENCES

- [1] VaibhavPoonia, Dr. Narendra Singh Yadav,"Analysis of modified Blowfish Algorithm in different cases with various parameters", International Conference on Advanced Computing and Communication Systems (IEEE) Jan. 05 – 07, 2015.
- [2] Huy Hoang Ngo, Xianping Wu, Phu Dung Le, Campbell Wilson, and BalasubramaniamSrinivasan,"Dynamic Key Cryptography and Applications",International Journal of Network Security, Vol.10, No.3, PP.161{174, May 2010.
- [3] Md. AsifMushtaque and Hash Dhiman "Implementation of New Encryption Algorithm with Random Key Selection and Minimum Space Complexity",International Conference on Advances in Computer Engineering and Applications (IEEE),March 2015.
- [4] Syed Zulkarnain Syed Idrus, Estelle Cherrier, Christophe Rosenberger, Jean-Jacques Schwartzmann. "A Review on Authentication Methods". Australian Journal of Basic and Applied Sciences,pp.95-107,May 2013.
- [5] M. Skrobot and J. Lancrenon, "On Composability of Game-Based Password Authenticated Key Exchange," IEEE European Symposium on Security and Privacy (EuroS&P), London, United Kingdom, pp. 443-457, April 2018
- [6] 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.
- [7] 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
- [8] 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
- [9] 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.
- [10]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.
- [11]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.
- [12]Nicholas Micallef andNalinAsankaGamagedaraArachchilage"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.