Journal of Cases on Information Technology
Volume 24 • Issue 4

Secure Chess-Based Data Exchange and User Validation

Dushyant Singh, Vivekananda Global University, India*
Baldev Singh, Vivekananda Global University, India

ABSTRACT

In each and every organization, data communication is an essential part. On a daily basis, data is exchanged within the organization as well as outside the organization. The passwords and OTPs play a critical role in securing the data. Now, how long and how well these OTP will work will depend on the strength of these passwords and OTPs. In the article, the authors have used the novel concept of applying the chess game in the process of the OTP or password generation. Here, they have made use of the four-player chess, with the dynamic movement of the kings, bishops, and other components. The formation of the OTP for the user authentication as well as data sending is done on the basis of the movement of the moveable objects. For testing the strength of the pattern, they have tested it using the various entropy checking tools, and the results are quite satisfactory compared to the results of the others.

KEYWORDS

Chess Game, Data Security, Graphical Password, Secure Communication

INTRODUCTION

With the growth of the Internet, various students, colleges, universities, offices, government organization are now online or linking themselves over internet. The main advantage of the internet is that, all information is available, just a matter to search the information we desire. Like a proverb, "Great Power, comes Great Responsibilities ", with the great benefit that the information or all data is available at one place or over internet, there are chances that the data can be misused. Just like the authentic users are growing day by day, unauthentic users like hackers are also growing day-day, causing the threat to the information which is available over the internet. (M. Abdalla, 2014).

First and the foremost thing is to authenticate the user before accessing any data. Users' authentication is a mean of recognizing the customer and confirming that the customer is allowed to get to some restricted administrations. Customer authentication means working up a connection between the customer and some character. A character is the peculiarity property of a customer which ideally can't be fabricated or copied. Before long, personalities are completed by things which customers know (passwords), have (puzzle keys or security tokens) or properties which they have (biometrics). (M. Abdalla, 2014).

DOI: 10.4018/JCIT.296718 *Corresponding Author

In the case of networks, when the user when require to send the data, such data communication requires some costs in terms availing the proper secure channel or environment.

This infers the organization workplaces will make the recognized data accessible just to explicit people, generally the people who pay for getting the administration. For this situation, a network should in all likelihood perceive real customers from the strange ones. In authentication, a customer sends his ID (e.g., name, IP address) and verification of his character to a sensor with the objective that the sensor can pick whether the personality is genuine and in fact has a spot with the customer of that name. Upon productive authentication, the sensor approves the customer who is enabled access to the data. (J. Becerra V. et al, 2017).

In order to maintain the proper data security in the organization it is required to perform some basic operations as shown in fig 1. The formal training of employees required for training the employees about the necessity of data security. Performing measures for maintaining onsite as well as online data security, like authentication process, encrypting data and soon. (M. Abdalla et al 2014).

Some measures of data security are as follows:

- **Authentication:** The target of this organization is to allow trustable correspondences between 2 extraordinary hubs. Precisely once a hub gets parcels from a supply, it should check that concerning character of the supply hub. A technique to agitate provides this organization is victimization accreditations, whoever while not central management unit, key conveyance and key the officers square measure contestable. (M. Abdalla et al 2014).
- **Information secretly:** Per this organization, every hub or application should approach incontestable organizations that it's the consent to induce to. out and away most of organizations that measure given by info on the coding procedures anyway in networks there's no central organization, key circulation went up against numerous troubles and from time to time immeasurable. (F. Benhamouda O et al 2015)

The essential plan is to vary a puzzle message into varied concepts by secret sharing plans and subsequently expire the concepts by strategies for varied free approaches to the goal. In like manner,

Figure 1. Data security measures

paying very little heed as to whether barely any hubs that square measure accustomed hand-off the message shares, been undermined, the puzzle message beat all is not undermined. victimization multipath passing on causes the range of deferral in parcel transport for various bundles. It equally prompts out-of-demand bundle movement. (F. Benhamouda O et al 2015):

- **Genuineness:** Per decency security organization, primarily supported hubs will create, modify or eradicate parcels. for instance, Man-In-The-Middle assault is against this organization. during this assault, the aggressor gets all bundles and subsequently clears or modifies them.(S. Jarecki H. el al 2018).
- **Non-Repudiation:** By victimization this organization, neither supply nor goal will deny their lead or info. By the day's finish, if a hub gets a bundle from hub two, and sends a solution, hub two cannot deny the parcel that it's been sent.(S. Jarecki H. el al 2018).

LITERATURE REVIEW

F. Z. Glory et al, 2019, in this paper author proposed the unique concept of generating password using the random text extraction. The basis for the formation of the password is the information which is input or gathered from the user, for example, favorite novel name, number of grad mother's children, important dates and so on. The text is fetched on the random basis from the provided information and from the strong passwords.

Y. Zhu et al, 2018, author proposed the Multi-fAcet Password Scheme (MAPS) and used it for the mobile based authentication. MAPS are the main basis for the formation of the password, and are generated by making use of the multiple facets, which means the simple movement results in the generation of the password. Thus, the main advantage of the concept is that we have to remember on the movements, not the long password sequence pattern.

Pooja M. Shelke and F. M. Shelke, 2016, author proposed the 3D password which is the multi-factor based authentication scheme, one that combines the existing of the authentication techniques into the 3D Based Virtual Environment. In this environment, their are various kinds of the virtual objects. The password is formed by the motion or the movements of the virtual objects.

RESEARCH GAPS

The password generation process in the Four-player diamond ring chess will be more secure as compared to the two-player chess because we will increase the number of players and combinations used in the generation process. The systems generally involve the two player chess systems.

We compare the complexity and strength of proposed algorithm with existing algorithms like (Four-Pin based password, Text based password, alphanumeric password, and two players chess system) to prove that our algorithm is better than the other available. (Various online tools like, Password-meter, Password-Kaspersky and my1login) (Pooja M. Shelke and F. M. Shelke, 2016).

We will also perform user study on suitable population. To support the statement that our algorithm is better than others and actable by end users.

PROPOSED ALGORITHM

The proposed algorithm is used to specify the working of all the sub-processes which are involved in the proper functioning of the system:

1. Registering the User in the system.
2. Sending the Data over the system.
3. Receiving the data over the system.

Algorithm for Registration

[
Input: User information, Password Length
Output: Outcome success, then details saved in the system with the password details.
]
In this module we are concerned with the registration of the new users for the system.
Step 1: Read User Credentials like user name, DOB, Email Address and Password Length.
Step 2: Password Length will form the basis for the number of movements required for the generation of the password.
Step 3: Four Player Chess with the diamond ring chess concept are generated on the graphical screen with the moveable object shown on the screen.
Step 4: The movement of the moveable object is flexible and the movement of the object will form the basis for the generation of the password pattern.
Step 5: The pattern is generated as follows –
Present-Position_Moved-Position_team_name_character_ corrospoding_ to difference in position and so on.
Step 6: Verify the user details with the database.
Step 7: If Details Exists Then:
Failure, Details will not saved
Else:
Success, Details will be saved
[End of If structure]
Step 8: Stop.

Algorithm for Sending Data

[
Input: Sender User Name, Receiver User Name, Data
Output: Success Return TID and Session OTP
]
This algorithm concern with the generation of the transaction ID and session OTP, Which will be required for the initiating the transaction for the transfer of data to the receiver.
Step 1: Input user name, Password Length
Step 2: Password Length will form the basis for the number of movements required for the generation of the password.
Step 3: Four Player Chess with the diamond ring chess concept are generated on the graphical screen with the moveable object shown on the screen.
Step 4: The movement of the moveable object is flexible and the movement of the object will form the basis for the generation of the password pattern.
Step 5: The pattern is generated as follows, Present-Position_ Moved-Position_team_name_character_corrospoding_ to difference in position and so on.
Step 6: If Details Exists Then

```
   a. Generate the transaction ID unique of the transaction.
   b. Again generate the Session OTP for the message exchange,
      again using the graphical interface of the moveable objects
      in 4-plaer chess.
   c. Save the details in the database.
  Else:
   Write "No Details of user Exists"
  [End of If structure]
Step 7: Stop.
```

Module for Receiver

```
[
Input: Sender User Name, Receiver User Name
Output: Success Message or File Accessed
]
In this module we deals with the receiver end module, which is
concern with the secure data delivery.
Step 1: Read the concerned Transaction ID and the session OTP.
Step 2: Verify the details in the database module for the
   transaction related data.
Step 3: If Details Verified then:
   a. Fetch the data from the database.
   b. Deliver the data to the receiver
  Else:

   Write "Invalid Details"
 [End of Outer If structure]
Step 4: Stop
```

IMPLEMENTATION

The implementation of the secure data communication system is done in the web-based language PHP and the database which is required for the simulation work is created in MYSQL.The system consists of the various modules which are involved in the implementation of the proposed algorithms. In the Fig 2, the figure shows the registration module which takes in initial registration details and then in the Fig 3, will proceed for the generation of password using the moveable objects.

In Fig 3, the graphical screen is shown with the four player chess.

The Fig 4 is the data sharing form in which, the file is selected containing the data which is to be shared and the unique transaction ID and the session OTP is generated after the file specification.

RESULT ANALYSIS

Although we are working on the strength comparison but we have found the various tools which are available online which can be used for the testing of the strength of the password which is generated for the authentication of the user, at the time of the registration process using the movement of the chess players. (Richard Shay et al, 2010).

The strength of the password is generally judged on the entropy more the entropy more will be strength of the password and more difficult for the hackers to break or to crack the password pattern. Together with the entropy of the password, we have also checked for the bit-strength and also on the number of years required for a tool or other program to crack a password pattern. (Michelle L Mazurek et al, 2013):

Figure 2. User registration initial screen

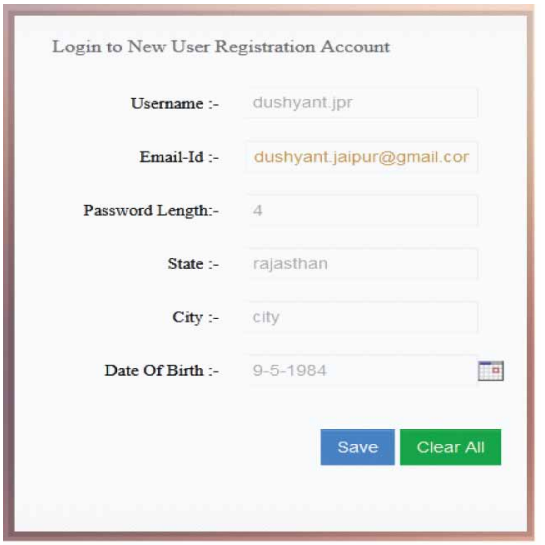


Figure 3. Chess screen

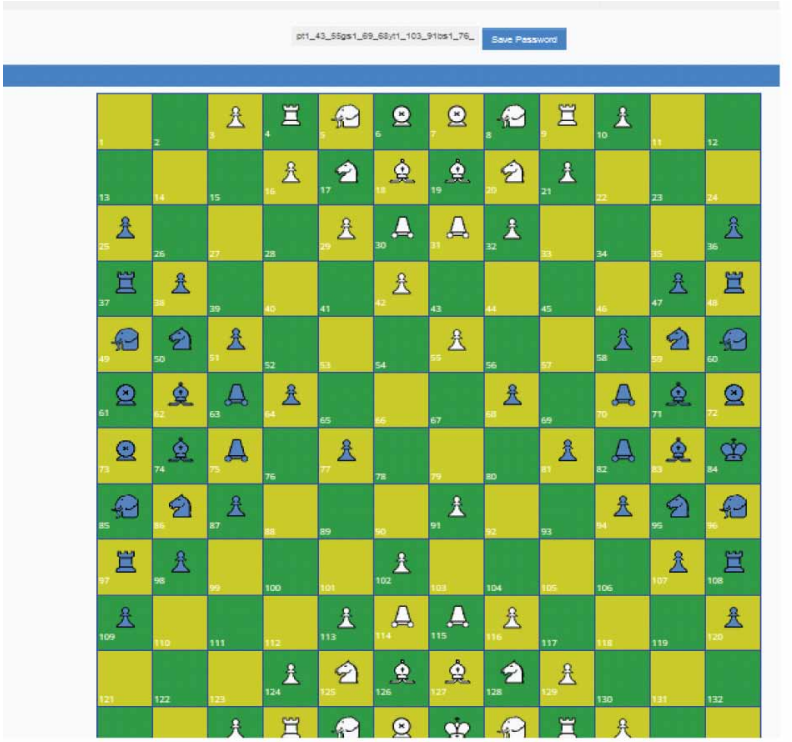
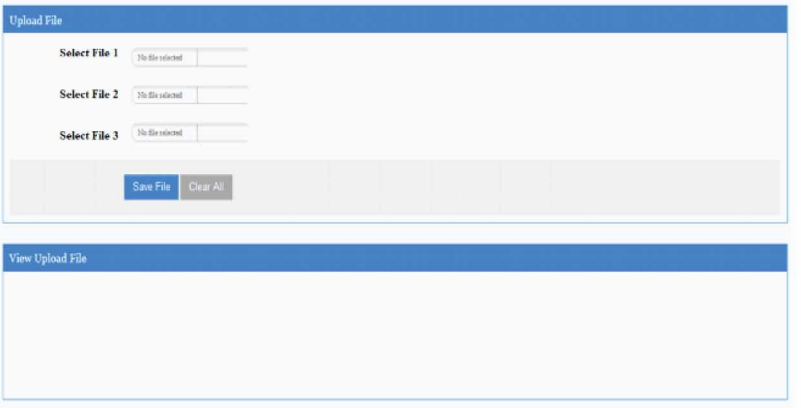


Figure 4. Data sharing



Base Paper Password Pattern {urAn29iRfan-

Proposed Password Pattern pt1_PAWN_ 42_54_ 3gs1_PAW N_81_80_(yt1_ PAWN_113_1 01_3bs1_PAWN_ 64_65_(

Result Analysis on Basis of Years Required

Password Monster Tool

The first tool which we have selected for this purposed is Password Monster website, which check the pattern and result in the number of years which are required to break the pattern:

Result for Base Pattern = 0.000005 trillion years
Result for Proposed Pattern = 4 hundred trillion trillion trillion trillion trillion trillion years

This shows that proposed pattern is more effective.

Thycotic.com Password Checker Tool

The next tool which we have selected for this purposed is thycotic.com website, which check the pattern and result in the number of years which are required to break the pattern:

Result for Base Pattern = 1.86E-67 quattuorvigintillions years
Result for Proposed Pattern = 102 quattuorvigintillions years

This shows that proposed pattern is more effective.

How Secure is My Password Checker Tool

The next tool which we have selected for this purposed is howsecureismypassword.net website, which check the pattern and result in the number of years which are required to break the pattern:

Result for Base Pattern = 4.6E-68 quattuorvigintillions years
Result for Proposed Pattern = 25 quattuorvigintillions years

This shows that proposed pattern is more effective.

Thus, the results on the basis of the time period required are summarized in the Table 1.

Result Analysis on Basis of Entropy

In the case of the Entropy, the password strength is measured in terms of the bit strength, and the concept which is followed for measuring the bit strength is as follows:

```
< 28 bits = Very Weak
28 - 35 bits = Weak;
36-59 bits = Reasonable
60-127 bits = Strong
128+ bits
```

Rumkin Tool

The first tool which we have selected for this purposed is http://rumkin.comwebsite, which check the pattern and results in the number of bits for the password strength:

Result for Base Pattern = 60.9 bits
Result for Proposed Pattern = 299.9 bits

This shows that proposed pattern is more effective.

Password.BluePassword Checker Tool

The next tool which we have selected for this purposed is password.blue website, password.blue tools which is a password meter that tests entropy using zxcvbn by Dropbox:

Result for Base Pattern = 43 bits
Result for Proposed Pattern = 219 bits

This shows that proposed pattern is more effective.

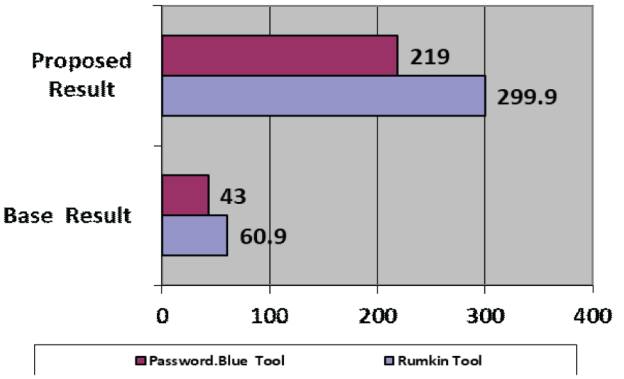
Table 1. Result Analysis on Basis of Time Period

Website/Tool	Base Result	Proposed Result
Password Monster Tool	0.000005 trillion years	4 hundred trillion trillion trillion trillion trillion trillion trillion years
Thycotic.com Password Checker Tool	1.86E-67 quattuorvigintillions years	102 quattuorvigintillions years
How Secure is My Password Checker Tool	4.6E-68 quattuorvigintillions years	25 quattuorvigintillions years

Table 2. Result analysis on basis of entropy

Website/Tool	Base Result	Proposed Result
Rumkin Tool	60.9 bits	299.9 bits
Password.Blue Tool	43 bits	219 bits

Figure 5. Result analysis graph



Thus, the results on the basis of the time period required are summarized in the Table 2. The Fig 5 shows the graph on the basis of the Entropy strength in the number of bits.

CONCLUSION

In the modern IT work, the complex level of the security is always required and working on the improvement of the security mechanism is the ever going process, just like the countries every year increase their defense budget. Instead of the defense budget improvement, in the modern IT world, the improvement in the concept level of the security is always desired and the proposed work is the attempt towards that.

We are working in order to provide the interactive mechanism to users for the authentication purpose, together with that the strong pattern which will make the task of cracking password more difficult for hackers.

FUTURE WORK

In future, we will first on the real time execution of the proposed work, where we will like to approach some banking and similar financial organization for the implementation of our concepts in their organizations.

Next, as security is the never ending field, we will try to explore the new dimensions of security like DNA Cryptography, Retina Based Security, Role Base access and more.

REFERENCES

Abdalla, M. (2008). *Password-Based Authenticated Key Exchange: An Overview. ProvSec ser*. LNCS Springer.

Abdalla, M., Catalano, D., Chevalier, C., & Pointcheva, D. (2008). *Efficient Two-Party Password-Based Key Exchange Protocols in the UC Framework. Topics in Cryptology - CT-RSA, ser*. LNCS Springer.

Becerra, J., Iovino, V., Ostrev, D., & Škrobot, M. (2017). On the Relation between SIM and IND-RoR Security Models for PAKEs. ICETE, SECRYPT, 151-162.

Benhamouda, Blazy, Chevalier, Pointcheval, & Vergnaud. (2015). New Techniques for SPHFs and Efficient One-Round PAKE Protocols. *IACR Cryptology ePrint Archive*.

Glory, F. Z., Ul Aftab, A., Tremblay-Savard, O., & Mohammed, N. (2019). Strong Password Generation Based On User Inputs. *IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada* (pp. 416-423). Academic Press.

Jarecki, Krawczyk, & Xu. (2018). OPAQUE: An Asymmetric PAKE Protocol Secure Against Pre-Computation Attacks. *Advances in Cryptology - EUROCRYPT*.

Mazurek, Komanduri, Vidas, Bauer, Christin, Faith, & Cranor. (2013). Measuring password guessability for an entire university. *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, 173-186.

Shay, R., Komanduri, S., Kelley, P. G., & Leon, P. G. (2010). Encountering stronger password requirements; user attitudes and behaviors. *Proceedings of the Sixth Symposium on Usable Privacy and Security*. doi:10.1145/1837110.1837113

Shelke & Shelke. (2016). Advance Authentication Technique: 3D Password. *International Journal on Recent and Innovation Trends in Computing and Communication*.

Zhu, Y., Gurary, J., Corser, G., Oluoch, J., Alnahash, N., Fu, H., & Tang, J. (2018). CMAPS: A Chess-Based Multi-Facet Password Scheme for Mobile Devices. *IEEE Access: Practical Innovations, Open Solutions*, *6*, 54795–54810. doi:10.1109/ACCESS.2018.2872772

Dushyant Singh is currently pursuing PhD in CSE from Vivekananda Global University, Jaipur. He has 11 years of versatile experience. He has guided more than 15 students in their MTech dissertation. His expertise field is Information security and cloud computing. He has dynamic personality and always ready to acclimatize himself according to new technologies.

Baldev Singh is currently working as Dean of Faculty (Engineering) at Vivekananda Global University. He has 23 years of versatile experience. He has guided more than 10 students in their MTech dissertation and 5 students in PhD. His expertise field is Information security and cloud computing.