ENHANCEMENT IN SECURITY OF DATA EXCHANGE USING OBJECT MOVEMENTS IN MULTIPLAYER CHESS

D. Singh and B. Singh
Department of Computer Science & Engineering, Vivekananda Global University, Jaipur, MS, India

ABSTRACT

Increase in the growth of technology has its pros and cons. With the rise in techno-power, hackers are also getting more techno-skilled. In order to perform the data communications or data exchange in between users securely, more innovative methods of security are required. For the purpose of enhancing the data security, we proposed four player chess-based security schemes. The concept of key generation for user authentication and data sharing is done by making use of the dynamic movements of King, Bishop and other objects on chessboard. The generated key is envaulted and analyzed using the various entropy testing tools and given satisfactory results on comparison with previous approaches.

Keywords: *Chess Game, Graphical Password, Data Security, Secure Communication.*

1. Introduction

The collection of standards and technologies which are used to protect the data from any of the accidental or intentional misusage or destruction of data referred to as data security. There are numerous techniques and methods which can be used for implementing the data security, like logical controls, standards, crypto-techniques and more. Various financial organizations like banks and Government data centers deals with the enormous volume of data containing the personal information of their clients which need to be safeguarded [1]

The main objective of data security is to protect the data exchange from unauthorized access. The integrity of data is also the main concern. Any sort of data leaks can harm the organization reputation and can suspect them to immense fines and penalties. Thus, in such scenario all concern required to be given to enhance the data security. [1]

Data Security can be implemented in number of ways and methods for overcoming data threats. The various methods for securing the data are as follows, [2]

- **Encryption of Data:** According to this concept the crucial data is encrypted using the key and the access is granted to person one who has the valid key for the decryption of data.
- **Masking of Data:** In order to safeguard the important data, sometimes that data is masked with some other characters like X or * so that it is not accessible to public. Example of such data is credit card number.
- **Erasure of Data:** After accessing the data related to some user is of no use, the data required is to be deleted.
- **Resilience of Data:** Data is suspectable to data breaches or even accidental damages, thus it is required that the proper backup copies of such data should be maintained on local or on server machines. [2]

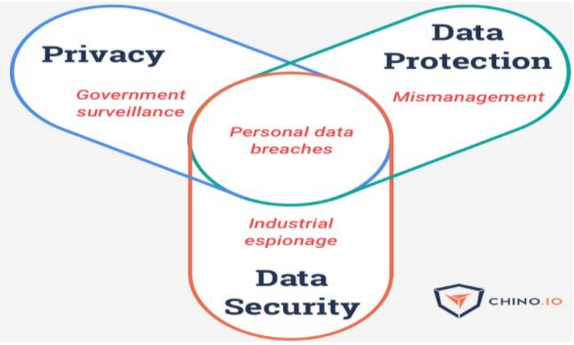


Fig 1 Data Security (ref. China.io)

The most productive way of monitoring and controlling the data security is to have a check on the person accessing the data. This concept of checking is also known as AAA, where A-Authentication, A-Authorization and A-Accounting.[3]

The term "Authentication" refers to check the identity of the user accessing the data. This process is conducted via username and password entry. In the modern trends, multi-factor authentication concept is also used involving the concept of OTP, biometrics and more. [3]

The term "Authorization" refers to concept which controls the portion of data which the user can access. Hackers or attackers can be overcome from manipulating the user details and gaining unauthorized access. [3]

2. Literature Review

F. Z. Glory, et al. 2019 introduced the novel approach of creating passwords using random text extraction. The information provided or obtained from the user forms the foundation for the password, such as the user's favorite novel name, the number of grand mother's children, key dates, and so on. The text is retrieved at random from the specified information as well as strong passwords.

The Multi-facet Password Scheme (MAPS) was proposed by Y. Zhu et al. 2018 and utilized for mobile based authentication. MAPS are the primary foundation for the creation of passwords, and they are formed by combining many aspects, which means that a simple movement can result in the creation of a password. As a result, the concept's key benefit is that we just have to memorize the motions rather than the complex password sequence pattern.

Pooja M. Shelke and F. M. Shelke proposed the 3D password in 2016, which is a multi-factor based authentication strategy that incorporates current authentication approaches into a 3D Based Virtual Environment. There are numerous types of virtual items in this environment. The random motions of the virtual objects create the password.

3. Research Gaps

Though we have increased the number of players and permutations utilized in the creation process, the password generating process in the four-player diamond ring chess will be more secure than the two-player chess. Generally the systems are typically two-player chess systems. We compare the complexity and strength of our proposed algorithm to existing algorithms such as (Four-Pin based password, Text based password, alphanumeric password, and two-player chess system) to show that it is superior than the others.

(Password-meter, Password-kaspersky, and my1login are just a few examples of online utilities.)

We would also undertake user study on relevant population to substantiate the notion that our algorithm is better than others and actable by end users.

4. Proposed Algorithm

The proposed work is divided into the three segments of user registration, login and lastly the data transfer.

4.1 Registration Process of New User

This algorithm explains the concept or the steps which are involved in the registration of the new user of system.

Step 1:In first step the user name, DOB and other details are required to be entered.

Step 2:In the second step of the detail's specification, we are required to enter the length of the password or pattern which is equivalent to the total placements by the users playing the game.

Step 3:The novel concept of the pattern generation using the chess game is suggested, in which the pattern is generated on the basis of the movement of the player on the board.

Step 4: Total movements are governed with the length of the password pattern, which is specified initially.

Step 5:The process of formation of pattern is governed as ,

Initial-Position_NextPlaced-Position_team_name_character_corrospoding_to difference in position and therefore the next player movement and all such movement patterns are concatenated to form the total pattern.

Step 6: Check into the database

Step 7: If data is in Database then

Generation of Error

Else:
No Issues, Save Details
[End of If structure]
Step 8: Stop.

4.2 Authentication of Registered User

This process involves the authentication of the registered users of the system, in order to transfer the message.

Step 1:In first step the user name is required to be entered.

Step 2:In the second step of the detail's specification, we are required to enter the length of the password or pattern which is equivalent to the total placements by the users playing the game.

Step 3:The novel concept of the pattern generation using the chess game is suggested, in which the pattern is generated on the basis of the movement of the player on the board.

Step 4: Total movements are governed with the length of the password pattern, which is specified initially.

Step 5:The process of formation of pattern is governed as,
Initial-Position_NextPlaced-Position_team_name_character_corrospoding_to difference in position and therefore the next player movement and all such movement patterns are concatenated to form the total pattern.

Step 6: If User Details Found Then:

a. For the each of the transaction a unique number representing the transaction ID is generated.
b. Now, the same process adopted for the generation of pattern in registration of user or authentication of user, the same is adopted for the generation of the key for the data exchange between the two users.
c. Specify the Receiver
d. All transactions detailed information is stored in table.

Else:
Write "User Denied to Access"
[End of If structure]
Step 7: Stop.

4.3 Module for Receiver

This algorithm operates at the receiver end for the access of the message sent by the sender.

Step 1: First at the sender end, authentication process derived in the algorithm 4.2 will be performed.

Step 2: For accessing the message of the sender, required the unique number which is the transaction ID and the key which is used for the validation of the session among the two users for the data exchange.

Step 3: If Specified information correct then:

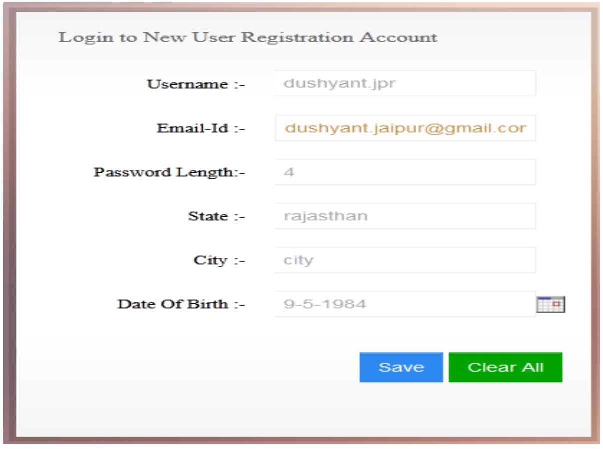
a. Message is accessed by the receiver.

Else:
Write "Details not match"
[End of Outer If structure]
Step 4: Stop

5. Implementation

The system for the concept of the chess based concept of the data security and data exchange is developed using the web based platform of the PHP and MYSQL

The webform corresponding to the registration of the new users is shown in the fig 2. It shows the formwhere the user related information need to be filled with the length of the password.

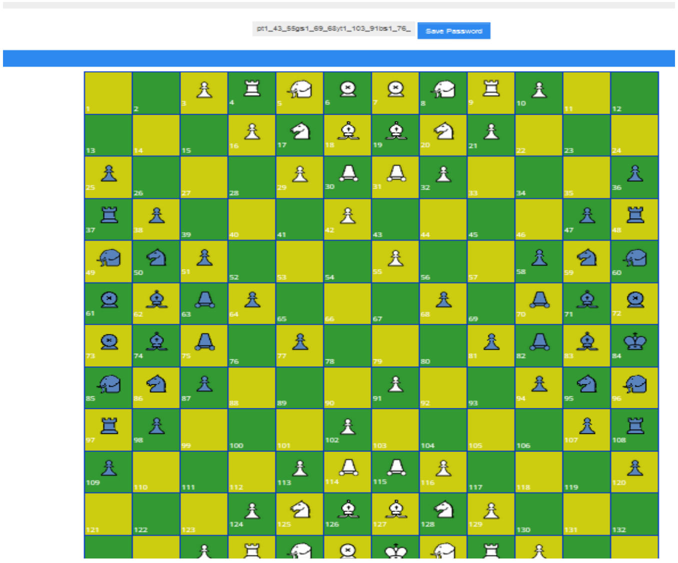


Login to New User Registration Account

Username :- dushyant.jpr
Email-Id :- dushyant.jaipur@gmail.cor
Password Length:- 4
State :- rajasthan
City :- city
Date Of Birth :- 9-5-1984

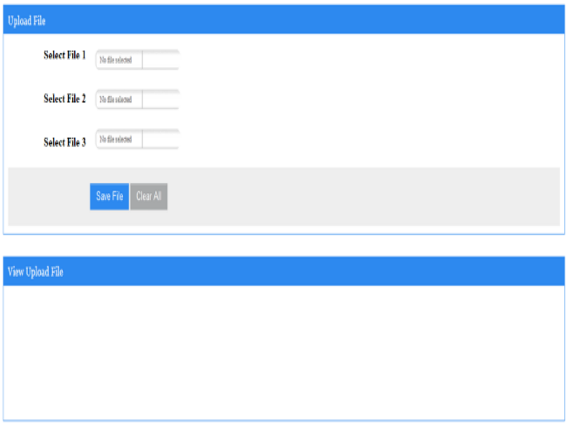
Fig 2 Webform for registration

The chess board pattern which is used for the process of the generation of the pattern is shown in the fig 3



pt1_43_55gs1_69_68yt1_103_91bs1_76_

Fig 3 Chess Board for Pattern Generation



Upload File

Select File 1: No file selected

Select File 2: No file selected

Select File 3: No file selected

View Upload File

Fig 4 Data Exchange Form

The webform used for the specification of the data which is to be exchanged as followed by the generation of the unique number based transaction Id and key for the exchange of the data, is shown in fig 4.

6. Result Analysis

The concept which we generated for the purpose of improving the security is quite efficient and we show the strength of the model proposed by making the comparison of the key generated with the earlier approaches.

Base Paper Password Pattern

{qsBm17kSahy-

Proposed Paper Password Pattern

pt6_BHISHOP_31_44_-gs6_BHISHOP_71_57_.yt1_PAWN_113_101_,bs5_HORSE_86_88_"

Table 1

Result Analysis

Website/Tool	**Base Result**	**Proposed Result**
Kaspersky Password Entropy	Time Period : 19 Centuries	Time Period : 96 centuries
Thycotic Entropy Test	Time Period : 186 million years	Time Period : 16,095 Quadragintillion years
Password Checker Online	Strength : 84%	Strength : 100%

7. Conclusion

In the current IT job, the complicated degree of the security is constantly necessary and working on the enhancement of the security mechanism is the ever going process, because of this the governments every year enhance their military expenditure.

Instead of the defense budget improvement, in the present IT world, the improvement in the concept level of the security is constantly required and the offered work is the attempt towards that.

We are striving to give users with an interactive mechanism for authentication, as well as a robust pattern that will make the process of breaking passwords more difficult for hackers.

References

1. M. Abdalla "Password-Based Authenticated Key Exchange: An Overview" in ProvSec 2014 ser. LNCS Springer vol. 8782 pp. 1-9 2014.
2. J. Becerra V. Iovino D. Ostrev and M. Škrobot "On the Relation Between SIM and IND-RoR Security Models for PAKEs" in ICETE 2017 - Volume 4: SECRYPT 2017 SciTePress pp. 151-162 2017.
3. M. Abdalla D. Catalano C. Chevalier and D. Pointcheval "Efficient Two-Party Password-Based Key Exchange Protocols in the UC Framework" in Topics in Cryptology - CT-RSA 2008 ser. LNCS Springer vol. 4964 pp. 335-351 2008.
4. F. Benhamouda O. Blazy C. Chevalier D. Pointcheval and D. Vergnaud "New Techniques for SPHFs and Efficient One-Round PAKE Protocols" IACR Cryptology ePrint Archive vol. 2015 pp. 188 2015.
5. S. Jarecki H. Krawczyk and J. Xu "OPAQUE: An Asymmetric PAKE Protocol Secure Against Pre-Computation Attacks" in Advances in Cryptology - EUROCRYPT 2018 ser. LNCS Springer 2018.
6. F. Z. Glory, A. Ul Aftab, O. Tremblay-Savard and N. Mohammed, "Strong Password Generation Based On User Inputs," 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 2019, pp. 0416-0423.
7. Y. Zhu et al., "CMAPS: A Chess-Based Multi-Facet Password Scheme for Mobile Devices," in IEEE Access, vol. 6, pp. 54795-54810, 2018.
8. Pooja M. Shelke and F. M. Shelke, "Advance Authentication Technique: 3D Password",IJRITCC(International Journal on Recent and Innovation Trends in Computing and Communication) June-2016.
9. Richard Shay Saranga Komanduri Patrick Gage Kelley Pedro Giovanni Leon Michelle L Mazurek Lujo Bauer et al. "Encountering stronger password requirements; user attitudes and behaviors" Proceedings of the Sixth Symposium on Usable Privacy and Security pp. 2 2010.
10. Michelle L Mazurek Saranga Komanduri Timothy Vidas Lujo Bauer Nicolas Christin Lorrie Faith Cranor et al. "Measuring password guessability for an entire university" Proceedings of the 2013 ACM SIGSAC conference on Computer &amp; communications security pp. 173-186 2013.
11. Matt Weir Sudhir Aggarwal Michael Collins and Henry Stern "Testing metrics for password creation policies by attacking large sets of revealed passwords" Proceedings of the 17th ACM conference on Computer and communications security pp. 162-175 2010.
12. Hristo Bojinov Elie Bursztein Xavier Boyen and Dan Boneh "Kamouflage: Loss-resistant password management" European symposium on research in computer security pp. 286-302 2010.
13. Patrick Gage Kelley Saranga Komanduri Michelle L Mazurek Richard Shay Timothy Vidas Lujo Bauer et al. "Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms" 2012 IEEE symposium on security and privacy pp. 523-537 2012.
14. Saranga Komanduri Richard Shay Patrick Gage Kelley Michelle L Mazurek Lujo Bauer Nicolas Christin et al. "Of passwords and people: measuring the effect of

password- composition policies" Proceedings of the SIGCHI Conference on Human Factors in Computing Systems pp. 2595-2604 2011.

15. Richard Shay Saranga Komanduri Adam L Durity Phillip Seyoung Huh Michelle L Mazurek Sean M Segreti et al. "Designing password policies for strength and usability" ACM Transactions on Information and System Security (TISSEC) vol. 18 no. 4 pp. 13 2016.
16. Cormac Herley and Paul Van Oorschot "A research agenda acknowledging the persistence of passwords" IEEE Security &amp; Privacy vol. 10 no. 1 pp. 28-36 2011.