Research Article

Secured Banking Authentication by Pixel Correlation for Online Shopping

Kavitha Esther Rajakumari[a], . Jeyasruthi[b], B Lakshmi Shivani[c], N Hariharan[d]

[a,b,c,d,] Department of Information Technology, Hindustan Institute of Technology and Science, Chennai, India
[a] kavithaer@hindustanuniv.ac.in,[b] jeyasruthi.selvam@gmail.com, [c] lakshmishivani11@gmail.com

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

Abstract: This paper presents a secure way for bank transaction during online shopping with the help of graphical passwords that is image processing.The project's aim is to assist users in choosing and constructing a stronger password that cannot be easily compromised. This paper also talks about the clustering and recommendation of items that are bought by the user's during online shopping. Item based recommendation is used so that unwanted items that are not relevant to the user's shopping arenot recommended [Noise recommendation]. Multilevel clustering is used to cluster all the items and then group them. This project helps to avoid phishing attack.The attacker uses phishing e-mails to send different types of links or attachments that can be compromised, including credential details such as login details or account information of the user, in this type of cyber-attack.This method was introduced to overcome textual passwords, pins and other trivial passwords methods which were difficult to remember and prone to external attack. When a client forgets their password, they must create a new one that is both difficult to remember and easy to hack. A graphical password is easier to remember than a text password, and users can generate their own passwords using images. As a result, some researchers have proposed using a graphical password instead of a text-based one. As a result, several researchers have suggested graphical password as an alternative to text-based password. The user will select a particular part of the screen to confirm the process. We propose a framework having pixel correlation for user verification based on double hashing.

Keywords: Graphical Passwords, Image Processing, Phishing Method, Double Hashing

1. Introduction

In today's world online shopping has become a common thing where different products are bought and sold. Clustering is a subjective process that the same set of data items often needs to be divided differently for different applications [1]. The items are clustered using multi-level clustering. The system chooses candidate recommendation sets based on related users' item knowledge, then assigns a guess to the candidate item set and generates recommendation items [14].One of the most important concerns today is the security of private and sensitive data from rivals, competitors, and hackers. As a result, we strive to find a simple and effective solution that takes into account the users' needs as well as the risks associated with data transmission. To mitigate the inconvenience of accessing the account in public locations, the suggested solution is to create a clever way to authenticate the user's bank account using a pictorial password and inserting an indirect pin into the framework [18].This project's main aim is to establish a payment gateway security measure[15].Phishing is a type of cybercrime in which an intruder impersonates a real individual or organization by posing as an official person through e-mail or other means of communication.[15].Code clones can be helpful or detrimental to the programmer, depending on the type of clones discovered[13].The encryption is used to verify the identity of the user who is making an online payment. The user's authentication is checked using the Graphical Password Scheme. Passwords provide a protection mechanism for authentication and services that protects resources from unauthorized access. One secure alternative to textual passwords is a graphical-based password [19].As the name indicates, this technique uses photos (pictures) as a password rather than text. Furthermore, according to a psychological review, humans can recall images more quickly than text. Furthermore, according to a psychological review, humans can recall images more quickly than text. [2]. A new graphical password protection technique is proposed that is resistant to shoulder surfing and other types of attacks [2]. Shoulder surfing attack has become more so this paper gives you an alternate idea to avoid it. The introduction of smartphones and sudden advancement of computer systems and services have changed the way of living, resulting in more interaction with computer devices than ever before [3]. As discussed earlier to avoid hacking, textual passwords can be replaced using graphical passwords. The most common authentication method used in most of the devices is textual or numerical passwords, it includes pin passwords too. Textual passwords are error prone and time consuming. Creating a list of passwords, then encrypting each word in two steps using random functions to achieve effective double security [4]. This paper introduces a modern hash-based encryption scheme that includes a built-in double hashing mode [5].Reversible data hiding is one of the most well-known techniques for hiding data in a cover picture and extracting it with less distortion at the receiver side with the hidden secret message. [16]. We have introduced a new graphical technique that can prove to be effective the personal information from such external attacks. In fig 1 we have explained the working process as of how the registration is going to work. If you are an existing user, it will take you to the verification process. If it's a yes it

will take you to a view user account, followed by upload files and then view upload files. If it's a no, then it's a wrong password. This is the procedure for existing user. Now, if you are a new user you will create a new account and then add the registration details followed by create by user ID. Then it will end the process.

The proposed idea of graphical password is to provide reliability to the users who are very protective when it comes to their confidentiality of data. Four process are involved in the process of this project.

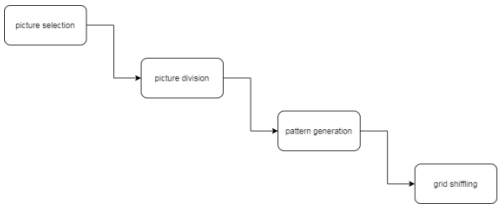

Fig1: Picture Division

Once's when the picture is uploaded it is divided into 4 stages that is picture selection. Picture selection selects the picture that is uploaded for image 1 process during the authentication. Then the picture is divided for the click point process so that the users can register their click point. After the division process it goes on to the pattern generation and then to the grid shuffling.He or she can set a password and apply it by clicking on the points of the images. After that a unique ID is generated for each users.

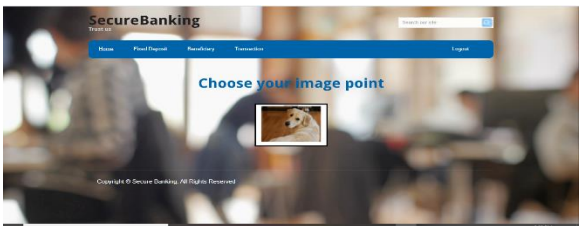

Fig2: 1st Click Point

This figure describes the user-selected click points that serve as the password. For each image, the pixel positions are stored in the database.

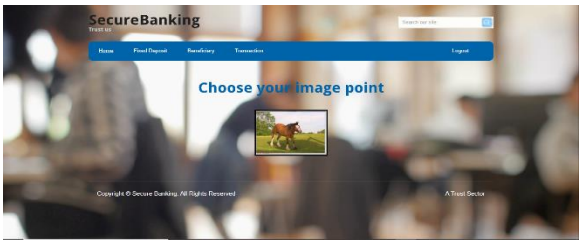

Fig3: 2nd Click point

For the password, the user chooses the second click point. The password is set to the click pointRELATED WORKS:

Now a days Hackers can use the computational power of computers to build ways to decrypt data without using passwords. Here we present the summary of visual cryptography and it is used in banking system. Phishing is a fraudulent acquisition of confidential data. These systems, especially those based on k-nearest neighbor collaborative filtering, have had a lot of success on the web [6]. This helps the hackers to easily hack all the data. The user-item matrix is used to assess item-based techniques and identify object relationships, which are then used to compute recommendations for users indirectly [6]. Clustering is the division of data into similar groups of objects. Each cluster is made up of objects that are identical to one another but not to objects from other classes. [9]. Clustering takes place when the items are selected by the users. The objects are suggested based on the user's preferences. For researchers, Cluster Analysis is one of the most important data mining techniques because it helps them to analyses data and categories data attributes into different classes [7]. The most popular algorithm that uses an iterative refinement technique is K Means clustering [7]. The randomness of the cluster centres must be handled and monitored in order to keep the number of iterations in the traditional algorithm to a minimum while reducing complexity and increasing accuracy [7]. The compressed image's pixel position is then permuted by the sequence provided by 2D-LASM to improve the root phase's security[12].In other websites all the items are recommended whereas in this the items which are related to previous purchase of the customers are recommended. For example, if a user buy's a mobile phone, a phone cover or earphones are recommended based on his purchase. Cryptography

helps us in ensuring protection of data [8]. Cryptographic methods allow for safe data transmission and storage through networks, ensuring that only the intended receiver can understand it [8]. It is concerned with safeguarding data from unauthorized access [8]. Much of the time, shoulder side attacks will see our passwords. To address the difficulty of accessing the account in public locations, the suggested solution is to create a smart way to authenticate the user's bank account using a graphical password and inserting an indirect pin into the framework. The advantages of the Graphical Password Scheme are easy and greater security [10]. Image processing is done using cued click point. To confirm authentication, the user will click a specific area of the picture [10]. A sequence of images will be shown based on the previous image click [10]. According to a psychological analysis, people are more likely to recall a visual picture than a collection of textual characters. Our proposed system can significantly improve the security of the graphical password.

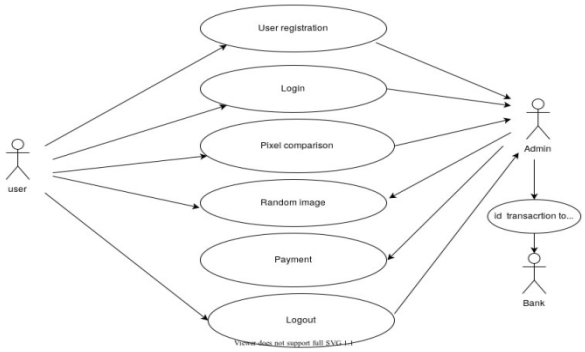

Fig 4: UML Diagram

2. Proposed System:

In this proposed system each and every item that are been brought by the customers are first clustered. The confidence of sellers and transactions is a critical problem in e-commerce and e-service environments. This approach is divided into two phases to evaluate an accurate recommendation for a client: collaborative filtering and clustering [11].For a more effective and faster product search, a clustering technique was used [11]. After selecting the items clustering takes place. Recommendation plays a major role in this project. Recommendation helps to recommend similar items that have been clustered. For example, if you are planning to buy a mobile phone, it recommends phone cover, headphone and similar items that are related with mobile phone. Once when the items are selected with the help of clustering and recommendation, it moves to the next step that is payment gateway. Payment gateway is done with the help of using image processing. Image processing is a part of graphical passwords. It consists of two images and cued click point. Cued click points acts as a password for the payment gateway. A secured way for banking transaction for online shopping is been initiated in this paper. We have used three algorithms they are Clustering; Item based Recommendation and Cued click point. Clustering is used to divide the data point into multiple groups with same data points. The multi-level association rules mining algorithm is currently the subject of numerous studies. It entails mining association laws both at the same level and at different levels [17]. The K-Means clustering algorithm is used in this article. The K-means algorithm has been the most widely used partitioned clustering algorithm for a long time. [20]. Item based recommendation is used to recommend based on the user's choice. The item based collaborative filtering is the most successful approaches used by the recommendation systems [21]. Cued click point is used in the payment gateway for secure bank transaction.

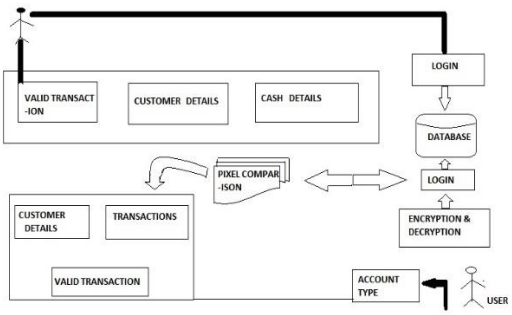

Fig 5: System Architecture

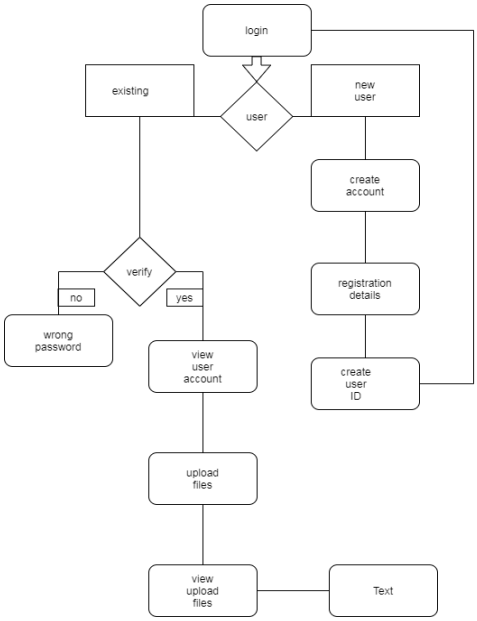

Fig6: Working Process

CLUSTERING(K-MEANS) &ITEMBASED RECOMMENDATION:

1 begin
2 for i=1....n
3 do find closest center fk ∈ S to instance pi
4 determine pi -> Sk
5 update step:for i = 1.....k
6 do set s,<- center of mass of all points
7 do sort s in alphabetic order
8 For each sensitive itemset
9 if s corresponds sensitive itemset
10 compute transaction s is added to inverted index list
11 For each transaction s in x
12 initialize labels to each group and select item with victim item
13 While N_iteration>0
14 Remove victim items from sensitive transactions
15 End

CUED CLICK POINT:

Begin
If X is not in database
register m, n, x
else break;
(image1.jpg) is displayed
Step 2: ax, ay and fx, fy is calculated in 1st image
user click point -> x1,y1
radius=8.5;
Compute ID for tolerance square for first image
for(k=2:k<=15)
x(k)<-(2*radius)*n1+fx1;
n1←n1+1;
for(l=2:l<=20)
y1(l)←(2*radius)*n2+fy1;
n2←n2+1;
t←y1(i)+1;
end
g←x1(j)+1;
end
Step 3: Shows next image.
For (k=1:k<=12)

break;
end
p2←imread('image2.jpg');
display(image2);
Step 4: ax, by, fx, fy is calculated in second image
Step 5: Repeat steps2for 2nd images to continue with payment gateway.
Step6:Calculatehash(fx1,fy1,mx1,ny1.....fx2,fy2,mx2,ny2)
Idgrid←[fx1; fy1; fx2; fy2];
Double hash←[fx1, fy1, ax1, ay1, fx2, fy2, ax2, ay2];
calculate CRC (hash)
Step 7: Encryption for 2 images
Step 8: Encrypted images,(fx1, fy1, fx2, fy2) CRC hash are saved in database.
End

3. Results and Discussion:

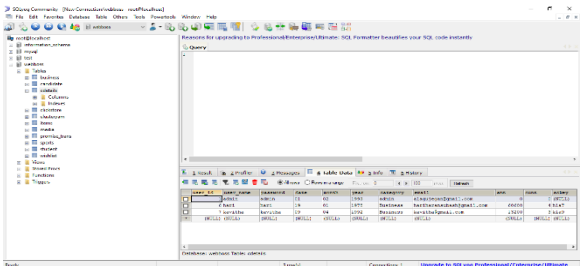

Fig 7: Credential Details

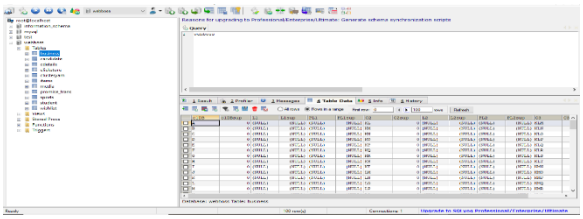

Fig 8: Clustering

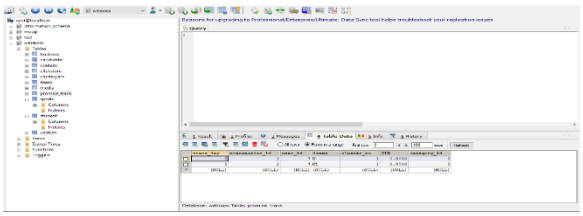

Fig 9: Promise Transaction

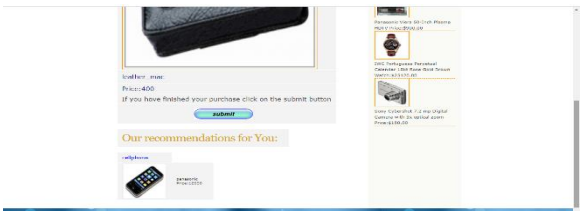

Fig 10: Recommendation

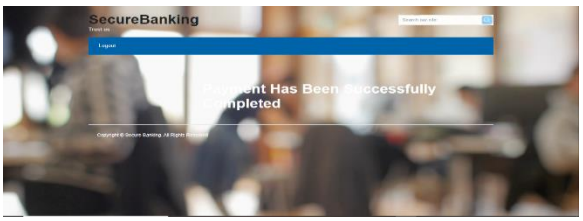

Fig 11: Final Output

The screenshot of the credential details, promise transaction, the items that are clustered, recommendations and the final output are upended.

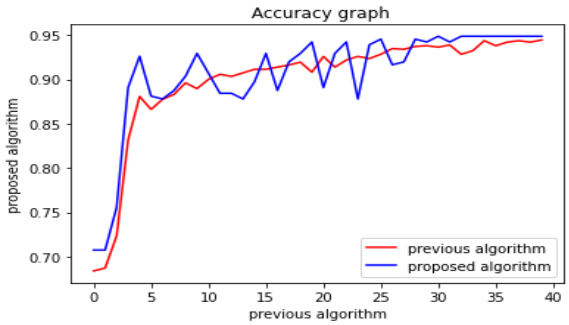

Fig 12: Accuracy Graph

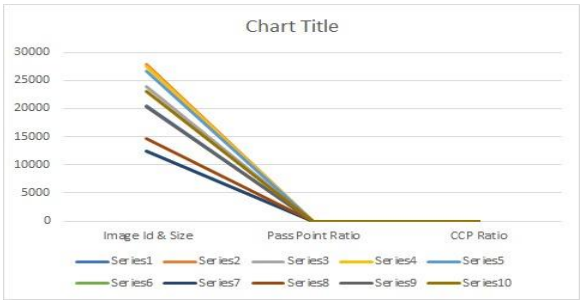

Fig 13: CCP Accuracy

The proposed algorithm is compared to the previous algorithm in the above graph, and it is plotted accordingly. Among these results the high rate clustering values are taken into the account.

4. Conclusion

This project concludes that a different graphical password approach has taken place. This is a secured way for payment gateway where hacking or phishing attack doesn't take place. This also reduces noise recommendation and multilevel clustering. It makes sure that there is a safe and a secure way for bank transaction during online shopping

References

1. A.K. Jain, M.N. Murty and P.J. Flynn. Data Clustering Algorithms year 2001
2. A.S.Gokhale and V.S.Waghmare. The Shoulder Surfing Resistant Graphical Password Authentication Technique. year 2017
3. Ahmed qasim, Nida asmat, Hafiz syed. Conundrum-Pass: A new pass graphical password approach. Year:2019
4. Ala Balti, Farhat Fnaiech ,HabibHamam and SofienneSrihi. Banking Security System Based on SVD Fingerprints and Cryptography Year:2018
5. Almuhammadi, S., &Amro, A. (2017). Double-Hashing Operation Mode for Encryption. year 2017.
6. Badrul Sarwar, George Karypis, Joseph Konstan, and John Riedl Item-Based Collaborative Filtering Recommendation Algorithms year 2013
7. Bhatia, S. (2014). New improved technique for initial cluster centers of K means clustering using Genetic Algorithm. International Conference for Convergence for Technology-2014.
8. Bonny B Raj, V.Ceronmani Sharmila, "An Survey on DNA Based Cryptography", International Conference on Emerging Trends and Innovations in Engineering and Technological Research, 2018.
9. Comparisons between data clustering algorithms.Osama Abu Abbas,International Arab Journal of Information Technology (IAJIT) 5 (3), 2008
10. Divya Gupta SachinKaja,Graphical, Password Scheme usingPersuasive Cued Click Points. Year 2017
11. Gowri, R., Kumar, A., Arvind M. J., &JericRajan K. (2015). C2F: A Clustering Based Collaborative Filtering approach for recommending product to ecommerce user. 2015
12. Jie, F., Ping, P., Zeyu, G., &Yingchi, M. (2019). A Meaningful Visually Secure Image Encryption Scheme.year 2019.
13. Kavitha Esther Rajakumari, "Towards A Novel Conceptual Framework for Analyzing Code Clones to Assist in Software Development and Software Reuse",2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), 13-15 May 2020.

14. Li Sa Liaoning Shiyou University Collaborative filtering recommendation algorithm based on cloud model clustering of multi-indicators item evaluation year 2011.
15. MuhammetBaykara, ZahitZiyaGürel Detection of phishing attacks. Year: 2018
16. V, T., Patel, S., & S, S. (2020). Secured Data Transmission through Dual Domain Reversible Data Hiding and Encryption in Images. Year 2020.
17. Qinglan, H., &Longzhen, D. (2013). Multi-level Association Rule Mining Based on Clustering Partition.year 2013
18. M. Shanmuganathan ,R. Sudha. An Improved Graphical Authentication System to Resist the Shoulder Surfing Year:2017
19. Ms. Shilpa. L. Dhapade Implementation of Persuasive Cued Click-Points Techniques for Folder Security using Secure Hash Algorithm year 2013
20. Thein, H. T. T., & Tun, K. M. M. (2015). Evaluation of differential evolution and K-means algorithms on medical diagnosis. year 2015
21. Zhang, H., Ganchev, I., Nikolov, N. S., &O'Droma, M. (2016). A trust-enriched approach for item-based collaborative filtering recommendationsyear 2016.