Journal of Harbin Engineering University
ISSN: 1006-7043
Vol 44 No. 8
August 2023

Secure Cloud Communication for Banking Sector

[1] Sukesh Bhardwaj, [2] Ashish Bhardwaj
[1] Assistant Professor, [2] Sr. Manager
[1] International Institute of Health Management Research [2] DMI LLC

Abstract: Banking and other financial transactions are growing all over the world. With the advancement of technology and growth in the cloud platforms in the banking industry, information sharing in the organization is becoming easier, but with that more vulnerable to attacks. Proper user authentication is a major issue in such platforms. In this paper, we proposed a concept in which the image is segmented and organized in grid to form the pattern and the image click count is clubbed with the pattern, the way of formation of password is easy and together with that the pattern form is quite strong to overcome the various types of attacks like brute force, password guessing etc. Similarly, the concept of the combined key is also the unique concept which we have applied to act as the session key, which is used in the process of the sharing of the secure information between the two authorized users. Together with the session key, the use of the image hash in the transaction will make the authentication stronger. The pattern generated is tested over the various tools to test the strength and the results obtained are quite impressive.
Index Terms– Image Password, Grid Organization, SHA-512, Cyber Security, User-Authentication

Introduction

The banking sector is one of the most growing sectors of the world. To share information across the branches of a particular bank, cloud platforms are often used. This enables us for online rapid information sharing. Seeing the other side of this, with the introduction of the cloud platforms in the banking sectors, these sectors are also vulnerable for the various types of attacks, which are related to the user authentications. [1] The simplest way to protest the user identity is to use the password; here we have two types of the password which are generally used, a) Text Passwords and b) Graphical Passwords. [1]

Text passwords are simple alpha-numeric patterns which are used to protect the user identity. Graphical passwords are more interactive and make use of some graphical concepts for the formation of the passwords. In the banking sectors, the crucial cliental data is required to be protected from the unauthorized access. So, the aim of this paper is device the concept which is not cumbersome for the user to remember the credentials required for the authentication purpose and with that also taken in consideration that, the method, which is adopted, will be able to overcome the attacks like dictionary attack, brute-force attack, and many more similar types of attacks. [1]

Cyber Security Statistics for Financial Services [2]

- 67% of financial organizations reported a significant rise in cyber-attacks during the past 12 months.
- 26% encountered a destructive attack.
- 79% of CISOs stated that the threat actors are deploying severe sophisticated attacks.
- In last one year 21% suffered a watering-hole attack.
- 32% of institutions encountered island hopping, leveraging one compromised organization to enter another.
- Malware attacks are roughly tallying at the 25% that hit banking system and other types of financial sector, it is more prominent than any other contributing sector.
- It has been observed that Credit cards are easily compromised and there is a significant rise approx. 212% every year, Credential leaks are also contributing a sharp rise of 129%, and 102% increase in malicious apps.
- Wire transfer fraud increased by 47%.
- Home equity loan fraud increased by 31%.
- Cybercriminals have become more sophisticated and leveraging highly targeted social engineering attacks which roughly stands at 79% reported by business entities.
- 32% reported that they are experiencing counter incident response.

- 21% reported they experienced C2 on a sleep cycle.
- As many as 70% institutions expressed their reason of worries about financially motivated attackers.
- 30% from the domain industry reported they are most concerned with nation-state activity.
- Types of Sources and Global attack types:
  - Web attacks – 46%
  - Service-specific attacks – 28%
  - DoS/DDoS 8%
- 69% of CISOs are planning to increase cyber security spending by 10% or more in 2019 and 47% emphasized their organizations that are operating threat hunt teams out of which 32% specify that they carried out on a monthly basis.
- 70% of cybercrimes targeting surveyed financial institutions that involves lateral movement.

Literature Survey

Pathik Nandi, et. al 2022 asserts the concept of user registration using color authentication using the username and password where password is the combination of characters and numbers. Further the password created at the time of registration using the color will be cross checked with Color image-based authentication at the time of login. [1]

Abhijith S, et. al 2021 focuses on the concept of graphical authentication mechanisms using passwords and provides the most suitable approach to logins that is easier than remembering and creating simple passwords. Users can log in by tapping the appropriate dot or making the appropriate gesture on a pre-selected image [2]

Juraj Zelenaya, et. al 2019 proposed the concept to access the data which utilizes the authentication mechanism of username and password and the encryption of data which required encryption key to decrypt the stored data and is only accessible for the authorized users which are defined with multiple-level access control. [3]

H. Hui, et. al 2018 authors proposed a complex model of cloud security in BPO organizations, named the model as Business Process Outsourcing Cloud Computing Platform (BPO-CCP), and suggested that this similar platform could be applied to all banks. and the insurance industry. This BPO-CCP model addresses cloud data security, user access control, user-based authentication and authorization, and cloud computing auditing. [4]

A. Mahalle, et.al 2018 draws attention on the banking and related financial services, developing data and data-related applications in-house to dominate the market has become standard practice. As such, financial institutions store different types of customer data, and this type of data is generally critical. Data breaches can result in huge losses for financial institutions. This white paper discusses various aspects of cloud computing related to data protection and system security in the banking and financial services industry. [5]

S. P. Tripathi, et. al 2017 proposed to secure platform for the online banking using the concept of the fingerprint and password which they used in association with the fingerprints are the textual passwords. For the registration of the user, they require account credentials, with the fingerprint and the password which is given the user registering.[6]

Research Methodology

The research papers we considered in our study are focused on the selection of password at the time of user's registration, and it is the general tendency of the user to adopt the password, which is in general have relevance to their family members, items they like, any actor name, date of birth and so on. For the research comparison, we have assumed that the ideal password which the user can choose can't be more than 10 characters and we have taken in point that here user has to remember that. So, such password cannot be come under the category of strong password, so vulnerable to brute-force [6] and password guessing attacks.

Secondly, if we go for very long passwords then directly remembering them is quite difficult, so we require adopting some creative process for the formation of the password pattern.

Proposed Concept

The proposed model of the security approach for the banking service contains four segments, a)

Registration of User, b) Login of User, c) Data Sending, and d) Data Receiving.

4.1 Registration of User

In this section, the concept of the registration process of the bank personals for accessing the system is explained. This module contains the following steps,

Step 1: Accept the username and Email ID from the user.

Step 2: Select the Image from the available list of pictures.

Step 3: Click on the Image to increment the image click count.

Step 4: Proceed to the Grid Formation

Step 5: Select the Number of Segments in which image to be divided.

Step 6: Arrange the image in the Grid, for this click on the image segment which you want to move and click on the empty block on grid to move that segment, in that block.

Step 7: The pattern is form using the concept that is imagecount_blockpositionmoved_postiontowhich moved_ASCIIvalueblockposition_fizesize.

Step 8: Generate SHA-512 Hash for Image Selected.

Step 9: If user record exists then:

Print "Record of User exists"

Else:

Print "Store User Information in Database"

[End of If structure]

Step 10: End

4.2 Login Process

In this section, the concept of the login process of the bank personals for accessing the system is explained. This module contains the following steps,

Step 1: Accept the username and Email ID from the user.

Step 2: Select the Image from the available list of pictures.

Step 3: Click on the Image to increment the image click count.

Step 4: If Details Correct Then Move to Step 5 Else Goto Step 11.

Step 5: Proceed to the Grid Formation

Step 6: Select the Number of Segments in which image to be divided.

Step 7: Arrange the image in the Grid, for this click on the image segment which you want to move and click on the empty block on grid to move that segment, in that block.

Step 8: The pattern is form using the concept that is imagecount_blockpositionmoved_postion to whichmoved_ASCIIvalueblockposition_fizesize.

Step 9: Generate SHA-512 Hash for Image Selected.

Step 10: If User Record Validated then

a. Login Successful

b. Move to User Section

Else:

Print "Details not Matched."

[End of if Structure]

Step 11: End

4.3 Sending Secure Information

In this section, the concept of sending the secure data by bank personals in the user section is explained. This module contains the following steps,

Step 1: After the Sender Login, the Sending Information option is selected.

Step 2: Details of User Login are accessed, and SHA-512 hash of sender image is accessed.

Step 3: Select the Receiver Name.

Step 4: Details of Receiver is accessed internally, and SHA-512 hash of receiver image is accessed.

Step 5: Combined Key using 32 characters of Server and Receiver hash is generated.

Step 6: Select Image for Transaction and generate SHA-512 hash for image.

Step 7: Enter the Message for Receiver.

Step 8: Generate SHA-512 for the message.

Step 9: Store the Details for Information Sent.

Step 10: Generate a unique number used as Transaction Key.

Step 11: End.

4.4 Receiving Secure Information

In this section, the concept of receiving the secure data by bank personals in the user section is explained. This module contains the following steps,

Step 1: After Receiver Login, Receiving Information option is selected.
Step 2: Details of User Login are accessed, and SHA-512 hash of sender image is accessed.
Step 3: Enter the Transaction Key and Combined Key.
Step 4: check the details in database with the user login.
Step 5: If details correct then: Goto Step 6 Else: Goto 11
Step 6: Fetch the message for User.
Step 7: Access the SHA hash for Message.
Step 8: Verify the Hash code for Message.
Step 9: If verified then Goto Step 10 Else: Goto 11
Step 10: Show Message for Receiver
Step 11: End

Implementation

The implementation for secure information sharing in banking environment is done in VS 2010 and SQL Express 2008 and the GUI forms involved in the implementation is explained in this section.

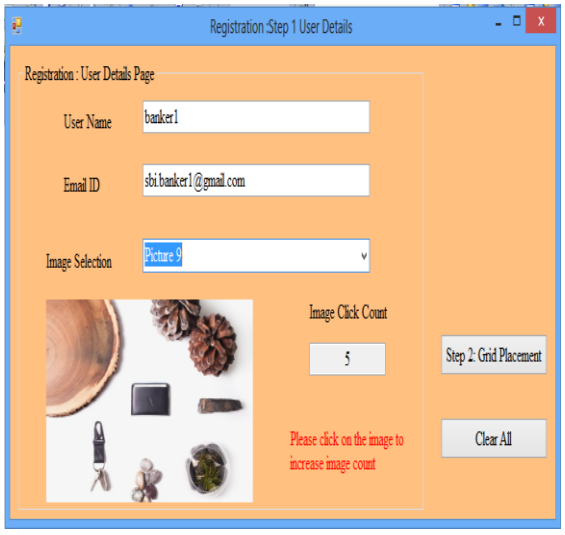

Fig 1. Sender Registration

In fig 1, the first form of the user registration process is explained, in this the details of users like username, email id is input and after that the user will select the image and click on the image to increment the image click count. After that, click on the Grid Placement button.

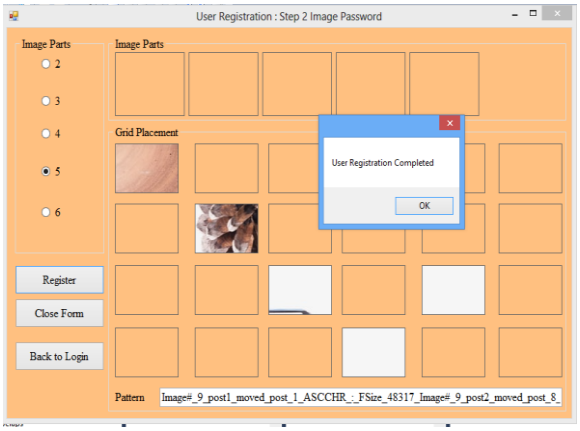

Fig 2 Grid Placement

In Fig 2 the Grid Placement form of the user registration is explained, in which the first process is to select the number of segments in which the image is divided. Click on the segment of image which we want to move and then click on the grid block, the segment will then move to that grid block. The generated pattern is shown in the pattern textbox.

Similar process is adopted for the login process , which contains two step validation in which first the user details are matched with the image selected and cout over the images . After that validation the next is to validate the grid movement after that the user section will get displayed as shown in Fig 3. This process is adopted for the sender as well as receiver login.

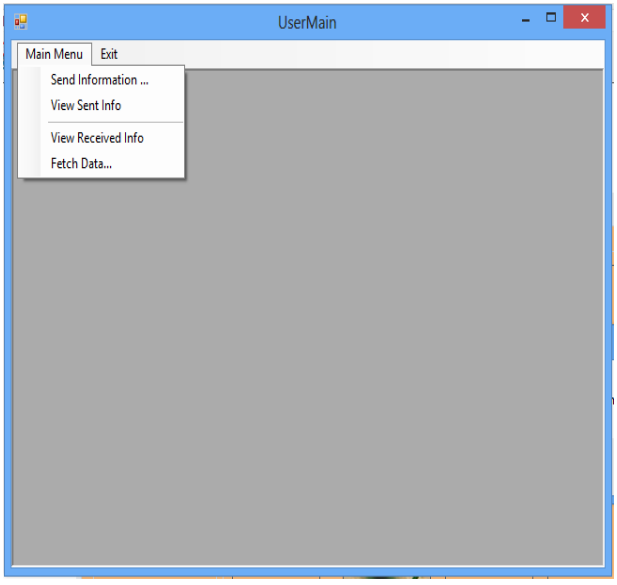

Fig 3 Banker User Section

For the simulation first the sever will login and send the information , for this seelect the Main Menu and select the “Send Information” option.

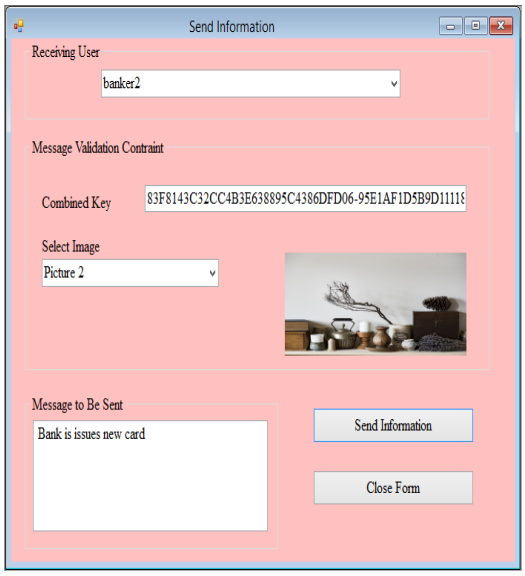

Fig 4 Sending Information

In Fig 4 , sending information to other banker form is shown in which we have to select the receiver. Then the combined key is generated using the image SHA hash of the sender and receiver. Then, select the image for the transaction and type the message. Then , when the user click on “Send Information” and details for transaction will ger stored and the transaction key will get generated.
After the receiver login , the user will select the Receivintg Information will get selectedand the form is shown in Fig 5.

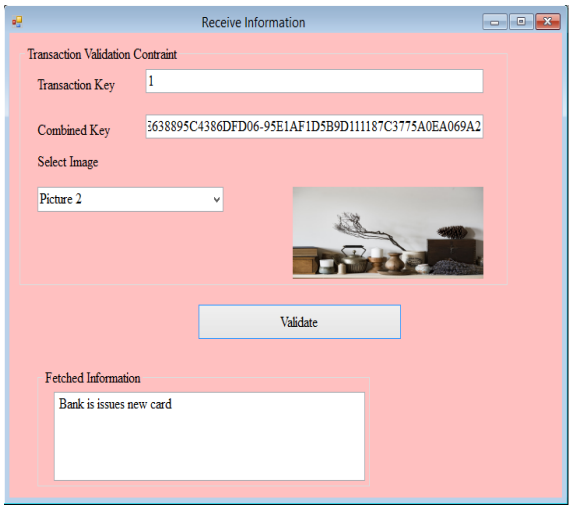

Fig 5 Receving Information

In Fig 5, transaction key and combined key is entered by the user , also select the transaction image and after all the details are verified in the database , message will get fetched from the database and show to the receiver.

Result Analysis

In the base paper, the simple text password are taken, as they are taken as per the user capability remember it , so we have taken it of maximum length 10
Sample password for base concept: {`x~Nt6)Mu
In the result analysis we have taken two cases, first for the length 6 and second for max length 10.
And, in the proposed concept for comparison with base 4 and 5 segments are taken.

6.1 Base Password (6 Characters) and Proposed Work (4 Segments)

For the comparison of the password patterns strength, we have evaluated the entropy of these password patterns using the various online and offline tools.

Base Password (6 characters): \E7$e+
Proposed Work (4 Segments):
Image#_6_post1_moved_post_1_ASCCHR_:
_FSize_64627_Image#_6_post2_moved_post_8_ASCCHR_A_FSize_64627_Image#_6_post2_moved_post_15_ASCCHR_H_FSize_64627_Image#_6_post4_moved_post_22_ASCCHR_O_FSize_64627_

6.1.1 ZXCVBN Test

This tool is based on the ZXCVBN code developed in Java for the strong password generation and validation.

Table 2
Strength Test using ZXCBN Test

	Base Approach	Proposed Approach
Entropy Measure	19	639

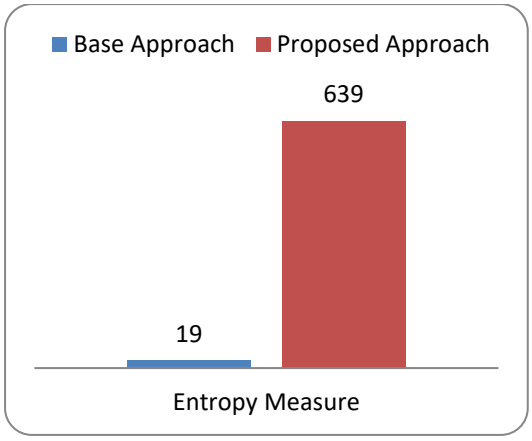

Fig 6 ZXCVBN Test Case I

The more entropy result shows the more strength in the proposed work password pattern.

6.1.2 Rumkin Test

This tool is based on the Rumkin tool calculates the password strength in the entropy bits.

Table 3
Strength Test using Rumkin Test

	Base Approach	Proposed Approach
Entropy Measure	25.6	977.5

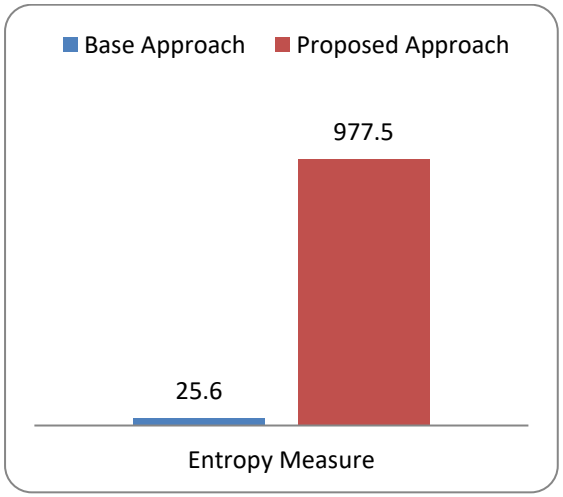

Fig 7 Rumkin Test Case I

6.1.3 Cryptool2

This tool is based on the cryptool2 tool calculates the password strength in the entropy bits, bit strength and overall score.

Table 4
Strength Test using Cryptool2.

	Base Approach	Proposed Approach
Entropy Measure	2.585	4.41

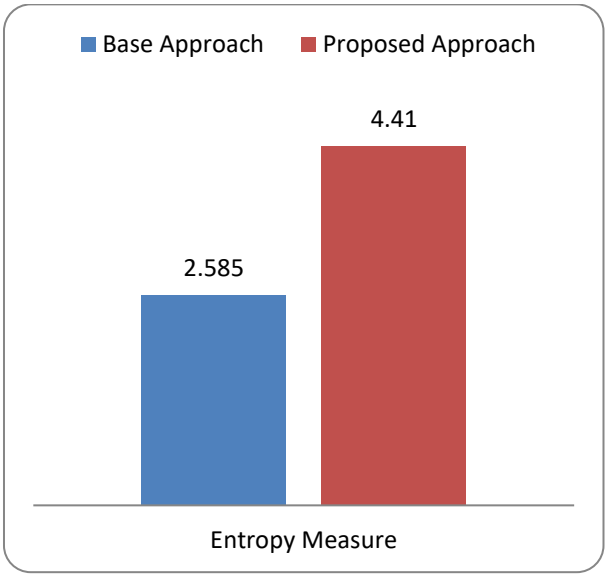

Fig 8 Cryptool2 Test Case I

6.2 Base Password (10 Characters) and Proposed Work (5 Segments)

For the comparison of the password patterns strength, we have evaluated the entropy of these password pattern using the various online and offline tools.

Base Password (6 characters): rv2fJD5(}%
Proposed Work (4 Segments):
Image#_9_post1_moved_post_1_ASCCHR_:
_FSize_48317_Image#_9_post2_moved_post_8_ASCCHR_A_FSize_48317_Image#_9_post3_moved_post_15_ASCCHR_H_FSize_48317_Image#_9_post4_moved_post_22_ASCCHR_O_FSize_48317_Image#_9_post5_moved_post_17_ASCCHR_J_FSize_48317_

6.2.1 ZXCVBN Test

This tool is based on the ZXCVBN code developed in Java for the strong password generation and validation.

Table 5
Strength Test using ZXCBN Test

	Base Approach	Proposed Approach
Entropy Measure	33	803

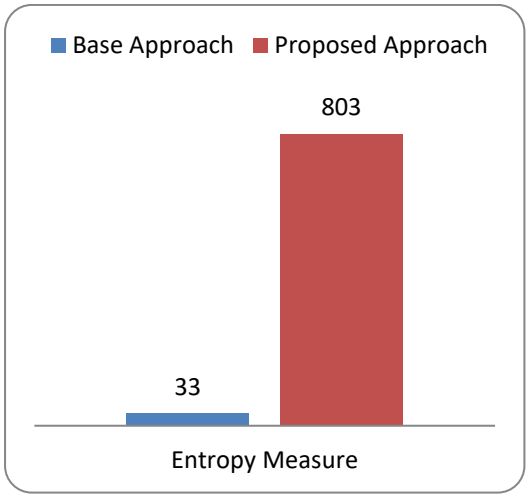

Fig 9 ZXCVBN Test Case II

The more entropy result shows the more strength in the proposed work password pattern.

6.2.2 Rumkin Test

This tool is based on the Rumkin tool that calculates the password strength in the entropy bits.

Table 6
Strength Test using Rumkin Test

	Base Approach	Proposed Approach
Entropy Measure	47	1226.8

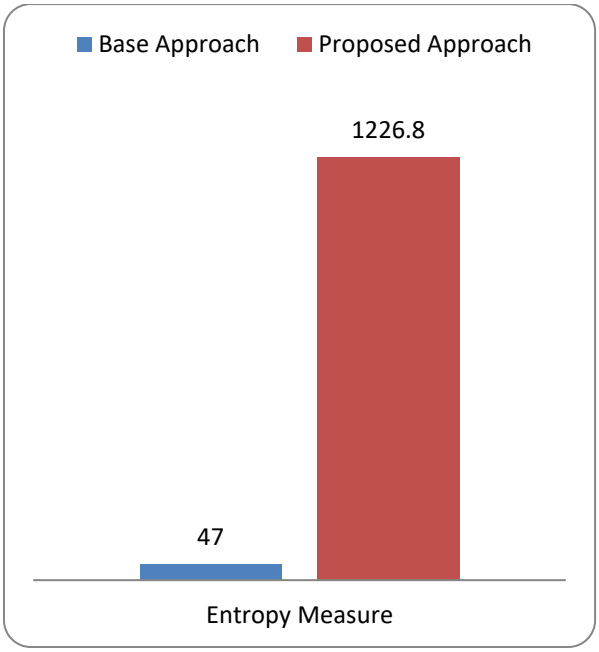

Fig 10 Rumkin Test Case II

6.3.3 Cryptool2

This tool is based on the cryptool2 tool calculate the password strength in the entropy bits, bit strength and overall score

Table 7
Strength Test using Cryptool2.

	Base Approach	Proposed Approach
Entropy Measure	3.322	4.508

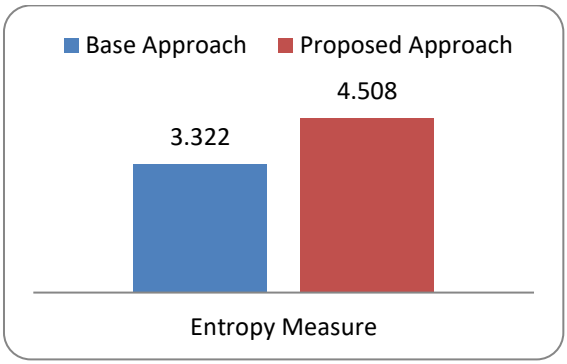

Fig 11 Cryptool2 Test Case II

Conclusion

Secure communication and proper authentication concept is the primary requirement of any financial and other type of organizations. In this paper, with the usage of the grid concept of the pattern password formation is not only the easy concept of memorizing the password but also the pattern which resulted is also strong and overcome the various type of attacks. Together with that the pattern form is quite strong to overcome the various types of attacks like brute force, password guessing etc. Similarly, the concept of the combined key is also the unique concept which we have applied to act as the session key, which is used in the process of the sharing of the secure information between the two authorized users. Together with the session key, the use of the image hash in the transaction will make the authentication stronger. The pattern strength is being justified in the paper by checking the entropy output by making use of the various offline and online tools.

References

[1] Pathik Nandi & Dr. Preeti Savant, Graphical Password Authentication System, 10 INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY 1759–1765 (2022)

[2] Sreelekshmi K U et al., Web based Graphical Password Authentication System, 9 INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (2021), www.ijert.org (last visited Dec 9, 2022)

[3] M. Singh, K. S. Tanwar and V. M. Srivastava, "Cloud Computing Adoption Challenges in the Banking Industry," in IEEE Int Conf. Adv. Big Data, Comp. Data Comm. Sys. (icABCD), Aug 2018, pp. 1-5.

[4] Cimpanu, C., 2020. Financial Sector Is Seeing More Credential Stuffing Than DDOS Attacks | Zdnet. [online] ZDNet. Available at: <https://www.zdnet.com/article/financial-sector-has-been-seeing-more-credential-stuffing-than-ddos-attacks-in-recent-years/>.

[5] S. P. Tripathi, A. Kumar and R. Astya, “Study on secured framework for cloud based online banking," in Int. Conf. on Comp., Comm. and Auto. (ICCCA), May 2017, pp. 853-858.

[6] H. Hui, D. McLernon and A. Zaidi, "Design of the Security Mechanism for a BPO Cloud Computing Platform," in IEEE Int. Conf. Soft. Eng. Serv. Sci. (ICSESS), Nov 2018, pp. 1092-1095.

A. Mahalle, J. Yong, X. Tao and J. Shen, "Data Privacy and System Security for Banking and Financial Services Industry based on Cloud Computing Infrastructure," in IEEE Int. Conf. Comp. Supp. Coop. Work Desig. ((CSCWD)), May 2018, pp. 407-413.

[7] S. Kurita, K. Komoriya and R. Uda, "Privacy Protection on Transfer System of Automated Teller Machine from Brute Force Attack," in IEEE Int. Conf. Adv. Inf. Net. App. Work., Mar 2012, pp. 72-77.

[8] S. Zhang, J. Zeng and Z. Zhang, "Password guessing time based on guessing entropy and long-tailed password distribution in the large-scale password dataset," in IEEE Int. Conf. Anti-counter., Sec. Ident. (ASID), Oct 2017, pp. 6-10.

[9] R. Buyya C.S. Yeo S. Venugopal J. Broberg and I. Brandic "Cloud computing and emerging IT platforms: vision hype and reality for delivering computing as the 5th Utility" , J. Fut. Gen. Comp. Sys. ,vol. 25 no. 6,pp. 599-616 2009.

[10] S. H. Abbdal, H. Jin, A. A. Yassin, Z. A. Abduljabbar, M. A. Hussain, Z. A. Hussien and D. Zou, “An Efficient Public Verifiability and Data Integrity Using Multiple TPAs in Cloud Data Storage,” in IEEE 2nd Int. Conf. Big Data Sec. Cloud (BigDataSecurity), IEEE Int. Conf. High Perf. Smart Comput. (HPSC), and IEEE Int. Conf. Intellig. Data Sec. (IDS), April 2016, pp. 412-417.

[11] S. Hiremath and S. R. Kunte, “Ensuring Cloud Data Security using Public Auditing with Privacy Preserving,” in IEEE 3rd Int. Conf. Comm. Electron. Sys. (ICCES), Oct. 2018, pp. 1100-1104.

[12] S. Patii and N. Rai, “An effectual information probity with two TPAS in cloud storage system,” in IEEE 3rd Int. Conf. Sci. Technol. Engineer. Manage. (ICONSTEM), March 2017, pp. 432-434.

[13] A. K. Udagatti and N. R. Sunitha, “Fault tolerant public auditing system in cloud environment,” in IEEE 2nd Int. Conf. Appl. Theoret. Comput. Comm. Technol. (iCATccT), July 2016, pp. 359-362.

[14] J. Raja and M. Ramakrishnan, “Public key based third party auditing system using random masking and bilinear total signature for privacy in public cloud environment,” in IEEE Int. Conf. Intellig. Comput. Cont. Sys. (ICICCS), June 2017, pp. 1200-1205.

[15] A. Wójtowicz and K. Joachimiak, “Model for adaptable context-based biometric authentication for mobile devices,” Per. Ubiquit. Comput., vol. 20, pp. 195-207, 2016.

[16] W. C. Garrison, A. Shull, S. Myers and A. J. Lee, "On the Practicality of Cryptographically Enforcing Dynamic Access Control Policies in the Cloud," IEEE Sym. Sec. Priv., pp. 819-838,2016.

[17] Y. Wang, Y. Ma, K. Xiang, Z. Liu and M. Li, “A Role-Based Access Control System Using Attribute-Based Encryption,” in IEEE Int. Conf. Big Data Artific. Intellig. (BDAI), June 2018, pp. 128-133.