ISSN No:-2456-2165

Secure Online Banking using Cued Click Point Graphical Password Algorithm

[1]SOWMIYA M., [2]ACKSHAYA R ., [3]INFANT MACREEN M., [4]NIVETHA T
[1]Assistant Professor, Dept. of Computer Science and Engineering
Meenakshi Sundararajan Engineering College Chennai, India

Abstract:- This paper proposes a system to securely login to a console and transfer money using a graphical password. The proposed framework in this project includes extra pixel distinguishing proof framework, as well as proficient feasible client verification using numerous cryptographic basics, such as encryption. Cued Click Point graphical password algorithm is used to enhance the security and reduce the risk of data leakage and hacks. Customers only have to submit a one-time username and confirmation code and select points in image, therefore this proposed approach is very simple to understand and use.

Keywords:- *Image Processing, Graphical Password, Cued Click Point, Secure Login.*

I. INTRODUCTION

Internet Banking is a set of services provided by a group of sorted out banks. Customers of the bank can access their assets via the internet from any location or working environment. The most significant issue in Internet Banking is the client's legitimacy. It is impossible to accept the confidentiality of information on the web due to the inescapable hacking of databases on the internet. Phishing is a method of online information deception that aims to get sensitive data from clients, such as electronic cash passwords and information from payment exchangers.

System shows the username, the mystery phrase, and the carefully selected picture pixels in this system. In the event that wrong point is choosen, the motive behind the photo pixels implies that the photo will be altered in a deliberate manner. Using these cryptographic technologies, the route for customer-driven access control that reduces the risk of numerous ambushes will be set. Its design makes it resistant to a variety of mysterious word-related attacks, such as bear surfing ambushes and direct observation attacks.

The client is prevented from using static usernames and passwords, which can be viewed via warm imaging or identified using a mechanical vibration test.

The content of this paper is divided into five sections. In the first section, the background is introduced along with the motivation and purpose of this paper. In the second section, the technology and documents that are related to this paper are mentioned. In the third section,the structure of the system built in this paper is explained. In the fourth section, the construction of the system is presented in detail. In the last section, conclusions are made along with future enhancement possibilities.

II. RELATED WORKS

A. POSITION BASED KEY GENERATION:

The suggested methods are unique in that they generate random secret bits not only from the magnitudes of orthogonal frequency division multiplexing subchannels, as has been done in the past, but also from the indices/positions of the subchannels with the highest gains. As a result, the suggested algorithms provide new dimensions to improving overall key rates. The proposed algorithms' efficiency is measured in terms of key mismatch rate (KMR) and key generation rate (KGR). The proposed methods can improve the overall performance of physical layer key based algorithms by adding new dimensions for secret key creation, according to simulation results.

Effective algorithms for generating secret keys from wireless channels are described, where key bits are created not only by subcarrier amplitudes but also by subcarrier indices corresponding to the largest channel gains. In the first step, communicating nodes use random interleaves to turn the channel's associated frequency response into random order.

The key bits are generated by comparing the amplitudes of individual subcarriers to their mean, as well as by using a look-up table to find the indices/positions of good sub-channels in each subblock. The proposed unique dimensions for secret key generation improve total KGR without compromising overall performance.

B. ENCRYPTED NEGATIVE PASSWORD:

The received plain password from a client is first hashed using a cryptographic hash algorithm in ENP (e.g., SHA-256). After that, the hashed password is turned into a negative one. Finally, a symmetric-key algorithm (e.g., AES) is used to encrypt the negative password into an Encrypted Negative Password (abbreviated as ENP), and multi-iteration encryption could be used to boost security even more. Passwords from ENPs are difficult to crack due to the cryptographic hash function and symmetric encryption. Furthermore, for a given plain password, there are several equivalent ENPs, making precomputation attacks like lookup table assault and rainbow table attack impossible.

C. CHANNEL BASED MAPPING DIVERSITY:

In order to confuse an eavesdropper, the CBMD technique takes advantage of the wireless channel's intrinsic unpredictability as well as the numerous mappings possible for an M-ary phase shift keying (M-PSK) constellation. It is demonstrated that when the legitimate and eavesdropper channels are independent of one another, an eavesdropper with a symbol error rate (SER) of M1 M is induced.

ISSN No:-2456-2165

When the channels are correlated, however, optimal and sub-optimal techniques at the source and eavesdropper for their respective optimal performances are derived. Also developed is a closed-form equation for a lower-bound on the SER at the eavesdropper.

D. DOUBLE HASH STRING MATCHING:

The Boyer-Moore-Horspool, Rabin-Karp, and Raita algorithms are all used in this unique hybrid algorithm. They compare the rightmost characters, employ two distinct hash algorithms, and don't verify each character individually, leaving a very low chance of a false positive result if one exists.

When the pattern is quite long, the suggested algorithm performs particularly well since it skips character by character comparisons. Once the last character does not match, the double-hash jumps swiftly.

A rapid hash function just travels over the first half of the string or pattern to generate hash value 1 after the final character match, allowing it to swiftly decide whether or not there is a mismatch. The longer the pattern, the higher the overall search performance.

E. STEGANOGRAPHY AND DATA HIDING:

To make it easier for users to remember their passwords, the idea of Least Significant Bit based image steganography and data concealment approach is used to create an image-based authentication. By hiding the password in the cover image, the proposed solution also alleviates the stress of remembering all passwords for all accounts and prevents "Shoulder surfing." Although there are a growing number of new techniques to authenticate users, text-based passwords remain a popular and widely used method, the suggested strategy intends to improve existing authentication and address text-based authentication's limitations.

Random embedding, picture segmentation, and columnar transposition all contribute to the complexity of extracting the password from the cover image. Simultaneously, the use of one-time pad encryption offered an extra layer of security to the password storage. The password is maintained safe and secure in this manner.

III. SYSTEM ARCHITECTURE

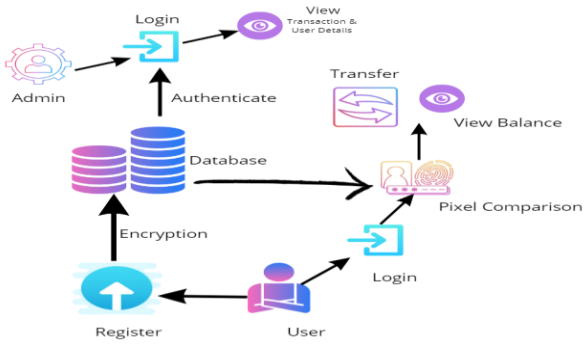

Fig. 1

System Architecture denotes a holistic solution built on logically related and consistent ideas, concepts, and attributes. The architecture contains features, traits, and characteristics that, to the greatest extent possible, satisfy the issue or opportunity described by a set of system requirements and life cycle ideas, and is implementable using technologies.

The system is divided into two phases: administrative and user. The transaction, customer information, and cash information can all be viewed by the administrator. In the user section, they begin by creating an individual bank account. User data will be encrypted for security, and before logging in, a blocking chain for pixel comparisons will be introduced. If the chosen pixel matches, the user is permitted to log in. Users can conduct transactions, and while transferring funds, an E-coin is produced at random based on the note, and the funds are placed into the account in the form of that e-coin key.

IV. SYSTEM IMPLEMENTATION

The front end of the system is built with HTML and CSS, while the backend SQL database is connected with a servlet. Aside from that, the proposed system uses java to write the programs and connections. The pixels are encrypted and stored as hash values using blockchain encryption while registering. The proposed system's architecture is basic and straightforward. The first step is to activate the database and connect to the local host using Netbeans. Once the program is started in the Netbeans console, the servlets are opened and the connection is established. When a user registers or makes a transaction, the information is immediately encrypted and stored in the database. The modules in the system, as well as their associated procedures, are listed below.

A. USER ACCOUNT CREATION:

Every last customer who visits the page initiates a transaction and uses this application. Validity is the assurance that a message, exchange, or other data transaction originated from the source claimed. Character verification is part of validness. Validity can be verified through confirmation. On the landing page, there are options for enrolling and logging in. For login, each and every client must register as a new client. For security reasons, the client must complete all prerequisites, including all delicate components and distinctive points of interest.

B. SECURED LOGIN:

Individual gadgets that employ various cryptographic natives, such as encryption, advanced mark, and pixel determination, are used in an effective and convenient client confirmation scheme. The method benefits from the widespread use of calculating and other smart convenient devices that enable clients to carry out a secure verification procedure. It maintains static username and secret key tables in order to distinguish and verify the authenticity of login clients.

During registration, the user must choose precise spots or locations on a picture using the cued click point technique. To log into the system, the user must click on the identical

ISSN No:-2456-2165

locations that they chose during registration. This will improve security by reducing the number of intruder attacks.

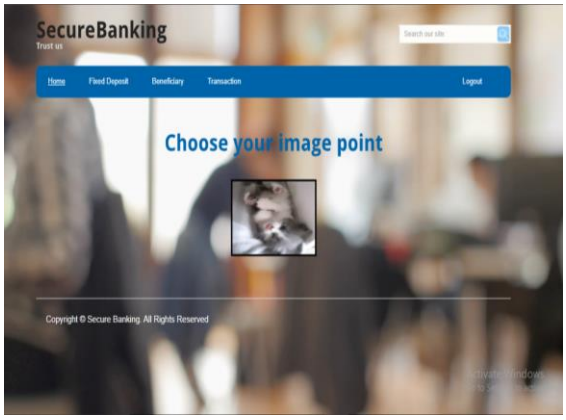

Fig. 2

C. CUED CLICK POINT:

The Cued Click-Point approach is simple to use and provides excellent security through the use of the hotspot technique. By utilizing the user's capacity to recognise images as well as the memory trigger connected with viewing a new image. Cued Click Point is a more secure way of graphical authentication than the preceding approaches. CCP makes it more difficult for attackers by requiring them to first obtain image sets for each user and then analyze each image for hotspots. In terms of convenience, security, and a memorable authentication mechanism, the Cued Click-Points approach outperforms existing password schemes.

D. CREDIT AMOUNT:

This grants the individual model initial monetary standards in exchange for Admin's permission to access them. After logging in with administrator validation subtle elements, the Admin can access all procedures except the E-coin programme. The underlying cash is used as an incentive for each client by that administrator. When a customer keeps money in their account, it means that the administrator will create a special incentive for each money note. That one-of-a-kind esteem warehouses are based on the rupee note number and the amount of the rupee note, such as two thousand, five hundred, or one hundred rupees. After that, put money in the client's account. Administrators have the ability to inspect each and every client's exchange points of interest, as well as the id of those monetary standards.

E. ENCRYPTED TRANSACTION:

As it were, the client initiated each and every transaction. Clients must input the correct outsider record number and payee name. After that, the client must choose how much money will be sent to others and how many monetary standards they will send from a variety of options such as Thousand Currencies, Five Hundred Currencies, and Hundred Currencies.

The currencies id will switch from one client table to the payee account table. As a result, they can easily identify the currency and whose client possesses certain monetary types. So now that dark money can be identified and easily reduce the dark money population.

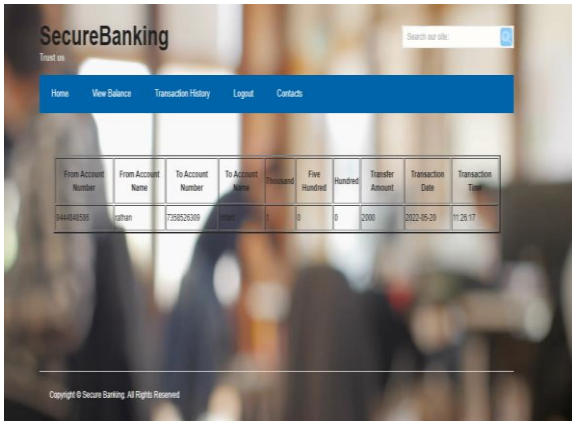

Fig. 3

V. CONCLUSION AND FUTURE WORK

Customers only have to submit a one-time username and confirmation code, therefore the proposed method is very simple to understand and use. Then, if the pixel of the picture is right, input it, taking into account that pixels change reliably for the most part. The client is directly prevented from utilizing static usernames and passwords, which can be spotted through thermal imaging or recognised by a mechanical vibration study.

To validate authentication, the user will click on a certain section of the image. The persuasion cued click points will display a series of graphics, increasing security by placing a burden on attackers. A succession of images will be displayed dependent on the previous image click.

Other NDB generation techniques will be investigated and added to the ENP in the future to boost password security even more. The password authentication framework will also include other techniques such as multi–factor authentication and challenge–response authentication.

REFERENCES

[1.] Alhothaily, A. Alrawais, X. Cheng, and R. Bie. A novel verification method for payment card systems. Personal and Ubiquitous Computing, 19(7):1145–1156, 2015.

[2.] Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang. The tangled web of password reuse. In Symposium on Network and Distributed System Security (NDSS), 2014.

[3.] Marforio, N. Karapanos, C. Soriente, K. Kostiainen, and S. Capkun. Smartphones as practical and secure location verification tokens for payments. In Proceedings of the Network and Distributed System Security Symposium, NDSS, 2014.

[4.] Borchert and M. Gunther. Indirect nfc-login. In Internet Technology and Secured Transactions (ICITST), 2013 8th International Conference for, pages 204–209. IEEE, 2013.

[5.] Miers, C. Garman, M. Green, and A. Rubin. Zerocoin: Anonymous distributed e-cash from bitcoin. In Security and Privacy (SP), 2013 IEEE Symposium on, pages 397–411, May 2013.

[6.] A. Alrawais, A. Alhothaily, C. Hu, X. Xing, and X. Cheng. An attribute based encryption scheme to secure fog communications. IEEE Access, 2017
[7.] X. Fang and J. Zhan. Online banking authentication using mobile phones. In Future Information Technology (FutureTech), 2010 5th International Conference on, pages 1–5. IEEE, 2010
[8.] L. O. Gorman. Comparing passwords, tokens, and biometrics for user authentication. Proceedings of the IEEE, 91(12):2021–2040, 2003.
[9.] A. Hiltgen, T. Kramp, and T. Weigold. Secure internet banking authentication. IEEE Security Privacy, 4(2):21–29, March 2006.
[10.] Y. S. Lee, N. H. Kim, H. Lim, H. Jo, and H. J. Lee. Online banking authentication system using mobile-otp with qr-code. In Computer Sciences and Convergence Information Technology (ICCIT), 2010 5th International Conference on, pages 644–648. IEEE, 2010.