

Steganography Security on Bank System

Shaik Arshiya, B. Aruna, P. Guru Prasad, Ravi Kumar Tenali

Abstract Paper : *In this paper we are developing an application based on security as the rate of internet users are increasing and most of the users either use internet for money transaction and social media the rate of cybercrime is increasing rapidly and there is a need to secure bank system to prevent customer from cybercrime. we have developed a three-tier architecture in which the concept of image steganography is inspired from google which checks whether it's a human or robot and all the data is applied with encryption and decryption. The customer need to provide the details during the registration process and the images will be also selected during the time of registration and during the transaction process to be done based on the images selected the admin provides steganography on the given images and the user need to select the original image and if the image that is applied is correct then the puzzle is set up with mathematical expression and user further continues with the following transaction process by generating his one time password (otp) and transaction is successful.*

Index Terms: *cybersecurity, image steganography, bot detection, encryption, decryption*

I. INTRODUCTION

The rate of cybercrime is increasing rapidly and there is a need to protect system and user from cyberattacks through cyber security and most of the applications are to be build based on cybersecurity as the need is increasing much more because most of the people are addicted to internet use of social media and money transaction and banking fields of security. They are different methods to produce security to bank applications like considering biometrics as using data as authentication and another is storing original image and comparing against and verifying for authentication. All the mechanism is used to prevent from hacking and data loss and prevent hackers from un-authorization. The block diagram represents the banking system in Fig.1 shows the details of new user and existing user after all the data is stored in the database the data need to be kept private by using AES algorithm and encryption and decryption is used to keep the data in encrypted form only the admin can encrypt and decrypt the data.

Revised Manuscript Received on 30 May 2019.

* Correspondence Author

Shaik Arshiya, shaik Arshiya*, student Qualification B. tech(UG) Branch ECM Streamn cyber security College, KLEF. A. P. India.

B. Aruna, Mrs. B. Aruna, Assistant Professor with Departments of M.C.A and CSE from 1998 to 2018 in Engineering college of Kanchipuram and KL University, A. P. India.

P. Guru Prasad, student Qualification Btech (UG) Branch ECM Stream cyber security College, KLEF. A. P. India

Ravi Kumar Tenali, Assistant Professor in Department of ECM, Koneru Lakshmaiah Education Foundation (KLEF). A. P. India

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an [open access](http://creativecommons.org/licenses/by-nc-nd/4.0/) article under the CC-BY-NC-ND license <http://creativecommons.org/licenses/by-nc-nd/4.0/>

Many preventive measures are taken to prevent users and system from cyber theft The Bank framework in India we have propelled changes and are presently supplanted new advances and have concocted computerized change, with the target of the high incomes. We have likewise observed client changing the earlier towards the advanced change. There is an earlier, that the ascent of development digital security rehearses has not kept any pace with the improvement and rate of development of center business with the empowering advance innovation. While in contrast with that few different banks are certainly observed substantially more making them in the contributing and improving their safety efforts practice, such measures might be as yet deficient thinking about the difficulties with the conventional methodology towards the IT security and the cybercrime is likewise expanding now a days due to fast improvement of innovation. The impact of users on banking is increasing and the preventive methods and the need to be implemented to prevent users from malicious attacks on bank systems and customers .

1.1 Cyber Security:-

Computer security, cybersecurity is the information technology security that can be protection for computer systems from the damage to hardware, the software and electronic data, as well as from disruption of the services they provide and securing the information and design and providing security to applications.

1.2 Vulnerability:-

Vulnerability is weakness in the design, implementation, operation or internal control. Most of the vulnerabilities that have been discovered are documented in the Common Vulnerabilities and Exposures database . An exploitable vulnerability is one for which at least one working attack exists. Vulnerabilities are often hunted or exploited with the aid of automated tools or manually using customized scripts.

1.3 Steganography:-

It is the term defined for hiding and storing the secret data that may involve file or image and provide secrecy the file may involve image or an audio file and steganography and if possible message extraction and can be used to hide and read the existence.

II METHODOLOGY

Cyber Crime and the Cyber law is the part of the overall system that deals with the Internet information and the cyberspace, and in concern with respective legal issues. Cybercrimes can be basically divided into 3 major categories and most of the cybercrimes happen and root cause for all the crimes is as follows:

Steganography security on bank systems

1. Cybercrime against the Persons-colleagues issues, grudge
2. Cyber Crimes against the Property-family issues
3. Cyber Crimes against the Government-terrorist

Protect your databases, avoid giving out any information and about yourself, Use the latest anti-virus software, Back up your web site after every update and the reason for the crime is most of the people are not aware of the activities that occur on system and not aware of applications like anti-virus and malware so there is a need to socialize people. preventing users from phishing attacks most of the attacks occur on finance ,robbery, bank system.. They are not aware about risk factor of being affected by the malicious software. From personal and business point of view it is one of the difficult tasks to protect their data from the threats. Firewall, Intrusion Detection System (IDS), and Honeypot are some of the security services available in the market which can prevent users data from being trapped and based on the working application it can easily identify and prevent the data from malicious misuse and prevent data of customers from un-authorization. The client information and cause an un-authorize access and they develop the information by creating financial loss to the bank and members accessing it and to prevent the system for malicious misuse we need to developed cyber security for the system that can effectively from the system from hacking and hackers. The new information technology is turning into the most important factor in the future development of banking of markets: e-finance, e-money, E-banking, e-brokering, e-insurance, e-exchanges, and even e-supervision to the existing module of application we have added a level of security to the existing system by adding images which is called as puzzle as graphical password (CaPR) in which the original image is applied steganography which the user need to select the customized image and based on the actual image selected by the user the puzzle is set and the customer can do this and transaction successfully. when an image is applied steganography the original image is compressed and a set of images are produced among all the images if a user select the original image then next to that a puzzle part is set and user is ready and verified the account and transaction process is built up successfully.

Advantages Of Proposed System:

- The security offers the usage and appears to be fit well with banking applications and systems for improving online security systems and its new application
- This threat is to be considered as a high attack on cyber security risk. Defense against online and the system and dictionary attacks is a more observed problem than it might appear in cyber.
- Puzzle redirecting and login process are the top of Puzzle technology Using mathematical problems. Image Puzzle Solving with AES Algorithm the most helpful in preventing the users from cybercrime by providing authorized access.

Example of image steganography:

The most used technique in hiding the secret image through digital image the image pixels can be represented by a chromatic like brightness and each of the pixels can be

represented in terms of binary of 1s and 0s..A 24 bit map will have 8 bits representing each with different values and colors.

LSB Coding:

If we have a 24-bit colour, the amount of change will be minimum and invisible to the human eye. As an example, of that suppose that we have three adjacent pixels each of 9 bytes with the significant following RGB encoding.

```
[ 10010101 00001101 11001001 10010110 00001111  
11001010 10011111 00010000 11001011]
```

Now if we want to "hide" the following 9 bits of data (the hidden data is usually compressed prior to being hidden): 101101101. If we use these 9 bits over the LSB of the 9 bytes above, we get the following

Steganography= cover + hidden + stego

Fig 2.1:-original image



Fig 2.1:-compressed image after steganography is applied



Compressed image

III HELPFUL HINTS

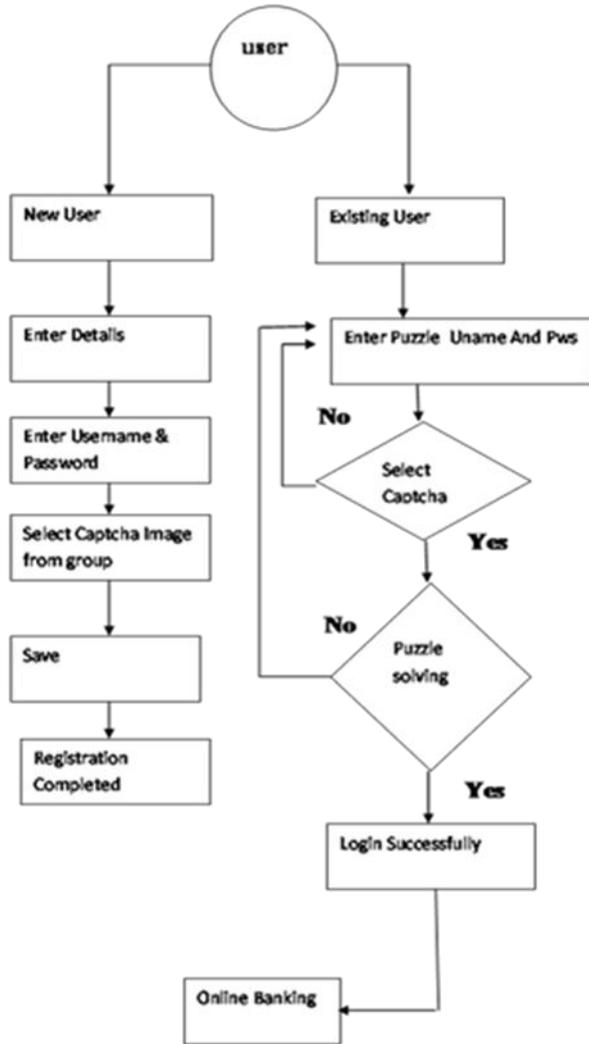


Fig: Block diagram of Bank Security System

Figures and Tables



Fig 3(b): Shows the registration page of the user

Fig 3: Login and Registration page



Fig 3(c): Images selected during the registration

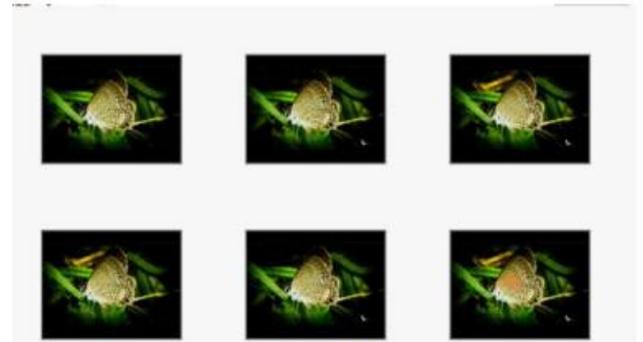


Fig 3(d): steganography applied Image in original image



Fig 3(f): Transcation page with OTP

IV. CONCLUSION

The software puzzle is developed based on and built upon a data puzzle and it further integrated with the existing server-side data puzzle scheme, and easily deployed as the present captcha can also be used for mathematical expression and call puzzle as graphical password (CaPR) can also be solved through setting puzzle for mathematical calculations and used in layer of security and algorithm can also be applied mathematically to applications where and computer application can also be built manually by using on to the applied image steganography. They are different mechanism to develop security for bank system. A few of them are online application and some are based on embedded systems which involve both hardware and software. Among all the security systems puzzle is the top security for bank systems.

The crime can not only be about transaction or money it can also be data corrupting and they are many existing systems working for the banking application even our proposed a idea can also work good with bank security and application by maintain security using image steganography set in the application.

V. FUTURE SCOPE

The banking sector is considered to as the backbone of the Indian economy and offers various career opportunities to students from all fields: science, commerce humanities. The economy should be protected and the rate of future crime increases further so preventive measure need to be maintained and cybersecurity is must to bank system .The call puzzle as graphical password works like key my maintaining secret information's and the future is gone be high demand for puzzle security mechanism for applications . Many companies have begun to strengthen security measures in order to decrease the likelihood of cyberattacks, particularly banks, are a frequent target and no secret that the banking industry is undergoing an incredible amount of technological change as these firms release new and exciting features of the hopes of gaining a competitive edge in an ever-changing market.

REFERENCES

1. How to attack twofactor authentication internet banking,” Adam, A. Azodi, et.al, in Proc. 17th Int. Conf. Financial Cryptography, 2013, pp. 322–328.
2. Two factor authentication using mobile phones,” F. Aloul, et.al, Proc. Comput. Syst. Appl., 2009, pp. 641–644.
3. Graphical passwords: Learning from the first twelve years,” .R. Biddle, et.al, ACM Computer. Surveys vol. 44, no. 4, p. 19, 2012.
4. S.Chiasson, et.al, in Proc. 3rd Symp. Usable Privacy Security, 2007, pp. 1–12. “A second look at the usability of graphical passwords,”
5. J. Bonneau, et.al, in Proc. IEEE Symp. Security Privacy, 2012, pp. 553–567. “The quest to replace passwords: A framework for comparative evaluation of web authentication schemes,”
6. S. Chiasson, et.al, in Proc. 12th Eur. Symp. Res. Comput. Security, 2007, pp. 359–374
Graphical password authentication using cued click points,”
7. NewVision of Computer Forensic Science: Need of Cyber Crime Law”,. Latika Kharb, et.al, TomarThe Internet Journal of Law, Healthcare and Ethics, 2007. Volume 4, Number 2. ISSN: 1528-8250.
8. Android malware acts as an SMS relay,” M. Balanza, Trend Micro Labs, 2011.
9. Secure internet banking authentication,”A. Hiltgen, The IEEE Security and Privacy, vol. 4, no. 2, pp. 21–29, 2006.
10. Usable security: User preferences for authentication methods in e-banking and the effects of experience,” C. S. Weir, G. Douglas, T. Richardson, and M. Jack, Interacting with Computers, vol. 22, no. 3, pp. 153 – 164, 2010.
11. Effect of trust on customer acceptance of internet banking,” Electronic Commerce Research and Applications, B. Suh et.al, vol. 1, no. 3-4, pp. 247 – 263, 2002. [4] P. Hanaek, et.al, “The E-banking security “ Security Technology, ICCST 2008, 42nd Annual IEEE International Carnahan Conference on, 2008, pp. 326 –330.
12. Secured Data sharing in Cloud Using Single Key Based Decryption Method,” in Journal of Advanced Research in Dynamical & Control Systems-JARDCS, M.Ramesh Kumar, Ravi Kumar Tenali ,et.al, , BBVSV, 2018, vol. 10, pp. 1777-1782.
13. Coronary Illness Syndrome Identification System Using Data Mining Methods” in Journal of Advanced Research in Dynamical & Control Systems-JARDCS, M Spandana, RK Tenali, et.al, 2018, vol. 10, pp. 1584-1590.
14. Storage and Retrieval of Secure information in the Cloud Systems” Ravi Kumar Tenali , M.Ramesh Kumar, M.Spandana, PSSR in Journal of Advanced Research in Dynamical & Control Systems-JARDCS, 2018, vol. 10, pp. 773-778.

15. Tenali Ravi Kumar ,et.al, TBAR 2018, vol. 07, pp. 186-188. “Human resource management leave and tour management data retrieval system” in International Journal of Engineering & Technology-IJET(UAE),

AUTHORS PROFILE



Name: shaik Arshiya. Designation: student
Qualification :Btech(UG) Branch: ECM Stream: cyber security College:KLEF



Mrs.B.Aruna, received her BSc. Computer Science Degree from St.Teresa Women’s college ,Eluru, Andhra University. In 1997 .M.C.A degree from University of Madras ,Chennai in 2006 and M.Phil Computer Science degree from Anna University ,Chennai in 1009 She was in the fiel of teaching since 21 years as Lecturer, Assistant Professor with Departments of M.C.A and CSE from 1998 to 2018 in Engineering college of Kanchipuram and KL University respectively Her research interst include Bio Informatics ,Web Service and Cyber Security.



Name: punugupati guru rasad Designation: student
Qualification :Btech(UG) Branch:ECM Stream:cyber security College:KLEF



An efficient Assistant Professor, received M.Tech (C.S.E) from Swarnandra College of Engineering and Technology (JNTUK) .working as an Assistant Professor in Department of ECM, Koneru Lakshmaiah Education Foundation (KLEF) .He has 14 years of teaching experience. He has published many papers in International Journals & his areas of Interest includes Computer Networks, Data mining, Cloud computing.