IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 11, November 2022

DOI: 10.17148/IJARCCE.2022.111138

Avoiding Phishing Attack Using Visual Cryptography

Sasmit V. Nakhate[1], Ashish B. Deharkar[2], Vijay M. Rakhade[3]

B.Tech Final Year Student, Computer Science and Engineering Department, Shri Sai College of Engineering and Technology, Bhadrawati, Maharashtra[1]

Assistant Professor, Computer Science and Engineering Department, Shri Sai College of Engineering and Technology, Bhadrawati, Maharashtra [2]

Assistant Professor, Computer Science and Engineering Department, Shri Sai College of Engineering and Technology, Bhadrawati, Maharashtra [3]

Abstract: Phishing is one amongst the foremost common social engineering attacks that users over the web fall for. Associate degree example is balloting systems, and since such systems ought to be correct and error free, phishing interference techniques square measure crucial. Visual Cryptography (VC) is employed for economical electoral system authentication to solid votes. VC is one amongst the foremost secure approaches for privacy protection because it ensures the confidentiality of the electoral system. This paper discusses planned phishing interference strategies and compares totally different proposed strategies.

Keywords: Remote Voting System (RVS), Voting System (VS), Shares Ballots, Commons Attribution International Authentication, Visual Cryptography, Phishing, Captcha.

I. INTRODUCTION

Elections are control round the world, voters in democratic countries have the power to elect a representative for his or her party to settle things in an exceedingly democratic way. However, voters should solid their ballots at a polling location. This might weaken citizen support, so, web-based ballot makes this process easier. Electronic ballot systems supply numerous options that build them different from ancient ballot strategies, as they conjointly increased legal system features over ancient ballot strategies as well as quality, privacy, simplicity, accuracy, and flexibility. On the opposite hand, ballot systems may be exposed to a fresh threat like phishing that affects the system security. When fraudsters gain your personal info, they will use it to commit numerous varieties of identity fraud, jeopardizing voters, and name. Having a secure and reliable choice system, crypto graphical and steganographic techniques ought to be applied. One among the suggested solutions is VC. Systems square measure won't to safeguard into from hackers. It's a mechanism for encrypting visual knowledge that may be decrypted by the human sensory system while not the utilization of computers.

II. LITRATURE SURVEY

2.1) Online voting system using biometric verification

2.1.1) Features:

This paper offers the info concerning the system that's wholly automatic, unbiased and on-line forecasting the tactic of choice, increasing security and reducing the count time. The system is split into a pair of sections those area unit elector registration section and actual choice section. At intervals the elector registration technique the data of the elector area unit saved at intervals the repository beside the voter's distinctive identification and finger prints knowledge. Throughout actual choice the user area unit verified with the help of a biometric device.

The biometric device checks the info of the user saved in repository by local area network communication and if the user is documented the user is approved to vote. This technique is straightforward to implement and straightforward to use.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 11, November 2022
DOI: 10.17148/IJARCCE.2022.111138

2.1.2) Disadvantages:

1) In gift day situation, EVM results may be tampered by the program keep in EVM and by putting in a glance alike part which may be taught to tamper results.
2) Errors square measure a part of all human beings; it's impossible for humans to be 100% economical in knowledge entry.
3) The obscurity of the citizen is preserved and there are no thanks to link the citizen to the vote casted by the voter.

2.2) An efficient and securable online voting system

2.2.1) Features:

An online electoral system that involves the procedures like registration of voters, polling, vote count and declaring the results would represent a decent answer to switch current system and also the planned system during this provides the knowledge concerning their own system or organized by government the system contains totally different ways for ballot like electronic ballot that helps the voters to solid votes in AN electronic approach means that in computerized instrumentality. The system additionally includes the pc within which electronic ballot machines trying like ATM or personal computers wont to solid the votes by bit screen or a pointer.

2.2.2) Disadvantages:

1) The process of collecting data and entering the data into database takes too much time and is expensive to conduct.
2) The process involves too much paper work and paper storage.
3) The system is totally insecure as malicious user can easily attack by doing any changes throughout the system.

2.3) Title: Online voting system using mobile

2.3.1) Features:

The traditional electoral system will be modified to a more modern and effective approach termed as mobile option.The mobile electoral system provides the convenient, simple and economical thanks to vote eliminating the defect a conventional approach. during this paper the planned to create the E- electoral system that is essentially an internet electoral system through the good phones or web site. to attain the protection they're victimization just the one time password (OTP) principle. The system will be used anytime and from anyplace by the voters. nobody will forged votes on behalf of others and multiple votes. It saves time and having distinctive identification by victimization aadhar card or elector id.

2.3.2) Advantages:

1) There's no documentary proof and tangible results for election.
2) It's potential for hackers to access and modify the results once obtaining any user id.

III. TYPES OF SECURITY ATTACK

Before planning this technique we have a tendency to studied completely different attacks which may be done on the legal system. The attacks area unit as follows

A. Phishing Attack

Phishing attack could be a technique during which the malicious user will produce a pretend web site as kind of like the first web site to get info of elector.

B. Pharming Attack

In pharming attack malicious user can send the first web site.

C. SQL injection

In this malicious user can destroy all the information of original web site by mistreatment sql question.

D. Password Attack

Password attacks are often enforced mistreatment many ways, as well as brute-force attacks, worm programs, IP spoofing, key loggers, packet sniffers, and wordbook attacks. Though packet sniffers and informatics spoofing will yield user accounts and passwords, word attacks sometimes check with continual makes an attempt to spot a user account, password, or both. These continual makes an attempt area unit referred to as brute force attacks.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

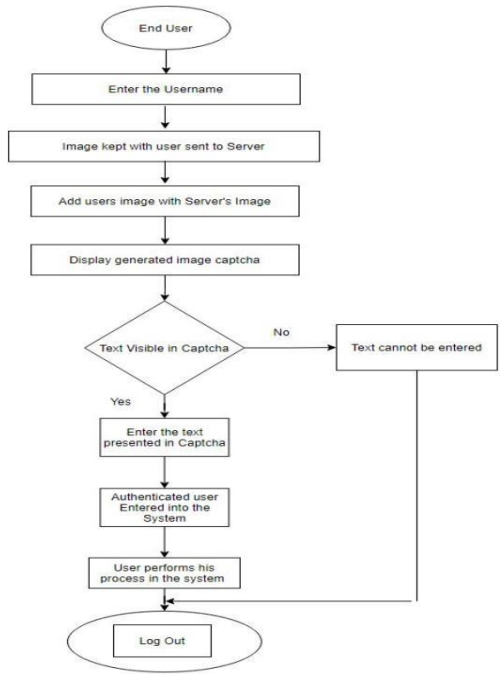
ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 11, November 2022

DOI: 10.17148/IJARCCE.2022.111138

E. Man in the middle Attack

A complex sort of informatics spoofing is named man-in-the middle attack, wherever the hacker monitors the traffic that comes across the network and introduces himself as a stealing intermediator between the sender and also the receiver

IV. PROPOSED ONLINE VOTING SYSTEM



In this system, first off the phishing detection are going to be done as explained in section three. The hindrance are going to be exhausted the system as show within the figure. The choice method are going to be divided into 2 parts. Initial the registration part then the particular choice part. In the registration part, the image can divided into 2 halves and shared between the user and therefore the server. Throughout choice part, the user can enter its username. The a part of the image unbroken with the user are going to be sent to server. This user's half are going to be superimposed with server's image and generated captcha image are going to be displayed. If the text is visible in captcha then the user is AN documented user and he/she is allowed to enter the system by coming into the text in captcha. Else if the text isn't visible then the text in captcha cannot be entered and user cannot enter the system.

V. CONCLUSION

Voting plays a vital role for any democratic country. If this planned system is enforced, then the citizen doesn't got to go to the choice center. this method is extremely helpful for those peoples World Health Organization live in other countries conjointly for the peoples World Health Organization square measure physically disabled. Since Visual Cryptography Technique is employed, user will ready to conclude whether or not he's in phishing web site or original web site simply. planned on-line legal system is extremely effective and it'll helpful for voters and organization in some ways and it will scale back the price and time.

REFERENCES

[1] Network Security, accessed on May 2015.
[2] Joey Paquet, accessed on May 2015.
[3] Implementation of Electronic Voting System in Mobile Phones with Android Operating, ISSN 2079-8407, Volume-4, Number9, Sept-2013, JETCIS.
[4] Abdalla Al-Ameen and Samani Talab, “The Technical Feasiblity and Security of E-Voting”, the International Arab Journal of Information Technology, Vol.10, No.4, July 2013, p.no.397-404.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 11, November 2022
DOI: 10.17148/IJARCCE.2022.111138

[5] The Design of Web Based Secure Internet Voting for Corporate Election, ISSN 2319-7064, Volume-2, Issue-7, July-2013, And IJSR.
[6] An Efficient Online Voting System, ISSN 2249-6645, Volume-2, Issue, July-Aug-2012, IJMER.
[7] Villafiorita A, Weldermariam K, Tiella R, "Development, Formal verification and evaluation of an e-voting system with VVPAT", IEEE Transactions on Information Forensics and Security, 2009, p.no. 651661.
[8]Nisha, S. and Madheswari, A.N. (2016) Prevention of Phishing Attacks in Voting System Using Visual Cryptography. 2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS), Pudukkottai, 24-26 February 2016, 1-4.
[9] Hodeish, M. and Humbe, V. (2017) A New XOR-Based Visual Cryptography Scheme for Authentic Remote Voting System.
[10] Nayan, A. and Ardak, P. (2022) Visual Cryptography Scheme for Privacy Protection.
[11] Rane, S.S., AdwaitPhansalkar, K., Shinde, M.Y. and Kazi, A. (2020) Avoiding Phishing Attack on Online Voting System Using Visual Cryptography. 2020 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, 22-24 January 2020, 1-4.
[12] Singh, A., Nandini, S., Pawana, S., Supriya, C. and Biswagar, D. (2021) Prevention of Phishing Attacks on Online Voting Using Visual Cryptography. Journal of University of Shanghai for Science and Technology, 23, 246-249.
[13] Tiwari, M.G.D. and Kakelli, A.K. (2021) Secure Online Voting System Using Visual Cryptography. Walailak Journal of Science and Technology, 18.
[14] Walake, A. and Chavan, P. (2015) Efficient Voting System with (2, 2) Secret Sharing Based Authentication. IJCSIT, 6, 3739-3743.
[15] Naidu, P.S., Kharat, R., Tekade, R., Mendhe, P. and Magade, V. (2016) E-Voting System Using Visual Cryptography & Secure Multi-Party Computation. 2016 International Conference on Computing Communication Control and Automation (ICCUBEA), Pune, 12-13 August 2016, 1-4
[16] Liang H., & Xue Y., "Understanding security behaviours in personal computer usage: A threat avoidance perspective", Association for Information Systems,11(7), pp. 394–413, 2010
[17]Nalin Asanka Gamagedara Arachchilage, Steve Love, Security awareness of computer users: A phishing threat avoidance Perspective, Computers in Human Behaviour (38), pp. 304–312, 2014.
[18]Yuancheng Lia et al., "A semi-supervised learning approach for detection of phishing web pages", Optik, (124), pp. 6027–6033, 2013.
[19]Anti-Phishing Working Group (APWG), Phishing activity trends report for the month of June, 2007
[20]Ollmann G. The Phishing Guide Understanding & Preventing Phishing Attacks, NGS Software Insight Security Research.
[21]Anti-Phishing Working Group, Global Phishing Survey: Trends and Domain name use in 1H2009, 2009Anti-Phishing Working group.
[22]Dhamija, R. and Tygar, J. D. 2005. The battle against phishing: Dynamic Security Skins. In Proceedings of the2005 Symposium on Usable Privacy and Security, SOUPS '05, vol. 93, ACM Press.
[23]Evgeniy Gabrilovich and Alex Gontmakher. "The Homograph Attack" (PDF), February 2002, ACM.