www.s2is.org

International Journal on Smart Sensing and Intelligent Systems

ISSN 1178-5608

AN ANTI-EMULATION STRUCTURE FOR INTERNET DESPOSITORY USING SECURED IMAGE VALIDATION SCHEME

Anupriyan K [1]*, Santhosh kumar C[2], Nagaraj N[3]

Priyadarshini Engineering College, Vaniyambadi, 635751.

Email: anupriyan00@gmail.com

Submitted: May 27, 2017 Accepted: June 15, 2017 Published: Sep 1, 2017

Abstract- Emulation attack is an effort by an individual or a group to steal personal confidential information such as passwords, credit card information etc, New approach called visual secret sharing scheme (VSS) for cloning websites classification to solve the problem of Phishing attack. The novel system is developed with the things that eradicate the drawbacks of the existing system. The main aim of visual secret sharing scheme is to conserves the solitude of image by decay the original image into two shares that as been stocked in independent database servers such that the authentic image can be revealed only when they are equally gathered. The specific sheet of representation does not declare the status of the original visual image which was generated previously. Once the unique visual image is discovered to the user then that picture can be used as a password for detecting phishing. In the proposed system, privacy enabled secure database is built. The security level is much enhanced from its actual level. The authentication process can be secured by using double level security.

Index terms: phishing attack, visual secret scheme, visual cryptography, anti-phishing validation scheme.

I. INTRODUCTION

Online transactions are nowadays become very common and there are various attacks present behind this. In these types of various attacks, phishing is identified as a major security threat and new innovative ideas are arising with this in each second so preventive mechanism should also be so effective.

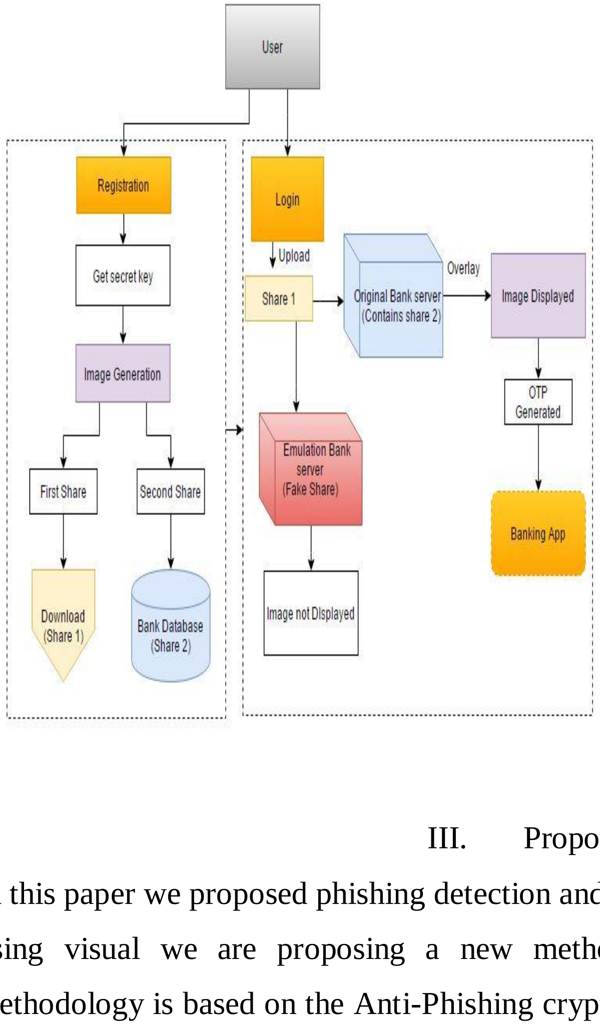
Thus the security in these cases be very high and should not be easily tractable with implementation easiness. Today, most applications are only as secure as their underlying system. Since the design and technology of middleware has improved steadily, their detection is a difficult problem.

As a result, it is nearly impossible to be sure whether a computer that is connected to the internet can be considered trustworthy and secure or not. Phishing scams are also becoming a problem for online banking and e-commerce users. The question is how to handle applications that require a high level of security. phishing is a form of online identity theft that aims to steal sensitive information such as online banking passwords and credit card information from users. Phishing scams have been receiving extensive press coverage because such attacks have been escalating in number and sophistication. one definition of phishing is given as “it is a criminal activity using social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication”. The conduct of identity theft with this acquired sensitive information has also become easier with the use of technology and identity theft can be described as “a crime in which the impostor obtains key pieces of information such as Social Security and driver's license numbers and uses them for his or her own gain”. Phishing attacks rely upon a mix of technical deceit and social engineering practices. In the majority of cases the phisher must persuade the victim to intentionally perform a series of actions that will provide access to confidential information. Communication channels such as email, web pages, IRC and instant messaging services are popular. In all cases the phisher must impersonate a trusted source for the victim to believe. To date, the most successful phishing attacks have been initiated by email – where the phisher impersonates the sending authority.

So here introduces a new method which can be used as a safe way against phishing which is named as "A novel approach against Anti-phishing using visual cryptography". As the name describes, in this approach website cross verifies its own identity and proves that it is a genuine website (to use bank transaction, E-commerce and online booking system etc.) before the end users and make the both the sides of the system secure as well as an authenticated one. The concept of image processing and an improved visual cryptography is used. Image processing is a technique of processing an input image and to get the output as either improved form of the same image and/or characteristics of the input image. Visual Cryptography (VC) is a method of encrypting a secret image to shares, such that stacking a sufficient number of shares reveals the secret image.

So it can able to protect many of confidential information and other such data's and also protect from clone webpages.

II. System Architecture



III. Proposed Approach

In this paper we proposed phishing detection and Prevention, secured image validation scheme using visual we are proposing a new methodology to detect the phishing website. Our methodology is based on the Anti-Phishing cryptography. Choice of shares for a white and black pixel is randomly determined by 16 bit key generation. It denotes the shares of a white pixel and a black pixel. pixels in the secret image will be encrypted using independent random choices. Two shares are superimposed. Only when both the share are match , it will allow the user to access data or else it will avoid. If P is a black pixel, we get two black sub pixels. If it is a white pixel, we get one black sub pixel and one white sub pixel. **.** In the proposed system, privacy enabled secure database is built. The security level is much enhanced from its actual level.

Advantage

1. It prevents password and other confidential information from the phishing websites.
2. Protect from clone web site.
3. Provide double level security for internet .

IV. Modules Description

4.1 Registration With Secrete Code

In the registration phase, the user details user name, password, email-id, address, and a key string(password) is asked from the user at the time of registration for the secure website. The key string can be a combination of alphabets and numbers to provide more secure environment. This string is concatenated with randomly generated string in the server.

4.2 Image captcha Generation

A key string is converted into image using java classes BufferedImage and Graphics2D. The image dimension is 260*60.Text color is red and the backround color is white.Text font is set by Font class in java.After image generation it will be write into the userkey folder in the server using ImageIO class.

4.3 Shares Creation(VCS)

The image captcha is divided into two shares such that one of the share is kept with the user and the other share is kept in the server. The user's share and the original image captcha is sent to the user for later verification during login phase. The image captcha is also stored in the actual database of any confidential website as confidential data.

4.4 login phase

When the user logs in by entering his confidential information for using his account, then first the user is asked to enter his username (user id).Then the user is asked to enter his share which is kept with him. This share is sent to the server where the user's share and share which is stored in the database of the website for each user, is stacked together to produce the image captcha. The image captcha is displayed to the user.

V. Conclusion

Currently phishing attacks are so common because it can attack globally and capture and store the users' confidential information. This information is used by the attackers which are indirectly involved in the phishing process. Phishing websites as well as human users can be easily identified using our proposed "Anti-phishing framework based on Visual Cryptography". The proposed methodology preserves confidential information of users. verifies whether the website is a genuine/secure website or a phishing website. If the website is a phishing website (website that is a fake one just similar to secure website but not the secure website), then in that situation, the phishing website can't display the image captcha for that specific user (who wants to log in into the website) due to the fact that the image captcha is generated by the stacking of two shares, one with the user and the other with the actual database of the website. The proposed methodology is also useful to prevent the attacks of phishing websites on financial web portal, banking portal, online shopping market. This application can be implemented for all kinds of web application which needs more security.

REFERENCES

[1] Aizat Azmi, Ahmad Amsyar Azman, Sallehuddin Ibrahim, and Mohd Amri Md Yunus, "Techniques In Advancing The Capabilities Of Various Nitrate Detection Methods: A Review", International Journal on Smart Sensing and Intelligent Systems., VOL. 10, NO. 2, June 2017, pp. 223-261.

[2] Tsugunosuke Sakai, Haruya Tamaki, Yosuke Ota, Ryohei Egusa, Shigenori Inagaki, Fusako Kusunoki, Masanori Sugimoto, Hiroshi Mizoguchi, "Eda-Based Estimation Of Visual Attention By Observation Of Eye Blink Frequency", International Journal on Smart Sensing and Intelligent Systems., VOL. 10, NO. 2, June 2017, pp. 296-307.

[3] Ismail Ben Abdallah, Yassine Bouteraa, and Chokri Rekik , "Design And Development Of 3d Printed Myoelctric Robotic Exoskeleton For Hand Rehabilitation", International Journal on Smart Sensing and Intelligent Systems., VOL. 10, NO. 2, June 2017, pp. 341-366.

[4] S. H. Teay, C. Batunlu and A. Albarbar, "Smart Sensing System For Enhanceing The Reliability Of Power Electronic Devices Used In Wind Turbines", International Journal on Smart Sensing and Intelligent Systems., VOL. 10, NO. 2, June 2017, pp. 407- 424

[5] SCihan Gercek, Djilali Kourtiche, Mustapha Nadi, Isabelle Magne, Pierre Schmitt, Martine Souques and Patrice Roth, “An In Vitro Cost-Effective Test Bench For Active Cardiac Implants, Reproducing Human Exposure To Electric Fields 50/60 Hz”, International Journal on Smart Sensing and Intelligent Systems., VOL. 10, NO. 1, March 2017, pp. 1- 17

[6] P. Visconti, P. Primiceri, R. de Fazio and A. Lay Ekuakille, “A Solar-Powered White Led-Based Uv-Vis Spectrophotometric System Managed By Pc For Air Pollution Detection In Faraway And Unfriendly Locations”, International Journal on Smart Sensing and Intelligent Systems., VOL. 10, NO. 1, March 2017, pp. 18- 49

[7] Samarendra Nath Sur, Rabindranath Bera and Bansibadan Maji, “Feedback Equalizer For Vehicular Channel”, International Journal on Smart Sensing and Intelligent Systems., VOL. 10, NO. 1, March 2017, pp. 50- 68

[8] Yen-Hong A. Chen, Kai-Jan Lin and Yu-Chu M. Li, “Assessment To Effectiveness Of The New Early Streamer Emission Lightning Protection System”, International Journal on Smart Sensing and Intelligent Systems., VOL. 10, NO. 1, March 2017, pp. 108- 123

[9] Iman Heidarpour Shahrezaei, Morteza Kazerooni and Mohsen Fallah, “A Total Quality Assessment Solution For Synthetic Aperture Radar Nlfm Waveform Generation And Evaluation In A Complex Random Media”, International Journal on Smart Sensing and Intelligent Systems., VOL. 10, NO. 1, March 2017, pp. 174- 198

[10] P. Visconti ,R.Ferri, M.Pucciarelli and E.Venere, “Development And Characterization Of A Solar-Based Energy Harvesting And Power Management System For A Wsn Node Applied To Optimized Goods Transport And Storage”, International Journal on Smart Sensing and Intelligent Systems., VOL. 9, NO. 4, December 2016 , pp. 1637- 1667

[11] YoumeiSong,Jianbo Li, Chenglong Li, Fushu Wang, “Social Popularity Based Routing In Delay Tolerant Networks”, International Journal on Smart Sensing and Intelligent Systems., VOL. 9, NO. 4, December 2016 , pp. 1687- 1709

[12] Seifeddine Ben Warrad and OlfaBoubaker, “Full Order Unknown Inputs Observer For Multiple Time-Delay Systems”, International Journal on Smart Sensing and Intelligent Systems., VOL. 9, NO. 4, December 2016 , pp. 1750- 1775

[13] Rajesh, M., and J. M. Gnanasekar. "Path observation-based physical routing protocol for wireless ad hoc networks." International Journal of Wireless and Mobile Computing 11.3 (2016): 244-257.

[14]. Rajesh, M., and J. M. Gnanasekar. "Congestion control in heterogeneous wireless ad hoc network using FRCC." Australian Journal of Basic and Applied Sciences 9.7 (2015): 698-702.

[15]. Rajesh, M., and J. M. Gnanasekar. "GCCover Heterogeneous Wireless Ad hoc Networks." Journal of Chemical and Pharmaceutical Sciences (2015): 195-200.

[16]. Rajesh, M., and J. M. Gnanasekar. "CONGESTION CONTROL USING AODV PROTOCOL SCHEME FOR WIRELESS AD-HOC NETWORK." Advances in Computer Science and Engineering 16.1/2 (2016): 19.

[17]. Rajesh, M., and J. M. Gnanasekar. "An optimized congestion control and error management system for OCCEM." International Journal of Advanced Research in IT and Engineering 4.4 (2015): 1-10.

[18]. Rajesh, M., and J. M. Gnanasekar. "Constructing Well-Organized Wireless Sensor Networks with Low-Level Identification." World Engineering & Applied Sciences Journal 7.1 (2016).

[19] A. Almomani, B. B. Gupta, S. Atawneh, A. Meulenberg, and E. Almomani, "A Survey of Phishing Email Filtering Techniques," in iEEE Communications Surveys & Tutorials, vol. 15, pp.2070-2090, 2013.

[20] S. S. Tseng, K. Y. Chen, T. J. Lee, and 1. F. Weng., "Automatic content generation for anti-phishing education game," in iEEE International Conference on Electrical and Control Engineering, pp.6390-6394, 2011.

[21] F. Frattolillo, "Watermarking Protocol for Web Context," in iEEE Transactions on Information Forensics and Security,voI.2,no.3,sept , pp.350-363, 2007.

[4] P. Sun, and H. Lu, "An efficient web page watermarking Scheme," in iEEE, pp.163-167, 2009.

[22] H. Wang and C. Liao, "Compressed-Domain Fragile Watermarking Scheme for Distinguishing Tampers on Image Content or Watermark,“ in IEEE, pp.480-484, 2009.

[23] A .P. Singh, V. Kumar, S. S. Senger, and M. Wairiya, "Detection and Prevention of Phishing Attack using Dynamic Watermarking," inVInternational Conference on Advances in Information Technology and Mobile Communication ,vol. 147, pp 132-137,2011.