

Enhancing Web Security Based on Network Algorithm

Nisha Jebaseeli¹, L. Jayasimman², B. Senhtil Kumar^{3*}

¹Assistant Professor Department of Computer Science, Bharathidasan University Constituent College, Lalgudi,

²Assistant Professor Department of Computer Science, Srimad Andavan Arts & Science College, Tiruchy,

³Former Principal, ES Pan Asian College, India

Available online at: www.ijcseonline.org

Received: 28/Aug/2016

Revised: 10/Sept/2016

Accepted: 25/Sept/2016

Published: 30/Sep/2016

Abstract— The aim of this research work is to study the security issues in the Web learning environment. Problems in Web learning system are related to networking issues, database management issues, operating system related issues, memory and sharing issues, resource channeling issues, learners' authenticity related issues, load related issues, virtualization-related issues, management information system, etc., These above said issues are very common and hurdle in Web learning environment. From Web service providers to learners there are many possibilities in security lapse. The service providers have possibilities to control the system, but controlling the flow of information and controlling the technology such as networking and database usage, virus and information related laws are difficult to manage. There are possibilities to control the flow of information from every stage from the main service provider to users. Data losses can be minimized by maintaining the local backups separately. By developing the infrastructure, a service provider can facilitate the communication between the learner and the educator. Storing the sensitive data in a secured place is the best method to save. Storing the important data in the Web has a potential risk. This review paper critically analyzes the various issues related to Web security

Keywords— *Web learning, Web computing, Security, Network, Web security issues, Data loss, Information laws, Backups, etc.*

I. INTRODUCTION

Web computing has many security problems in several ways. Problems such as DoS (Denial of Service), sensitive and non-sensitive data loss, data privacy, DNS failure, data segregation, provider viability, data recovery, user accessibility, etc., Distributed Denial of Service is the main problem in Web computing which breaks the communication paths between the user and the Web service provider. It is one of the primary and main problems in the current scenario of Web computing environment. Hackers can attack the main server activities and programs in the Web computing environment. The well-constructed intelligent network may reduce the risk of hackers attack on the Web's main server. There are possibilities to develop the new networks such as genetically based network, artificial intelligent network, parallel processing network, etc., to reduce the risk of network security. Threats are very common on the Web because it has many different web hosts and network configurations and system. Main Challenges in Web computing: Management of Web environment, Data protection, Data availability and recovery, Regulatory and compliance restrictions are the main challenges in Web computing. Attacks on Web environment can be DoS (denial of service), Side channel attacks, a man in the middle cryptographic attacks and authentication attacks.

II. REVIEW OF LITERATURE

Thiruselvan et al, (2012), proposed a new algorithm named fast-Flux Swarm network to reduce the security issues in Web computing. It had many advantages. J. Mirkovic et al, (2005), developed a new technique named D-WARD technique to detect the unauthorized access to the Web network. It helped to reduce the others' suspicious activities in the Web network. Stoica et al, (2002), developed the idea of multipurpose internet indirection infrastructure. It did not require the provider to be aware of the user. Gangadevi (2011), found the potential use of Iris biometrics technique to reduce the authentication issues in a Web environment. Seungwon (2012), developed a new network algorithm named Cloud Watcher to control the safety in a Web environment.

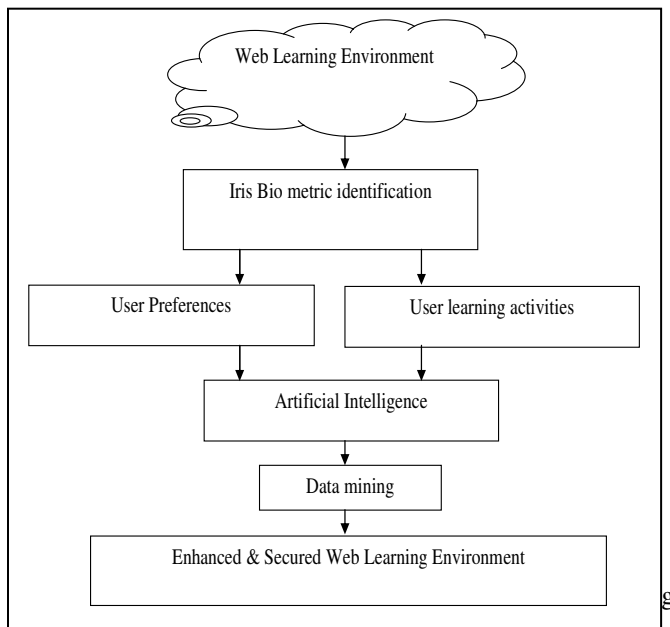
Data mining technique can be used to analyze the users' preferences, users' satisfaction level and their comfortable level in the online learning environment. Artificial intelligence is very useful to search the learners' learning behaviors and activities in the online and virtual learning system. KDD (Knowledge Discovery Database) is the useful data mining technique which has many potential applications to reduce the security lapse in Web learning environment (Ala, 2001). According to Jayasimman, "enhancing the web

learning system using cognitive load and cognitive aspects of the learners is possible through a proper algorithm (Jay, 2012).” Jayasimman developed a new algorithm called PSOPMLP-particle swarm optimization technique based on cognition of the learner in a web-based learning system. He successfully classified the learners’ preferences with accuracy. Much research evidence is available for the genetic algorithm, particle swarm optimization, CART, Naïve Bayes, Random Forest, etc. Even though learning environments such as e-learning, online learning, and distance learning looks similar, there are many differences in its methods and learning delivery (Joi, 10). Thus, Web learning environment has certain distinct qualities than general web learning, e-learning and distance learning (NiK, 2008).

III. OBJECTIVES OF THIS STUDY

- To study about Web learning system security in the learning environment.
- To study about various algorithms related to networking.
- To review the related works in order to find the new algorithm.
- To propose a framework to enhance the Web security
- To study about the possibilities to improve the current Web learning environment

IV. FRAMEWORK TO ENHANCE THE WEB SECURITY



Great advances in computing technology have resulted in thousands of specialized courses in e-learning and web

learning. But infrastructure such as internet, storage capacity, speed, accuracy is very poor in this environment. Without proper online learning environment, mere trial and error may result in a waste of time and effort. The learners have many problems in communication because of today’s highly competitive and complex world. As forcing to study online would result in wastage of efforts, dissatisfaction, underachievement and waste of time, etc. planning a full-fledged online learning system needs high speed, accuracy, storage capability, infrastructure, etc. Web computing is the good answer for this issue. Furthermore, studying about the enhancement of security in Web computing is essential to reach the mass illiterate people with the available and limited infrastructure.

V. CONCLUSION

Current Web learning environment has many security issues in networking aspects. The main aim of this research is to propose a new algorithm to reduce the security risks in data transmissions, storage and loss. By studying the security issues in data, infrastructure, network, user identification, etc., this proposed research work tries to minimize the risks related to security in Web learning environment. This research outcome can be applicable to public Web environment as well in a private Web environment. The Web learning environment is developing in a fast phase and the security issues are growing in a very fast phase. To address those issues, research work related to security in Web learning environment is the need of the hour. By identifying the students’ learning styles and activities any Web learning environment can be improved. Furthermore, classification of accuracy in students’ learning preferences by using the artificial network and iris-based biometric authentication tool can help to enhance the Web learning environment security. User interface design of the learning system in a Web learning environment should be in a proper design based on design principles and communication principles.

VI. REFERENCES

- [1]. Thiruselvan, ArunShanmugam, kesavamoorthy, (Jan 2012), “An intelligent fast-flux swarm network for minimizing DDoS attacks in Web computing”, International conference on recent trends in information processing”, pp. 297-303, ISSN 978-81-8371-412-9
- [2] J. Mirdovic and P. Rieher, (2005), “D-WARD: A source-end defense against denial of service attacks”, IEEE Trans, Dependable and secure computing, Vol,2, 2005, 216-232.
- [3] J. Stoica et al, (2002), “Internet Indirection infrastructure”, proceedings of conference applications, techniques, architecture, and protocols for computers common, Pittsburgh, PA
- [4] Gangadevi, (Jan 2012), “A new web-based architecture, based on iris biometrics technique to decrease credit cards frauds over

- the internet”, International conference on recent trends in information processing”, pp. 280-283, ISSN 978-81-8371-412-9
- [5] Shin, S., &Gu, G. (2012, October). WebWatcher: Network security monitoring using OpenFlow in dynamic Web networks (or: How to provide security monitoring as a service in Webs?). In Network Protocols (ICNP), 2012 20th IEEE International Conference on (pp. 1-6). IEEE.
- [6] Alan Jolliffe, Jonathan Ritter, David Stevens (2001), “The online learning” Higher Education Supplement, Kogan Page Ltd, 2001.
- [7] L. Jayasimman, E. George Dharma Prakash Raj (2012), “Web Learning Systems and Cognitive Learning: A Survey”, International Journal of Computer Science and Telecommunications, UK, Volume 3, Issue 7, pp. 91-94, July 2012, ISSN 2047- 3338
- [8] Cook DA, Dupras DM. (20104), “A practical guide to developing effective web Based learning”, Journal of General Internal Medicine, Vol. 19, No. 6, PP. 698-707, 2004.
- [9] Joi L. Moore, Camille Dickson-Deane, Krista Galyen, (2011), “E-Learning, online learning, and distance learning environments: Are they the same?” The Internet and Higher Education, 2010 Elsevier Inc.14 (2011) 129–135.
- [10] Nikos Tsianos*, Zacharias Lekkas*, Panagiotis Germanakos*t, Costas Mourlas*, George Samarast (2008), “Personalizing web environments on user intrinsic characteristics”, IEEE- IET 4th International Conference on Intelligent Environments, 2008. DOI: 10.1049/cp:20081173