International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN : 2456-3307

User Navigation Guard Approach and Web Record Exploration Based On Apriori Algorithm

G. Elakkiya
Department of Computer Science, Tamil university, Thanjavur, Tamilnadu, India

ABSTRACT

User's access records are arrested by implementing a datamining algorithm on the website. Web usage mining is unique technique to fetch user necessities from web log record. By spending this application, product based organization will get to recognize the demand of certain products and it helps organization to target exact consumers. By using web usage mining technique to mine the evidence from the web access behavior of the user at the identical time as they are browsing and exploring through the Web. Intruders may abuse weblog records because that holds user requirements. So the challenge is exactly how to protect weblog records from intruders. Timing attack may allow intruders to fetch user requirements from weblog illegally. The proposed system is User Navigation Guard Approach (UNG) and it helps to protect user requirements records from timing attacks. At the matching time UNG Approach protected webserver from intruders. The proposed system also contains existing system features such as Customer will catch accurate product according to their first choice and this scheme will be valuable for those customers who frequently purchase products online. The main goal of the proposed system is to provide existing system feature with protected environment.AES is a robust encryption algorithm and it implements a public-key cryptosystem that permits protected communications. By using AES algorithm webmaster can encrypt user requirements and it comforts user to feel safe from attacks or intruders.

Keywords : Web Usage Mining, Weblog Records, User Navigation Guard Approach, AES Algorithm, Intruder.

I. INTRODUCTION

Nowadays, the Internet is one of the greatest effective and efficient methods to interconnect. The internet provides us the chance to associate with all kinds of different individuals and read update and evidence from all over the world. Online shopping is more popular today, because they focus customers from different countries and also supports wholesalers and retailers to advertise their products straightforwardly. This environment is more user-friendly and users can purchase products just by one click. Online shopping services users to reduce their time, more convenient, no crowds, better prices etc.; which is compared to the real shopping. E-commerce websites faces many problems by intruders because intruders enter into sites by the way of timing attack. Today reducing timing attack is a big challenge and they suffer users severely. Because timing attack explores the contents of a web browser's cache and stores a malicious form of cookie on the client's system. The cookie can allow the designer to collect information on how to access password protected sites. And also cross side scripting is a client side code injection attack and it allows intruders can execute malicious scripts into web applications. By using cross side scripting attack intruders can convince a user to visit their malicious page and also to get user inputs illegally. For example credit card number, email id, account number etc.; Another challenge of

proposed system is to explore user behavior by using apriori algorithm.

II. EXISTING SYSTEM

The existing system more problematic to evaluate the web access logs and cannot understand the user navigation accurately. In some cases, existing system did not support organization to aim right consumers. The most importantly it does not provide protected environment to customer so this system may allow intruders and it tolerates to fetch weblog records illegally it means intruders collect web log records without knowledge of webmaster. The main difficulties of standing system is as follows:

- The existing system is not efficient
- This system does not provide protected environment
- This system may allow intruders
- Very difficult to analyze user navigation and web structure

III. PROPOSED WORK

The proposed system is User Navigation Guard Approach and it affords user to works in protected environment. UNG Approach provide protection for web log record and kick out intruder from web log record. This system is more efficient than existing system and because the proposed system expending Apriori algorithm to find user navigation details and also to filter user interest that services product based organization to recognize the demand of certain products with the benefit of web usage mining technique. This Methodology brings the improvement within the exactitude of the pages that exposed to the client or users. When a user interacts with the web, their navigation pasts save in zone like a container called as web log. Web logs hold evidence of user's navigation details or user communication evidence from the web. The advantages of planned system is as follows:

A. User Navigation Guard Approach and Recommendation Process

The proposed system is User Navigation Guard Approach and it protects user from attacks or protects web server from intruder. Once the attack detected by the UNG at the identical time the data automatically encrypted which is maintained by webmaster from web record to identify the demand of products. By using AES Algorithm data will be encrypt data when intruder enters and data decrypt automatically when admin logged into their account.

B. Proposed System Architecture

The proposed system architecture shows in Figure:1 is protected under User Navigation Guard Approach and it acts as safeguard. UNG Approach protects users from intruder who can fetched data illegally by without knowledge of webmaster. This paper describes how to filter user interest from web logs and how to protect weblog details from intruders. Protecting weblog from intruders is the big challenge. The proposed approach helps user to feel safe while using E-Commerce websites. And it contains two algorithms, one is Apriori Algorithm it helps to fetch and filter user details depending upon their interest or recommendation process shows in Figure:2. Second one is AES Algorithm, it helps to protect data from intruders and it acts as safeguard. AES algorithm performed as major role in this paper because protecting data is the main process. Recommendation process helps user to search products depending on their interest and at the same time user navigation details recorded into the web record. By using this web record, which is, contains user navigation details webmaster have a chance to fetch data from web record and it helps webmaster to identify the demand of products. And webmaster can filter user interest from fetched data from web record by using apriori algorithm technique and to catch the demand of certain products.

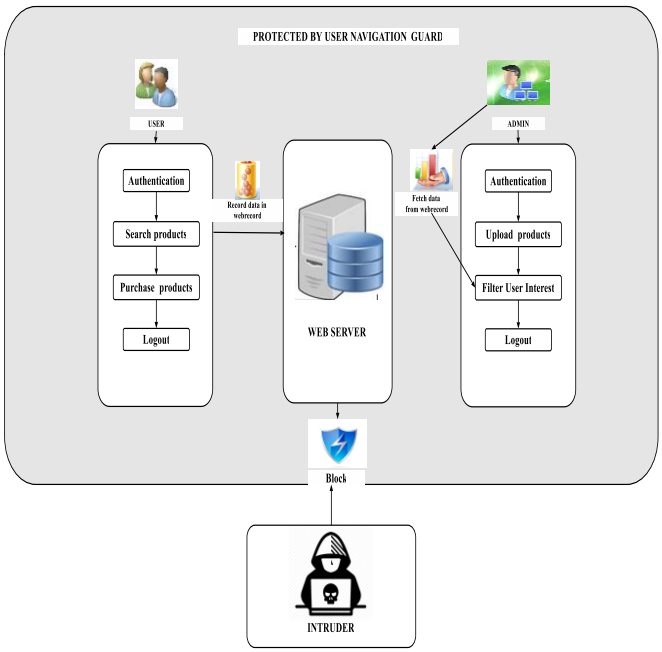

Figure 1. Proposed System Architecture

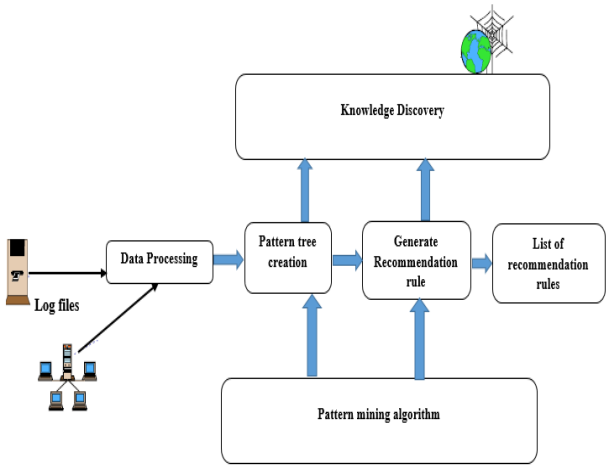

Figure 2. Recommendation Process

IV. RELATED WORK

Ajith Abraham [1] The rapid e-commerce growth has made both business community and customers face a new situation. Due to intense competition on the one hand and the customer's option to choose from several alternatives, the business community has realized the necessity of intelligent marketing strategies and relationship management. Web usage mining attempts to discover useful knowledge from the secondary data obtained from the interactions of the users with the Web. Web usage mining has become very critical for effective Web site management, creating adaptive Web sites, business and support services, personalization, network traffic flow analysis and so on. This paper presents the important concepts of Web usage mining and its various practical applications. Further a novel approach called \intelligent-miner" (i-Miner) is presented. i-Miner could optimize the concurrent architecture of a fuzzy clustering algorithm (to discover web data clusters) and a fuzzy inference system to analyze the Web site visitor trends. A hybrid evolutionary fuzzy clustering algorithm is proposed to optimally segregate similar user interests. The clustered data is then used to analyze the trends using a Takagi-Sugeno fuzzy inference system learned using a combination of evolutionary algorithm and neural network learning. Proposed approach is compared with self-organizing maps (to discover patterns) and several function approximation techniques like neural networks, linear genetic programming and Takagi Sugeno fuzzy inference system (to analyze the clusters). The results are graphically illustrated and the practical significance is discussed in detail. Empirical results clearly show that the proposed Web usage-mining framework is efficient.

Clemens Scott Kruse[1], Brenna Smith[1], Hannah Vanderlinden[1], Alexandra Nealand[1] [2] The privacy of patients and the security of their information is the most imperative barrier to entry when considering the adoption of electronic health records in the healthcare industry. Considering current legal regulations, this review seeks to analyze and discuss prominent security techniques for healthcare organizations seeking to adopt a secure electronic health records system. Additionally, the researchers sought to establish a foundation for further research for security in the healthcare industry. The researchers utilized the Texas State University Library to gain access to three online databases: PubMed (MEDLINE), CINAHL, and ProQuest Nursing and Allied Health Source. These sources were used to conduct searches on literature concerning security of electronic health records containing several inclusion and exclusion criteria. Researchers collected and analyzed 25 journals and

reviews discussing security of electronic health records, 20 of which mentioned specific security methods and techniques. The most frequently mentioned security measures and techniques are categorized into three themes: administrative, physical, and technical safeguards. The sensitive nature of the information contained within electronic health records has prompted the need for advanced security techniques that are able to put these worries at ease. It is imperative for security techniques to cover the vast threats that are present across the three pillars of healthcare.

David S. Wall [3] The critical importance of electronic information exchanges in the daily operation of most large modern organizations is causing them to broaden their security provision to include the custodians of exchanged data – the insiders. The prevailing data loss threat model mainly focuses upon the criminal outsider and mainly regards the insider threat as 'outsiders by proxy', thus shaping the relationship between the worker and workplace in information security policy. A policy that increasingly takes the form of social policy for the information age as it acquires the power to include and exclude sections of society and potentially to re-stratify it? This article draws upon empirical sources to critically explore the insider threat in organizations. It looks at the prevailing threat model before deconstructing ' the insider ' into various risk profi les, including the well-meaning insider, before drawing conclusions about what the building blocks of information security policy around the insider might be.

Dhanant Subhadrabandhu[1], Saswati Sarkar[1], and Farooq Anjum[2][4] Detecting intrusions in wireless ad hoc networks using the misuse detection technique. It allow for detection modules that periodically fail to detect attacks and also generate false positives. Combining theories of hypothesis testing and approximation algorithms, we develop a framework to counter different threats while minimizing the resource consumption. We obtain computationally simple optimal rules for aggregating and thereby minimizing the errors in the decisions of the nodes executing the intrusion detection software (IDS) modules. But, we show that the selection of the optimal set of nodes for executing the IDS is an NP-hard problem. We present a polynomial complexity selection algorithm that attains a guarantee able approximation bound. We also modify this algorithm to allow for seamless operation in time varying topologies, and evaluate the efficacy of the approximation algorithm and its modifications using simulation. We identify a selection algorithm that attains a good balance between performance and complexity for attaining robust intrusion detection in ad hoc networks.

Fukun BI[1], Chong FENG[1], Hongquan QU[1*], Tong ZHENG[1], and Chonglei WANG[2][5] At present, advanced researches of optical fiber intrusion measurement are based on the constant false alarm rate (CFAR) algorithm. Although these conventional methods overcome the interference of non-stationary random signals, there are still a large number of false alarms in practical applications. This is because there is no specific study on orthogonal polarization signals of false alarm and intrusion. In order to further reduce false alarms, we analyze the correlation of optical fiber signals using birefringence of single-mode fiber. This paper proposes the harmful intrusion detection algorithm based on the correlation of two orthogonal polarization signals. The proposed method uses correlation coefficient to distinguish false alarms and intrusions, which can decrease false alarms. Experiments on real data, which are collected from the practical environment, demonstrate that the difference in correlation is a robust feature. Furthermore, the results show that the proposed algorithm can reduce the false alarms and ensure the detection performance when it is used in optical fiber pre-warning system (OFPS).

V. CONCLUSION

User Navigation Guard Approach is a safeguard which is used to exchange information between two parties over an unconfident network. Cryptography techniques offers extensive range of algorithms to guard such communications so that information can be spread securely over the network and provide authentication, data integrity, privacy and non-repudiation. This paper propose a User Navigation Guard which is protects users from intruders in insecure network by using AES Algorithm. And also enhance the web record exploration from weblog using Apriori Algorithm. This paper discover new techniques to explore and protects data from webrecord.

VI. REFERENCES

[1] Ajith Abraham, "Business Intelligence from Web Usage Mining", Journal of Information & Knowledge Management Vol. 2, No. 4, pp.375-390, 2003.

[2] Clemens Scott Kruse[1], Brenna Smith[1], Hannah Vanderlinden[1], Alexandra Nealand[1] "Security Techniques for the Electronic Health Records", J Med Syst, pp. 1-9, 2017.

[3] David S. Wall "Enemies within: Redefining the insider threat in organizational security policy", Security Journal, Vol. 26, 2, pp. 107–124, 2013.

[4] Dhanant Subhadrabandhu[1], Saswati Sarkar[1], and Farooq Anjum[2], "RIDA: Robust Intrusion Detection in Ad Hoc Networks", IFIP International Federation for Information Processing, pp. 1069–1082, 2005.

[5] Fukun BI1, Chong FENG1, Hongquan QU1*, Tong ZHENG1, and Chonglei WANG2 "Harmful Intrusion Detection Algorithm of Optical Fiber Pre-Warning System Based on Correlation of Orthogonal Polarization Signals", Photonic SensorsVol. 7, No. 3, pp. 226–233, 2017.

[6] Hassan Artail*, Ammar El Halabi, Ali Hachem and Louay Al-Akhrass, "A framework for identifying the linkability between Web servers for enhanced internet computing and E-commerce", Journal of Internet Services and Applications, pp. 1-19, 2017.

[7] Nikolaos Pitropakis1*, Dimitra Anastasopoulou1, Aggelos Pikrakis2 and Costas Lambrinoudakis1 "If you want to know about a hunter, study his prey: detection of network based attacks on KVM basedcloud environments", Journal of Cloud Computing: Advances, Systems and Applications, pp. 1-10, 2014.

[8] Peter Galdies "Business Intelligence The insider threat to data assets" Journal of Direct, Data and Digital Marketing Practice VOL. 15 NO. 3 PP 197–200 2014.

[9] Roey Tzezana1, "Scenarios for crime and terrorist attacks using the internet of things", Blavatnik Interdisciplinary Cyber Research Center at Tel Aviv University, pp. 1-7, 2016.

[10] Rongmao Chen*, Yi Mu, Senior Member, IEEE, Guomin Yang, Member, IEEE, Fuchun Guo, Xinyi Huang, Xiaofen Wang and Yongjun Wang, "Server-Aided Public Key Encryption with Keyword Search", IEEE Transactions on Information Forensics and Security, pp. 1-10, 2016.

[11] Samiksha Sharma and Vinay Chopra Data Encryption using Advanced Encryption Standard with Key Generation by Elliptic Curve Diffie-Hellman International Journal of Security and Its Applications Vol. 11, No. 3, pp.17-28, 2017.

[12] SHE Chundong1, MA Yaqi1, JIA Luting1, FEI Ligang2, KOU Baohua2 "Intrusion-detection model integrating anomaly with misuse for space information network", Journal of Communications and Information Network Vol.1, No.3, pp. 91-96, Oct. 2016.

[13] Tzvi Chumash and Danfeng Yao, "Detection and Prevention of Insider Threats in Database DrivenWeb Services", IFIP International Federation for Information Processing, pp. 117–132, 2009.

[14] Veeran Ranganathan Balasaraswathi*, Muthukumarasamy Sugumaran, Yasir Hamid "Feature selection techniques for intrusion detection using non-bio-inspired and bio-inspired optimization algorithms", Journal of Communications and Information Networks, Vol.2, No.4, pp. 108-119, Dec. 2017.

[15] Xiaokui Shu, Jing Zhang, Danfeng (Daphne) Yao, *Senior Member, IEEE*, and Wu-Chun Feng, *Senior Member, IEEE* "Fast Detection of Transformed Data Leaks", IEEE transactions on information forensics and security vol. 11, no. 3, pp. 528-542, Jan. 1979, March 2016.