Nat. Volatiles & Essent. Oils, 2021; 8(4): 5202-5212

Design Of Intrusion Detection System For Web-Based System Using Deep Learning Technique

Naresh E[1], Chaitra H V[2], Kadiri Thirupal Reddy[3*]

[1]Assistant Professor, Department of Information Science and Engineering, M S Ramaiah Institute of Technology, Bangalore, INDIA. nareshkumar.e@gmail.com

[2]Associate Professor, Department of Computer Science and Engineering, Nitte Meenakshi Institute of Technology, Bangalore, INDIA. chaitra.nan@gmail.com

[3]Associate Professor, Bharat Institute Of Engineering And Technology, Hyderabad, India. k.thirupalreddy2009@gmail.com

Abstract–In today's world internet is being accessed by a very huge population, but they are prevented from various access domains. When communication takes place between the various clients and servers, the activity is tracked and every detail is observed where the user login, logout, communication, data search, and various other such features are recorded and stored for further analysis. Security is a major concern in this domain as there are various threats including privacy intrusion, hacking etc. Feedback is an important aspect in today's world that helps in evaluating the need of the user and helps in improving the overall user experience. The opinions are taken in the form reviews and they are evaluated and implemented. This would help to increase the recommendations by people and hence leads to exponential increase in the product usability and transaction ability. For every request to the server in the form of navigation request etc. a session tracking is performed and the behavior based files are generated.

Keywords: Intrusion Detection,Log File, Deep learning, Denial of Service, Cyber Crimes, Data mining, Least Common SubSquare Method

1. Introduction

Cyber Security is that part of Computer Technology that manages security in the internet. The internet alludes to the depiction of approaches with respect to the systems and PC frameworks. The approaches spread out in the Cyber security are for the explanation of maintaining a strategic distance from the vindictive movement or unapproved access to verified data. Since the development of high organized systems, there emerges a worry about how brilliantly these systems are verified. Digital alludes to

something that should be possible on web. Wrongdoing alludes to something that is done wrongfully or without approval. Each one of those violations that are done on the web so as to access verified data or approval rights is named as ''Cyber Crime''.

2. Objectives of Project

The first objective is to track each button click as well as the navigation patterns of the users for each session and then obtain the habits of the user.The second objective of the project is to classify the user for a given set of sessions into denial service of attacks and non-denial of service attacks.The third objective of the project is to block the user for a certain period of time to avoid any kind of operations.

3. Literature Survey on Design of Intrusion Detection System for Web-Based System Using Deep Learning Technique

Reference to the work [1] the authors describe the security related topics for the network administrator's network security administrator or professional assemble the technical tools needed to build, maintain, analyze, and learn from a honey net within their organization.

In any company 2 kinds of user - IT team, Management/Develop/Testing team. For access to the resource's certain application s time management, Income Tax etc, there will be roles created. This paper talks about a centralized system which maintains the roles and assigns those roles to specific user. User cannot access all applications and security is improved. There is separate role for set of actions to be performed

It can be applied to only internal users and for external users this has to be extended to have licensing concept .It is applied here for desktop applications and not web applications

In the paper [2] the authors describe that a review of various detection techniques from datamining perspective. Existing studies in data mining focus generally on finding patterns from large datasets and using it for organizational decision making. However, finding outliers did not receive much in the data mining field as other topics received.

In this paper we are obtaining the sales logs.The data is plotted in the format of number of times a product has been purchases versus the product ids.From this plot a linear line is drawn and then products are classified into low selling stock and high selling stock. This data helps the retail organization in order to advertise low selling products

Advantages areWe can come to conclusions related to increase in the revenue of the retail application. We capture the information of purchases made by the user. User Specific recommendation are not given which can increase the revenue. The execution of the algorithm has to be done manually when the

server is not in use during an offline period so that load is less on the server because data set that is considered is across all users

Reference to the paper [3] the authors describe thatSystem traffic can be considered as a limitless information stream. In this way, our information digging approach is particular for mining stream information. There are two significant issues identified with stream information arrangement. To begin with, it is unreasonable to store and utilize all the verifiable information for preparing, since it would require unbounded stockpiling and running time. Second, there might be idea float in the information. For instance, with regards to bot nets, the bot ace for the most part refreshes the bot programming every now and again, which may change the qualities of bot net traffic, bringing about an idea float in the information. In the event that there is an idea float in the information, we have to refine our theory to oblige the new idea. In this manner, the greater part of the old information must be disposed of from the preparation set. There are two standard strategies accessible for stream information grouping: single classifier approach, and gathering classifier approach.

- Monitoring of traffic - IPAddress, How many users are access specific , time
- Huge -- Segmentation real time monitoring
- Take the history of previous access logs
- 5 months previous history is taken out
- Find out from the historic data set specific functionaries which has been in use for huge amount of then
- From the historic data we come to know a metric

On reference of paper [5] the authors describe that Forswearing of administration assault allows the gatecrashers to get to the system benefits in this way forestalling the authentic clients to get to the administrations. To defeat the deficiencies of the DoS assault, it is exceptionally fundamental to plan an interruption discovery framework. Interruption recognition framework (IDS) is programming that works as a system security instrument to shield the PC organize framework from assaults. With expanding number of information being transmitted bit by bit starting with one system then onto the next, the IDS recognize the interruptions in such huge datasets adequately. Information mining is a productive device applied to diagram the interruption recognition framework and keep the monstrous system information from the gatecrashers. Anomalies are designs in information that don't match to a well-characterized idea of ordinary conduct.

To the Reference of the paper [6] the authors the most decimating impacts on IT security have different online assaults. Security specialist have gigantic weights additionally included in order to safe guard arrangements.Henceforth, it gets crucial to do these assaults in little test conditions so as to compensate them better. These ongoing assaults are estimated and investigated utilizing traffic screens. Notwithstanding that, this venture likewise subtleties different systems that can be implemented on switches so as to relieve these assaults.

In the paper [10] the authors describe that administration determination for programmed dynamic assistance piece with customer's prerequisites situated help choice turns out to be increasingly extreme. The current arranging and determination calculations are for the most part intended for administration revelation. Further, as far as anyone is concerned, there are just a couple of works that join end-client prerequisites into administration organization.

With expanding number of information being transmitted bit by bit starting with one system then onto the next, the IDS recognize the interruptions in such huge datasets adequately. Information mining is a productive device applied to diagram the interruption recognition framework and keep the monstrous system information from the gatecrashers. Anomalies are designs in information that don't match to a well-characterized idea of ordinary conduct.

4. PROPOSED METHODOLOGY

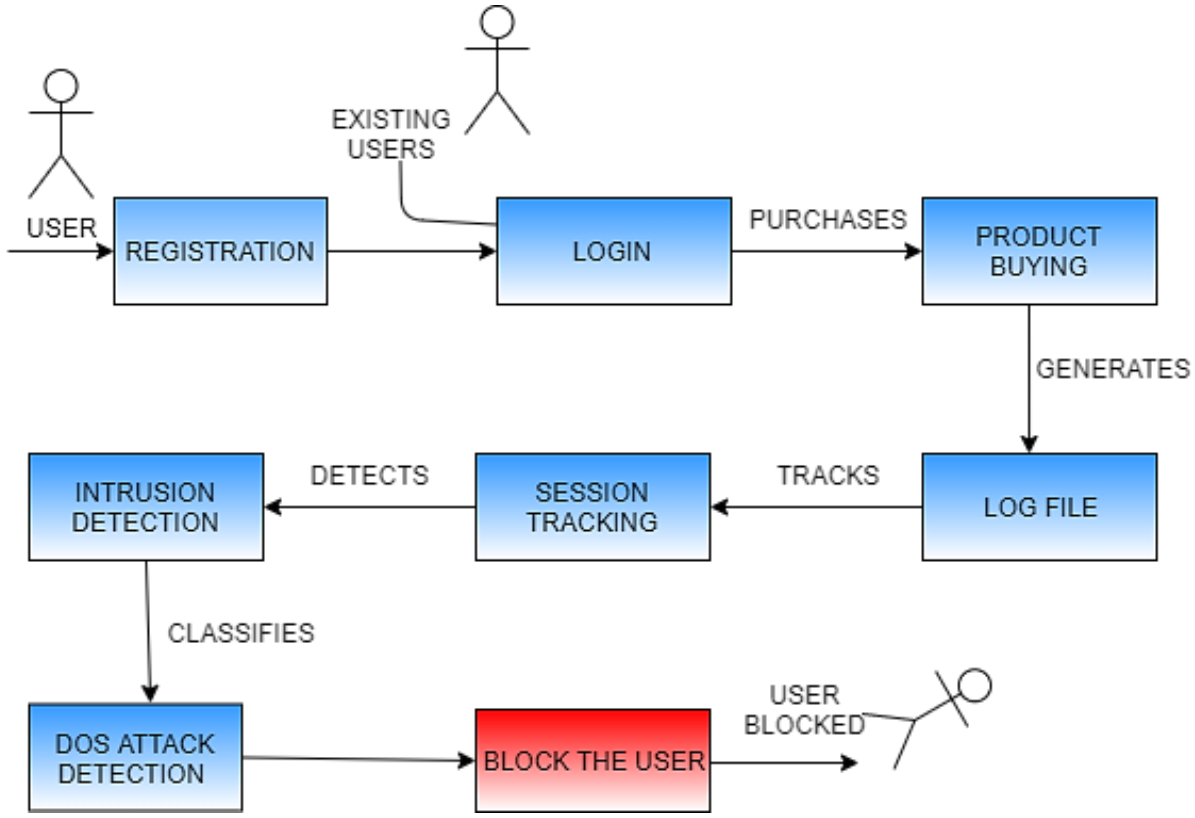

Fig 1.1 Proposed Methodology

The methodology of the research can be defined as follows:

Registration

This Module is responsible for allowing any external customer to perform the registration by proving the details like First Name, Last Name, User Id, Password, Email, City, State and Country. If the user id already exists then user is not allowed to register as shown in figure 1.1.

Login

Login Module is responsible for allowing the user to access the user with valid credentials and deny the access for user with invalid credentials. The Users are of two kinds one is Admin and other is Customer. If it is Admin then he/she can see the habitat file for each session of the users using the application which has the session tracking, Find Suspicious pattern using LCS and Detect Dos Attack. If it is customer then he/she can purchase product and then get the recommendations

Product Buying

Product Buying is responsible for purchasing the products by providing the valid IPIN and Account No. If the credentials are valid and also user has sufficient balance then product is purchased and then two important information's are tracked namely Order Information and Order Details. The Order information can be described as below

Session Tracking and Habitat File

Table1.1 Order information

Name	Description
ORDERID	Unique ID representing the Order and acts like the primary key
LOGINID	Login ID of the user
ORDERDATE	The Date of purchase
TOTALAMOUNT	Total Transaction Amount
Email	Email Id of the Logged in User

In this module whenever clicks on the link or clicks on the button or user navigates from one page to another page each time independent request is made and tracked based on the user id and session id. The habitat file is set of records which are set of actions performed by the user in each session.

Table1.1 Order information

Name	Description
ORDERID	Unique Order Id and acts like a primary key. The ORDERID of Order Details and Order Information are maintained in sync
PRODUCTID	The id of the product which is being purchased
QUANTITY	The quantity of the product purchased in a single transaction

Intrusion Detection using LCS

This module is responsible for taking a set of patterns and finds the LCS for each of the pattern. The pattern refers to one habitat of the user for specific session. If the LCS is new as compared to previous activities then the pattern is regarded as intrusion.

Dos Attack Detection

This Module is responsible for finding the Dos Attacks over a period of window by measuring the frequency of the actions performed by the user and then ranking based on the highest frequency of steps.

In this module whenever clicks on the link or clicks on the button or user navigates from one page to another page each time independent request is made and tracked based on the user id and session id. The habitat file is set of records which are set of actions performed by the user in each session.

Block The User

The users are classified based on the outcomes and Blocked until admin decides to unblock the user.

System Architecture

The following figure shows the System Architecture of the project. As shown in the fig first an application is needed in order to implement the Audit and in this case we consider the access to application with internal functions as well as external functions. Event Computation is a process in which each action of the user in the application is captured based on action name and user id. The action name can be button click, URL click or some other actions.

SYSTEM ARCHITECTURE

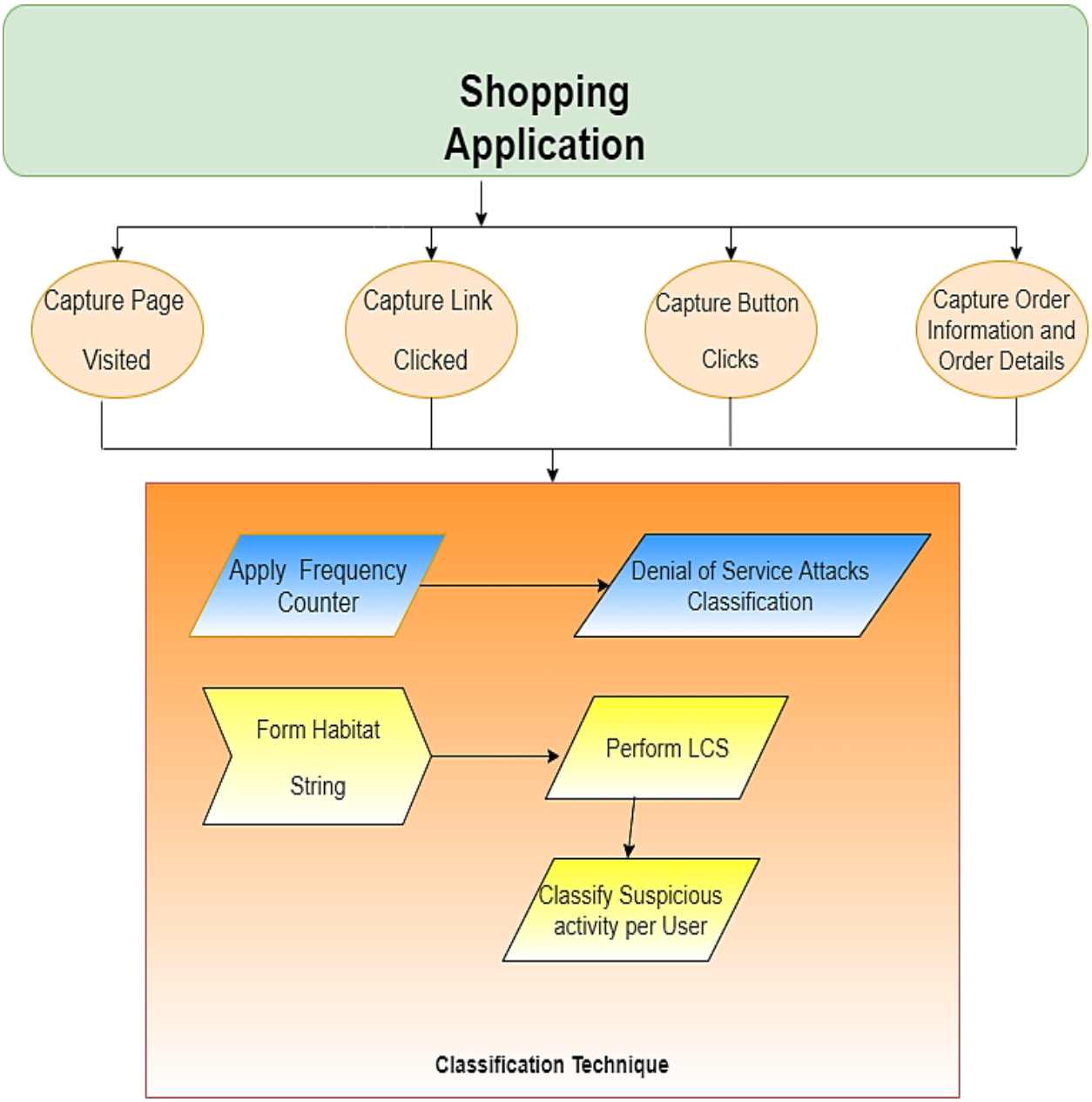

Fig1.2 Proposed System Architecture

Mathematical Equation

The weight computation is given by

$$W_{ij} = \frac{f_{ij}}{f_{ij} + 0.5 + \frac{1.5 ns_j}{ns_{avg}}} \quad \frac{\log(\frac{N + 0.5}{M_i})}{\log(N + 1)}$$

$$i = 1,2,3,4,.....k$$

$$j = 1,2,3,4,.....N$$

Where,

$f_{ij} = frequency\ of\ apperance\ of\ Command / Action$

$ns_j = total\ number\ of\ patterns\ of\ user$

$ns_{avg} = average\ number\ of\ patterns\ across\ users$

$M_i = Number\ of\ user\ patterns$

Comparison of Existing with Proposed approach

- The previous approach does not take into consideration the set of actions which the user performs and track them where as the proposed approach will track each user action and navigation patterns to track the user behavior over a period of time.

- The previous approach does not take session specific user behavior over a period of time whether the proposed approach does that.

Proposed Approach

In the proposed approach the data mining techniques namely association rule mining and clustering algorithms are applied on the log file of the web application and then a grouping is made of the user who is trying to do the denial of service attacks. Denial of service attacks is an attack which brings the system down after huge number of same repetitive requests are made to the application.

5. Applications of Project

- The DOS attacks identification based on the session tracking can be used in any kind of applications like banking.
- It can be used in any ecommerce websites.
- It can be used in railway reservation system
- Food ordering apps can implement this method to track the intruders

6. Limitations of the Work

- It can be applied to only internal users
- For external users this has to be extended to have licensing concept
- It is applied here for desktop applications and not web applications

7. Future Enhancement

- The application can be extended for various categories of products rather than just books of various categories.
- The application can perform recommendations based on the amount used within the month by the end user for various purchases.
- The application can be extended to protect itself from Cross Site Scripting attack and SQL injection attacks.

References

1. Ibrahm Salim, T.A.Razzack,"A study on IDS for Preventing denial of service attack using outliers techniques", March 2016, 2nd IEEE international conference on Engineering and technology.
2. Klen, F. Ishikawa and S. Honidem, "Efficient heuristic approach with improved time complexity for qos-aware service composition", IEEE, 2011.
3. Tripathy and M.Khan,"Dynamic web service composition with QoS clustering", 2014, IEEE, International Conference on Web services.
4. Jonathon Ng and Depti Joshi,"Applying Data Mining Techniques to IntrusionDetection", IEEE, 2015.
5. D. Sophia Navi Mary, "An Algorithm for Moderating Dos Attack In Web Based Application",2017, IEEE.
6. YongJon Park, "Web Application Intrusion Detection System for Input Validation Attack",2018, IEEE.
7. Anup K. Ghosh,"Automating Intrusion Response via Virtualization for Realizing Uninterruptible Web Services", 2016,IEEE.
8. Tan Chunhuui, "Research of Intelligent Intrusion Detection System Based on Web Data Mining",IEEE,2018.
9. JaeChul Park, "Web Application Intrusion Detection System for Input Validation Attack" , 2018, IEEE.

10. Rajani Muralidharan, “Cross Layer Denial of Service attacks in Wireless Sensor Network Using Swarm Intelligence”, Princeton University, IEEE, 2014.
11. Subramani Rao, “Denial of Service attacks and mitigation techniques”,Real time implementation with detailed analysis, SANS Institute, 2015
12. Simona Ramanauskaite, “Composite DoS Attack Model”, ISSN 2029-2341 print / ISSN 2029-2252 online, 2012.
13. R.Jagannathan,and R.Lee, “A Real-Time Intrusion-Detection Expert System”, Number SRI-CSL-88,2015.
14. S.J. Stolfo,“Data Mining Approaches for Intrusion Detecion”, 7th USENIX Security Symposium, 2018.
15. Lee, Wenke, S.J. Stolfo, and KuiW Mok,“A data mining framework for building intrusion detection models”,Security and Privacy, IEEE, 2009.
16. W.Lee, “A framework for constructing features and models for intrusion detection systems”,ACM Transaction on Information and System Security, 227-261, November 2014.
17. Z.A. Othman and A. Bakar,“Improving signature detection classification model using features selection based on customized features”, Intelligent Systems Design and Applications,November,2014.
18. Al-Jarrah and A. Arafat, “Network Intrusion Detection System using attack behavior classification”, pp.1 -6, 2013.
19. Z. Wanlei,“Detection of and Defense Against Distributed Denial-of-Service (DDoS) Attacks”, IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2013.
20. Beniwal, Sunita, and Jitender Arora,“Classification and feature selection techniques in data mining”, International Journal of Engineering Research and Technology, Vol. 1, 2012.
21. Neha, G. Relan and D.R. Patil, “Implementation of network intrusion detection system using variant of decision tree algorithm”, International Conference in Nascent Technologies, 2015.