Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 05, May -2018

DETECTION OF CYBER CRIME BY DATA MINING TECHNIQUE

Prof. Rukaiya Shaikh[1] , Aman Memon[2] , Manoj Kumar[3] , Ismaeil Pathan[4]

[1] *Department of Computer Engineering, Al-Ameen College of Engineering, Koregaon Bhima, Pune, India*
[2] *Department of Computer Engineering, Al-Ameen College of Engineering, Koregaon Bhima, Pune, India*
[3] *Department of Computer Engineering, Al-Ameen College of Engineering, Koregaon Bhima, Pune, India*
[4] *Department of Computer Engineering, Al-Ameen College of Engineering, Koregaon Bhima, Pune, India*

Abstract —*This Nowadays internet is accessed by number of peoples all over the world. The client and server communicates with each other by exchanging messages among each other. The activity of exchanging can be observed by Log files. Log files include the detailed description of activities that occur over internet. It shows the IP address, login and logout durations, etc. There are many attacks that occur over internet but our focus is on the Dos attack. The Denial of Service attack is identified by one of Data mining technique called pattern recognition. DoS attack is one of the dangerous attack which overload the server by sending multiple messages or requests from unknown users. We have built a system in which DoS attack is detected and described under this paper.*

Keywords- *Cyber Crime, Data Mining, Data Collection, Denial of Service, SQL Injection attack, U2R attack, Log File, Data mining techniques.*

I. INTRODUCTION

In computing, a denial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected. Victims of DoS attacks often target web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations. Though DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle. There are two general methods of DoS attacks: flooding services or crashing services. Flood attacks occur when the system receives too much traffic for the server to buffer, causing them to slow down and eventually stop.

DoS – denial of service «A denial of service (DoS) is an action that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as central processing units (CPU), memory bandwidth, and disk space.

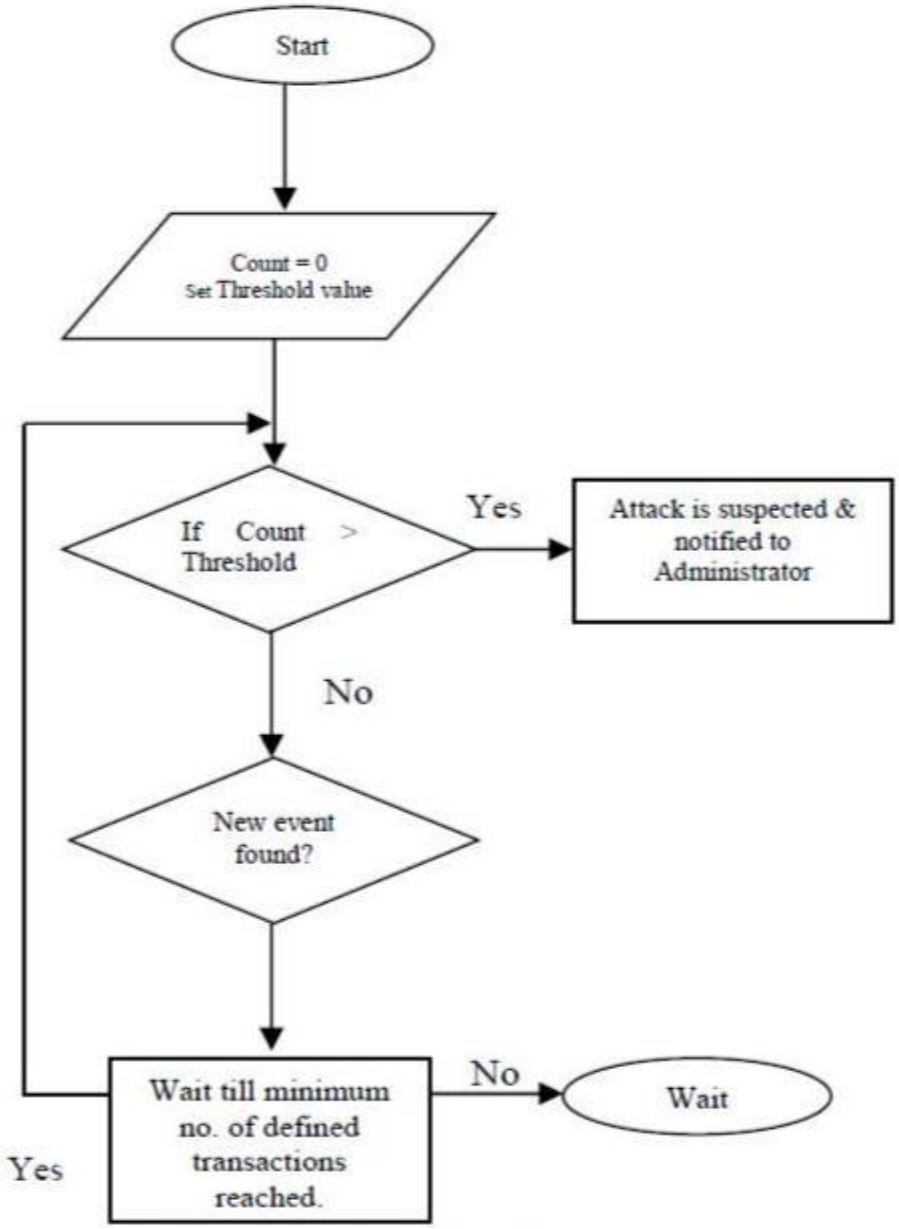
Categories of resources which can be attacked: network bandwidth, system resources, application resources .
Typical aims of DoS attacks:

1. Consuming bandwidth with large traffic volumes
2. Overload or crash the network handling software
3. Send specific types of packets to consume limited available resources Risk & Security Management – DoS Attacks

II. RELATED WORK

In this system we have detected the Denial-of-Service attack. We have also prevented some other cyber attacks like SQL Injection attack and U2R attack. In this system we have used famous data mining technique called as pattern recognition on the log file. We set a threshold value. If the number of similar requests are received at the server, which is greater than the threshold value, we assume this as an attack and the administrator is been informed. By this approach we can identify the denial of service attack easily as in DoS attack, the attacker or the hacker sends same multiple requests in order to mitigate the server performance.

III. PROPOSED ALGORITHM



- Step 1: Start
- Step 2: Let the Count=0, set the threshold value. The threshold value can be set based on the working environment.
- Step 3: Check if the counts of matched rules have crossed the threshold value. • If true, intimate the administrator assuming as an attack. • If false, continue.
- Step 4: Check whether new event is recorded in log file.
- Step 5: If no new event found, wait If event_found, go to step 2.

IV. SIMULATION RESULTS

The below fig shows the result of the system. In below Fig the attack is detected and displayed to the Administrator.

Fig :- Home Page

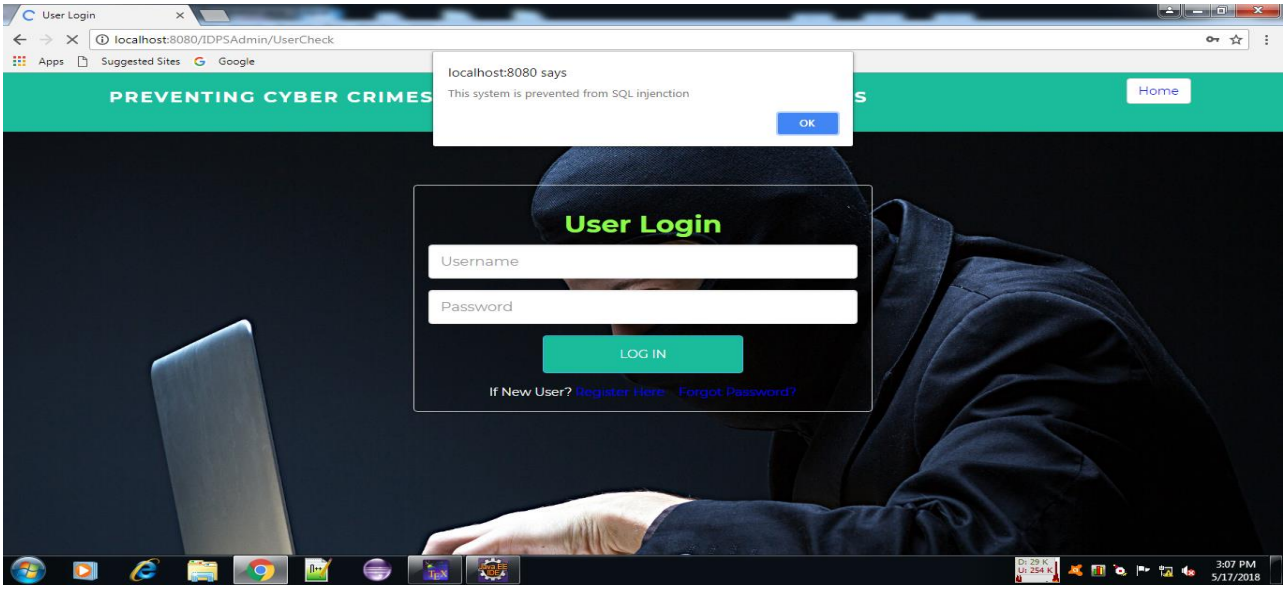


Fig :- SQL Injection Attack Detected

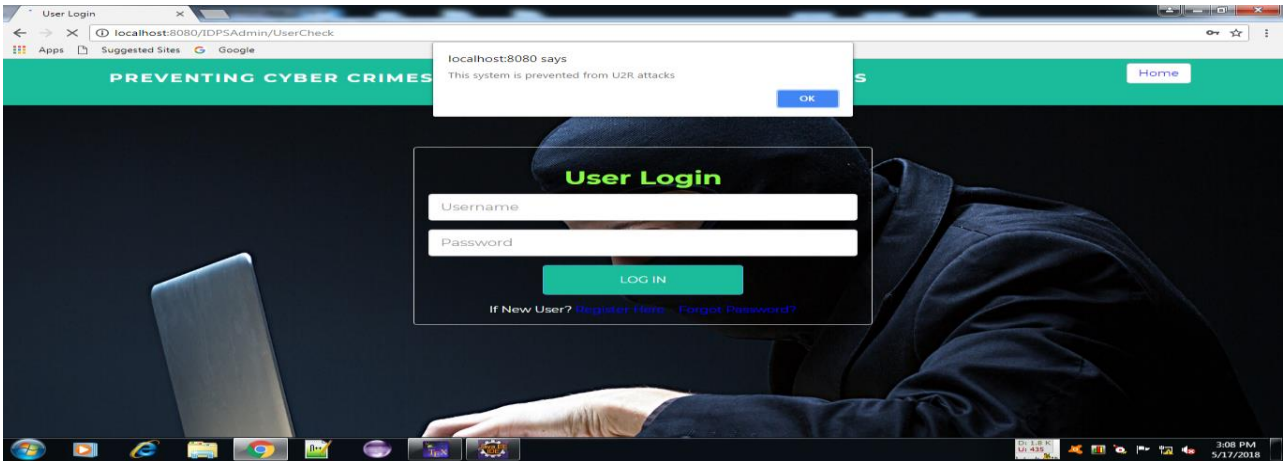


Fig :- U2R Attack Detected

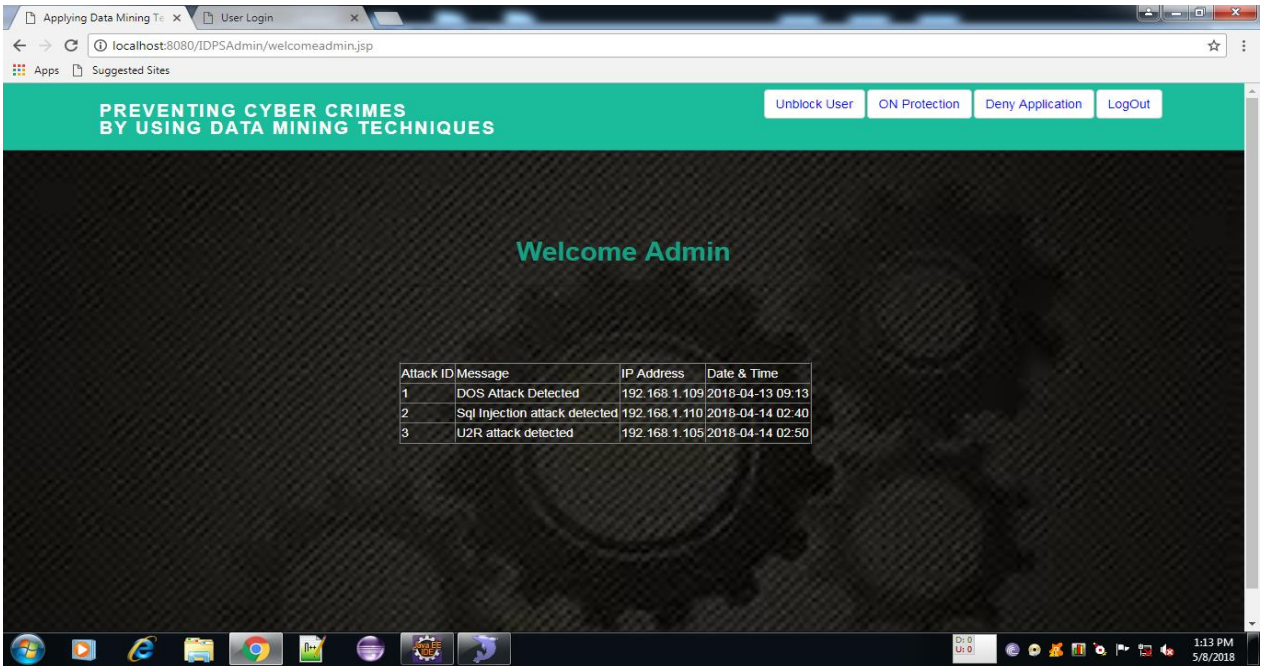


Fig :- DoS Attack Detected

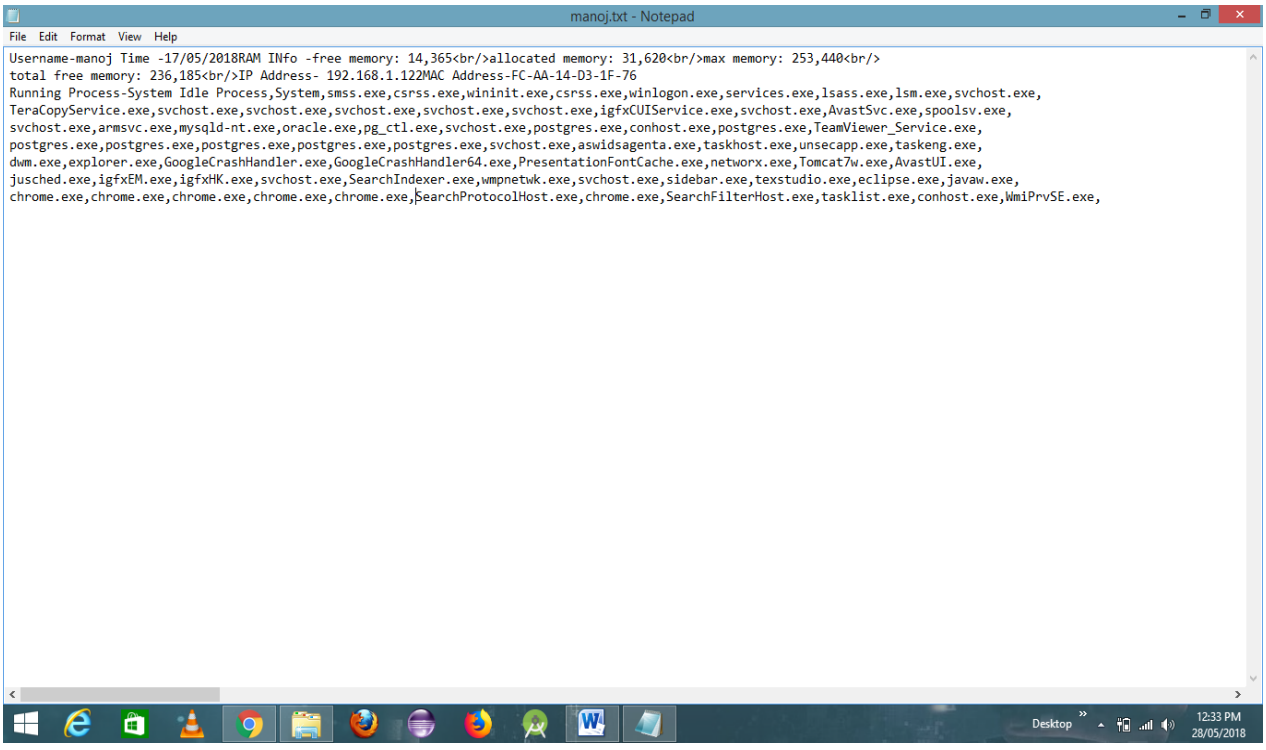


Fig :- Log File

V. CONCLUSION AND FUTURE WORK

In this system we have applied the data for detecting dos attack. The attack is very dangerous as it can overload the server. Our system successfully detect the dos attack and turn off the server so as to secure the data. The intruder can easily the access data as server is overloaded (i. E hanged or may be slow) so to secure the informaton of the clients the server get shut down . In this system we have also prevented some other cyber attacks like SQL Injection attack and U2R attack. In future the image of the intruder can also get captured through web cam by using the above technique.

REFERENCES

1. Know Your Enemy: Learning About Security Threats, 2nd Edition.ISBN: 0321166469. The Honeypot Project 2004.
2. M.Khan, S.K.Pradhan, M.A.Khaleel, "Outlier Detection for Business Intelligence using data mining techniques", International journal of Computer Applications (0975 -8887), Volume 106- No. 2, November 2014.
3. Masud, M.M, Gao,J.Khan, "Peer to Peer Botnet Detection for Cyber Security: A Data Mining Approach". In proceedings: Cyber-security and information Intelligence research workshop. Oakridge national Laboratory, Oakridge May 2008.
4. Internet Security Threat Report, Volume 21, April 2016, Symantec Crime Report.
5. Ibrahim Salim, T.A.Razzack,"A study on IDS for Preventing denial of service attack using outliers' techniques", 2nd IEEE international conference on Engineering and technology, March 2016.
6. S.S Rao, SANS Institute Infosec Reading Room." Denial of service Attack and mitigation techniques: Real time implementation with detailed analysis", 2011.
7. Data Mining: Concepts and Techniques, Third Edition, Jiawei Han and Micheline Kamber, ISBN-13, 9780123814791.
8. Mining of Massive Data Sets, Anand Rajaraman, Jure Leskovec, Jeffrey D. Ullman,2014
9. A. Klein, F. Ishikawa, and S. Honiden. Efficient heuristic approach with improved time complexity for qos-aware service composition. In ICWS, pages 436–443. IEEE, 2011.
10. Tripathy, M.Khan, M.R.Patra, H.Fatima, P.Swain, "Dynamic web service composition with QoS clustering" IEEE, International Conference on Web services, 2014.
11. D. E. Brown, "The regional crime analysis program (RECAP 1998) : A Frame work for mining data to catch criminals," in Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics, Vol.3, pp.2848-2853
12. IEEE proceedings Rushinek, A, Rushinek, SF (1993). "Using Experts for Detecting and Litigating Computer Crime". Managerial Auditing Journal. 8.7:19-22. Security Focus. Florida.
13. Anshu Sharma, Shilpa Sharma, An Intelligent Analysis of web Crime Data Using Data Mining, International Journal of Engineering and Innovative Technology, 2012.
14. S. Yamuna, N. Sudha Bhuvaneswari, Data Mining Technique to Analyse and Predict Crime, The International Journal of Engineering And Science, 2012.
15. Malathi. A, Dr. S. Santhosh Baboo, Anbarasi. A, An Intelligent Analysis of a City Crime Data Using Data Mining, Internation Conference on Information and Electronics Engineering, 2011
16. Devesh Bajpai, Emerging Trends in Utilization of Data Mining in Criminal Investigation: An Overview, Journal of Environmental Science, Computer Science and Engineering & Technology, 2012
17. R.G Uthra Emerging Trends in Utilization of Data Mining in Criminal Investigation: An Overview, Journal of Data Mining Technique to Analyze Crime Data, International Journal for Technological Research in Engineering , 2013

