CYBER ATTACK DETECTION SYSTEM

Akshay burkure#, Trushali Dhomne*, Abhijit Kapse# , Manoj Chaudhari*
Information Technology Department, RTMNU, Nagpur, Maharashtra
[1]akshayburkure05@gmail.com, [2]trushalidhomne@gmail.com, [3]kapse.abhijit5@gmail.com,
[4]manojchaudhary2@gmail.com

***Abstract*— A cyber-attack is deliberate exploitation of computer system. Cyber attack uses malicious code to alter computer code logic or data. Cyber attack is also known as computer attack where cyber attack is launched through a series of computer actions to compromise the security (e.g. availability, integrity, and confidentiality) of a computer and network system. Hence we are going to develop software that will help to avoid such attack. With the help of this software we can detect attack and prevent over cyber attack. This application can be used by web based server and router server for detecting the network traffic and finding the security attacks like DoS attack. Depending on the attack the user will be allowed for services or user will be blocked. We are developing Online voting website. Now a days many illegal work occur on voting websites like increase or decrease of votes that are given by voters. The intension of attacker could be stilling of information about voters and by using that information attacker can do any illegal work. Cyber attack detection system using Markov Chain application will provide security to online voting server when attack will be happened on server.**

***Keywords*— Detection, Markov chain, Security, Attack, Intrusion.**

I. INTRODUCTION

Cyber-attack detection is used to identify cyber-attacks while they are acting on a computer and network system to compromise the security (e.g., availability, integrity, and confidentiality) of the system [8]. Cyber-attack is launched through a series of computer actions to compromise the security (e.g. availability, integrity, and confidentiality) of a computer and network system. A Cyber Attack is an attack initiated from a computer against another computer or a website, with a view to compromise the integrity, confidentiality or availability of target and the information stored in it [8]. Day today life internet threat has been increased significantly. There is a need to develop model in order to maintain security of system. The most effective techniques are Intrusion Detection System (IDS).The purpose of intrusion system through the security devices detect and deal with it [6].

Our basic aim to make this software is to detect and prevent vulnerability exploits. This software will help to identify cyber attack while they are attacking on server and network system. There are many dangerous attack to which antivirus is unable to handle. For that we can use this software. There are five basic types of attack like Worms, Trojan horse, Viruses, DoS attack and Malware attack. Basically in our project we are dealing with Dos attack.

II. PROBLEM DEFINITION

The internet has brought considerable change to economic transaction ,social interaction and military operation. There are many software available to handle cyber attack problems but many times they are unable to handle dangerous attack. It is very important to develop a web sites with proper security otherwise their may be increase the chances of hacking and stealing the data. Many times problems occur during detection. Proper detection of attack is very important of preventing the data. Cyber attack affect million of internet user result in revenue losses. Denial-Of-Service is one of the most important attacks that a hacker can make in a computer network and exposes the vulnerability in the same.

Anti-virus software slows down PC or network, Installing and running anti-virus software can use up a lot of computer memory and hard disk space, slowing down your computer. With the help of Cyber attack detection system using Markov chain application we are overcoming these problems.

III. LITERATURE SURVEY

A. MARKOV CHAIN

The Markov chain Model is used with the event counter metric to determine the normalcy of a particular event, based on the events which preceded it. The model characterizes each observation as a specific state and utilizes a state transition matrix to determine if the probability of the event is high (normal) based on the preceding events. This model is particularly useful when the sequence of activities is particularly important. This model is basically used in two main approaches: Markov chains and hidden Markov models. A Markov chain keeps track of an intrusion by examining the system at fixed intervals and maintains the record of its state [2].

A Markov chain is a refers to the sequence of random variables such a process moves through, with the Markov property defining serial dependence only between adjacent periods where what happens next depends only on the current state of the system.

B. INTRUSION DETECTION SYSTEM (IDS)

Intrusion Detection System (IDS) monitors network traffic and its suspicious behavior against security. IDS is a set of techniques and methods that are used to detect suspicious activities both at the network and host level. There are two main types of Intrusion Detection System, HIDS and NIDS. Now a day’s potential damage caused by internet attack has increased exponentially, so the need for defending against these issues has increased significantly. Intrusion detection method is divided into two types, misuse detection and anomaly detection [9].

C. CYBER ATTACK DETECTION

1) Host Based Intrusion Detection and Prevention System (HIDPS):

Merging both IDS and IPS on a single host known as a Host-based Intrusion Detection and Prevention System. HIDPS normally maintains a database of system objects and also stores the system’s normal and abnormal behavior. A host-based IDS monitors all or parts of the dynamic behavior and the state of a computer system [7].

2) Network-Based Intrusion Detection and Prevention system(NIDPS):

Intrusion detection is network based when the system is used to analyze network packets. Network based Intrusion Detection and Prevention System capture the network traffic from the wire as it travels to a host. This can be analyzed for a particular signature or for unusual or abnormal behaviors [7].

D. DENIAL-OF -SERVICE ATTACK DETECTION

A denial of service attacks or distributed denial of service attack is an attempt to make computer resources exhausts or disable or unavailable to its legitimate users. These resources may be network bandwidth, computing power, computer services, or operating system data structure. When this attack is launched from a single machine, or network node then it is called denial of service attack. But now days in the computer wild the most serious threat is distributed denial of service attack. In distributed denial of service attack, the attacker first gain access to the number of host throughout the internet, then the attacker uses these victims as launch pad simultaneously or in a coordinated fashion to launch the attack upon the targets. So, even after being a legitimate user in the network, one cannot use that specific service which has been allotted to him by the network administrator [3].

There are many attacks virus, worm, Trojan horse etc. These attack could be attatch either with any word document or with email and with the help of internet attacker send these file to the thousands of user. When user open this file attack happened and start spread in system . Among all of these Dos attack is very dangerous attack hence we are detecting the Do attack in our project.

IV. CYBER-SITUATIONAL AWARENESS MODEL

The proposed research falls under the realm of "Cyber Situational Awareness" which provides a holistic approach to understanding threats and vulnerabilities, performing analysis (using data mining & predictive analytics) to evaluate the current security situation as well as perform a projection or forecast of the future security state to address potential situations. There are multiple levels to Situational Awareness [10].

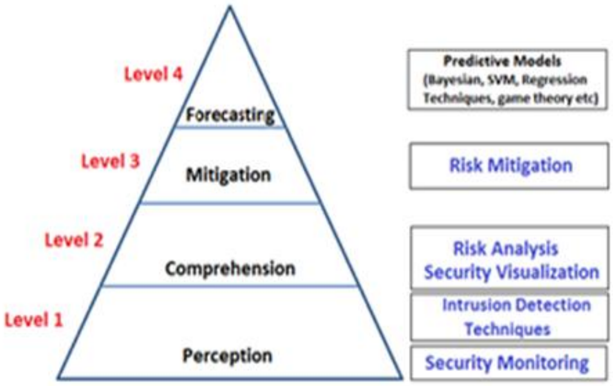

Figure 1. Cyber-Situation Awareness Model

V. APPROACHES TO DETECTING CYBER-ATTACKS

Following are the approaches to detect cyber attacks

- Pattern recognition
- Anomaly detection

Pattern-recognition techniques identify & store signature patterns of known attacks. They then match the subject's observed behavior with those known patterns of attack signatures, and signal attacks when there is a match. Pattern-recognition techniques have been used in many commercial software & research prototypes [1].

The anomaly based detection is based on defining the network behavior. The network behavior is in accordance with the predefined behavior, then it is accepted or else it triggers the event in the anomaly detection. The accepted network behavior is prepared or learned by the specifications of the network administrators [1]. It assumes that a cyber attack will always reflect some deviations from normal patterns. Anomaly detection may be divided into static and dynamic anomaly detection. A static anomaly detector is based on the assumption that there is a portion of the system being monitored that does not change. Dynamic anomaly detection typically operates on audit records or on monitored networked traffic data. Audit records of operating systems do not record all events; they only record events of interest [7].

VI. DRAWBACK OF ANTIVIRUS

There's more than one way to detect a virus, but one big disadvantage to some antivirus programs is that they may not employ all detection techniques. Most modern antivirus systems offers real-time protection for their users since monitoring and analyzing files while they are being accessed lets protect the user better than on-demand scans. Different antivirus systems have different methods for doing that, but the main disadvantage of real-time monitoring is high system resource consumption. According to [11]. Scanning means searching your computer for known virus code patterns. When you install anti-virus , It is not a firewall and will not prevent you from getting hacked, Antivirus software does not fully protect your system and Anti-virus software slows down PC or network, Installing and running anti-virus software can use up a lot of computer memory and hard disk space, Many copies of anti-virus software are unable to detect old viruses because many users forget or don't update their virus scanner's virus databases until it is too late.

With help of "Cyber Attack Detection System using Markov Chain" we can provide full security to any websites. With help of this system we can also provide an authentication to user and when he/she got authentication from administrator then we can use the websites. In this we preventing a websites from Dos attack.

VII. PROPOSED METHOD

A. FLOWCHART

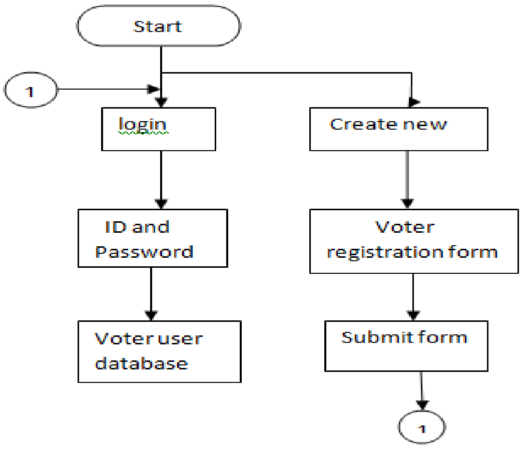

Fig. 1 Voter System

B. BLOCK DIAGRAM

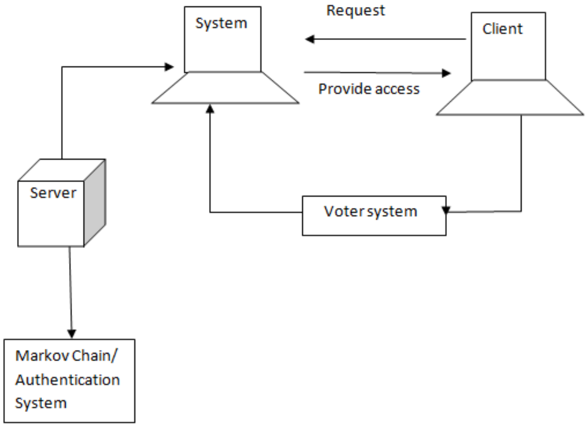

Fig. 2 Attack

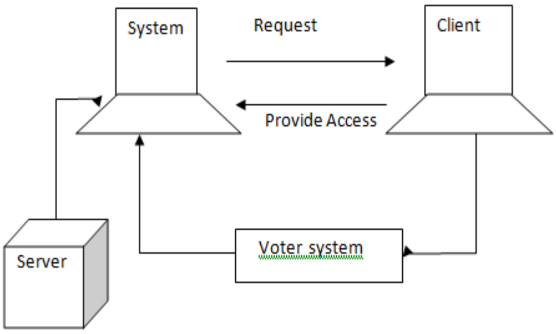

Fig. 3 Attack Detection System

To perform the cyber attack we are creating a web site. Now a days many illegal work occur on Election voting web sites. Therefore to perform cyber attack we are creating a voting web site. For developing this website we have used html. In this we are dealing with Dos attack.

In that website we have developed login page that contain username and password another is registration page that contain attribute like name, email, adhar card number, address and phone number. After filling the registration form information will store in MySQL server. MySQL server contain all the entries of the client.

Basically there are three content that are present in our server as follows.

- Hitlogs : It will show the information about the voters that how many times voter is trying to open his/her account including date and time. If any unnecessary work occur then he/she will directly blocked by administrator.
- Usermaster : In this it will show all information about voter. Basically it provides information like name of voters and who is using the account.
- Ipmaster : in this we will get the information about ip address of user.

VIII. CONCLUSIONS

This application can be used by web based server and router server for detecting the network traffic and finding the security attacks like DoS attack. Depending on the attack the user will be allowed for services or user will be blocked. As there is increasing reliance on computer and network systems to support critical operations in defence, transportation, electric power, etc. Cyber-attacks have become an important threat to our society with potentially severe consequences. Cyber-attack detection aims at identifying cyber-attacks while they are acting on a computer and network system.

Anti-virus software slows down PC or network, Installing and running anti-virus software can use up a lot of computer memory and hard disk space, slowing down your computer. With the help of Cyber attack detection system using Markov chain application we are overcoming these problems.

The Cyber attack detection system can be used by web based server and router server for detecting the network traffic and finding the harmful security attacks by identify types of attack application will block that i.e. It will provide proper prevention over the network.

REFERENCES

[1] Jyothsna V., Rama Prasad.V.V., Munivara Prasad.K., ”A Review of Anomaly based Intrusion Detection Systems*”, International Journal of Computer Applications (0975 – 8887),*Vol.28, No.7, pp: 283–304, 2011.

[2] Gyanchandani, Rana.J..L, Yadav.R.N., ”Taxonomy of Anomaly Based Intrusion Detection System: A Review”, *International Journal of Scientific and Research Publications*, Vol.2(12), ISSN 2250-3153, 2012.

[3] Rahul Rastogi1, Zubair Khan2, M. H and Khan , “*Network Anomalies Detection Using Statistical Technique : A Chi- Square approach*”, *IJCSI International Journal of Computer Science Issues*, Vol. 9(2), No 3, pp.515-522, 2012.

[4] Seongjium Shin, Seungmin Lee, Hyunwoo Kim, Sehum Kim , “Advanced Probabilistic Approach For Network Intrusion Forecasting and Detection“, *Expert system with applications*, Vol.40, pp. 315 – 322, 2013.

[5] Lee, A., Girgensohn, A., Zhang, J., “Browsers to support awareness and Social Interaction,” *Computer Graphics and Applications, IEEE Access* , Vol.24(10**)**, pp.66-75, 2012**.**

[6] Brindasri S,Saravanan K, “Evaluation Of Network Intrusion Detection Using Markov Chain”, *International Journal on Cybernetics & Informatics*, Vol. 3, No**.** 2,pp. 23-45, April 2014**.**

[7] Singh S, Silakari S, “A Survey of Cyber Attack Detection Systems”, *International Journal of Computer Science and Network Security*,Vol.9, No.5**,** pp.897-567, May 2009.

[8] Nong Ye, Yebin Zhang, C.M. Borror,” Robustness of the Markov chain model for cyber-attack detection”,*IEEE Reliability Society*,Vol.53(1),pp. 116-123,April 2004.

[9] Dr. S. Vijayarani, Ms. Maria Sylviaa S,” INTRUSION DETECTION SYSTEM – A STUDY”, *International Journal of Security, Privacy and Trust Management*, Vol 4,No 1,pp. 678-435, February 2015.

[10] Subil Abraham and Suku Nair,” Cyber Security Analytics: A Stochastic Model for Security Quantification Using Absorbing Markov Chains”, *Journal of Communications*, Vol. 9, No**.** 12, pp. 267-678, December 2014**.**

[11] L. Radvilavicius, L. Marozas and A. Cenys,” Overview of Real-Time Antivirus Scanning Engines ”, *Journal of Engineering Science and Technology Review,*Vol. 5(1), pp. 63-71, 2012.