



A HYBRID COMPUTING BASED INTRUSION DETECTION MODEL

Manirathnam.J¹, Kiran Baskar.S², Krishna Kumar.S³, A.Thilagavathy⁴
^{1,2,3}Student,B.E.(CSE), ⁴Associate Professor,

Department of computer science and engineering
R.M.K Engineering College, R.S.M. Nagar, kavaraipettai., Tamil Nadu, India

Abstract

This idea is to develop we are going to propose the intrusion detection model based on the user request. We are going to predict the multiple requests and block them that particular user and analyze the auditing logs. There could be a large number of users accessing the same system which tries to induce the DDOS attack. The entire system analysis the data and those data are manipulated and send those data to the motherboard and serial number is accepted, Mac address and ip will block them viewing the other user's data as the data is collected from the cloud. This allows the user to prevent his data from unknown sources accessed by user. This model allows user to access their data with privacy and allows him to access his data alone and prevents accessing of others data. This ensures the protection and privacy of data. This model helps to access the data of users through particular device with its identity.

Keywords: DDOS (Distributed Denial of Service), OSI (Open Systems Interconnection), DOS (Denial of Service), IP (Internet Protocol), MAC (Media Access Control).

I. INTRODUCTION

Since cloud has become a dependent source for computing platform. Its role in computing has increased drastically. Intrusion Detection model helps in accessing data of the user using their request and allow them to access their data alone with protection. In addition it predicts multiple requests and also blocks that allowing a particular user to analyze the auditing logs. A particular user when induce large number of requests from his system to

initiate and induce the DDOS (Denial Distributed Of Service) attack. The large number of requests are then identified and then checked to identify targeted user data. Then we analyze and get sufficient details of the user motherboard serial number, MAC (Media Access Control) address and IP (Internet Protocol) address and will block those viewing from other user's data. This allows the user to prevent his data from unknown sources accessed by user. This model allows user to access their data with privacy and allows him to access his data alone and prevents accessing of others data. This ensures the protection and privacy of data. This model helps to access the data of users through particular device with its identity. This method would stop attacks particularly sniffer in which one user could access the other user's data by entering the firewall with same IP (Internet Protocol) address and access the targeted user's data and use without their knowledge which leads to data theft and using this model this data theft could be avoided by checking their device credentials.

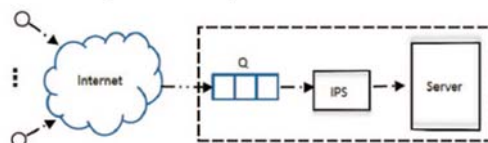


FIG 1[1]

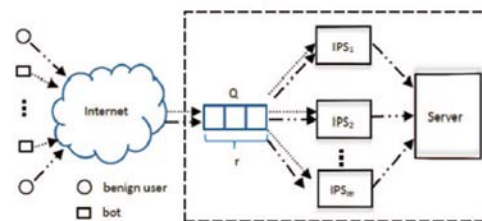


FIG 2[1]

The detailed working and accessing of user's data using MAC (Media Access Control) and IP (Internet Protocol) and motherboard id is described.

II. EXISTING SYSTEM

The present system is used to detect the DDoS (Denial Distributed Of Service) attacks which induces to bring the down the whole services as for the user gives the multiple requests to access the data which is mainly performed through networking layer and that is based upon the user's request. This DDoS (Denial Distributed Of Service) attack which causes multiple attacks is an kind of malicious attempt done by multiple systems or attacks that are caused from the source of system which is used to induce from the network layer. In the present system the multiple user requests are not allowed and is always blocked. This enables the user to give multiple requests form a single source and thus causing the DDoS (Denial Distributed Of Service) attacks. This could make the user to access their data from the source that is required. When a data is said to be attacked it losses the user's privacy and therefore it leads to data theft and multiple requests from single source should be avoided.

III. IMPLEMENTATION SYSTEM

1) What is DDoS?

DDoS-Distributed Denial of Service It's a type of attack which is an subclass of Denial Of Service in which it contains multiple connected online devices which are known as botnets that uses to target an website with an fake address. Another form of attack is like when multiple requests attack a target like server, website or any other source which leads to the Denial of Service to the users for the resources targeted.

- **IP address:**

IP (Internet Protocol)

The IP address is something which has some numbers that are separated by full stops which helps in the identification of particular computer which uses the internet protocol to communicate over a network. This IP address is used with other credentials so that an protected access to access the data occurs. This helps the data in privacy and protection.

- **MAC address:**

MAC (Media Access Control)

The MAC address is an network adapter and a unique identifier which is assigned to network interface for controllers for communications at an particular layer in the segment of the network. This is an unique number provided to

every computer which would be used to identify each device on the network. This also helps the data in privacy and protection

- **Motherboard number:**

The motherboard number is said to be the PCB (Printed Circuit Board) in a computer which will be listed in a barcode format. This motherboard serial id could be fetched through program by entering the required command. This plays a major role and is different from other security mechanisms which could be safer as it fetches the serial id from computer and then it confirms that the particular request is from motherboard serial id and other credentials and then enters to the server side.

2) What is OSI?

OSI (Open Systems Interconnections) is an networking layer in which DDoS (Distributed Denial of Service) are induced. The main function of the OSI is that it standardizes the communication functions of the computing systems without the need of internal structure and technology. This OSI is very important because the modular approach which is used to design the network that divides the required functions to seven layers.

3) WORKING MODULES

The project is based upon intrusion detection hybrid computing model that is based upon web analyser and block attacker modules that are used to protect the data from theft and other security issues. There are some basic methods that are to be taken care as of working with the certain modules. The modules are web logs analyzer and the block attacker which allows the user based on their request. Further the analyzer works with type of requests and then it predicts the multiple requests and help in blocking the particular user and analyze the auditing logs. This logs helps in determining the type of attacks such as DDoS (Distributed Denial of Service), Sniffer, Ip Spoofing, etc. Then with the help of block attacker we will analyze the user other board serial number, MAC (Media Access Control) address and Ip address then block them viewing the other user's data. Then the server will trigger and email to the server admin, regarding the attack induced on the server.

- a) **Analyze web logs:**

Analyze web logs which is the main working part of the intrusion and detection model in which all the requests are received from the user and when these requests hit the firewall of the particular server and then it is processed by particular application and then the multiple requests from the

user is blocked and analyze the auditing logs which leads to various attacks such as DDoS (Distributed Denial of Service), Sniffer attack and IP spoofing.

b) Block Attacker:

Block attacker is used when a user is induced to large number request from his system, then the user will try to induce an DDoS (Distributed Denial of Service) attack. After this attack we would analyze the user's motherboard serial number, MAC (Media Access Control) address and IP (Internet Protocol) address, with these will then block them viewing the other user's data. Then user will trigger and respond with an email to the server admin regarding the attack that has occurred which has been induced on the server.

c) Request Updates:

The request updates in the particular module is used to provide the details which are needed to provide for the server and then the server gets the particular details from the user and then verifies the details of the motherboard serial number, MAC (Media Access Control) address and IP (Internet Protocol) address, and then with this update the user is allowed to access the particular data from the server. When the user particular device is lost the user could provide the new device credentials that are

IV. SYSTEM ARCHITECTURE AND REQUIREMENTS

A. HARDWARE REQUIREMENTS

1) SYSTEM HARDWARE REQUIREMENTS

The following system requirements are required for the process in the entire project execution such as laptop or monitor device to perform the various request operations from server and to display. The system requires to process the program with pentium-3 processor with a speed of 1.1 GHz. This is necessary only with RAM (Random Access Management) of 256 MB of minimum as a requirement. This system required to process the program requires a storage of hard disk that could be minimum 20 GB with a floppy drive of 1.44 MB with output devices such as keyboard and mouse in which the keyboard should be standard windows keyboard and two to three button mouses. All these devices should

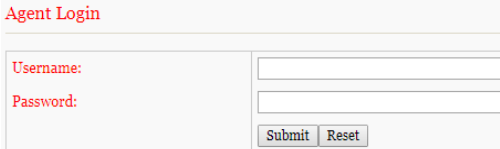
be there for performing the hybrid intrusion method.

B. SOFTWARE REQUIREMENTS

The following software system requirements are required for the process of entire project execution such as some programming language that are used. This is performed with the operating system with any of the configurations such as windows 95 or windows 98 or windows XP. The front end is performed with HTML, Java, Jsp and the script that is used to perform is Javascript and the server side script is completely done with Java server pages. The database which is very important to store the data of the server admin and the user details of a particular method. The connectivity that is used for database and the server is JDBC.

V. WORKING OF HYBRID COMPUTING BASED INTRUSION AND DETECTION BASED MODEL SYSTEM ARCHITECTURE

The outline of the project is to check whether the data is safe for the user for privacy and protection to avoid data theft and the method that is used to keep the data safe. The first work with the user is to send a request to the server.



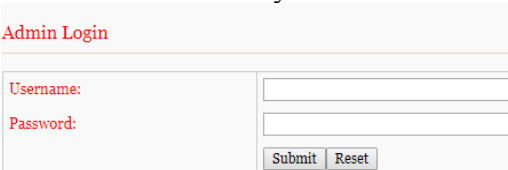
Agent Login

Username:

Password:

FIG 3

The analyzer checks for the request, if it seems to be a multiple request then the analyzer handles to be specific with the sniffer attack, then the analyzer will not allow the request to enter into the server firewall which may lead to data theft.



Admin Login

Username:

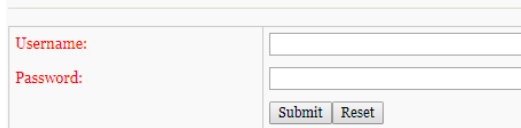
Password:

FIG 4

Then with the block attacker it blocks the multiple request that is used to induce the attacks and then if an registered user raises a request it is sent to analyzer and then proceeded to block attacker where it checks for the details of the motherboard serial number, MAC (Media Access Control) address and IP (Internet Protocol) address then with the verified process the analyzer allows the user to access the data in a protected and private method to avoid data theft. In this manner it works as an

secured manner for the user data.

Server Login



The image shows a web form titled 'Server Login'. It contains two input fields: 'Username:' and 'Password:'. Below these fields are two buttons: 'Submit' and 'Reset'.

FIG 5

This allows the data placed in server could be requested only through an proper IP (Internet Protocol) address and also the intrusion of hackers and data thefts can majorly avoided from the server. This can help prevent sniffer attacks occurring. required to sign up and further could proceed with the newly registered device.

VI. WORKING RESULTS

This module actually explains the detailed process that how the data is accessed in an safer manner by particular request in which the analyser finds for the request, if it seems to be an specific with the sniffer attack in the case another IP (Internet Protocol) address, through the analyzer which will not allow the request to enters the server firewall which leads to data theft.

Then the block attacker which blocks the multiple request which is used to cause the attacks. Since it is performed in an local server there is an separate sign up for the user, admin and the server and then if registered user gives an request, then the request is sent to analyser then to block attacker to check the details of the motherboard serial number, MAC (Media Access Control) address and IP (Internet Protocol) address after the verification process the analyser allows user to access data in a protected and private mode.

VII. ADVANTAGES

The data is safely handled by the particular user who has raised for the request and in addition to that the data can be viewed by the user who has requested. The data theft is reduced since the data are accessed by particular devices which are allowed by the admin and then the unique id which allows all the users to be unique and particular among others. So that the data anyway cannot be taken away or no illegal access by another user.

VIII. CONCLUSION

The System ensures that the data condition is safe and easy to access by the user. This system also helps the user to get through particular request in the server. The device can allow the user to access data in a secured way. The updated method can be allowed in a way where users can perform their additional devices for multiple purposes and fetch the data accordingly. This method should be taken in consideration for future purposes.

IX. REFERENCES

- [1] Can we beat DDOS attacks in cloud.
<http://ieeexplore.ieee.org/document/6567859/>
- [2] Preventing DDOS Attacks by Identifier or locator separation.
<http://ieeexplore.ieee.org/document/6678928/?denied>
- [3] Low-Rate DDOS Attacks Detection and Traceback by using New Information Metrics.
<http://ieeexplore.ieee.org/document/5696753/>
- [4] Traceback of DDoS Attacks Using Entropy Variations.
<http://ieeexplore.ieee.org/document/5467062/>
- [5] Hybrid Technique for DDoS Attack Detection.
<http://ijcsit.com/docs/Volume%208/vol8issue3/ijcsit2017080316.pdf>