

IP Address Blocking System

Harpreet Kaur
Randhawa
Information
Technology
Ramrao Adik Institute
of Technology
Nerul, Navi Mumbai,
India

Akankshya Purohit
Information
Technology
Ramrao Adik Institute
of Technology
Nerul, Navi Mumbai,
India

Aarti Sahu
Information
Technology
Ramrao Adik Institute
of Technology
Nerul, Navi Mumbai,
India

Reshma Gulwani
Assistant Professor
Information
Technology
Ramrao Adik Institute
of Technology
Nerul, Navi Mumbai,
India

Abstract- Hosting a site on the Internet makes it available everywhere. There are certain sites that are just meant for local use like local shopping marts that do not provide products for purchase in other countries. Also, there are certain websites which contain confidential information such as governmental websites of countries should not be allowed access in other countries. Allowing access to such websites in other countries has various disadvantages. First of all, it leads to security issues. Secondly, it increases the load on the server on which the website is hosted. Thus, infrastructure maintenance becomes a problem. Moreover, it increases the hardware cost because to handle this load devices like load balancers have to be used. Also, increase in unnecessary traffic to websites leads to bandwidth wastage and network traffic. It not only denies access to authentic users but also paves way for DDoS and DOS attacks, thus hampering the availability of websites to legitimate users. The Administrator has the rights that allow/deny their website from being accessed in other countries.

Keywords- IP Address, Blocking, security, Country, website administrators

I. INTRODUCTION

IP Address Blocking System prevents the connection between a server and certain IP addresses or ranges of addresses. It effectively bans undesired connections from hosts. It is used to commonly protect against brute force attacks. On a website, banning of an IP address is often used to prevent a malicious user from accessing the content. The IP addresses are dynamically allocated which makes it difficult to check the incoming IP Address of the machine requesting access to your website. This complicates the blocking process. Banning countries from accessing websites has its disadvantages as well. For instance, most of the attacks on the data of your website is generated from Nigerian countries. Due to this belief all business generating from this country is considered to be fraudulent making it difficult even for genuine businessmen to conduct their business.

When a site or application is supposed to serve some purpose in one country, there is no point to allow the website to be visible in other countries. This will reduce sever load as well as unnecessary attacks originating from various countries. Typically Apache Web Server supports the feature of allowing and denying a list of IP Addresses. With this module, one has to download a list of IP Address ranges in decimal format for various countries. The Administrator should be able to add the name of countries to the Block_Country table to prevent access of the website to users from that particular country. The website should be able to correctly convert the IPv4 address to its decimal notation and map it to the country that has been added to the list of blocked countries and deny access to its users.

II. RELEVANCE AND MOTIVATION

If you run a website, then by default it is accessible to the whole planet. All websites target different groups. Some of them are just not relevant to all groups of people. So, one shouldn't be expecting significant traffic from them. If there is a local shopping mart and it only serves the needs of the local people who are the members of your store, then there is no need to let any other countries access your server.

Here is a screenshot of SimilarWeb telling us that Japan is responsible for the second-largest volume of traffic to our college website 'www.rait.ac.in'.

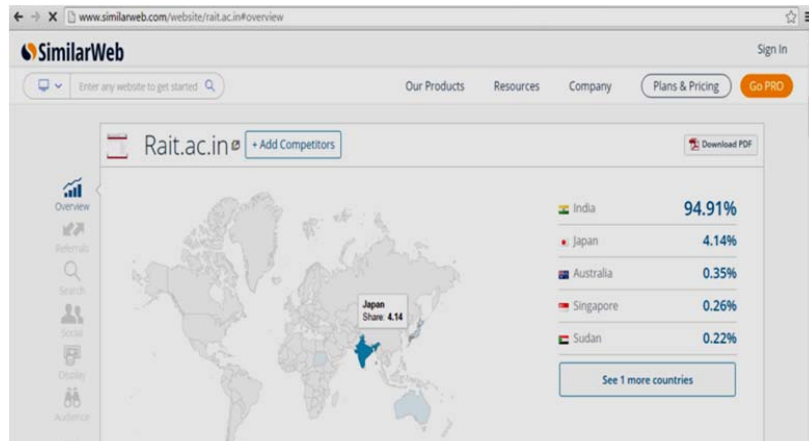


Fig. 1: Traffic generated for www.rait.ac.in from different countries

While it is certainly possible that Japanese people may find the content of the site useful, there is really no explanation for this activity. This website does not offer content to cater the needs of Japanese students specifically. There are some reasons against blocking access to countries to your website. But to increase the security and reduce server load blocking has become essential.

III. REVIEW OF LITERATURE

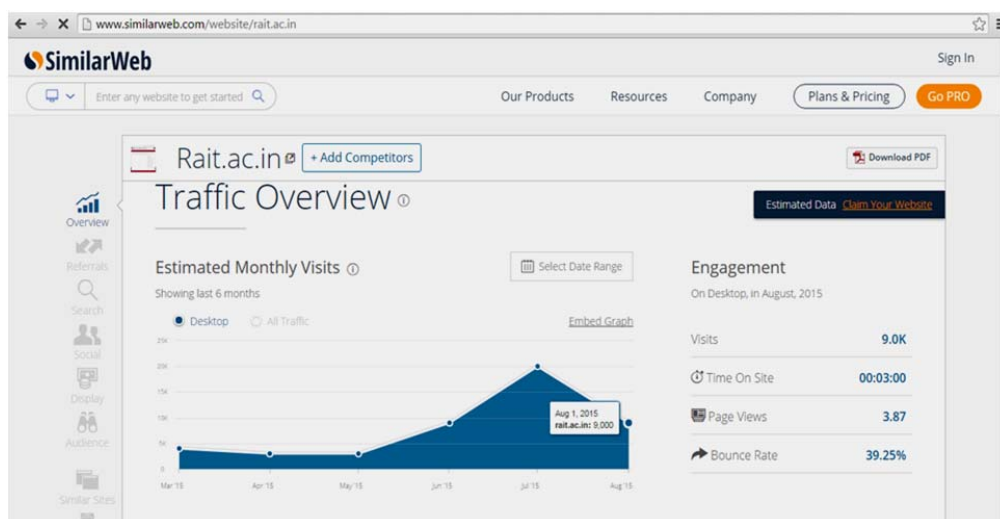


Fig. 2: Number of visits to www.rait.ac.in in the month of August

In fig. 2.1 it can be observed that the number of visits in the month of August for ‘www.rait.ac.in’ was 9000. This site is meant to be made accessible only in India, particularly to people related to RAIT . Such a huge traffic of (approx.) 9000 visitors per month from different countries increases server load thereby reducing site response time. By making the site accessible only in certain countries could improve the performance of the server. Some techniques that have been in practice to allow/block websites in particular countries are as follows:

A. .htaccess

.htaccess can be used as a tool to block access to your website by users from different countries. The following is the code snippet of how commands are typed in .htaccess

```
Order Deny, Allow  
Deny from 192.168.10.2
```

B. Use a hosting company that has blocking as a part of their built-in controls

Companies provide this feature in one of the two ways-

i. Bare Metal

A bare metal or VPS is a machine that you have complete control over. For example, Rackspace. Using a bare metal to block access gives user no control over the back end. A host that has country blocking as a part of its default plan and configuration has not been found. It acts as a basic firewall for adding IPs to blacklists or whitelists [1].

ii. Shared Hosting

You might get a server configured with Plesk control panel or cPanel. These are simply control panels for dealing with databases, emails, backups and many other things. A shared server typically comes with a control panel, which lets you easily add IPs to a firewall or allows editing of .htaccess. [1]

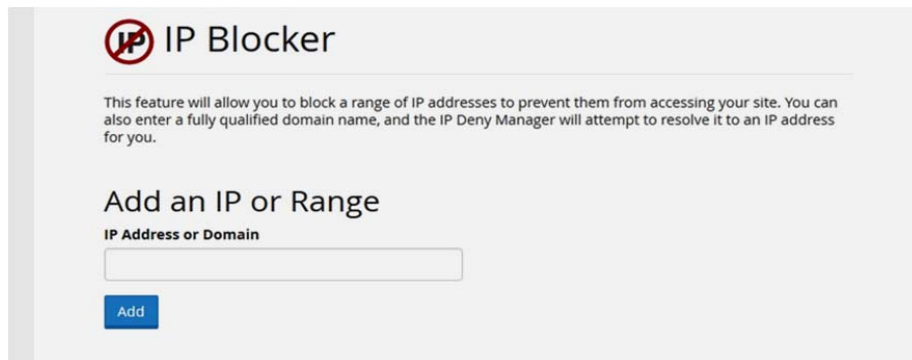


Fig.3: Screenshot of cPanel

C. Use a Proxy Service on Your Domain

Another method involves hiding your domain behind a proxy service that essentially handles all the source traffic before forwarding them on to your server. This works at the DNS level and often all you need to do is change DNS settings to use them. A tool named 'CloudFare' is used whose working is very simple. [1].



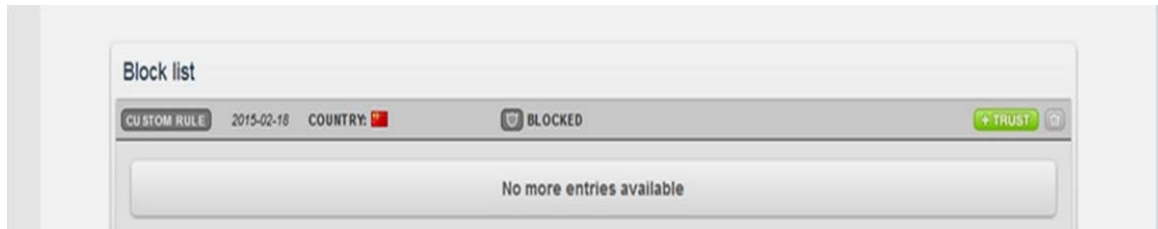


Fig. 4: Screenshots of CloudFare

IV. METHODOLOGY

A. Proposed System

A module will be developed that can be used by website developers to allow or deny people living in different countries to view their website. This will help improve the site availability. E-commerce, governmental and many other sites contain sensitive information such as user's contact information, credit card details that are prone to attacks by hackers. The proposed system will enhance the security of the sites belonging to the above mentioned domains.

B. Proposed Methodology

As a prerequisite in this module, all available IPv4 addresses are converted from their dotted decimal address to decimal format. They are stored in separate files with an extension php and are named based on the value of the first octet. The public IP Address of the client machine accessing the website is fetched using the function

```
$_SERVER['HTTP_X_FORWARDED_FOR']
```

and is stored in a variable named ip. This IP Address is split into 4 octets based on the delimiter {'.'} using the function

```
preg_split(" . ", $ip)
```

and is stored in an array variable named n. Based on the value of the first octet, the program accesses the respective php file. This IP Address is converted from its dotted decimal to decimal format using the formula

$$\text{\$code}=(\text{\$n}[0] * 256^3) + (\text{\$n}[1] * 256^2) + (\text{\$n}[2] * 256^1) + (\text{\$n}[3] * 256^0)$$

and is stored in a variable named code. The value stored in code is matched with the array values stored in the php files and the corresponding two-letter country-code is fetched. This two-letter country-code is stored in the Block_Country table of the database. If the two-letter country-code is not present in the Block_Country table, then the user is allowed to access the website else access is denied.

C. System Requirements

Hardware Requirements

Windows NT/7/8/8.1

Software Requirements

Front End – HTML5, CSS3, JavaScript

Back End – PHP & MYSQL

V. DESIGN OF SYSTEM

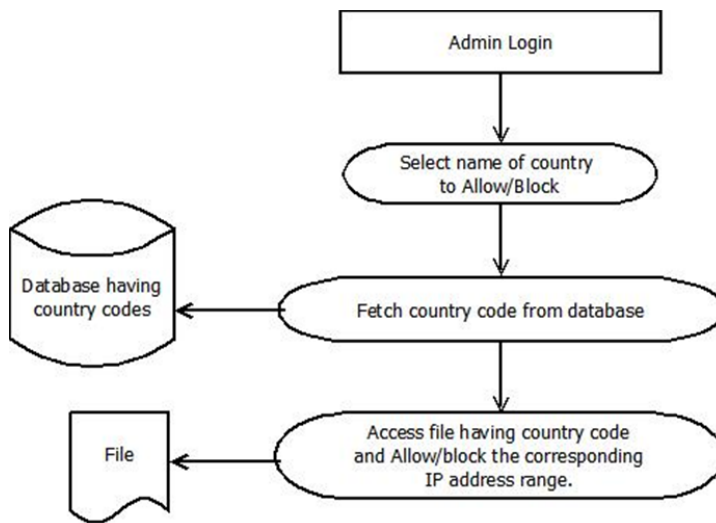


Fig. 5: Administrator System Diagram

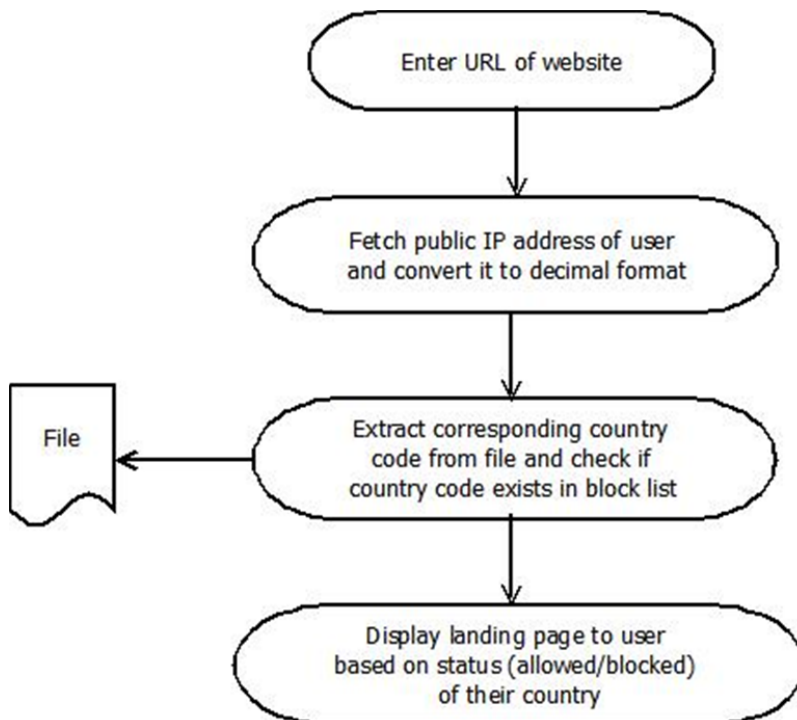


Fig. 6: User System Diagram

The administrator is provided with an interface that allows him to either allow or block the IP Addresses of countries from accessing the websites.

DFD Level 0

The DFD Level 0 represents the basic components of the system. The actors include the administrator of the website who will block XYZ country from accessing his/her website and on the other side are the USERS of country who will thus be blocked.

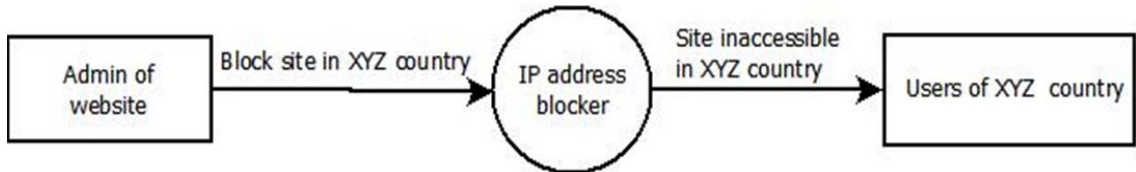


Fig. 7: DFD Level 0

DFD Level 1

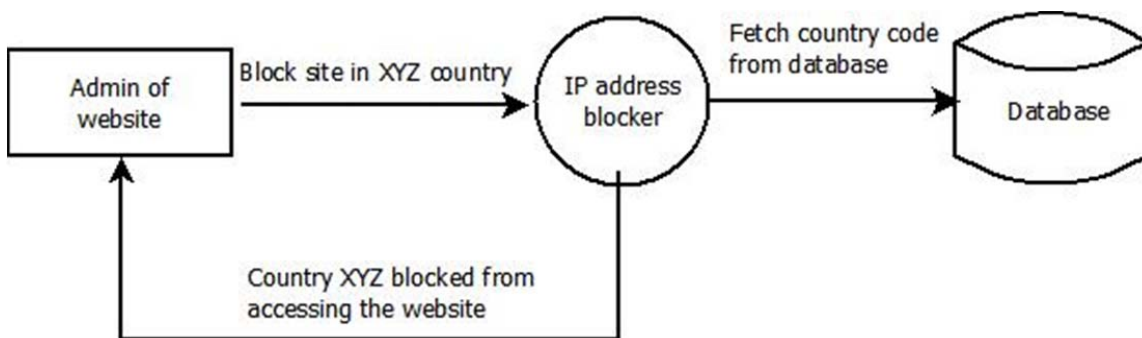


Fig. 8: DFD Level 1

DFD Level 2

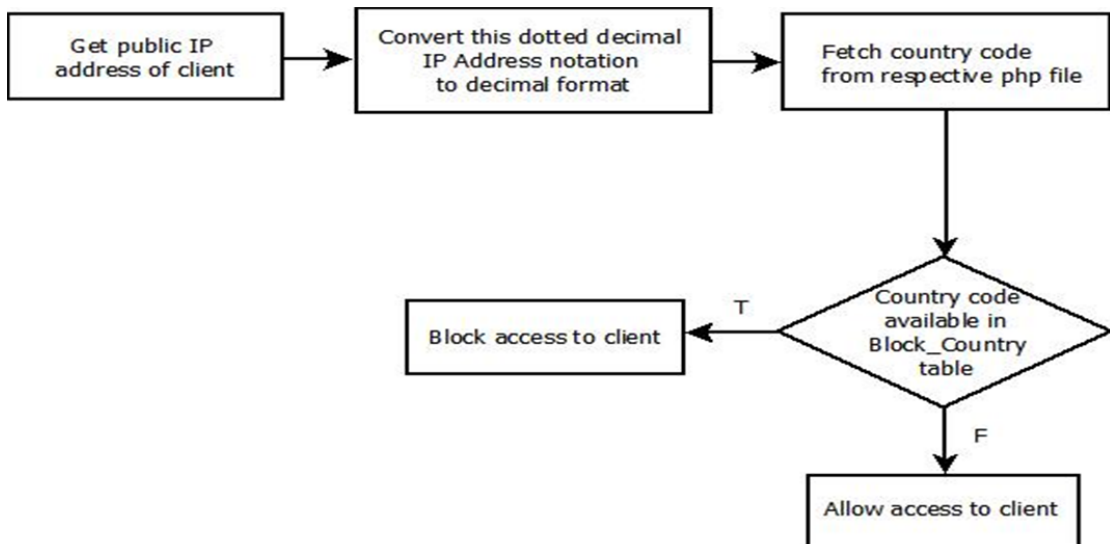


Fig. 9: DFD Level 2

VI. CONCLUSION

Internet has opened a wide range of scopes for even small businesses to prosper. Websites provide an opportunity for companies to connect to masses across the globe and in turn generate more revenue. The benefits of moving from an offline store to an online business are immense. At the same time, one cannot deny the threats websites are exposed to when hosted on the Internet. According to a recent survey, majority of attacks on the servers are DOS and DDOS attacks. Websites have become a favorite with hackers who are always on a lookout to reduce the availability of the server. Attackers do so, by bombarding the server with a lot of bogus requests. Hence, it becomes all the more essential for website developers to increase the security of their sites. It is extremely essential to block those IP addresses from where legitimate traffic is not expected. This in turn improves the server uptime. Blocking IP addresses also increases the bandwidth of the network. As a result, the website availability improves.

In this system, the administrator login has been authenticated so that only they are authorized to access the module to add or remove countries from the block list. Sometimes, attackers use Proxy servers to bypass their illegitimate requests. Care has been taken to handle such proxy requests as well.

VII. FUTURE SCOPE

With the advent of Cloud Computing and Internet of Things (IOT), we are accessing Internet from a wide range of devices like desktops, laptops, smart phones, PDAs. As a result of this we will soon run out of IPv4 addresses that are assigned to these devices. Thus, IPv6 addresses are now being assigned as a solution. Currently, our system is able to block only IPv4 addresses. The future implementation of the module would be to deal with IPv6 addresses. The current system has been implemented keeping in mind today's scenario. The amount of data that is present online has increased tremendously over the years. It includes confidential and sensitive information as well. Therefore, it is the prime responsibility of the organizations to protect their user data which if compromised can harm the reputation of the organization and put the privacy of the customers at stake. E-commerce and governmental domains are examples of sites that contain sensitive data and are susceptible to attacks. In the near future, there could be several other domains which will need to embed this security module into their system. The current system blocks IP addresses based on their country codes thus blocking entire IP ranges belonging to a particular country. In the future, the system can be upgraded to be able to block IP addresses belonging to a smaller geographical region such as a state or a city. Sometimes, the need may arise to block only certain parts or webpages of a website from illegitimate users rather than the entire website. This functionality can also be implemented in the future versions of the system.

VIII. REFERENCES

- [1] <http://www.sitepoint.com/how-to-block-entire-countries-from-accessing-website/>
- [2] <http://www.wikipedia.org/>
- [3] <http://www.github.com/>