International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IV, April 2018- Available at www.ijraset.com

Definite Proxy Gateway for Secure Web Access

Anjali P. Kadam[1], Rutuja A. Darak[2], Samruddhi A. Khadtare[3], Revati H. Jadhav[4], Aparna R. Korde[5]
[1, 2, 3, 4, 5]*Computer Engineering Department, B.V.C.O.E.W., SPPU*

Abstract: ***Internet is widely used these days by majority of the population for easy day to day activities like online shopping , social networking, bill payment to complex financial services. .Using Internet as a shared based medium of communication means privacy is not ensured. The source and destination of such communication could be easily traced by little. Nowadays online communication provides little very less anonymity. Eavesdroppers can easily identify with whom a user is communicating. The link ability of all traffic information generated by an Internet user allows for a malicious user to track interner habits of a user. This further could be extended to using the acquired information against the person in a wrongful way. The general goal of anonymity is to hide this Meta –information to eavesdroppers. The solution for such anonymity over the internet is Tor. This paper presents a web application on guidelines of TOR to preserve such anonymity. The paper also presents a systematic profiling of each users by maintain their record through logging in and sign up.***
Keywords: Proxy gateway, Secured anonymity, Tor relay, Allocation of IP address.

I. INTRODUCTION

First only the legitimate users are granted access to the web application by secure sign up/login. After logging to the application user is allocated an IP address from the pool of IP address. The pool of IP addresses is generated at a backend by creating a database which only enters the legitimate IP addresses of the users visiting the web application. This is done to maintain security. After allocation of IP user can browse the internet with the new IP address. The web application is deployed on Amazon Cloud. The logs are time stamped in a separate database to ensure malicious users do not use the web application.

II. PURPOSE

With the development in technology Internet has taken over majority of the human activities. Anything and everything is becoming possible online. However this has come at cost of security of personal data. In case of powerful authorities a journalists/individuals are not able to put forward their views honestly. At times military personal need to converse securely and anonymously over the web. Hence the project caters the need of such users to allow them to browse the web anonymously and securely.

III.PROJECT SCOPE

This paper proposes a system which allocates IP addresses to the users to protect their identity. A desired user of the system will log into his account (if already registered) or create a new account (first time user) to use the services of the system. . For the creation an account in order to maintain security user need to enter genuine credentials only after which account will be created. An email verification link as well as mobile OTP (one time password) will be provided for the same. After logging into the users respective account a dashboard will appear showing user statistics as well as pool of available IP addresses. A Duck Duck Go Search Engine will also be present. After assignment of the IP to the user the user will be able to browse the internet with the new allocated IP address.

IV.LITERATURE SURVEY

The literature survey is done by us by referring some IEEE papers and some journal papers. The papers surveyed are represented in the table below.

TABLE 1 - LITERATURE SURVEY

Year	Author	Paper	Objective	Methodology
2013	Alex Biryukov, Ivan Pustogarov, Ralf-Philipp Weinmann	Trawling for Tor Hidden Services: Detection, Measurement, Deanonymization	Tor is most popular volunteers based anonymity network consisting of more than 3000 volunteer-operatedrelays. Apart from making connections to servers hard totrace to their origin it can also provide receiver privacy forInternet services through a feature called “hidden services”In this paper we expose flaws both in the design andimplementation of Tor’s hidden services that allow an attacker to measure the popularity of arbitrary hidden services,	Botnets , Guard Nodes

			takedown hidden services and deanonymize hidden services..	
2011	SouadBenmeziane, NadjibBadache ,SihemBensimessaoud	Tor Network limits.	Tor is a volunteer run relay network designed for privacy, anonymity, and censorship resistance. Tor has become the most successful public anonymity communication service in the Internet because of its lowlatency. In this paper, we present a method to exploit the Tor limits in conjunction with public profile of user to reduce degree of anonymity.	TCP /UDP connections, onion routing
2014	Alex Biryukov, Ivan Pustogarov, Fabrice Thill, Ralf-Philipp Weinmann	Content and Popularity Analysis of Tor Hidden Services	The main purpose of Tor is to enable freedom of speech even in situations in whichpowerful adversaries try to suppress it. However, providinglocation privacy and client anonymity also makes Tor hidden services an attractive platform for every kind of imaginable shadyservice. In this paper we analyse the landscapeof Tor hidden services. We have studied 39824 hidden servicedescriptors collected on 4th of Feb 2013: we scanned them foropen ports; in the case of 3050 HTTP services, we analysedand classified their content. We also estimated the popularity of hidden services by looking at the request rate for hidden servicedescriptors by clients. We found that while the content of Tor hidden services is rather varied, the most popular hidden servicesare related to botnets. We also propose a method for opportunisticdeanonymisation of Tor Hidden Service clients. In addition, we identify past attempts to track “Silkroad” by consensus history analysis.	Onion Routing ,Port Scanning, Content Analysis, Tracking clients.
2008	KarstenLoesing , Werner Sandmann , Christian Wilms , Guido Wirtz	Performance Measurements and Statistics of Tor Hidden Services	Tor is mechanism to preserve identity of users while they access the services of the world wide web. For the majority of users the most important QoS after perseverance of anonymity is time taken by the relays to offer service reply after sending the request ie latency.This paper focuses on the latency aspect of Tor networks.	Quality of service, Relays, time factor.
2005	Mustafa Engin	Low-cost traffic analysis of Tor	This paper presents the author's experiences using a low-cost microcontroller evaluation board and a commercially available real-time operating system in the laboratory component of an undergraduate embedded and real-time system design course.	Routing of data, Tor relays

V. SYSTEM ARCHITECTURE

The architecture in Figure 1I shows the overall description of our system. We need a robot (i.e. a 4-wheel platform) that consists of a motor driver, 2 motors and an ESP module. We also need to install the smoke sensor at various points in the room. The sensors will be connected to the ESP module. Both the ESP modules need to be connected using Wi-Fi connection.

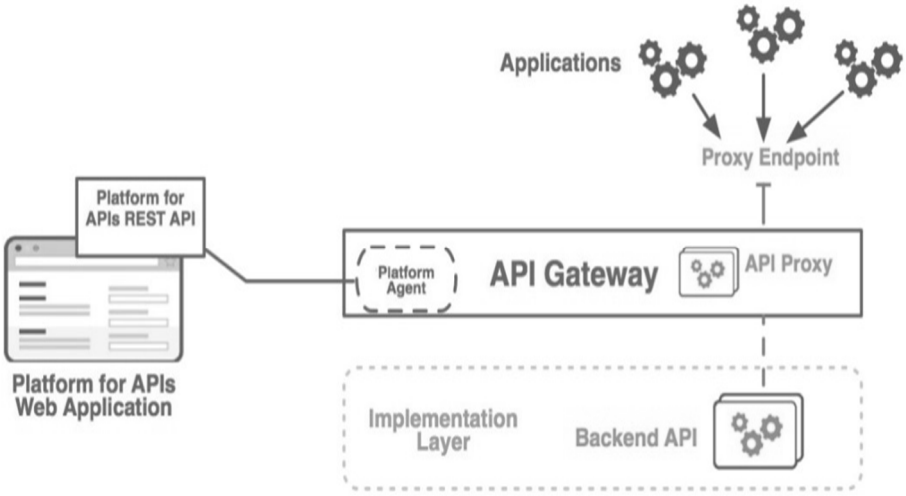

FIG. 1 SYSTEM ARCHITECTURE

VI. UML DIAGRAMS

There are a few UML diagrams that will explain our system model better.

A. *Activity Diagram*

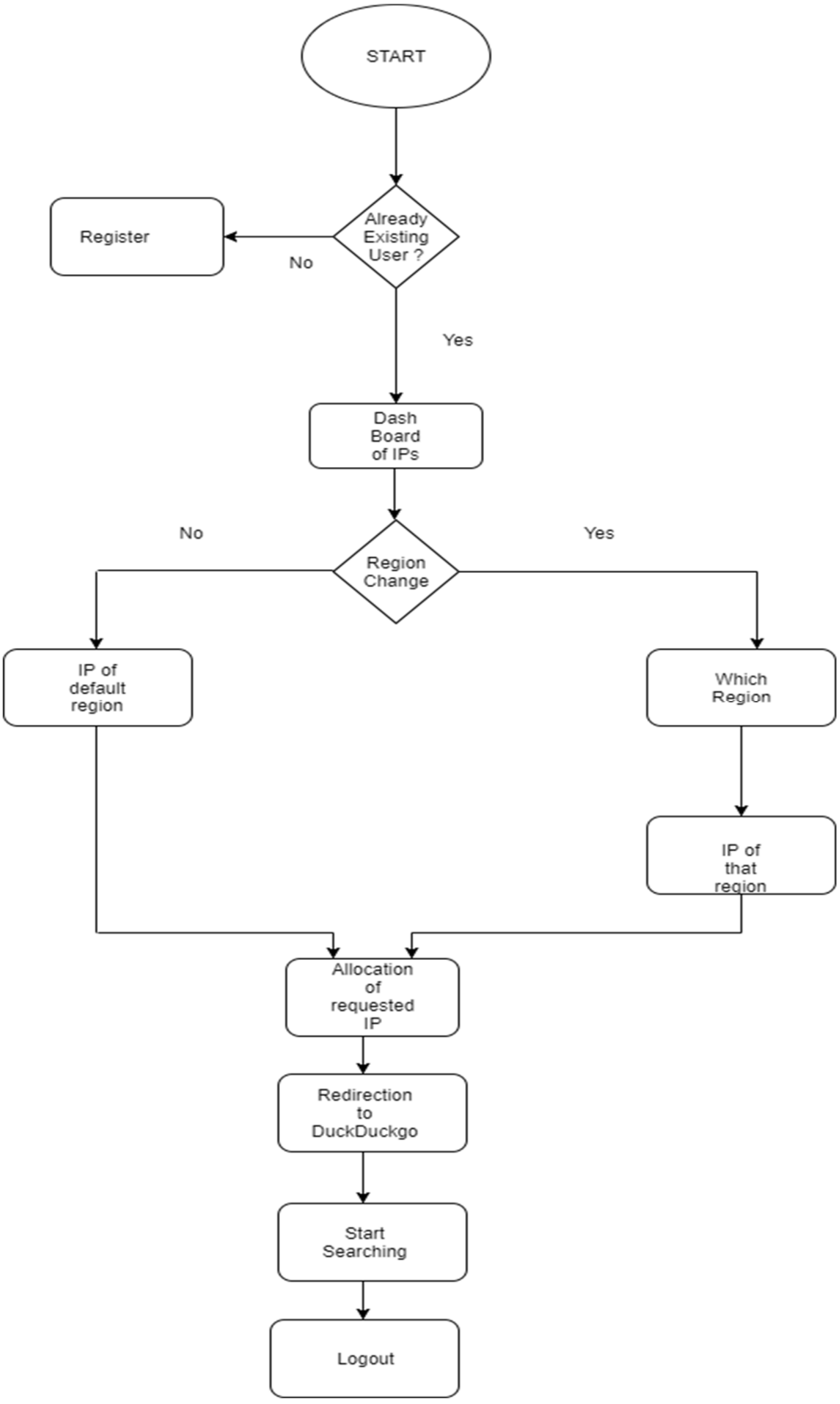

FIG. 2 ACTIVITY DIAGRAM

B. Sequence Diagram

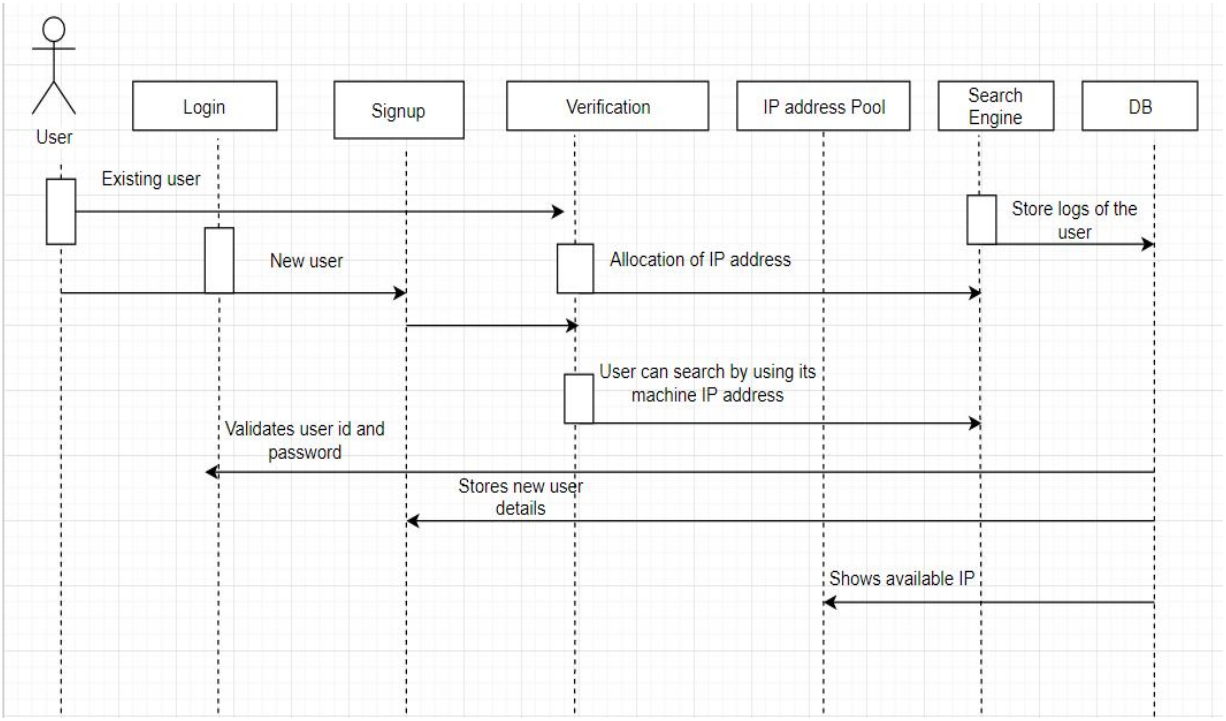

FIG. 6 SEQUENCE DIAGRAM

C. Use-Case Diagram

FIG. 8 USE-CASE DIAGRAM

VII. MATHEMATICAL MODEL

Let S be a closed system defined as, S = {I, O, A, DD, NDD, Su, Fa}
where,

I = Input State
= {User Credentials}
O = Output State
= {User can search data anonymously}
A = Set of actions
= {F1, F2, F3}
where,
F1 = Verification of users credentials
F2 = User is allocated with a IP address
F3 = User can search through the provided search engine
DD = Deterministic data
= {User gets logged in by verifying credentials}
NDD = Non-deterministic data
= {User can search required information}
Su = Success State
= {Su1, Su2}
where,
Su1 = {Success in getting logged in the web application}
Su2 = {Success in searching data anonymously}
Fa = {Fa1, Fa2}
where,
Fa1 = Failed to verify a user
Fa2 = Failed to allocate IP address

The state transition diagram according to our mathematical model is as shown in Figure 9.

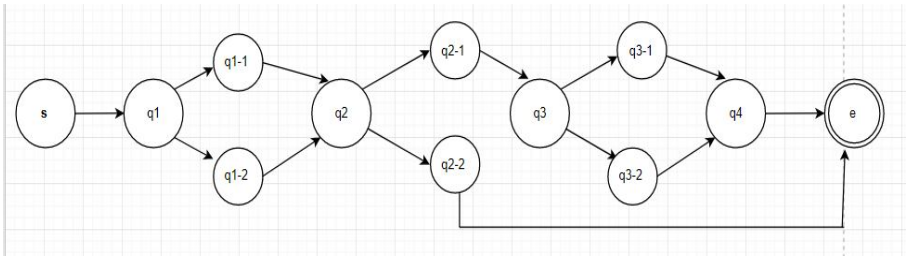

FIG. 9 STATE TRANSITION DIAGRAM

Where ,
s=initial state
q1=registration
q1-1=New user
q1-2=Existing user
q2=Verification of credentials
q2-1=If credentials are correct
q2-2=If credentials are incorrect
q3=IP address pool
q3-1=If user is allocated with IP address
q3-2=if user directly using his IP address
q4=Searching of the required data
e=end state

VIII. CONCLUSION

The user will log in to the application using his credentials .The search engine is made available for the user .The user will be provided with an IP address from the pool of IP address .The user can surf the data anonymously by hiding its true identity.
Major concern is the security of the user and data to be accessed anonymously.

IX. ACKNOWLEDGEMENT

First and foremost, we would like to express our gratitude to the H.O.D. of the Computer department, Prof. D. D. Pukale, as well as the entire teaching and non-teaching staff of the Computer department for giving us an opportunity to work on such an exciting project. Last, but not the least, we are extremely grateful to our family, friends and colleagues who have supported us right from the inception of the project. Thank you for all your encouragement and support.

REFRENCES

[1] Alex Biryukov, Ivan Pustogarov, Ralf-Philipp Weinmann “Trawling for Tor Hidden Services: Detection, Measurement, Deanonymization”,2013 IEEE Symposium on Security and Privac
[2] SouadBenmeziane, NadjibBadache,SihemBensimessaoud, “Tor Network limits”, 2011 International Conference on Network Computing and Information Security978-0-7695-4355-0/11 $26.00 © 2011 IEE
[3] Alex Biryukov, Ivan Pustogarov, Fabrice Thill, Ralf-Philipp Weinmann, “Content and Popularity Analysis of Tor Hidden Services”, 2014 IEEE 34th International Conference on Distributed Computing Systems Workshop
[4] KarstenLoesing , Werner Sandmann , Christian Wilms , Guido Wirtz,“Performance Measurements and Statistics of Tor Hidden Services”, 2008 Symposium on Applications of Internet
[5] MustafaEngin, “Low-cost traffic analysis of Tor”, 2005 IEEE Symposium on Security and Privacy.