ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

Blocking Misbehaving Users Using Multiple Nymbles in Blogs

Litty Antony, Leona Antony

M.Tech Student [Cyber Security], Sree Narayana Gurukulam College of Engineering, Kerala, India

ABSTRACT: A secure approach with the help of multiple Nymbles, for blacklisting misbehaving users. This overcomes the major limitations of anonymous networks i.e. posting bad terms in blogs. This system allows the server to blacklist a misbehaving user without compromising its anonymity. Server can blacklist users for whatever reason. The privacy of the blacklisted users is maintained. This system provides anonymous authentication where, a user can access web without prompting username and password. The capability of performing speed authentication and it also provides revocation auditability where a user can check whether it is blacklisted or not and can request admin to unblock. Server can selectively blacklist the misbehaving ones, without compromising their anonymity and thereby allow the genuine users to continue their access. This is mainly concentrating in blogs. It uses Google profanity services from Google to identify bad words posted in while creating blogs. And also it provides admin to have privilege to unblock a user which has been blocked by Nymble manager. Multiple Nymble have the ability of load balancing.

KEYWORDS: Nymble; Anonymous users; Blogs.

I. INTRODUCTION

Nymble is to allow for responsible, anonymous access online. It provides a mechanism for server administrators to block misbehaving users while allowing for honest users to stay anonymous; in fact even the blocked users remain anonymous. The name "Nymble" comes from a play on the word "pseudonym" and "nimble". Instead of giving users a simple pseudonym, the Nymble system assigns users "Nymbles"; that is, a pseudonym with better anonymity properties.

An anonymous blog is a blog without any acknowledged author or contributor. Anonymous bloggers may achieve anonymity through the simple use of a pseudonym, or through more sophisticated techniques such as layered encryption routing, manipulation of postdates, or posting only from publicly accessible computers. Motivations for posting anonymously include a desire for privacy or fear of retribution by an employer (e.g., in whistle-blower cases), a government (in countries that monitor or censor online communication), or another group. Blog provides anonymity, but some people abuse this anonymity. Since website administrators depend on blocking the IP addresses of misbehaving users, they are unable to block misbehaving users who connect through Tor—their IP address is hidden after all. Frustrated by repeated offenses through the Tor network, the usual response for websites such as Slashdot and Wikipedia is to block the entire Tor network. This is hardly an optimal solution, as honest users are denied anonymous access to these websites through Tor (or any anonymizing network for that matter).

By providing a mechanism for server administrators to block anonymous misbehaving users in blogs, hope to make the use of anonymizing networks such as Tor more acceptable for server administrators everywhere. All users remain anonymous— misbehaving users can be blocked without deanonymization, and their activity prior to being blocked remain unlinkable (anonymous).Nymble is based on two administratively-separate "manager" servers, the Pseudonym Manager (PM) and the Nymble Manager (NM). The PM is responsible for pairing a user's IP address with a pseudonym deterministically generated based on the user's IP address. The NM pairs a user's pseudonym with the target server. As long as the two managers are not colluding, the user's connections remain anonymous to the PM, pseudonymous to the NM (note that the user does not communicate directly with the NM, and connects to the NM through Tor), and anonymous to servers that the user connects to.

II. RELATED WORK

In [1] authors state a Nymble system which is able to block anonymous users in tor networks. It allow users a responsible, secured anonymous online access to blogs.The server administrators have the privilege to block

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

misbehaving users and also in fact even the blocked users remain anonymous but only discarded from the system. The main aim is to implement a system for the server administrators to block anonymous misbehaving users by keeping the utilization of anonymizingnetworks more acceptable for the server administrators. All users remainanonymous and the misbehaving users can be blocked without deanonymization.Anonymityhas received increasing attention in the literature due to user awareness of theirprivacy. Nowadays, anonymity provides protection to users to enjoy networkservices without being traced. Anonymizing networks such as Tor allow usersto access Internet services privately by using a series of routers to hide theclient's IP address from the server. Web site administrators routinely relyon IPaddress blocking for disabling access to misbehaving users, but blockingIP addresses is not practical if the abuser routes through an anonymizingnetwork. As a result, administrators block all known exit nodes of anonymizingnetworks, denying anonymous access to misbehaving and behaving users alike. To address this problem Nymble is developed, a system in which servers canblacklist misbehaving users in [2]. In [3],Anonymizing networks such as Tor allow users to access Internet services privately by using a series of routers to hide the client'sIP address from the server. The success of such networks, however, hasbeen limited by users employing this anonymity for abusive purposes such asdefacing popular Web sites. Web site administrators routinely rely on IPaddressblocking for disabling access to misbehaving users, but blocking IPaddresses is not practical if the abuser routes through an anonymizingnetwork. As a result, administrators block all known exit nodes of anonymizingnetworks, denying anonymous access to misbehaving and behaving users alike. To address this problem, we present Nymble, a system in which servers canblacklist misbehaving users, thereby blocking users without compromisingtheir anonymity. Our system is thus agnostic to different servers definitionsof misbehaviour servers can blacklist users for whatever reason, and the privacyof blacklisted users is maintained.

In [4] authors, Nymble systemis to allow its users a responsible, secured anonymous online access toother networks. It provides a reliable mechanism for the server administratorsto block misbehaving users while allowing the other users to stay anonymousand also in fact even the blocked users remain anonymous but only discardedfrom the system. The main aim is to implement a system for the server administratorsto block anonymous misbehaving users by keeping the utilizationof anonymizing networks more acceptable for the server administrators. Allusers remain anonymous and the misbehaving users can be blocked withoutdeanonymization. In [5] Authors contribute the advent of anonymizing networks assured thatusers could access internet services with complete privacy avoiding any possiblehindrance. This arrangement where series of routers form a network, hidethe users IP address from the server. However malfeasance of few malpractitionershas left this system with a loophole where users make use of thisanonymity to deface popular websites. Administrators who cannot practicallyblock a user using IP address are forced to shut all possible nodes that leadto exit. Thus deny access to both behaving and non-behaving users'altogether. And so end up blocking users with no compromise to their anonymity. Hencewe propose a system which is unidiomatic with different servers. Thus weaim at giving the administrator the right to block the malicious user withouthindering the anonymity of the rest. In [6] authors considered as company intranets continue to grow it is increasingly importantthat network administrators are aware of and have a handle on the differenttypes of traffic that is traversing their networks. Traffic monitoring and analysisis essential in order to more effectively troubleshoot and resolve issues whenthey occur, so as to not bring network services to a stand still for extendedperiods of time. Numerous tools are available to help administrators with themonitoring and analysis of network traffic. This paper discusses router basedmonitoring techniques and non-router based monitoring techniques (passiveversus active). It gives an overview of the three most widely used router basednetwork monitoring tools available (SNMP, RMON, and Cisco Net flow), andprovides information about two newer monitoring methods that use a combinationof passive and active monitoring techniques (WREN and SCNM).

III. PROPOSED SYSTEM

Now a day all website administrators are facing a big problem about spamposts and unwanted posts in their blogs, forums, etc. The main aim of thisNymble Blocking Misbehaving Users in Anonymizing Networks project is toblocking the users using multiple Nymble servers. It is very hard to delete eachpost entered by the unknown user or hard to delete his account, it is a timeconsuming process for website maintainers. This software application workswith the for major parts 1) Multiple Nymble manager 2) Pseudonym Manager3) Clients 4) Blog servers. It follows a user can login with his/her credentials, after login in to his profile he/she can create blogs with their needs. So hereadmin can have the rights to block/disable access to the users IP address, itcan record the user behaviour and also can unblock a valid user.

Web site administrators cannot blacklist individual malicious users IPaddresses; they blacklist the entire anonymizing network. Such measures eliminatemalicious activity through anonymizing networks at the cost of

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

denyinganonymous access to behaving users. In Nymble, users acquire an orderedcollection of Nymble, a special type of pseudonym, to connect to Websites.Without additional information, these Nymbles are computationally hard tolink, and hence, using the stream of Nymble simulates anonymous access toservices.

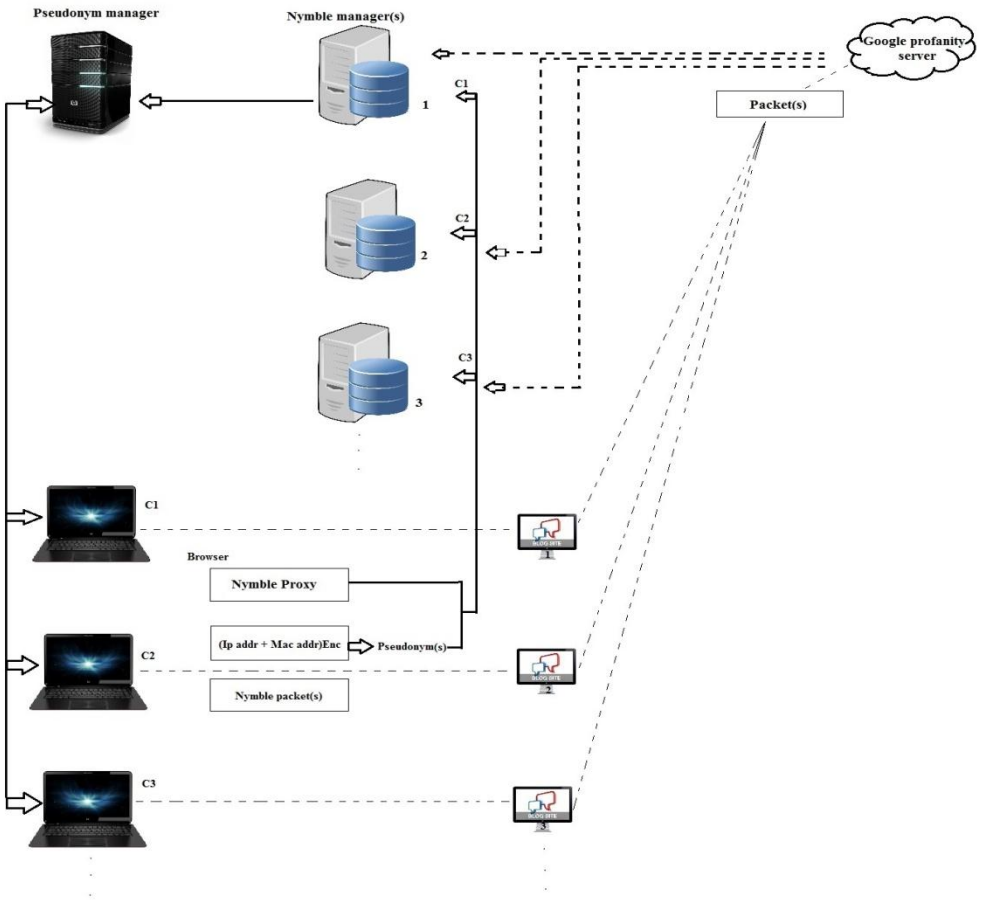

Figure 1: MultipleNymbles

A. *Pseudonym Manager*

The user must first contact the Pseudonym Manager (PM)[1] for authenticationpurpose and demonstrate control over a resource; for IP-address blocking, theuser must connect to the PM directly (i.e., not through a known anonymizing network), ensuring that the same pseudonym is always issued for thesame resource. After registration process, the pseudonym manager creates apseudonym by using IP address + MAC address of the particular system. It isa Hex decimal value. It can ensure that users are communicating with it directly. Pseudonymsare deterministically chosen based on the controlled resource, ensuring thatthe same pseudonym is always issued for the same resource. Note that the userdoes not disclose what server he or she intends to connect to and the PM duties are limited to mapping IP addresses (or other resources) to pseudonyms.

(a) How Admin unblock user?

If the user has been blocked, he/she has no more privilege to continue with theblog. So here the admin has the privilege to unblock a blocked user. If the user get blocked by the Nymble manager, can request the Nymble manager to unblock him/her with any specific request.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

B. *Multiple Nymble Managers(MNM)*

Servers can therefore blacklist anonymous users without knowledge of theirIP addresses while allowing behaving users to connect anonymously.This systemensures that users are aware of their blacklist status before they presenta Nymble, and disconnect immediately if they are blacklisted. Although itapplies to anonymizing networks in general. In fact, any number of anonymizingnetworks can rely on the same Nymble systems, blacklisting anonymoususers regardless of their anonymizing network(s) of choice. After creatingpseudonym, pseudonym manager send it to Nymblemanagers. After that client have to download an application to get control to theblog. If the login id and passwords are correct a ticket has given to the user cancreate blog. At the same time a Nymble packet will create by the pseudonymmanager.

Nymble packet has created with several constraints like Nymbletoken, timeetc. So here have to take the 1st field having 128 bit in size and named asNymble token. For the further purpose of Nymbletoken, it will be called asToken Id.This token id is hashed by using SHA-1 algorithm. After different steps in SHA-1,we get a hex value as signature. By the help of Nymble application, create sub tokens using ticket info. Finallyuser get ticket having particulartime period to access a blog.

(a) How misbehaving users blocked?

When user login through the Nymble application, he/she can access the blogsite for particular time period. If the user create a blog site, for a bad purposelike entering bad words, the word which he/she typed will go to Googleprofanity server(www.profanity.com).When it finds that the word is unparliamentarythen it will inform Nymble manager for further procedure. As we know by Nymble packet the users getblocked. When the user accessthe blog, the content in Nymble packet will be verified by Google profanityserver. If it founds any unparliamentary words, informs Nymble manager toblock the user. The Nymble manager takes signature (1st field) from Nymble packet, andalso takes the packet which is verified by the Google profanity server. If thesefields are equal, the particular user will be blocked.

(b) Use of multiple Nymble managers

A Nymble manager has to manager the entire client which would have been usedfor their purposes. So all clients will be redirect to only a Nymble manager, itmay create traffic. So as to avoid these problems, this method is introduced. Bymultiple Nymble, a user can use any of the Nymble managers. Single Nymble, where all of the accounts applications, databases, andfiles are stored and served from one server. Under some situations, however, it may be beneficial to operate from two or more servers. There are two commonreasons to add a server to your account: load balancing and consumingmore memory than one server can provide. If our account is host to a high-loadwebsite, may choose to add an additional server to your account. Rather thanseeing your site slows down due to the bottleneck of a single Nymble server, you can opt to spread the load across more than one machine. With an additionalmachine, you can use round-robin DNS load balancing: each incomingrequest is directed to one of your accounts servers in turn. While it is notautomatic failover or load-aware load balancing, this approach is simple andoften alleviates problems with high load websites. As in the case of Google servers, located in several areas all over the world.

One Google server cannot manager the whole request, processing etc. So asto avoid load balancing and for consuming more memory use multiple Googleservers. Same as in the case of multiple Nymble. Each Nymble manager issync with clients.

C. *Blog server*

Blog server notifies that its content has been updated. So anything which hasbeen created in blog by the client can be seen in blog server. So the servershould install in another system for easy access.

D. *Client*

Client first has to get the authorized access from the pseudonym server. Byusing Nymble application, client has to enter user-name and password foraccessing the blog site. If the user get blocked while typing bad words, he/shecan request admin to unblock by signing in the pseudonym web server. Andhe/she can view the log details.

IV. EXPERIMENTAL RESULTS

Blocking Misbehaving users using Multiple Nymble in Blogs deals with blockingmisbehaving ones. It is web based project; developed using J2EE and a java application in NetBeans 7.0.1.Belowshows screen shots.Fig 2 shows about the web page of pseudonym manager for login, registrationPurposes for user and admin.It also create pseudonym while creating a user for the blog access by the user.Fig 3 shows pseudonym managers, managers can put in different systems for blocking misbehaving clients.Figure 4 have Nymble application, we have to enter username and password if the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

user is valid and also can set duration to access the blog, then login it.Finally get a ticket with duration of 30 mintutes,after 30 mins the ticket will expire and user no more access blog site.Figure 5 shows a miniature of blog for creating blogs. It is having Home button, create new blog and created blogs. If we click on to create new blog, a page with have Name, subject and matter will be shown. So the user has to fill those fields. Any content he/she typed is a bad word e.g., "kill" and click to send, what will happen shows in figure 6.Automatic message will be shown when the user uses any bad word in the site. After that users ticket will be expired and he/she cannot access the site without requesting to unblock. User can login to pseudonym manager webpage for the log, if he /she has blocked then can request admin to unblock. When the admin login and see the request of the user is valid, then admin unblock the user and user can continue access.

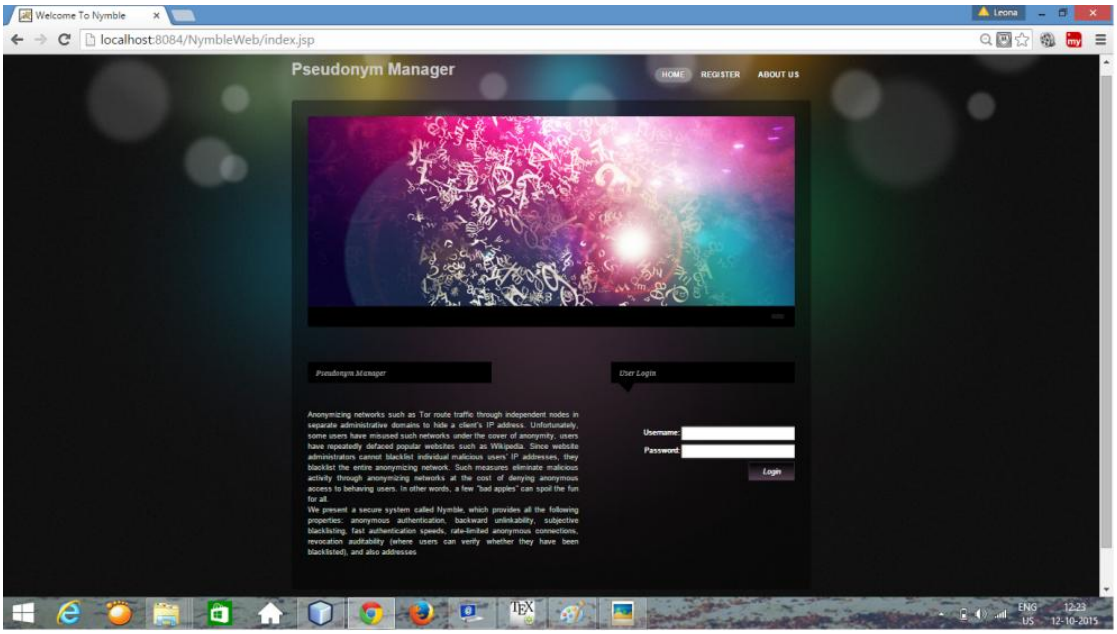

Figure 2: Pseudonym manager website

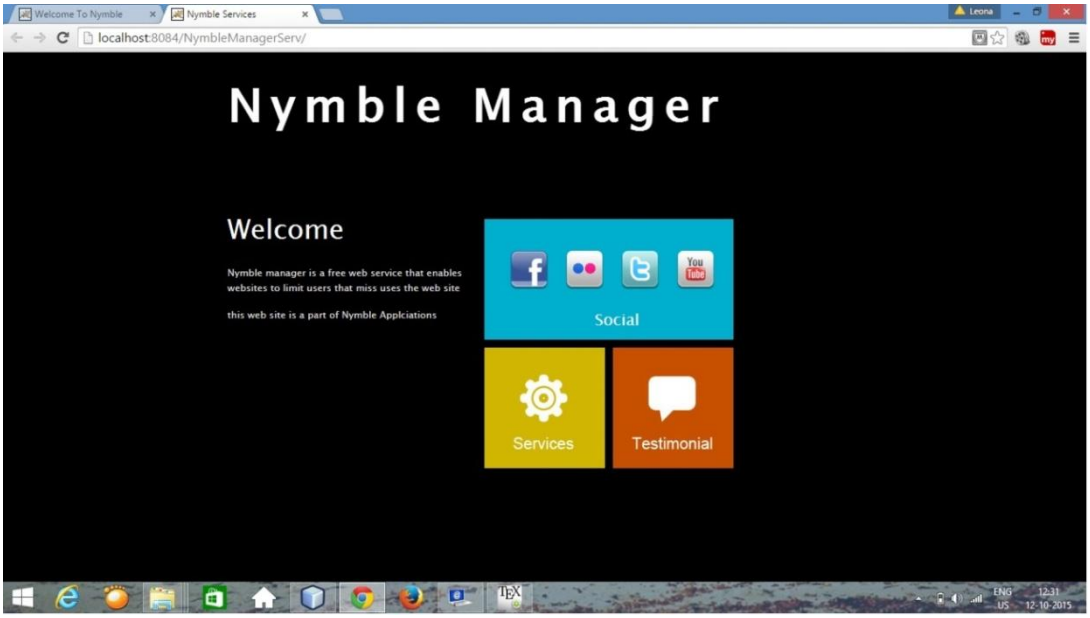

Figure 3: Nymble manager(s) webpage

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

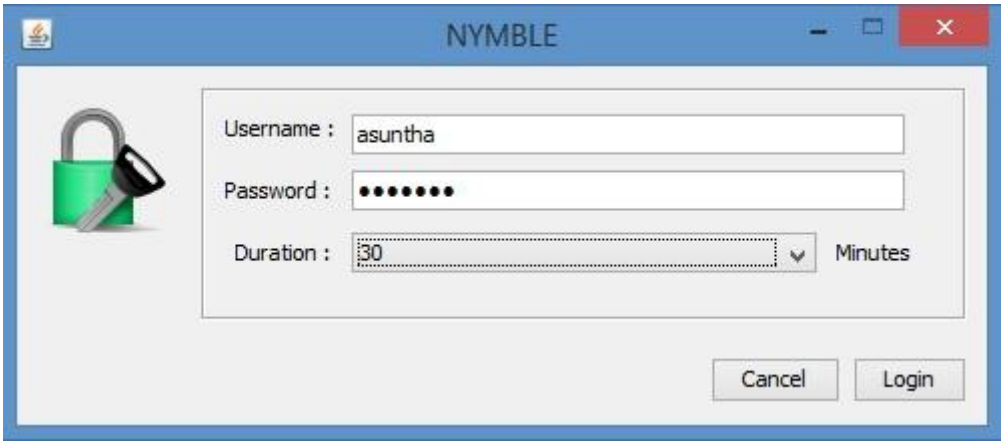

Figure 4: Nymble application

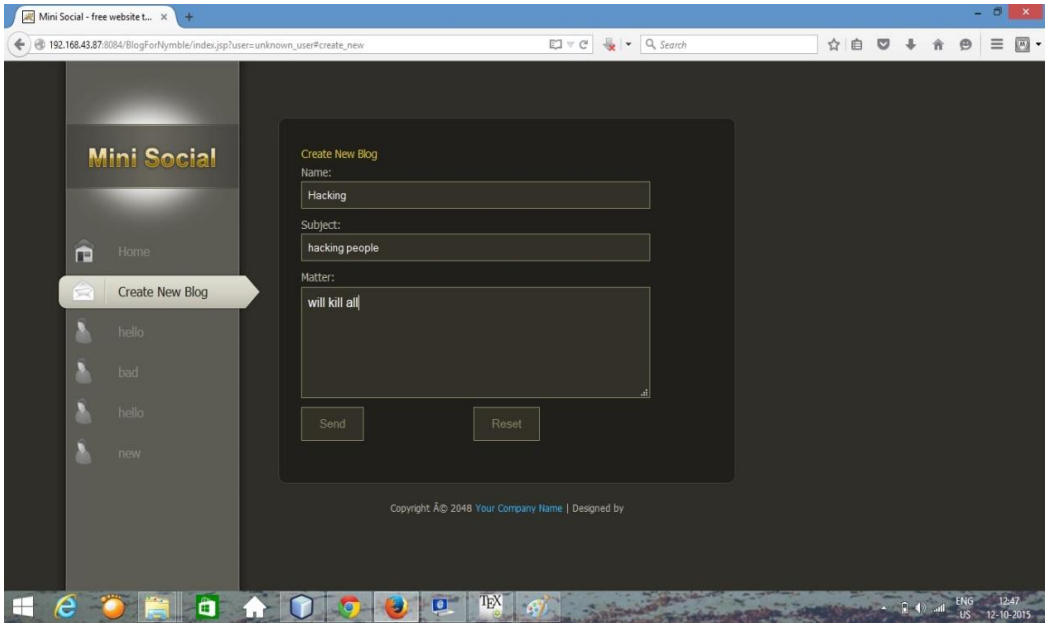

Figure 5: Bad words posted in blog

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

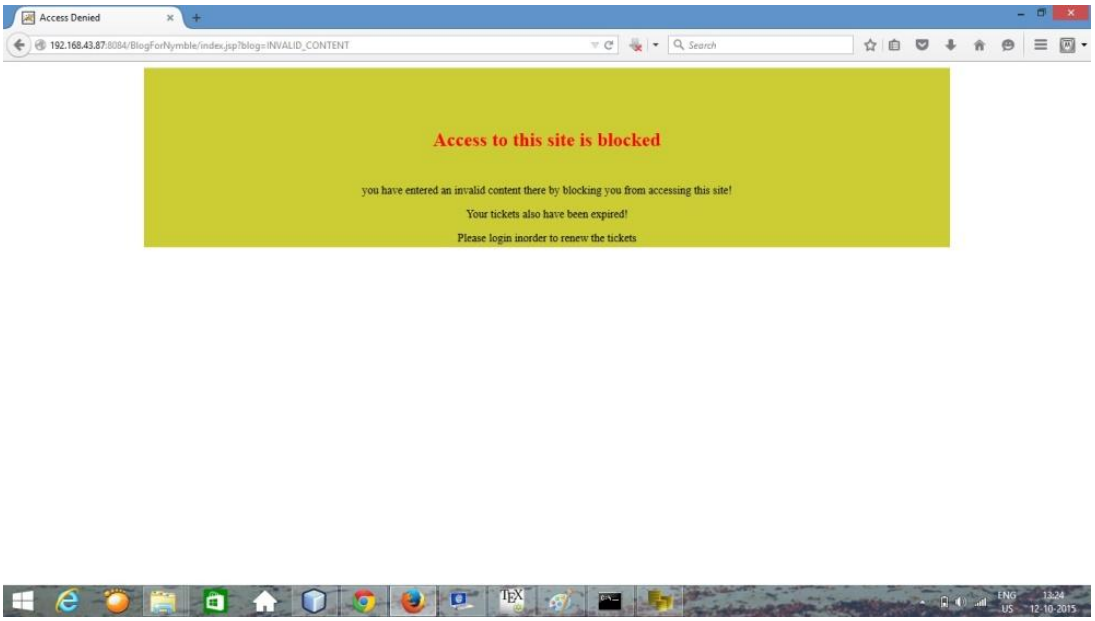

Figure 6: Access denied

V. CONCLUSION AND FUTURE WORK

A comprehensive credential system called Nymble, which can be used to add a layer of accountability to blogs. Servers can blacklist misbehaving users while maintaining their privacy, and we show how these properties can be attained in a way that is practical, efficient, and sensitive to the needs of both users and services. Hope it will increase the mainstream acceptance blogs been completely blocked by several services because of users who abuse their anonymity. The PM is responsible for pairing a user's IP address with a pseudonym deterministically generated based on the user's IP address. The NM pairs a user's pseudonym with the target server. As long as the two managers are not colluding, the user's connections remain anonymous to the PM, pseudonymous to the NM.

REFERENCES

1. SaurabhMalgaonker et al,"Nymble system which is able to block anonymous users in tor networks".2012 IEEE 11th International Conference on Trust.
2. M.Durga Prasad et al,"introduced Extended Nymble: Method For Tracking Misbehaving Users Anonymosly While Blocking" IEEE Security &Privacy, vol. 7, no. 1, 2009, pp. 50–57.
3. Patrick P. Tsang et al , "Blocking Misbehaving Users in Anonymizing Networks" Proc. 20th Annual Network & Distributed System Security Symp.(NSDD 13), 2013; www.internetsociety.org/doc/securityenhanced-se-android-bringing-flexible-mac-android.
4. SaurabhMalgaonkar et al," Implementation of Optimized Nymble System to Enhance Network Security". Security & Privacy, IEEE (Volume:8 , Issue: 2).
5. Prof. VinaLomte et al , "Nymble: Blocking Misbehaving Users In Anonymizing Networks" Proc. 22ndUsenix Security Symp. (Security 13), 2013, pp. 131–146.
6. Alisha Cecil et al., "Network Traffic Monitoring and Analysis TechniquesProc. 9th Int'l Conf. Mobile Systems, Applications, and Services (MobiSys 11), 2011,pp. 239–252.
7. Ryan Henry et al" Nymbler Nymble using VERBS,propose a new system modeled after NymbleTestability Assessment, 2004. IWoTA 2004.Proceedings.First International Workshop on DOI: 10.1109/IWOTA.2004.1428410 .
8. J.praveenkumar et al , "Mesh Technique for Nymble Architecture Sustaining Secrecy and Security in Anonymizing Networks" Proc. 11thUsenix Security Symp. (Security 02), 2002, pp. 17–31.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

BIOGRAPHY

Litty Antony received Master's degree in Cyber Security, from Sree Narayana Gurukulam College of Engineering, Mahatma Gandhi University, Kerala, India. She received Bachelor's degree in Information Technology in 2013 from Toc H Institute of Science and Technology, Cochin University of Science and Technology, Kerala, India.

Leona Antony received Master's degree in Cyber Security, from Sree Narayana Gurukulam College of Engineering, Mahatma Gandhi University, Kerala, India. She received Bachelor's degree in Computer Science and Engineering in 2013 from Toc H Institute of Science and Technology, Cochin University of Science and Technology, Kerala, India.