An Efficient Authentication and Access Control Scheme to Protect Integrity of Anonymous Networks

Santhosh S, Asst. Prof. Alok Ranjan

Abstract— **Concerns about privacy and security have received greater attention with the rapid growth and public acceptance of the Internet and the pervasive deployment of various network technologies. Anonymous network services is a large field of research and development that steadily continues to grow. Several credential systems have been proposed in which users can authenticate to services anonymously. Various anonymous network are readily available such as tor, i2p these allow users to access Internet services privately by using a series of routers to hide the client's IP address from the server. But this provision can be utilized both by the genuine users and misbehaving ones alike. Dishonest users take advantage of anonymity for abusive purpose such as website defacing. The administrators of these websites are unable to blacklist such users since their identity is not known. As a result they block the complete network using onion routing to ensure protection to their servers denying anonymous access to genuine and dishonest users alike. To surmount this problem, assuming a tor environment a credential system is proposed which enables the system administrators to detect any malicious activity and further block the malicious user continuing un-interrupted access to genuine users**

Index Terms—**Anonymous network, Backlist, Defacing, TOR**

I. Introduction

In today's scenario, most of the user activity is done online. Each user is having confidential information or important data in the online accounts. Reports have been generated saying that many users' data is leaked by the hackers and used for false purposes. This is causing a vital problem to the users of the system. There is no effective online monitoring scheme to record users' activity.

Attackers try to gain the personal details of the user's by using phishing activities and IP Spoofing. This has been causing many problems to the users personally as well as professionally. There are also hackers who would try to crack user security mechanisms by applying probabilistic methods. Attackers find it extremely fun to work with or they find it something to boast about. There is no effective online monitoring scheme to record users' activity. All the above mentioned problems are occurring because of absence of an effective security and monitoring system. Even though certain software have been built to identify the IP address and block the users from future accessing the system, the situation discussed in the paper deals with users using networks which hide the user's identity. This has been the main motivation behind this paper.

A. *Online Anonymity*

Anonymity [1] is a property of network security. An entity in a system has anonymity if no other entity can identify the first entity, nor is there any link back to the first entity that can be used, nor any way to verify that any two anonymous acts are performed by the same entity. A weaker, related property is pseudonymity. Pseudonymity means that one cannot identify an entity, but it may be possible to prove that two pseudonymous acts were performed by the same entity. For example, imagine that you have received a letter in the mail, with no signature, no return address, and no method for you to identify the sender or respond. This letter is anonymous. If the letter contains a secret key, and you then get later letters containing the same secret key, you can be pretty sure they came from the same entity. These latter letters are pseudonymous. If the letter contains instructions for responding, other than by some public channel, and you respond and the writer then responds to you, the writer is now pseudonymous [2] rather than anonymous. This is because you have two (or more) acts (mailing letters) that were performed by the same person.

Behaving and misbehaving users are the two faces of the same coin named anonymous networks. Since user identity can be disguised using anonymous networks malignant users use this advantage in a wrong way trying to deface websites, anonymously harassing users, trolling forums and chat rooms, and committing cyber vandalism. Due to few bad onions we can't discard the whole basket of onions. Anonymous networks provide huge benefits for behaving users for example, say Alice has a particularly embarrassing disease, when he goes into an anonymous chat room where she can discuss treatment of the disease with other sufferers, she doesn't expect her connection to be traced and her identity be revealed. Governments need anonymity for many reasons for example, law enforcement agencies do not always want to reveal that they are conducting intelligence gathering. Using anonymous networks they can maintain the integrity of their investigation. Onion routing helps protect this kind of anonymity.

Manuscript received Feb, 2013.

Santhosh S*, M.Tech student, Dept. of CSE, CEC, Mangalore, Karnataka, INDIA.*

Asst. Prof Alok Ranjan*, Dept. of CSE, CEC, Mangalore, Karnataka, INDIA.*

B. Advent of The Onion Router

Imagine a postal office containing N no of postman's working, one among them is handed a brown wrapper wrapped gift with his name on it. The person who hands it to postman tells to peel the paper with his name on it off of the gift to expose a new layer with a new postman name on it. His task is to deliver the gift to the new postman named, tell him to peel that layer of paper off and pass it on to the next person named and tell him to do the same. This goes on until the very center of the gift is handed off to the person to whom it is addressed. The idea is that the center of the gift contains a message sent to the final recipient by the very first person. But, because the gift travelled through so many hands, and along a random path through the crowd of postman's, anyone observing the receipt of the final message has no idea where it came from originally he or she only saw the final hand-off in a relay of hand-offs.

Onion routing [3] is a technique for anonymous communication over a computer network. Messages are repeatedly encrypted and then sent through several network nodes called onion routers. Like someone peeling an onion, each onion router removes a layer of encryption to uncover routing instructions, and sends the message to the next router where this is repeated. This prevents these intermediary nodes from knowing the origin, destination, and contents of the message. Onion routing [4] was developed by Michael G. Reed, Paul F. Syverson, and David M. Goldschlag, and patented by the United States Navy. In onion routing, instead of establishing a direct connection between the two hosts that want to communicate, the connection will be routed through a set of routers called onion routers and thereby allow the communication to be anonymous. Every node will only have information about its previous hop and the next hop. In fig 1 Alice chooses a path through the onion network to communicate with Bob. Darkened nodes are the chosen proxy servers (onion routers). Thick, dotted lines are encrypted links; thin, solid lines are potentially unencrypted.

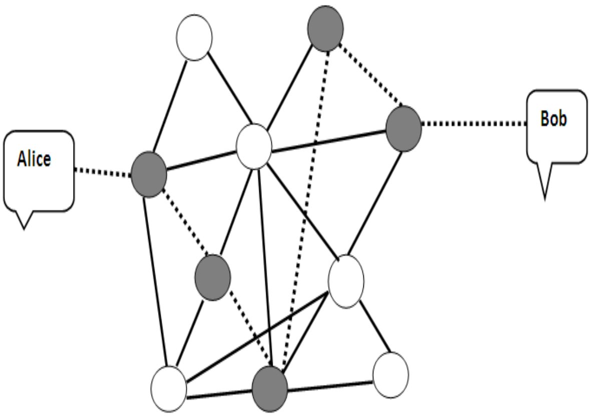
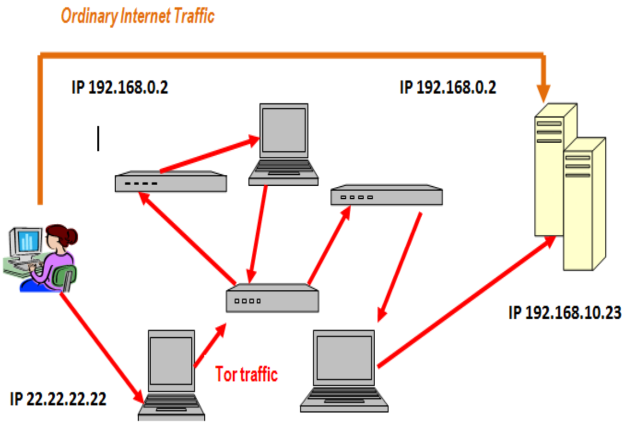


Fig 1: Onion Routing

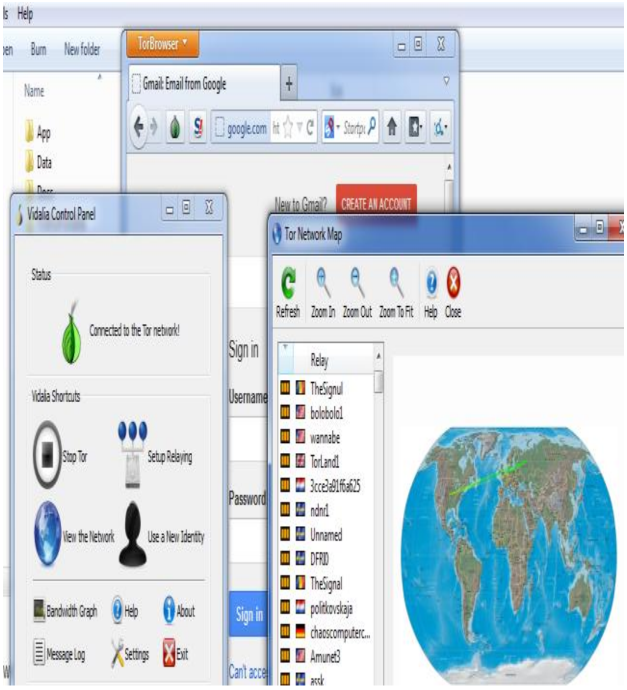
When a client application wishes to establish an anonymous connection to a server, it first of all connects to an application proxy. The packets are then forwarded to an onion proxy. The onion proxy creates a route over the onion network and then constructs a special data structure, an onion. An onion is a multiply encrypted layered structure, with information about the route through the network being spread across the layers. The onion is then passed on to an entry funnel. When an entry funnel (or any other onion router) receives an onion, it decrypts it, which reveals a layer containing information about the next hop in the route constructed by the onion proxy.

This layer is then stripped off and the onion is forwarded on to this next hop. Eventually, the onion reaches an exit funnel. The decrypted packet is identical to the packet that was produced by the application proxy at the beginning of the connection. This packet will then be sent to the destination host. This onion routing technique is predominantly use by TOR [5] technology. TOR is an anonymizing Internet proxy service that allows people and groups to improve their privacy and security on the Internet. Today, it is used every day for a wide variety of purposes by normal people, military, journalists, law enforcement officers, activists, and many others. TOR browser [6] can be effective tool for anonymous browsing.



User data request pass by randomly selected other volunteer node on network disguising the identity

Fig 2: Working Scenario of TOR



Connected to the Tor network!

TheSignul
bolobolo1
wannabe
TorLand1
3cce3a91f6a625
ndnr1
Unnamed
DFRI0
TheSignal
politkovskaja
chaoscomputerc...
Amunet3
ask

Fig 3: TOR Browser

II. Driving the existing systems

A. Pseudonymous Credential systems

The private signatures, group signatures and private credentials are the three main methods of the pseudonymous credential system. The system was made to stop and to put control on the misbehaving actions of the hidden IP address users by providing a direct permanent system to the new or blacklisted users and providing them the services in form of pseudonyms. This way the users can get complete anonymity plus their actions are completely traceable by the service providers through pseudonyms. If the users start to misbehave then the service providers simply stop giving the pseudonyms to the users and blocking them from the services. There is no need to revoke them, thus reducing complicated methods to trace the history of the user. On joining the pseudonyms [7] of the users and get the complete history of the user is obtained. This is a very successful formulization of anonymous blacklisting technique.

The status of the privacy can be selected by various privacy and security policies and the users are given credentials so that they can easily communicate with several other multiple organizations and communities without compromising their privacy however according to the level of security it is possible that some users have a low level of security and some of their information is under the risk of being revealed that is why it is necessary for the users to take all the precautions by enhancing the status of their security level by taking facilities from their service provider before communicating with other organizations or communities. The connection can be made form one credential to the other and the credential plays the act of resource of communicating but having the credential and communicating with the other organization through it makes the security of the users very low that is why the privacy policies can now be selected by the user to enhance the security.

B. Anonymous Credential Systems

When you submit your final version, after your paper has been accepted, prepare it in two-column format, including figures and tables. In Pseudonymous Credentials Systems, it assigns aliases to the users using which they login into servers. The servers can block the aliases of the users on the event of misconduct. Thus the purpose of anonymity is not achieved. Also it is very difficult to come up with a practical application scenario of using Pseudonym System by eliminating the constant communication between the entities. The anonymous credential systems have presented the signature systems which are allotted by the group manager to the group members or the users. These signatures [9] are traceable and whenever a user misuses his facilities the manager steps in and traces the history of the user by the signatures as these signatures enables the manager to set a trap door through which the activities and the history of the user can be traced with keeping the anonymity of the user. The signature system also holds lot of criticism that it might place the privacy of the concealed users at risk and that is why many different and efficient signature schemes are presented by different researchers, information technologists etc. The problem arises because the secret key which is kept by the signer is required to change between the invocations of the algorithms and the ideal random functions are the most remarkable signature schemes but these schemes are only applicable in the ideal structures, in the real system it is very difficult and requires many changes to make it successful. These schemes however can be used as the basic blocks or units for the cryptographic protocols and schemes. The latest scheme discussed has the basic solution of the secret key that it requires RSA assumption instead of the secret key but it is yet not reported as secure.

C. Traceable Signatures

In this mechanism, the data can now be signed like the documents of paper. The electronic signatures [10] can be assigned to each user to put them on their messages instead of names and the encoded message will also contain their signature so the receiver will have the authentication about the sender without knowing the IP address of the user or any other identity related information about him. On the other hand there are group signatures too which a group or a network can use to identify itself and its users through the signature. The signature tactic also ensures the identity of the users who deal with the e-cash system and their identity secrecy can lure them away from their goals that is why the signature will keep them on the right track as their will be the risk of getting caught otherwise. Drawbacks of Traceable Signature involve these signatures are traceable and whenever a user misuses his facilities the manager steps in and traces the history of the user by the signature.

D. Blacklistable Anonymous Credential Systems

The top most priority of every anonymous service providers is to keep the anonymity of the users even if they are blacklisted or are going to be revoked. Most of the IP concealing services involve the trusted third party to reveal the identity of user so that the service remains unknown from the real identity of the user and the users IP is revealed along with his details but this is a very big drawback for the anonymous IP service providers because the main goal of these services is to keep the privacy and when the same privacy is not kept then there is no use of taking their services that is why the new technologies introduced enables the services to revoke the users without involving any trusted third party [11] and revealing the identity of users is placed as the very last option when the person is involved in very serious criminal activities instead of misbehaving with various websites or double spending the e-cash.

There are popular websites like YouTube and Wikipedia which provide specific tools to their users especially when it comes to Wikipedia which allows its users to make changes according to their preferences in the documents which allows the anonymous IP address users to violate the terms of these websites. The misbehaving user’s identity is revealed by the IP concealing services by involving the trusted third party however the punishment off revealing the identity just because of misusing the facility by violating the rules of the websites is too big although if the users start to go beyond their limits like double spending their e-cash then they can be punished by getting their IDs revealed that is why the users don't get the identity revealed just because of violating the terms of websites but are only revoked or blacklisted because the increased involvement of the Trusted Third Party decreases the standard and the security level of the IP concealing.

E. Privacy Enhanced Revocation with Efficient Authentication

When you submit your final version, after your paper has been accepted, prepare it in two-column format, including figures and tables. The IP concealing companies prefer to take actions against their users with keeping their identities in secret. They keep on trying not to involve any third party and without knowing the identity of a user they take actions against him. The PEREA [12] is the completely new anonymous authentication scheme which is the modified and advanced form of the BLAC. It has a larger capability of revoking a list for a larger number of time unlike BLAC and its efficiency has been approved since it leaves no chance for the entrance of any third party because the third party's participation means that the identity of the blacklisted user will be revealed which is against the rules and motives of the anonymous authentication software. The blacklisted members are however deprived from the membership with the company having the non membership proofs. The subjective blacklisting includes the privacy enhanced revocation and also the security of the users.

To enhance the performance and security of the anonymous service the service providers have launched the technology of tickets. These tickets allow the users the authentication to use the anonymous IP services securely and these tickets are approved and allotted to the users by the mangers of the service because these tickets provide the history of the user and the ticket record is kept safe by the service providers as these tickets help to keep tabs on the users in case they try to misbehave by breaking the rules of the cyber world. With the help of these tickets the list of the users who are supposed to be blacklisted due to their behavior is made easily with fair tracing and is kept safe plus there is also a plus point that the service provider managers also have the proof of the misbehavior done by the users so that their actions cannot be claimed and even if claimed then the claims are proved baseless.

The security assurance of the users of the anonymous services is very necessary. The users which are revoked and blacklisted should not be able to get access with their anonymous IPs neither they should be able to use any kind of anonymous service provider's services and facilities. There are also hackers and mischief makers who try to use these facilities without even becoming the member of the service so that they don't even have to give any kind of information about them. These types of users are always having negative intentions and the security of the anonymous service providers should be very strong so that they can easily block such invaders. Another point which should be taken care of is that the involvement of the trusted third party should be avoided completely or should be decreased to a very low level so that there should be no threat against the security of the service so that the behaving users can feel completely secured in using the anonymous IP service.

F. Concerning Drawbacks

- Existing approaches does not provide the backward unlinkability were privacy of the blacklisted user is not at risk.
- Existing systems weakens the anonymity provided by the anonymizing network.
- Scalability Issues are Predominant.

III. ARCHITECTURAL DESIGN FOCUS

A. Renaissance of Proposed Solution

Anonymous network services is a large field of research and development that steadily continues to grow. The interests and demands of the general public are increasing all the time. With the next generation networks there is a big concern granting users with anonymity and privacy protection, although they also have to be accounted for any illegal activities that they perform on the network. A novel credential system is proposed which preserves integrity of the anonymous networks blocking malignant users if they indulge in defacing activity, behaving users are allowed to use the network uninterrupted. Proposed solution ensures secure communication in onion routing network between the server and user, when the identity of the user is not known to the server. The major components of the system are Alias Manager, System Manager which can be together addressed as System Administrators.

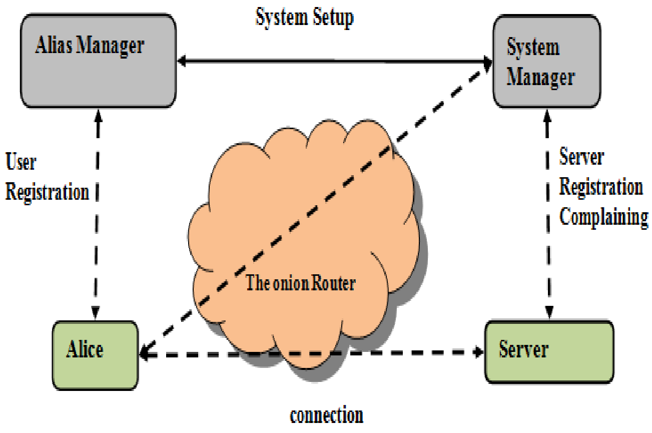


Fig 4: Architectural Design

In the registration phase, the user provides his identity resource to Alias Manager. Alias Manager assigns an alias name (pseudonyms) to a particular user. Using this information, the user communicates with the System Manager and requests for nymble tickets [13]. Using these tickets the user connects to desired server. The Alias Manager maintains the list of alias name of the users based on the IP address. The responsibility of the Alias Manager is to only to map the IP address to their corresponding alias names. The Alias Manager ensures that the same alias name is always assigned to the same IP address. User provides his registration credentials to the alias manager and the alias manager generates pseudonyms corresponding to the resources provided by the user and the same is submitted by the user to the System Manager. The System Manager is the major component of the proposed system which is also part of System Administrators of the whole system. After communicating with the Alias Manager, the user contacts the System Manager with the pseudonyms and at System Manager the nymble tickets are generated, with these tickets user communicates with the server. A new server, who wants to be a part of the proposed system, needs to communicate with the System Manager providing all the server details. If any misbehaving activity is noticed by the server it complaints to the System Manager and the malignant user will be blocked.

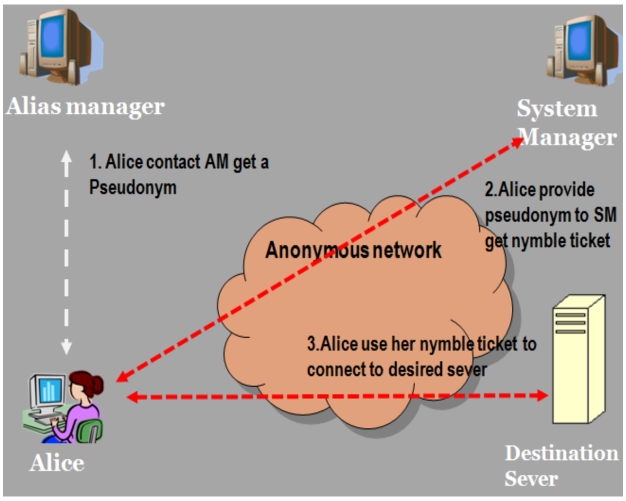

Alias manager
System Manager
1. Alice contact AM get a Pseudonym
2.Alice provide pseudonym to SM get nymble ticket
Anonymous network
3.Alice use her nymble ticket to connect to desired sever
Alice
Destination Sever

Fig 5: Connection to Deserved Server

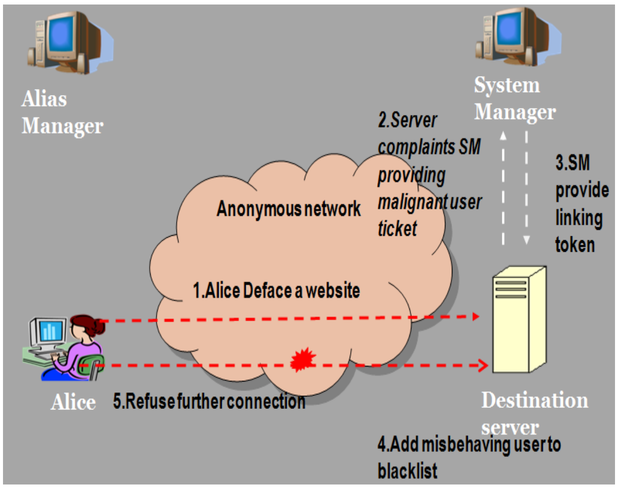

Alias Manager
System Manager
2.Server complaints SM providing malignant user ticket
3.SM provide linking token
Anonymous network
1.Alice Deface a website
Alice
5.Refuse further connection
Destination server
4.Add misbehaving user to blacklist

Fig 6: Block Malignant User

B. *Principle Methodology Involved*

Users acquire an ordered collection of nymbles, a special type of pseudonym, to connect to Websites. Without additional information, these nymbles are computationally hard to link, and hence, using the stream of nymbles simulates anonymous access to services. Web sites, however, can blacklist users by obtaining a seed for a particular nymble, allowing them to link future nymbles from the same user those used before the complaints remain unlinkable. Servers can therefore blacklist anonymous users without knowledge of their IP addresses while allowing behaving users to connect anonymously. If a user misbehaves, the server may link any future connection from this user within the current linkability window. A user connects and misbehaves at a server during time period *t** within linkability window [13] *w**. The server later detects this misbehavior and complains to the SM in time period t_c $(t^* < t_c \_ t_L)$ of the same linkability window *w**. As part of the complaint, the server presents the nymble ticket of the misbehaving user and obtains the corresponding seed from the SM. The server is then able to link future connections by the user in time periods t_c, t_c *+1,...,* t_L of the same linkability window *w** to the complaint. Therefore, once the server has complained about a user, that user is blacklisted for the rest of the day.

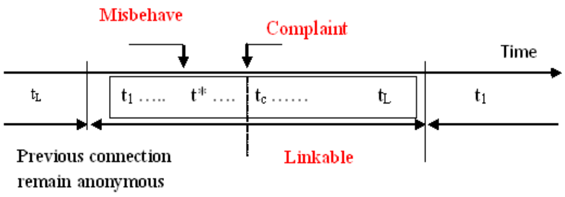


Fig 7: Life Cycle of a Misbehaving User

The main focus of the proposed paper involves

- Blacklist abusive users: Provides a means by which servers can blacklist misbehaving users of anonymous networks while maintaining their privacy.
- Uninterrupted access to genuine users: The legitimate users of the system can always be sure that they are provided uninterrupted access, their identity will remain unknown and also that they would not be deprived of using any server resources due to some malicious activity in the network.

Algorithm 1: Alias Manager

Start

Step1: User contacts AM, demonstrate control over a resource.

Step2: Generate alias names concerning to user resource.

Step3: System setup with System Manager to check the integrity of the pseudonyms generated.

Stop

Algorithm 2: System Manager

Start

Step1: User contact SM with alias name get rewarded with Nymble tickets

Step2: Server Registration

Step3: Server complaint misbehavior

Step4: SM provides linking token of malignant user

Stop

Algorithm 3: Server

Start

Step1: user connect to desired server using nymble tickets

Step2: server complaint SM about malignant user providing concerning tickets

Step3: server receives liking token from SM add user to blacklist

Step4: Refuses further connections from the same user.

Stop

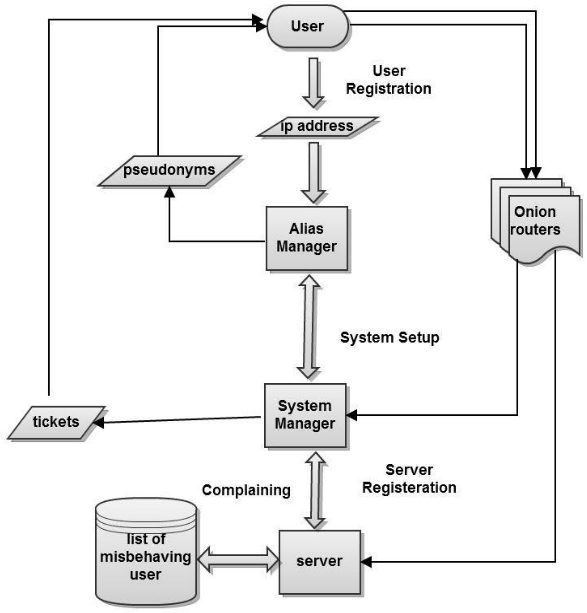


Fig 8: Flow Chart

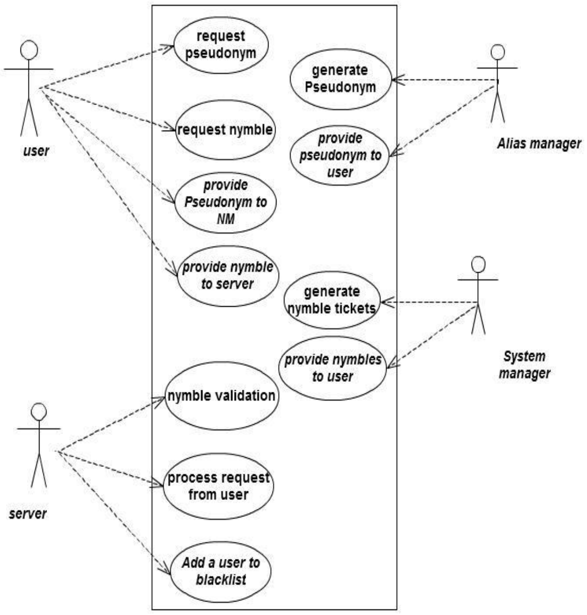


Fig 9: Use Case Diagram

IV. CONCLUSION

Online anonymity is a very difficult problem which pressed the need for more secure and robust networks. Just like many other technologies, onion routing can be used for both positive and negative purposes. Criminals can evade identification in some cases using Onion Routing but this just can't be a reason for completely condemning onion routing. The users who are benefitting from onion routing right now are a pretty good reason for onion routing to continue. While it attracts it share of attackers, it continues to be the best tool for anonymity and free information access on the internet. To surmount the above discussed problems, assuming a tor environment a credential system is proposed which enables the system administrators to detect any malicious activity and further block the malicious user continuing un-interrupted access to genuine users in anonymous networks increasing the mainstream acceptance of anonymizing networks such as Tor, which has, thus far, been completely blocked by several services because of users who abuse their anonymity.

ACKNOWLEDGMENT

The author wish to thank Ashwini Achar, Prof Alok Ranjan for their help in early stages. This paper presents a significant improved method for integrity maintenance of anonymous networks.

REFERENCES

[1] Boukerche, A.; El-Khatib, K.; Li Xu; Korba, L., SDAR: *"A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Networks"*, IEEE Comput. Soc. 29 -2004

[2] Ray Dillinger, Cyclopedia Cryptologia-an online encyclopedia of cryptographic protocols. http://www.disappearing-inc.com

[3] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digitial Pseudonyms", Communications of the ACM, Vol 24, No 2 (1981)

[4] Michael G. Reed, Paul F. Syverson, and David M. Goldschlag "*Anonymous Communication and Onion Routing"*, IEEE Journal on Selected Areas in Communication Special Issue on Copyright and Privacy Protection, 1998.

[5] Roger Dingledine, Nick Mathewson, Paul Syverson. Tor: "*The Second-Generation Onion Router"*. Usenix Security 2004, August 2004.

[6] url: https:// www.**tor**project.org.in/,

[7] Yuko Tamura and Atsuko Miyaji," *Anonymity-Enhanced Pseudonym System"*, Applied Cryptography and network security, Springer 2006

[8] Yuko Tamura and Atsuko Miyaji," *Anonymity-Enhanced Pseudonym System"*, Applied Cryptography and network security, Springer 2006

[9] Jan Camenisch1 and Anna Lysyanskaya, "*Signature Schemes and Anonymous Credentials from Bilinear Maps"*, Advances in Cryptology – CRYPTO, Springer 2004

[10] Stephen R. Tate, He Ge "*Traceable Signature: Better Efficiency and Beyond"*, Computation Science and its applications – ICSA, Springer 2006

[11] Patrick P. Tsang, Man Ho Au,Apu Kapadia,Sean W. Smith, "*Blacklistable anonymous credentials: blocking misbehaving users without ttps"*, Proceedings of the 14th ACM conference 2007.

[12] Man Ho Au, Patrick P. Tsang, Apu Kapadia, PEREA: *"Practical TTP-Free Revocation of Repeatedly Misbehaving Anonymous Users"*, Proceedings of the 2011 ACM workshop

[13] Patrick P. Tsang, Apu Kapadia, *"Nymble: Blocking Misbehaving Users in Anonymizing Networks"* IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 8, NO. 2, MARCH-APRIL 2011