ISSN:0975-9646

Enhancement of Nymble through Ontological Approach

Sateesh Gudla[1], Sarat Chandra Mongam[2], Sindhuri Boddu[3], Satish Mallampalli[4]

[1]Associate professor, Department of IT,
Lendi Institute of Engineering and Technology,
Andhra Pradesh, India

[23,4] Student, Department of IT,
Lendi Institute of Engineering and Technology,
Andhra Pradesh, India

Abstract: We present a security mechanism that can block the misbehaved users through ontological approach in the network and can provide access to the genuine users by blocking the particular user instead of blocking the IP address of the system which can block all the users who use the same system and thereby making the network more secure and accessible to the genuine users. Through the proposed system we are Providing more chance to the genuine users to continue the privileges given to the them and Security of the system is improved when compared to the existing system and fairness is also improved by making the blacklist table public thus Reliability is also enhanced as there is no chance for the genuine users to be blocked.

Keywords: Ontology, Anonymzing, Blacklisting, Dynamic blocking, forgiving.

1. INTRODUCTION:

Anonymizing networks such as Tor allow users to access Internet services privately by using a series of routers to hide the client's IP address from the server. The success of such networks, however, has been limited by users employing this anonymity for abusive purposes such as defacing popular websites. Website administrators routinely rely on IP-address blocking for disabling access to misbehaving users, but blocking IP addresses is not practical if the abuser routes through an anonymizing network. As a result, administrators block all known exit nodes of anonymizing networks, denying anonymous access to misbehaving and behaving users alike. To address this problem, we present a system in which servers can "blacklist" misbehaving users, thereby blocking users without compromising their anonymity. Our system is thus agnostic to different servers' definitions of misbehavior — servers can blacklist users for whatever reason, and the privacy of blacklisted users is maintained.

2. BACKGROUND OVERVIEW:

2.1 Existing System

In the existing system it is intended to provide SECURITY to the network. Nymble is a system that allows websites to selectively blacklist users of anonymizing networks such as Tor without knowing the user's IP-address [1]. Users not on the blacklist enjoy anonymity while blacklisted users are not allowed future connections for duration of time while their previous connections remain unlink able.

Drawbacks of Existing System:

The main drawback of Nymble is that it blocks IP address of the misbehaving user [1] (Each system is associated with unique IP address) hence making other users restricted to the website access and therefore providing a chance for the genuine users to be blocked sometimes.

3. THE PROPOSED SYSTEM:

This Application can be used in any organization where a network is created among a group of users to share data and mostly this Nymble mechanism is used where security is the major concern. Through this Nymble through Ontological Approach, the views of the user is personalized and analyzed and depending on the views, the user may be forgiven from blocking. So this mechanism provides more reliability to the genuine users to stay anonymous. Also, by blocking the user instead of IP address of the system can overcome this drawback and this provides more flexibility to the genuine users.

3.1 System Overview

In order to provide the security we will block the misbehaving. Whereas the Nymble System consists of the various modules User Registration module enables the user to register the user in the server. User Login will validate the particular user by given username and the password. Mainly the Nymble system consists of the two managers they are the Pseudonym manger and the Nymble manager. The Pseudonym Manager will authenticate the user .After the successful authentication the user is connected to the Nymble Manager; it will give the nymble ticket to the user. By that nymble ticket user will logon to the Server and access the resources. If a user want to access the resources from the blocked IP address. Then the system will ask the views (questions) to the user. If the views are appropriate then user has the permissions to access the resources over the network. If in the middle, the particular user tries to misbehave the resource. Then the system will block the user dynamically.

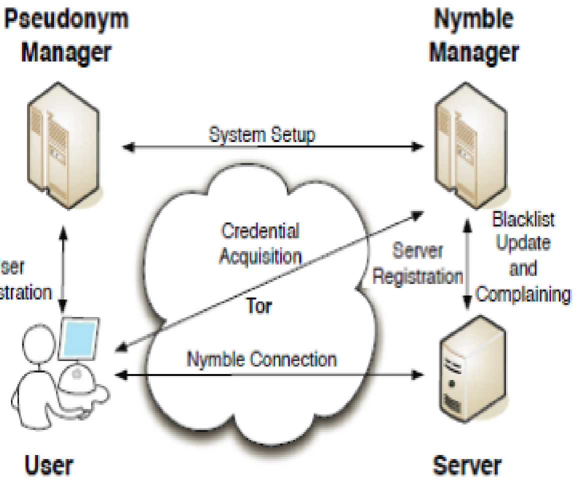


Figure 1: Architectural design

ONTOLOGICAL APPROACH:

Information extraction systems employ ontologies as a means to describe formally the domain knowledge exploited by these systems for their operation. Through this approach we can restrict the misbehaved users thereby we can easily assess the unique identity of the particular user, thus we can give access permission to the user who are genuine.

Modules:

Pseudonym Manager:

The user must first contact the Pseudonym Manager (PM) and demonstrate control over a resource; for IP-address blocking, the user must connect to the PM directly (i.e., not through a known anonymizing network), ensuring that the same pseudonym is always issued for the same resource**.**

Nymble Manager:

Servers can therefore blacklist anonymous users without knowledge of their IP addresses while allowing behaving users to connect anonymously. Our system ensures that users are aware of their blacklist status before they present a nymble, and disconnect immediately if they are blacklisted. Although my work applies to anonymizing networks in general, I consider Tor for purposes of exposition. In fact, any number of anonymizing networks can rely on the same Nymble system, blacklisting anonymous users regardless of their anonymizing network(s) of choice.

Blacklisting a user:

Users who make use of anonymizing networks expect their connections to be anonymous. If a server obtains a seed for that user, however, it can link that user's subsequent connections. It is of utmost importance, then, that users be notified of their blacklist status before they present a nymble ticket to a server. In My system, the user can download the server's blacklist and verify her status. If blacklisted, the user disconnects immediately.

NYMBLE-AUTHENTICATED CONNECTION:

Rate-limiting

It assures any honest server that no user can successfully nymble-connect to it more than once within any single time period. Non-frame ability guarantees that any honest user who is legitimate according to an honest server cannymble-connect to that server. This prevents an attacker from framing a legitimate honest user, e.g., by getting the user blacklisted for someone else's misbehaviour. This property assumes each user has a single unique identity.

3.2 *System Design:*

The importance of software design can be stated in a single word *"Quality"*. Design provides us with representations of software that can be assessed for quality. Design is the only way that we can accurately translate a customer's requirements into a finished software product or system without design we risk building an unstable system, that might fail it small changes are made or may be difficult to test, or one who's quality can't be tested. So it is an essential phase in the development of a software product.

In this application, we used Waterfall Model for software engineering process which is also called as Classic Life Cycle Model. This model suggests a systematic, sequential approach to software development that begins with Customer Specification of requirements and progresses through planning, modeling, construction, and deployment, culminating in on-going support of the complete software.

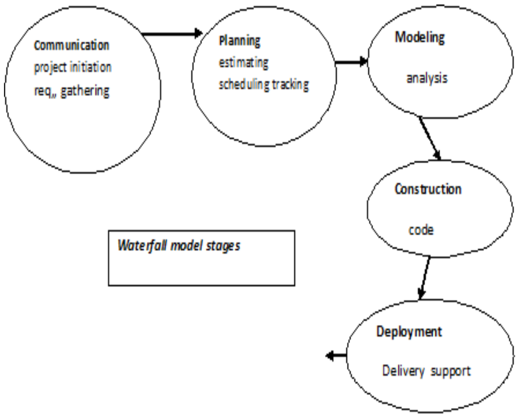


Figure 2: Waterfall Model Stages.

4. FEATURES:

The Following are the prominent features of the above discussed Application.

- More flexibility can be provided in a network.
- This Application can be used in any organization for security of the network.
- Status of the user can be seen by all the users in the network.

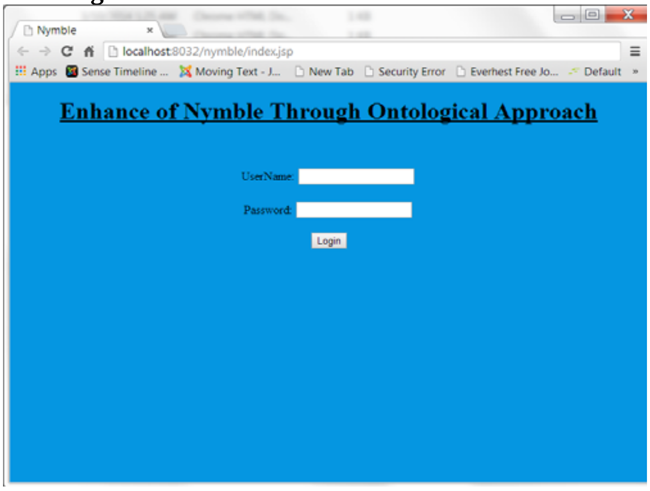
5. SCOPE AND APPLICATION:

- Block the Misbehaving users through the ontological approach covers only security aspect of a network and this software can be used only for security purpose i.e., Security Domain
- This Nymble can be used in any Organization to protect a network from being misbehaved by its users.
- This Ontological Approach for Nymble personalizes views of the user before blocking the user and if the views are appropriate the access can be given.

6. RESULTS:

The following are the results (fig3) that are generated through which no chance for the genuine users to be blocked and if misbehaviour is observed at any point of time in the respective Session, they will be blocked using Dynamic Blocking.

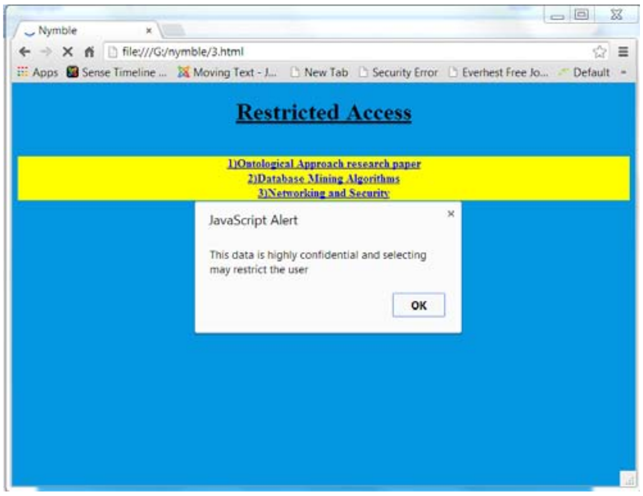
User Login Test:



Enhance of Nymble Through Ontological Approach

UserName:

Password:



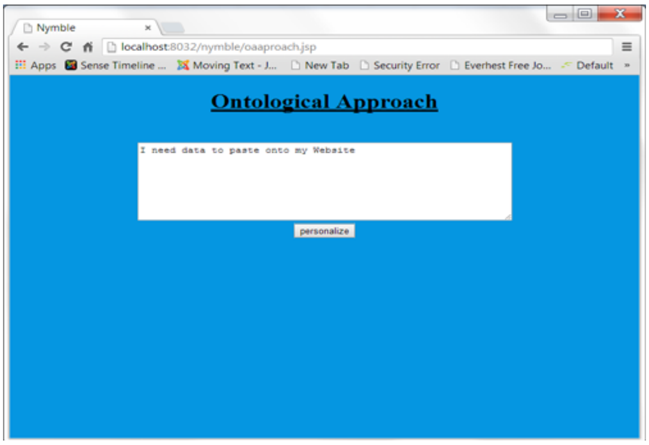
Restricted Access

1)Ontological Approach research paper
2)Database Mining Algorithms
3)Networking and Security

JavaScript Alert

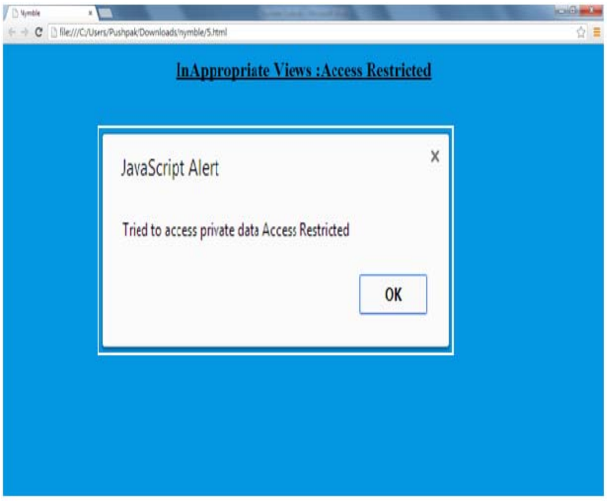
This data is highly confidential and selecting may restrict the user

Access File:



Ontological Approach

I need data to paste onto my Website



InAppropriate Views :Access Restricted

JavaScript Alert

Tried to access private data Access Restricted

Figure 3: Generated Results

7. CONCLUSION:

In this Implementation of Nymble through Ontological Approach there is a no chance for the genuine users to be blocked which is efficient technique that allows genuine users who are using blocked IP address of the particular system can still access the website until they continue to be genuine and if misbehiour is observed at any point of time in the respective Session, they will be blocked using Dynamic Blocking.

8. ACKNOWLEDGEMENT

We express our sincere and profound gratitude to our principal Dr.V.V.Rama Reddy, management members our chairman Sri P.Madhusudhana Rao, Vice-chairman Sri P.Srinivasa Rao and Secretary Sri K.Siva Rama Krishnan for their valuable support and guidance.

This Implementation of Nymble through Ontological Approach is possible only because of the support of my college (Lendi Institute of Engineering and Technology) Management and our guide Mr.G.Sateesh and Faculty members. They gave support by providing all facilities and also helped us in all aspects.

REFERENCES

[1] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik. A Practical and Provably Secure Coalition-Resistant Group Signature Scheme. In CRYPTO, LNCS 1880, pages 255–270. Springer, 2000.

[2] G.Ateniese, D.X.Song, andG.Tsudik. Quasi-EfficientRevocation in Group Signatures. In Financial Cryptography, LNCS 2357, pages 183–197. Springer, 2002.

[3] Software Engineering: A Practitioner's Approach by Roger Pressman.

[4] Patrick P. Tsang, Apu Kapadia, Member, IEEE, Cory Cornelius, and Sean W. Smith.

[5] M. Bellare, H. Shi, and C. Zhang. Foundations of Group Signatures: The Case of Dynamic Groups. In CT-RSA, LNCS 3376, pages 136–153. Springer, 2005.

[6] D. Boneh and H. Shacham. Group Signatures with Verifier-Local Revocation. In ACM Conference on Computer and Communications Security, pages 168–177. ACM, 2004.

BIOGRAPHIES

Mr.G.Sateesh, Associate Professor, Department of IT,
Lendi Institute of Engineering and Technology

M.Sarat Chandra, Student from Department of IT,
Lendi Instistute of Engineering and Technology

B.Sindhuri, Student from Department of IT,
Lendi Instistute of Engineering and Technology

M.Satish, Student from Department of IT,
Lendi Instistute of Engineering and Technology