Intelligent User Control System In Anonymous Network by A Method of Indexing And Pseudonymisation

S.Divya[1], K.Madhumitha[2], K.Aarthi[3], N.Saranya[4]
[1, 2] Dept of Computer Science
[1, 2] Sri Eshwar College of Engineering, Kinathukkadavu, India.

Abstract- *Two or more nodes that are linked in order to share resources or allow electronic communications is referred to as network. Anonymous Networks allows to exchange information in both secure and anomie ways. But what happens if the anonymous network itself compromised? Then we can assume One or more of the relaying nodes (which moves encrypted data) can fall in the hands of cyberpunk or data thief whom has desire to break the anonymity and locate the origin and destination of the traffic flowing. To avoid the data being insecure a combination of pseudonym server and indexing server with a Nymble (High-Performance Learning Name-Finder system in which servers can blacklist threatening users, thereby blocking users with a high importance to securing anonymity). This system is compactable to different servers' definitions of misbehaviour servers can blacklist users for whatever reason, and the privacy of blacklisted users is maintained. The most possible solution of high reliability and security is obtained*

Keywords- Anonymous Networks, pseudonym server, indexing server, Nymble, Misbehavior server, blacklisting users, security

I. INTRODUCTION

A network consists of two or more nodes that are linked in order to share resources exchange files, or allow electronic communications. The nodes (computers) on a network may be linked through telephone lines, satellites, cables or infrared light beams and radio waves.

The main goal of networking is "Resource sharing"(to make all programs, data and equipment available to anyone on the network without the regard to the physical location of the resource and the user), high reliability by having alternative sources of supply, saving money (Small computers have a much better price/performance ratio than larger ones. Mainframes are roughly a factor of ten times faster than the fastest single chip microprocessors, but they cost thousand times more.) And increase the systems performance as the work load increases by just adding more processors. With central mainframes, when the system is full, it must be replaced by a larger one, usually at great expense and with even greater disruption to the users.

Anonymous Networks allows to exchange information in both secure and anonime ways. An anonymity network enables users to access the Web while blocking any tracking or tracing of their identity on the Internet. This type of online anonymity moves Internet traffic through a worldwide network of volunteer servers. Anonymity networks prevent traffic analysis and network surveillance - or at least make it more difficult.

A viewer outside the network, which means somebody sniffs the traffic flowing between two nodes (Server or whatever), the network should provide security such that the intruder can neither know source nor know target/destination. But what happens if the anonymous network itself compromised? One or more of the relaying nodes (which moves encrypted data) can fall in the hands of intruder or hacker which desire to break the anonymity and locate the origin/source and destination of the traffic flowing.

In Introduction you can mention the introduction about your research

Identify the constructs of a Journal – Essentially a journal consists of five major sections. The number of pages may vary depending upon the topic of research work but generally comprises up to 5 to 7 pages. These are:multi-label learning, more than one class can be assigned to an instance. With the increase in the number of data

II. SYSTEM OVERVIEW

2.1 Existing System

The existing system is not secure because the anonymous users can enter in to the network by changing their

IP address and, this may flood and decrease the vulnerability of website. So the website prevent users by IP address block i.e. misbehaving IP addresses. But anonymous users can route the IP address and use IP changing software or some other proxy server and may enter into network.

2.1.1 Disadvantages of existing system

1. This system, is not secure because any users can change IP and enter into network.
2. There is less possibility to stop anonymity in this system and website admins can manually block only fake IP.
3. Cost is more and regular maintenance is required.
4. Servers must query the group manager for every authentication, and thus, lacks scalability
5. User must have all their connections linked, and users must worry about whether their behaviours will be judged fairly
6.

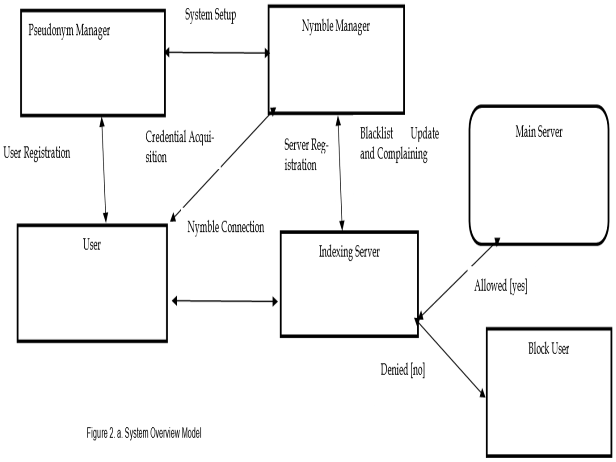


Figure 2. a. System Overview Model

.

2.2 Proposed System

The proposed system provides following properties:

Subjective blacklisting, Anonymous authentication, fast authentication speeds, backward unlinkability, revocation auditability rate limited anonymous connections, (where users can verify whether it have been blacklisted), and also secure us from cyber-attack [3] to make the network and security as strong.

In Nymble, an ordered collection of nymbles can be acquired by users, a special type of pseudonym, to connect to websites. These nymbles are computationally hard to link without any additional information and hence anonymous access to services can be acquired by using the stream of nymbles.

The Indexing server consists of millions of index and sensual coding which can automatically validate the nymblised users once again and ensure 3D security of data. The indexing server helps in fast access to focused data as well it can help in approving and declining access to data. The index server blacklist user based on criteria given by admin and block those users.

Servers can blacklist anonymous users without knowledge of their IP addresses. Our system ensures that users and admins aware of their blacklist status before they present a Nymble, and disconnect immediately if they are blacklisted.

Even though this system applies to anonymizing networks, we can also consider Tor (for purposes of exposition). The real fact is, any number of anonymizing networks can rely on the same Nymble system, blacklisting anonymous users regardless of their anonymizing network(s) of choice

2.2.1 Advantages of proposed system

1. This new system find client mac or physical address and each time the client entry is maintained.
2. When users misbehave in the website, Admins can block their mac or physical address automatically by setting condition in indexing server. So blocked user cant access internet services.
3. This system works perfectly in all network but have to host this software and IIS server used to store information all the physical address and mac address.
4. Provides fast access and 3D security for data.

III. SYSTEM IMPLEMENTATION

1. The Pseudonym Manager 2. The Nymble Manager 4. Indexing Manager 5. Client Request/Response

3.1 The Pseudonym Manager (PM)

The user is first acknowledged by the Pseudonym Manager (PM) and demonstrate control over a resource. .Pseudonyms are chosen deterministically based on the controlled resource environment, this will ensure that the same pseudonym is always issued for the same resource and it’s also responsible for allocating unique pseudonym to particular user. The user is required to connect to the PM directly for IP-address/ MAC /physical address blocking (i.e., not through a known anonymizing network). Pseudonym Manager has knowledge about Tor routers, and can ensure that users are communicating with it directly. Note: the user does not disclose what server user intends to connect to, and therefore the users connections are anonymous to the PM.

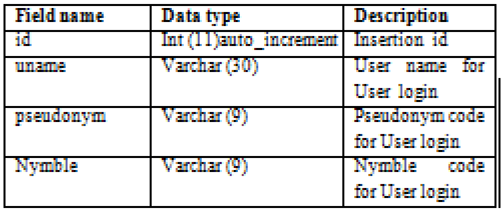
The user contacts the PM only once per liability window. The PMs Duties are limited to mapping IP addresses / MAC /physical address (or other resources) to pseudonyms. The PM checks if the user is allowed to register. In the current implementation, the PM infers the registering users IP address from the communication channel, and makes sure that the IP address does not belong to a known Tor exit node. If this is not the case, the PM terminates with failure. Otherwise, the PM reads the current linkability window then gives pseudonym to the user, and terminates with success.

3.1.1 USER REGISTRATION

A user identity UID must be registered with the PM. A user name, is also referred to as an account name (a string i.e., sequence of characters) that uniquely identifies a user. User names can be the same as or related to the real names of users, or they can be completely arbitrary. A password is likewise a string, but it differs from a user name in that it is intended to be kept a secret that is known only to its user

For the user registration, the user initiates a type- Basic channel to the PM, followed by the User Registration protocol described below. A login generally requires the user to enter two pieces of information, first a user name and then a password. This information is entered into a login window on a GUI (graphical user interface).

Table name : ticket
Primary key : id



Field name	Data type	Description
id	Int (11)auto_increment	Insertion id
uname	Varchar (30)	User name for User login
pseudonym	Varchar (9)	Pseudonym code for User login
Nymble	Varchar (9)	Nymble code for User login

3.2. The Nymble Manager

After obtaining a pseudonym from the PM, the user connects to the Nymble Manager (NM) through the anonymizing network, and requests nymbles for access to a particular server,

Nymbles are generated using the user’s pseudonym and the server’s identity (SID). The NM reads the current time period and liability window as tnow and wnow, respectively, and then obtains an svr State by running NM Register Server nm State (sid; tnow; wnow).The NM appends svrState to its nmState, sends it to the Server, and terminates with success
The users connections, therefore, are pseudonymous to the NM (as long as the PM and the NM do not collude) since the NM knows only the pseudonym-server pair, and the PM knows only the IP address/ MAC/ physical address - pseudonym pair. Note that due to the pseudonym assignment by the PM, nymbles are bound to the users IP address and the server’s identity.

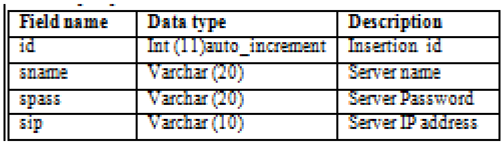
To provide the requisite cryptographic protection and security properties (e.g., users should not to be able to fabricate their own nymbles), the NM encapsulates nymbles within nymble tickets. Servers wrap seeds into linking tokens and therefore will speak of linking tokens being used to link future nymble tickets. The importance of these constructs will become apparent as proceed.

3.2.1 SERVER REGISTRATION

A server identity SID must be registered to participate in the Nymble system. Each server may register at most once in any likability window. Logins may be used to provide credentials when creating a client connection. Whether or not logins are required depends on the method calls used to start the server or create the connection.

To initiate server registration a type- Auth channel to the NM, and registers with the NM according to the Server Registration protocol below. For example, you might need logins for pooling. If you do not use logins, you must track and specify the user credentials manually.

Table name : sever
Primary key : id



Field name	Data type	Description
id	Int (11)auto_increment	Insertion id
sname	Varchar (20)	Server name
spass	Varchar (20)	Server Password
sip	Varchar (10)	Server IP address

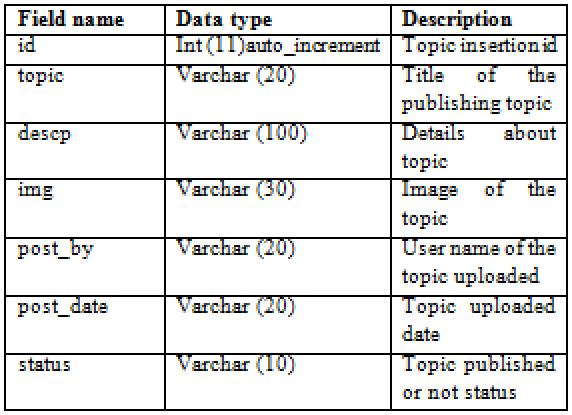
3.2.2. The Nymble Network

The Nymble Network is mainly used to connect the Nymble Manager, Pseudonym Manager, Index Manager and client. These four communicate with each other through on Nymble Network. The manger to validate the client through this network only. This network is formed in WCF concept. Through this network only the data will be stored in database.

3.3 Indexing Manager (IM)

IM is responsible for providing 3D security. IM verifies the UID and SID created by PM and NM after that it allows the user to access the front end GUI .Where users are not allowed to access the database or main server . The index server consist' s of millions of keywords. If the user is trying to misbehave or search unethical content the index server pre limit the data criticality. The index server also provide fast access to data by using focused search row technique.

Table name : topic
Primary key : admission _id

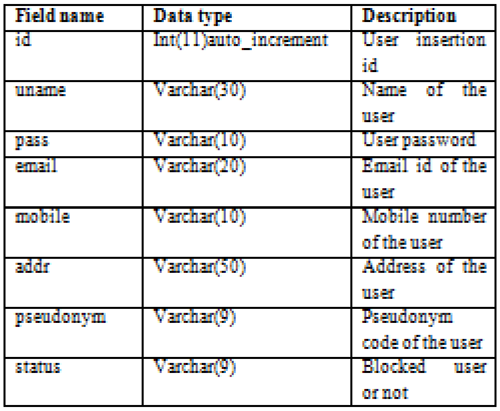


Field name	Data type	Description
id	Int (11)auto_increment	Topic insertion id
topic	Varchar (20)	Title of the publishing topic
descp	Varchar (100)	Details about topic
img	Varchar (30)	Image of the topic
post_by	Varchar (20)	User name of the topic uploaded
post_date	Varchar (20)	Topic uploaded date
status	Varchar (10)	Topic published or not status

3.4. Client Request/Response

This module having two things one is net access and second one is mail access. Net access is mean that the client use the allowed website only. If the client use blocked website the client net access will be blocked using an MAC address (physical address). Mail Access: The client sends the mail to any the message will be stored in database. If the admin only to send the mail in particular id.

Table name : user
Primary key : id



Field name	Data type	Description
id	Int(11)auto_increment	User insertion id
uname	Varchar(30)	Name of the user
pass	Varchar(10)	User password
email	Varchar(20)	Email id of the user
mobile	Varchar(10)	Mobile number of the user
addr	Varchar(50)	Address of the user
pseudonym	Varchar(9)	Pseudonym code of the user
status	Varchar(9)	Blocked user or not

IV. NYMBLE/INDEXER CONNECTION ESTABLISHMENT

To establish a connection to a server ID SID, the user initiates a type-Anon channel to the server, followed by the Nymble connection establishment protocol described below.

4. 1. Blacklist Validation

The server sends (blist; cert) to the user, where blist is its blacklist for the current time period and cert is the certificate on blist. The user reads the current time period and linkability window as t(U now) and w(U now) and assumes these values to be current for the rest of the protocol. For freshness and integrity, the user checks if VerifyBLusrState(sid; t(U now) ; w(U now); blist; cert)= true: If not, admin terminates the protocol with failure.

4.2. Privacy Check

Since multiple connection establishment attempts by a user to the same server within the same time period can be linkable, the user keeps track of whether the user has already disclosed a ticket to the server in the current time period by maintaining a boolean variable ticket Disclosed for the server in that state.

Furthermore, since a user who has been blacklisted by a server can have her connection establishment attempts linked to her past establishment, the user must make sure that she has not been blacklisted thus far.

Consequently, if ticketDisclosed in usrEntries[sid] in the users usrState is true, or User Check If Blacklisted user State (sid; blist) = true; then it is unsafe for the user to proceed and the user sets safe to false and terminates the protocol with failure.

4.3. Service Provision and Access Logging

If both the user and the server terminate with success in the Nymble connection Establishment described above, the server may start serving the user over the same channel to indexing server. The server records ticket and logs the access during the session for a potential complaint in the future. The below figure explains the same

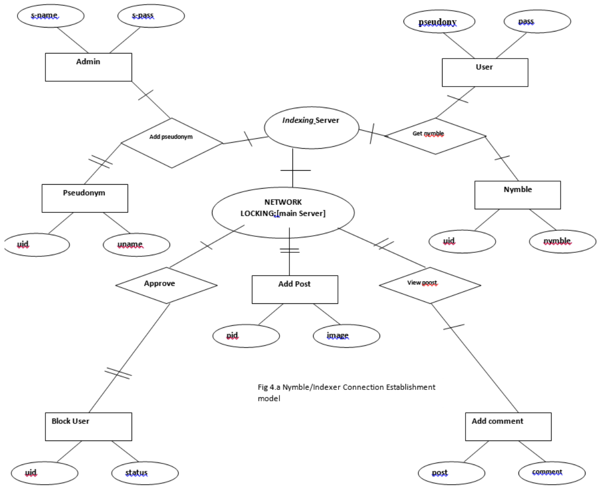


Fig 4.a Nymble/Indexer Connection Establishment model

4.3.1 User

After Registration here user has to login by using their unique username and password. Users are the only authorized person to access admin module for security purpose and admins have access to review user activity So others don't get rights to access this module.As the indexing server itself blocking the user the admin's role and task got reduced here.

4.3.1.1 Post Views

In this module user can view the admin posts such as news, events, pictures and etc... And also they can give comment specific topic or particular pictures. After given the comment it will be verified by admin. Admin will decide to post on wall. Other user doesn't get rights to access this module for security purpose

4.3.1.2 Work Model

In this module users can view architecture of this project to understand the terms of this project. Users are the only authorized person to access this module. Other user doesn't get rights to access this module for security purpose

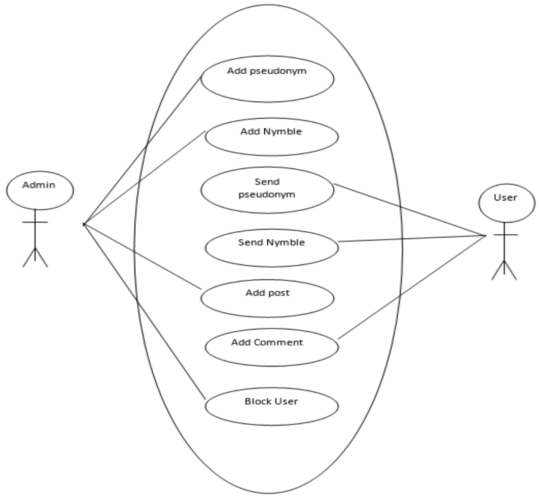


Figure 4.3.a User/Admin access model

V. CONCLUSION

In this comprehensive credential system called Nymble is built and is enhanced with Indexing module, which can be used to add a layer of accountability to any publicly known anonymizing network. Servers can blacklist misbehaving users while maintaining their privacy, and show how these properties can be attained in a way that is practical, efficient, and sensitive to needs of both users and services automatically. This system provide how to get physical address and mac address of client system. Then admin can set threshold in indexing server. For give permission or block access to particular web page each and every time must check whether the entered login id have access to this page or not. This system provide security to websites.

VI. FUTURE ENHANCEMENT

In future this system hosting to all sites and block the anonymous users by blocking their physical address and mac address instead of blocking their IP automatically.. The future system will be configured for adopting this feature by reduction of resource and initial cost.

REFERENCES

[1] Tsang .P.P, M.H. Au, A. Kapadia, and S.W. Smith, PEREA: Towards Practical TTP-Free Revocation in Anonymous Authentication, Proc. ACM Conf. Computer and Comm. Security, pp. 333-344, 2008.

[2] Bresson.E and Stern.J, Efficient Revocation in Group Signatures, Proc. Conf. Public Key Cryptography, Springer, pp. 190-206, (2001).

[3] Camenisch.J and Lysyanskaya.A, An Efficient System for Non-Transferable Anonymous Credentials with Optional

Anonymity Revocation, Proc. Intl Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT), Springer, pp. 93-118, (2001).

[4] Dingledine.R, N. Mathewson, and P. Syverson, Tor: The Second- Generation Onion Router, Proc. Usenix Security Symp., pp. 303- 320, Aug. 2004.

[5] Johnson.P.C and Kapadia.A, P.P. Tsang, and S.W. Smith, Nymble: Anonymous IP-Address Blocking, Proc. Conf. Privacy Enhancing Technologies, Springer, pp. 113-133, (2007).

[6] Douceur .J.R, The Sybil Attack, Proc. Intl Workshop on Peer-to- Peer Systems (IPTPS), Springer, pp. 251-260, 2002

[7] Tsang .P.P, M.H. Au, A. Kapadia, and S.W. Smith, Blacklistable Anonymous Credentials: Blocking Misbehaving Users without TTPs, Proc. 14th ACM Conf. Computer and Comm. Security (CCS 07), pp. 72-81, 2007.

[8] Ateniese.G, J. Camenisch, M. Joye, and G. Tsudik, A Practical and Provably Secure Coalition-Resistant Group Signature, Scheme, Proc. Ann. Intl Cryptology Conf. (CRYPTO), Springer, pp. 255-270, 2000.

[9] M. Bellare, R. Canetti, and H. Krawczyk, “Keying Hash Functions for MessageAuthentication,” Proc. Ann. Int’l Cryptology Conf. (CRYPTO), Springer, pp. 1-15, 1996.