OPEN ACCESS

International
Journal
Of Modern Engineering Research (IJMER)

Blind Signatures with Verifier-Effective Revocation

R. Aishwariya[1], R. Priya [2], S. Kiruthiga[3]
[1, 2, 3] *(PG Student, Department of Computer Science, Annamalai University, Tamil Nadu, India)*

***Abstract*:** *The nimble system in which servers can blacklist misbehaving users, thereby blocking users without compromising their anonymity. Our framework is along these lines freethinker to diverse servers' meanings of misconduct servers can boycott clients for whatever reason, and the protection of boycotted clients is kept up. In pseudonymous credential systems users are log into web sites using pseudonyms, which can be added to a blacklist if a user misbehaves. Anonymous credential systems employees group signatures. Fundamental gathering marks permit servers to repudiate a getting into mischief client's secrecy by grumbling to a gathering supervisor.*
***Keywords*:** *Nimble, Pseudonym, Black listing.*

I. Introduction

ANONYMIZING systems, course activity through free hubs in independent managerial areas to shroud a customer's IP address. Lamentably, a few clients have abused such systems under the spread of secrecy, clients have more than once damaged prevalent Web locales, for example, Wikipedia. Since Web website heads can't boycott individual malevolent clients' IP addresses, they boycott the whole anonymizing system. Such measures kill malignant movement through anonymizing systems at the expense of denying unnamed access to acting clients. As such, a couple of "rotten ones" can ruin the a good time for all. (This has happened over and over with Tor. There are a few answers for this issue, each one giving some level of responsibility. In pseudonymous qualification frameworks clients are log into Web destinations utilizing pen names, could be added to a boycott if a client gets out of hand. Unfortunately, this methodology brings about pseudonymity for all clients, and debilitates the secrecy gave by the anonymizing system. Anonymous credential systems employ group signatures. Basic group signatures allow servers to revoke a misbehaving user's anonymity by complaining to a group manager. Servers must inquiry the gathering supervisor for each confirmation, and hence, needs adaptability. Traceable signatures allow the group manager to release a trapdoor that allows all signatures generated by a particular user to be traced; such an approach does not provide the backward unlink ability that we desire, where a user's accesses before the complaint remain anonymous. Backward unlink ability allows for what we call subjective blacklisting, where servers can blacklist users for whatever reason since the privacy of the blacklisted user is not at risk. In contrast, approaches without backward unlink ability need to pay careful attention to when and why a user must have all their connections linked, and users must worry about whether their behaviors will be judged fairly.

The 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 Pseudonyms are deterministically chosen based on the controlled resource, ensuring that the same pseudonym is always issued for the same resource.

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 (such as Wikipedia). A user's requests to the NM are therefore pseudonymous, and nymbles are generated using the user's pseudonym and the server's identity. These nymbles are thus specific to a particular user-server pair.

Blacklisting a User

If a user misbehaves, the server may link any future connection from this user within the current link ability window. A user connects and misbehaves at a server during time period within linkability window. The server later detects this misbehavior and complains to the NM in time period of the same linkability window. As part of the complaint, the server presents the nymble ticket of the misbehaving user and obtains the corresponding seed from the NM. Therefore, once the server has complained about a user, that user is blacklisted for the rest of the day.

Notifying the User of Blacklist Status

In our system, the user can download the server's blacklist and verify her status. If blacklisted, the user disconnects immediately. Since the blacklist is cryptographically signed by the NM, the authenticity of the blacklist is easily verified if the blacklist was updated in the current time period (only one update to the blacklist per time period is allowed). If the blacklist has not been updated in the current time period, the NM provides servers with "daisies" every time period so that users can verify the freshness of the blacklist

In existing work proposes 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 Web sites. Web site 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. Unfortunately, this approach results in pseudonymity for all users, and weakens the anonymity provided by the anonymizing network server must query the group manager for every authentication, and thus, lacks scalability. User must have all their connections linked, and users must worry about whether their behaviors will be judged fairly.

Our proposed work gives a secure system called nymble, which provides anonymous authentication, backward unlinkability, subjective blacklisting, fast authentication speeds, rate-limited anonymous connections, revocation auditability that is the users can verify whether they have been blacklisted, Nymble thus represents a practical solution for blocking misbehaving users of anonymizing networks. Our system ensures that users are aware of their blacklist status before they present a nymble, and disconnect immediately if they are blacklisted in our system, the user can download the server's blacklist and verify her status. If blacklisted, the user disconnects immediately.

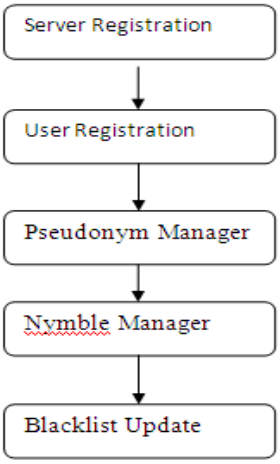
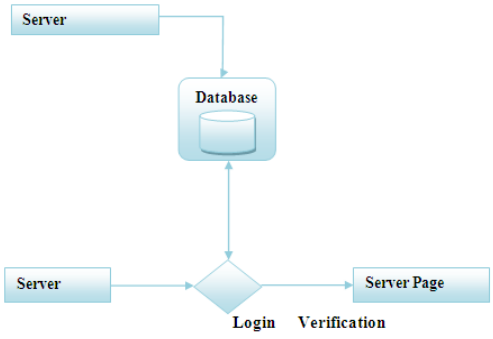


Fig-1: Block Diagram of the proposed work

II. MATERIALS AND METHODS

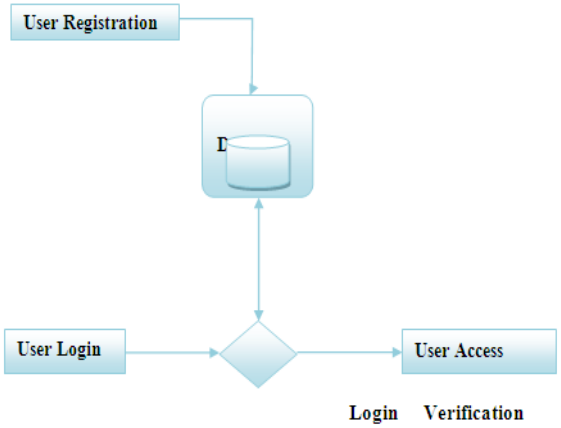
1. Server Registration:

To participate in the Nymble system, a server with identity Sid initiates a type-Auth channel to the NM, and registers with the NM according to the Server Registration protocol below. Each server may register at most once in any likability window.



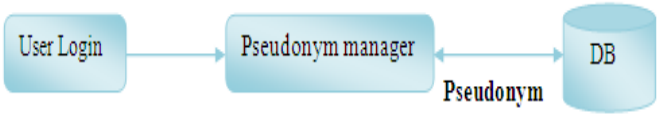
2. User Registration:

A user with identity uid must register with the PM once in each likability window. To do so, the user initiates a type- Basic channel to the PM, followed by the User Registration protocol described below.



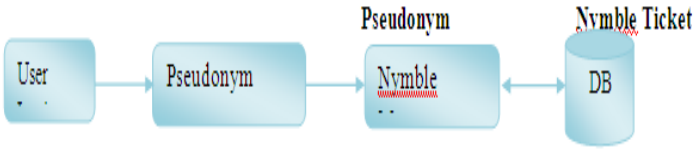
3. Pseudonym Manager:

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. We assume the PM has knowledge about Tor routers, and can ensure that users are communicating with it directly. Pseudonyms are deterministically chosen based on the controlled resource, ensuring that the same pseudonyms always issued for the same resource.



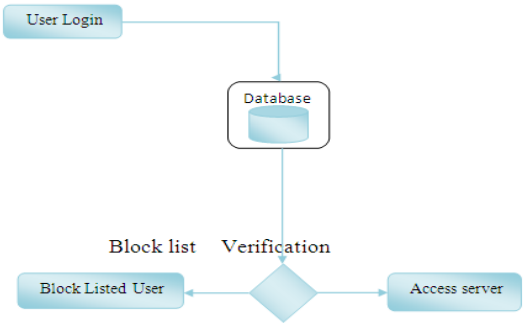
4. Nymble Manager:

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 (such as Wikipedia). A user's requests to the NM are therefore pseudonymous, and nymbles are generated using the user's pseudonym and the server's identity. These nymbles are thus specific to a particular user-server pair.



5. Blacklist Update:

Servers update their blacklists for the current time period for two purposes. First, as mentioned earlier, the server needs to provide the user with its blacklist (and blacklist certificate) for the current time period during a Nymble connection establishment. Second, the server needs to be able to blacklist the misbehaving users by processing the newly filed complaints (since last update).



Algorithm Used:

A server's blacklist is a list of nymble's corresponding to all the nymbles that the server has complained about. Users can quickly check their blacklisting status at a server by checking to see whether their nymble appears in the server's blacklist.

Input Design and Output Design:

Server Registration:

- Input: Server Register to Nymble
- Output: Nymble Accept the registration

User Registration:

- Input: User Register to Pseudonym Manager
- Output: Pseudonym Manager Accept the registration

Pseudonym Management

- Input: Pseudonym Manager provide Pseudonym
- Output: User gets the Pseudonym

Nymble Management:

- Input: Give Pseudonym name to Nymble Manager
- Output: Display complaints of user

Blacklist Update:

- Input: Give Pseudonym name to Nymble Manager
- Output: Display blacklist status of user

APPLICATIONS:

- Our system ensures that users are aware of their blacklist status before they present a nymble, and disconnect immediately if they are blacklisted.
- In our system, the user can download the server's blacklist and verify her status. If blacklisted, the user disconnects immediately.

III. RESULTS AND DISCUSSION

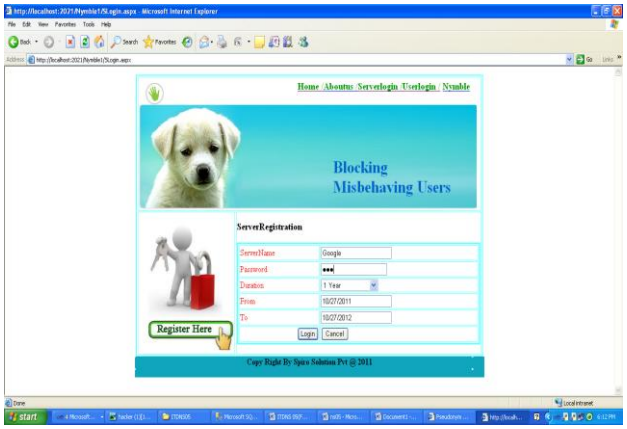


Fig-2: Home page image

Fig-3: Server registration

Fig-4: successful registration

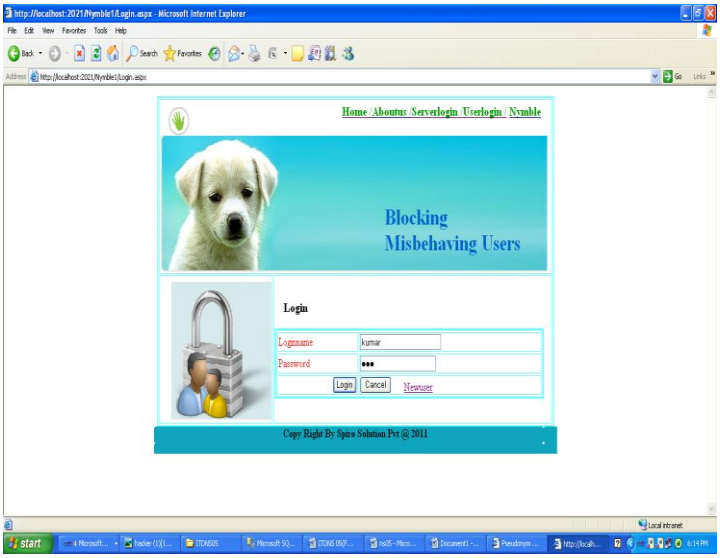


Fig-5: user registration

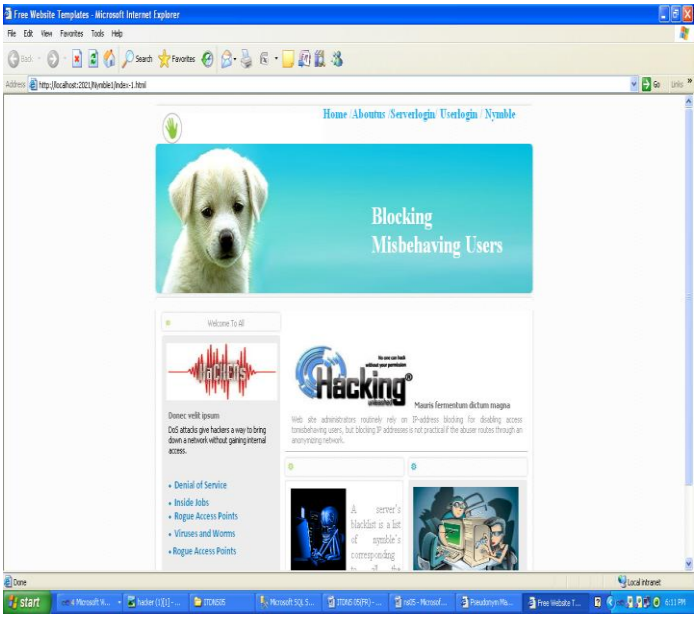


Fig-6: User Log in

IV. CONCLUSION

The proposed and built a comprehensive credential system called Nymble, 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 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. It will increase 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, to increase the mainstream acceptance of anonym zing networks such as Tor, which has been completely blocked by several services because of users who bused their anonymity.

REFERENCES

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

[2] G. Ateniese, D.X. Song, and G. Tsudik, "Quasi-Efficient Revocation in Group Signatures," Proc. Conf. Financial Cryptography, Springer, pp. 183-197, 2002.

[3] M. Bellare, R. Canetti, and H. Krawczyk, "Keying Hash Functions for Message Authentication," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 1-15, 1996.

[4] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway, "A Concrete Security Treatment of Symmetric Encryption," Proc. Ann. Symp. Foundations in Computer Science (FOCS), pp. 394-403, 1997.

[5] M. Bellare and P. Rogaway, "Random Oracles Are Practical: A Paradigm for Designing Efficient Protocols," Proc. First ACM Conf. Computer and Comm. Security, pp. 62-73, 1993.

[6] M. Bellare, H. Shi, and C. Zhang, "Foundations of Group Signatures: The Case of Dynamic Groups," Proc. Cryptographer's Track at RSA Conf. (CT-RSA), Springer, pp. 136-153, 2005.

[7] D. Boneh and H. Shacham, "Group Signatures with Verifier-Local Revocation," Proc. ACM Conf. Computer and Comm. Security, pp. 168-177, 2004.

[8] S. Brands, "Untraceable Off-Line Cash in Wallets with Observers (Extended Abstract)," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 302-318, 1993.

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

[10] J. Camenisch and A. Lysyanskaya, "An Efficient System for Non- Transferable Anonymous Credentials with Optional Anonymity Revocation," Proc. Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT), Springer, pp. 93-118, 2001.

[11] J. Camenisch and A. Lysyanskaya, "Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 61-76, 2002.

[12] J. Camenisch and A. Lysyanskaya, "Signature Schemes and Anonymous Credentials from Bilinear Maps," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 56-72, 2004.

[13] D. Chaum, "Blind Signatures for Untraceable Payments," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), pp. 199-203, 1982.

[14] D. Chaum, "Showing Credentials without Identification Transfeering Signatures between Unconditionally Unlinkable Pseudonyms," Proc. Int'l Conf. Cryptology (AUSCRYPT), Springer, pp. 246-264, 1990.

[15] D. Chaum and E. van Heyst, "Group Signatures," Proc. Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT), pp. 257-265, 1991.

[16] C. Cornelius, A. Kapadia, P.P. Tsang, and S.W. Smith, "Nymble Blocking Misbehaving Users in Anonymizing Networks," Technical Report TR2008-637, Dartmouth College, Computer Science, Dec. 2008.

[17] I. Damga°rd, "Payment Systems and Credential Mechanisms with Provable Security Against Abuse by Individuals," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 328-335, 1988.

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

[19] J.R. Douceur, "The Sybil Attack," Proc. Int'l Workshop on Peer-to- Peer Systems (IPTPS), Springer, pp. 251-260, 2002.

[20] S. Even, O. Goldreich, and S. Micali, "On-Line/Off-Line Digital Schemes," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 263-275, 1989.

[21] J. Feigenbaum, A. Johnson, and P.F. Syverson, "A Model of Onion Routing with Provable Anonymity," Proc. Conf. Financial Cryptography, Springer, pp. 57-71, 2007.

[22] S. Goldwasser, S. Micali, and R.L. Rivest, "A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks," SIAM J. Computing, vol. 17, no. 2, pp. 281-308, 1988.

[23] J.E. Holt and K.E. Seamons, "Nym: Practical Pseudonymity for Anonymous Networks," Internet Security Research Lab Technical Report 2006-4, Brigham Young Univ., June 2006.

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

[25] A. Juels and J.G. Brainard, "Client Puzzles: A Cryptographic Countermeasure Against Connection Depletion Attacks," Proc. Network and Distributed System Security Symp. (NDSS), 1999.