Volume 3, Issue 10, October 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Restricting Unauthorized Users and Illegal Access in Web Based Network

Sangamesh Kishore.M*
M.S(Software Engineering)
SITE, VIT University, India

Varun Kumar.M
Assistant Professor
SITE, VIT University, India

Asha.N
Assistant Professor
SITE, VIT University, India

Abstract— our paper is mainly concerned on use of anonymous access of the various websites through various search engines like Google, Bing etc. Our concept makes search engines can block the user who misbehave in the network using tokens and provide safe access to several website by anonymously to hide their identity in network. This type of hiding their identity in network will increase the popularity of search engines and increase the number of users of their search engine. This also provide features like alerting the user who steal their password of their social network sites and various mailing sites through mail and shut down the system of the person who try to steal password also provide illegitimate website blocking in organization.

Keywords— Restricting access, Mail System, Search Engine

I. INTRODUCTION

We present a secure system using network manager, which provides all the following properties: anonymous authentication, backward unlinkability, subjective blacklisting, fast authentication speeds, rate-limited anonymous connections and also addresses the Sybil attack to make its deployment practical. Here, users acquire an ordered collection of tokens, a special type of pseudonym, to connect to websites. Without additional information, these tokens are computationally hard to link, and hence using the stream of tokens simulates anonymous access to services. Websites, however, can blacklist users by obtaining a seed for a particular token those used before the complaint remain unlinkable. Servers can therefore blacklist anonymous users without knowledge of their IP addresses while allowing behaving users to connect anonymously. Our system will immediately shut down the block listed user system and also provide future unlinkability. Although our work applies to anonymizing networks in general, we consider Tor for purposes of exposition. In fact, any number of anonymizing networks can rely on the same NetworkManager, blacklisting anonymous users regardless of their anonymizing network of choice and this also provide access restriction to user to some websites. This blacklist websites is updated by admin of the system and alerting the user if someone try to steal their password so that alert message is come to the e-mail id of the owner.

II. DESCRIPTION

2.1 Network Manager:

Servers can therefore blacklist anonymous users without knowledge of their IP addresses while allowing behaving users to connect anonymously. Alsoshut down the user system who misbehaved. Although our work applies to anonymizing networks in general, we consider Tor for purposes of exposition. In fact, any number of anonymizing networks can rely on the same network system, blacklisting anonymous users regardless of their anonymizing network(s) of choice.

2.2 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. IP - Address blocking employed by Internet services. There are, however, some inherent limitations to using IP addresses as the scarce resource. If a user can obtain multiple addresses she can circumvent both network-based and regular IP-address blocking. Subnet-based blocking alleviates this problem, and while it is possible to modify our system to support subnet-based blocking, new privacy challenges emerge; a more thorough description is left for future work.

2.3 Authenticated Connection:

Blacklist ability assures that any honest server can indeed block misbehaving users. Specifically, if an honest server complains about a user that misbehaved in the current likability window, the complaint will be successful and the user will not be able to connect from network manager and shut down the system. Honest servers must be able to differentiate between legitimate and illegitimate users. Anonymity protects the anonymity of honest users, regardless of their legitimacy according to the (possibly corrupt) server; the server cannot learn any more information beyond whether the user behind (an attempt to make) a network-connection is legitimate or illegitimate.

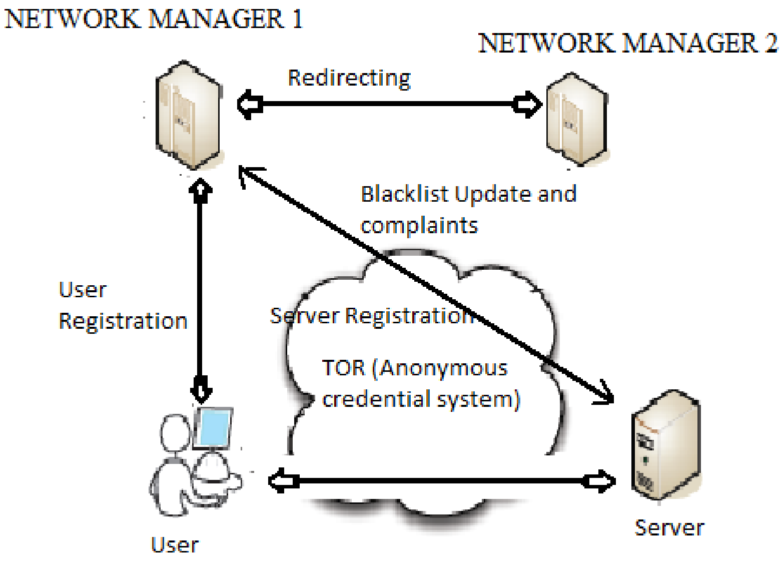


Fig.1. System overview

III. ARCHITECTURE

This system contain three tiers

- Application layer
- Process layer
- Database layer

In **application layer** user can interact system user friendly, in our system we have two user interfaces

1. Ordinary user: who need to use the system for browsing
2. Admin UI: who can change(or) update the system and can maintain it.

In **Database layer**, the whole database hold the information of block lists and have the social network user account.

In **Processing layer** will process information given by the user

1. authentication of the user will takes place in this layer
2. authentication of the administrator will also takes place in this layer
3. updating of the information takes place in this layer
4. user search query also entered and processed in this layer

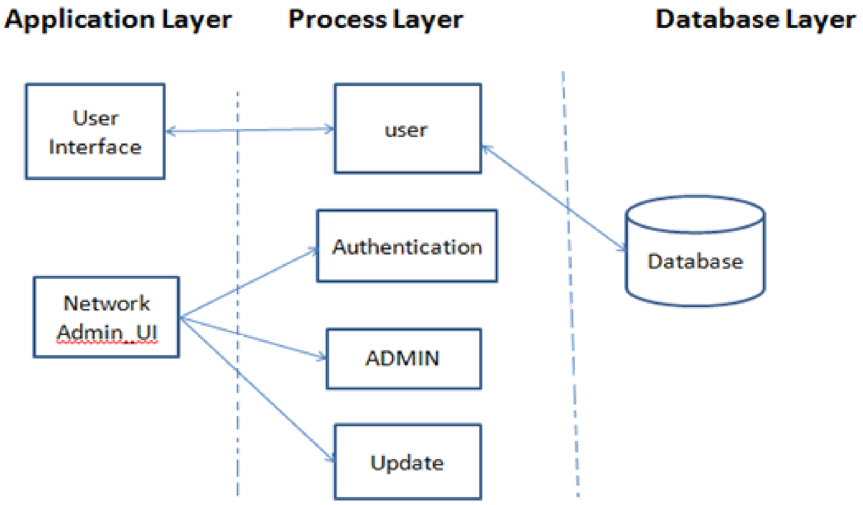
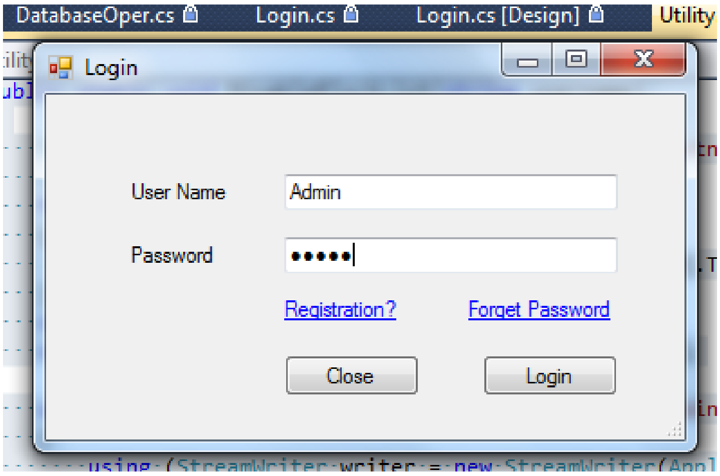


Fig.2. Architecture

IV. IMPLEMENTATION

This system has been implemented in the .NET platform (ASP.NET & Visual C#) and tested in alocal server. This system is designed to run on the web. It provide network token for every user before using entering into the websites so network manager identify the person using network token and shutting down the system of user who misbehave in the network.

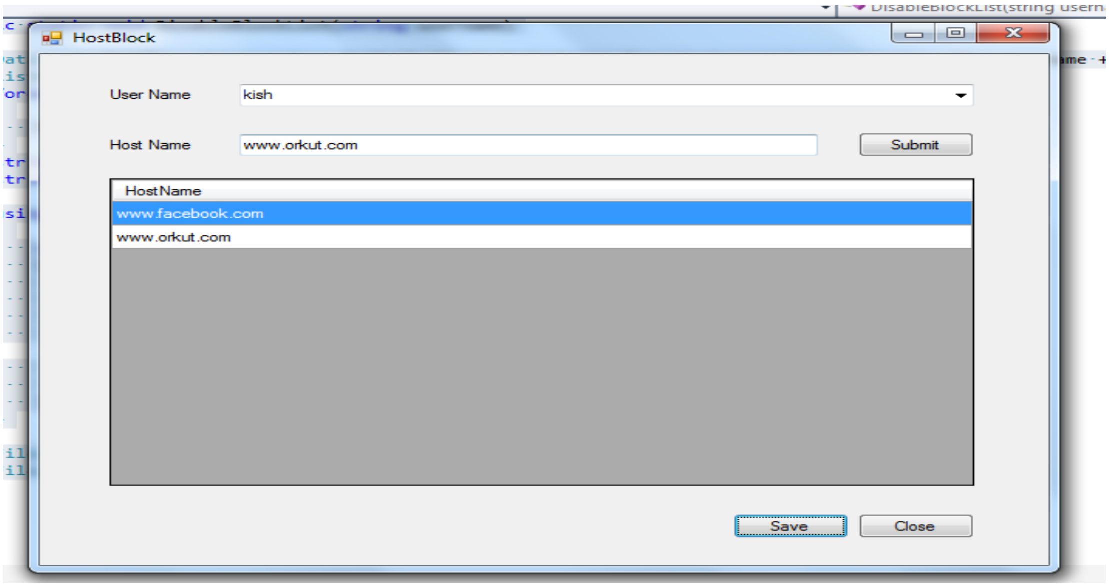


User Name Admin

Password •••••

Fig.3. Admin Login

The Administrator login is shown in Figure 3. Like other Systems it also provides fields like User name and Password for authentication purpose.



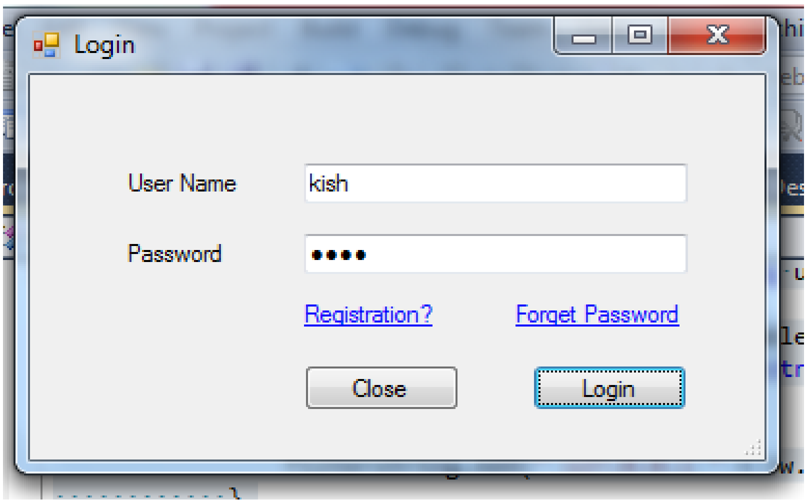
User Name kish

Host Name www.orkut.com

HostName
www.facebook.com
www.orkut.com

Fig.4. Host Blocking

Host Blocking is shown in figure 4, where the authenticated Administrator can change access rights to the users of the system by selecting their name from list of user names available and also enter the address of the website which they are not allowed to access.



User Name kish

Password ••••

Fig.5. User Login

User Login is shown in the figure 5, like other Systems it also provides fields like User name and Password for authentication purpose. And also provides the links for registering newly and also link for password recovery.

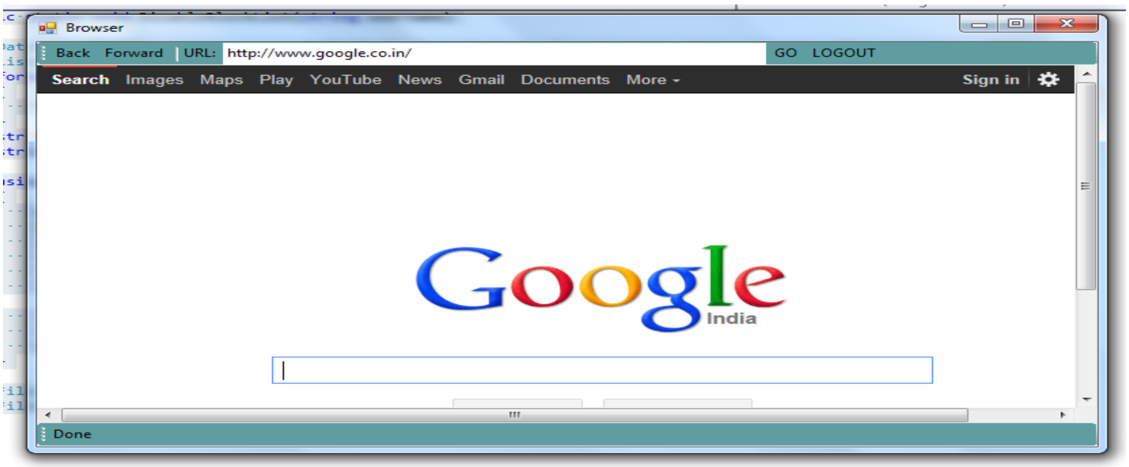
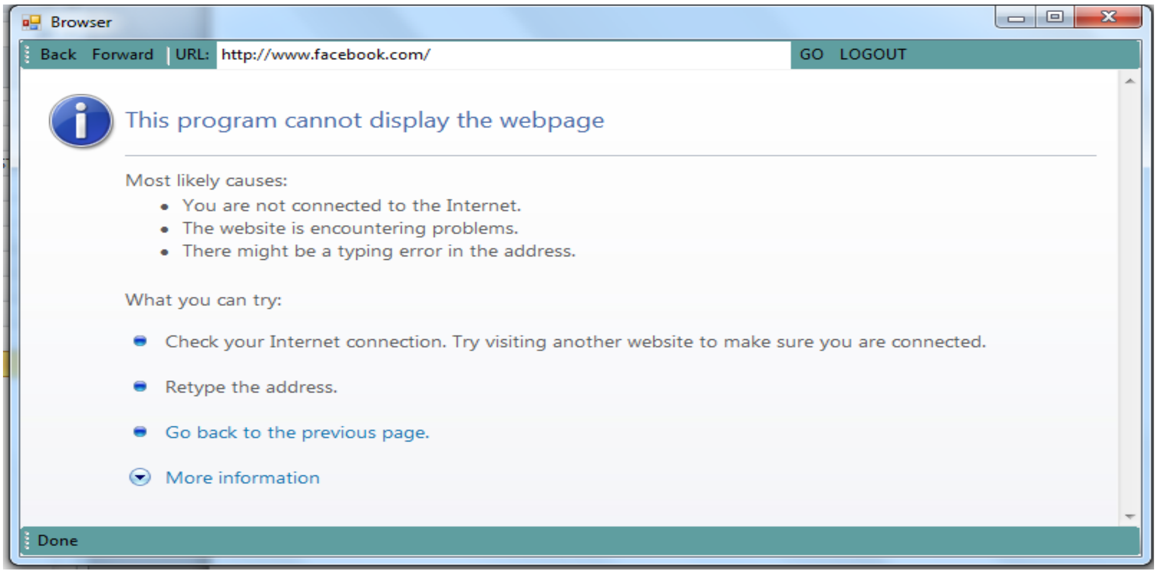

Browser
Back Forward URL: http://www.google.co.in/ GO LOGOUT
Search Images Maps Play YouTube News Gmail Documents More
Sign in
Google
India
Done

Fig.6. Web Browser

Web Browser is shown in the figure 6. it is a dynamic web browser where it will appear only after the authentication of the user. And homepage of the web browser is can be of any website.



This program cannot display the webpage

Most likely causes:

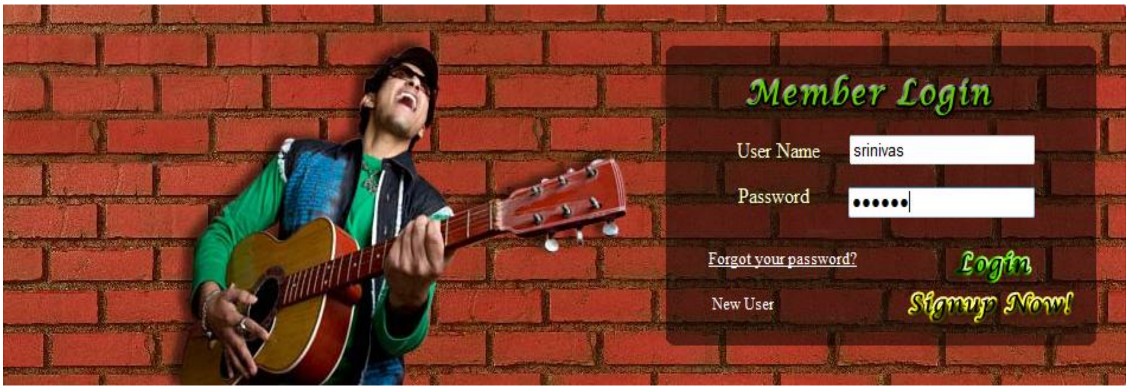
- You are not connected to the Internet.
- The website is encountering problems.
- There might be a typing error in the address.

What you can try:

- Check your Internet connection. Try visiting another website to make sure you are connected.
- Retype the address.
- Go back to the previous page.
- More information

Fig.7. Access Denial

Access denial is shown in Figure 7. When the user is trying to access the site which is being restricted for him then he cannot be able to access that particular website from any of the web browser available in his system.

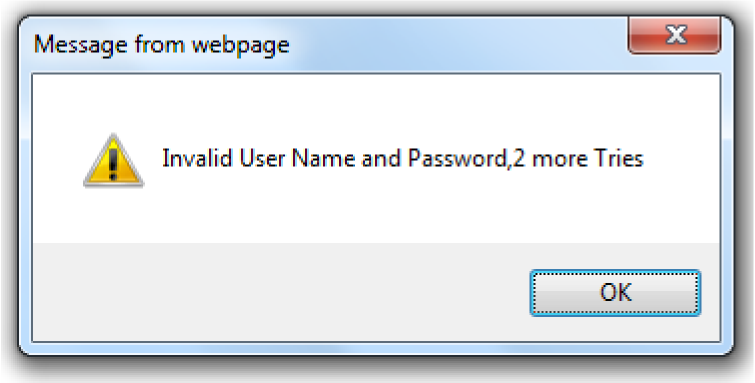


User Name: srinivas

Password: ••••••

Fig.8. Social Network Login

Social network Login page is shown in figure 8. We have built a social network for our organisation and it can be accessed only when the person is logged in through the network manager.

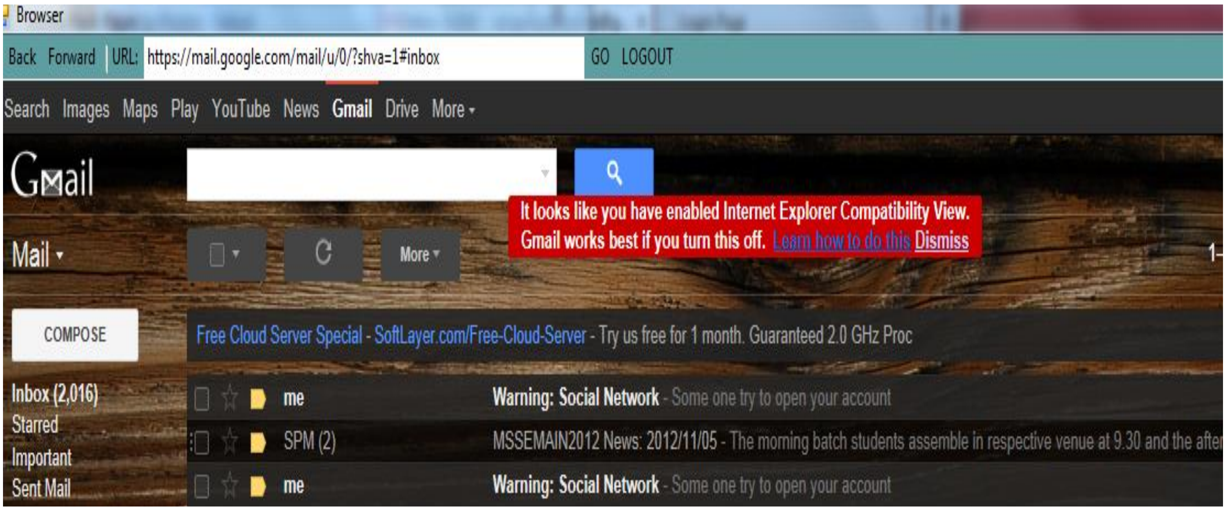


Message from webpage

Invalid User Name and Password,2 more Tries

Fig.9. Alert Message

Alert Message is shown in the figure 9. When the user or someone else tried to login to the social network with wrong password alert message will be shown. If it is an actual user he can be able to correct his password or if it is someone entering wrongly he is considered as a misbehaving user and as a punishment his system will be shutdown automatically after limited number of trials.



https://mail.google.com/mail/u/0/?shva=1#inbox

It looks like you have enabled Internet Explorer Compatibility View. Gmail works best if you turn this off. Learn how to do this Dismiss

Free Cloud Server Special - SoftLayer.com/Free-Cloud-Server - Try us free for 1 month. Guaranteed 2.0 GHz Proc

me	Warning: Social Network - Some one try to open your account	
SPM (2)	MSSEMAIN2012 News: 2012/11/05 - The morning batch students assemble in respective venue at 9.30 and the after	
me	Warning: Social Network - Some one try to open your account	

Fig.10. E-Mail Alert

E-mail alert is shown in the figure 10. E-mail will be sent automatically to the user whose account is being tried by someone else with wrong password.

V. CONCLUSION

We have proposed and built a comprehensive credential system, which can be used to add a layer of accountability to any publicly known anonymizing network.Admin server 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. We hope that our work 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.

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.