IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, June 2022
Impact Factor: 6.252

Blocking Fake Accounts in Online Social Networks

Mrs. M. Jasmine Sagaya Jonita[1], Ms. M. Deepa[2], Ms. R. Vainavi[3]
Assistant Professor, Department of Information Technology[1]
Final Year Student, Department of Information Technology[2,3]
Nirmala College for Women, Red Fields, Coimbatore, Tamil Nadu, India

Abstract: *The "BLOCKING FAKE ACCOUNTS IN SOCIAL NETWORKS" project is to 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. These fake social media accounts exist and it is important to identify them so that their activity is ignored or even reported. The purpose of these profiles is they can be created to give voice to a product of a brand, it does not inflict serious damage to the network.*

Keywords: Fake account

I. SOFTWARE SPECIFICATION

- Operating system : Windows 10 PRO
- Front End : HTML/CSS
- Middleware : PHP
- Back End : MY SQL

1.1 Software Description

Front End - HTML/CSS

HTML is markup language used to create static web pages and web applications.CSS is a style sheet language responsible for the presentation of documents written in a marakup language.HTML provides the structure of the page, CSS the (visual and aural) layout, for a variety of devices. Along with graphics and scripting, HTML and CSS are the basis of building Web pages and Web application.

Back End - My SQL

MY SQL is easy to use, extremely powerful, secure, and scalable, a database is a structured collection of data. To add, access and process data stored in a computer database we need a database management system such as MY SQL server. Database management system plays a central role in computing.

Middleware – PHP

PHP stands for Hypertext Preprocessor. PHP scripts run inside Apache server or Microsoft IIS. PHP and Apache server are free. PHP code is very easy. PHP is the most used server-side scripting language. PHP files contain PHP scripts and HTML.

Software Description

About HTML/CSS

HTML is markup language used to create atatic web pages and web applications.CSS is a style sheet language responsible for the presentation of documents written in a marakup language.HTML (HyperText Markup Language) and CSS (Cascading Style Sheets) are two of the core technologies for building Web pages. HTML provides the structure of the page, CSS the (visual and aural) layout, for a variety of devices. Along with graphics and scripting, HTML and CSS are the basis of building Web pages and Web application.

About PHP

PHP is a powerful server-side scripting language for creating dynamic and interactive websites. PHP widely used; PHP is perfectly suited for Web development and can be embedded directly into the HTML code. PHP is open source that it is readily available and absolutely free. PHP have multiple extensions and is extremely scalable.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, June 2022
Impact Factor: 6.252

Features of PHP

- PHP runs on different platforms (Windows, Linux, UNIX, etc).
- PHP is compatible with almost all server used today.
- PHP is free to download from the official PHP resource: www.php.net.

About MY SQL

MY SQL is an open-source relational database management system (RDBMS). MY SQL is easy to use, extremely powerful, secure, and scalable, because of its small size and speed, it is the ideal database solution for Web sites. MY SQL is a relational database management system. A database is a structured collection of data. To add, access and process data stored in a computer database we need a database management system such as MY SQL server. Database management system plays a central role in computing.

Features of MY SQL

- **Client/server Architecture:** MY SQL is a client/server system. There is a database server (MY SQL) and arbitrarily many clients (application programs), which communicate with the server.
- **SQL Compatibility:** SQL is a standardized language for querying and updating data and for the administration of a database.
- **Stored procedures:** Stored procedures (SPs for short) are generally used to simplify steps such as inserting or deleting a data record.
- **Triggers:** Triggers are SQL commands that are automatically executed by the server in database operations INSERT, UPDATE, and DELETE.
- **Replication:** Replication allows the contents of a database to be copied (replicated) on to a number of computers to increase protection against system and to improve the speed of database queries.
- **Platform independence:** MY SQL can be executed under a number of operating systems. The most important are Apple Macintosh OS X, Linux, Microsoft windows, and the Unix.
- **Speed:** MY SQL is considered a very fast database program.

II. SYSTEM STUDY AND ANALYSIS

2.1 Existing System

Existing users' credentials must be updated, making it impractical. Verifier-local revocation (VLR) fixes this shortcoming by requiring the server ("verifier") to perform only local updates during revocation. Unfortunately, VLR requires heavy computation at the server that is linear in the size of the blacklist.

Disadvantages of the Existing System

Anonymous authentication, backward unlinkability, subjective blacklisting, fast authentication speeds, rate-limited anonymous connections, revocation auditability (where users can verify whether they have been blacklisted), and also addresses the Sybil attack to make its deployment practical.Anonymous authentication, backward unlinkability, subjective blacklisting, fast authentication speeds, rate-limited anonymous connections, revocation auditability (where users can verify whether they have been blacklisted), and also addresses the Sybil attack to make its deployment practical.

2.2 Proposed System

We present a secure system called Nymble, which provides all the following properties: anonymous authentication, backward unlinkability, subjective blacklisting, fast authentication speeds, rate-limited anonymous connections, revocation auditability (where users can verify whether they have been blacklisted), and also addresses the Sybil attack to make its deployment practical In Nymble, 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.Websites, 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

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, June 2022
Impact Factor: 6.252

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 ensures that users are aware of their blacklist status before they present a nymble, and disconnect immediately if they are blacklisted. 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 Nymble system, blacklisting anonymous users regardless of their anonymizing network(s) of choice

- Blacklisting anonymous users. We provide a means by which servers can blacklist users of an anonymizing network while maintaining their privacy.
- Practical performance. Our protocol makes use of inexpensive symmetric cryptographic operations to significantly outperform the alternatives.
- Open-source implementation. With the goal of contributing a workable system, we have built an opensource implementation of Nymble, which is publicly available.We provide performance statistics to show that our system is indeed practical.

Advantages of the Proposed System

We present a secure system called Nymble, which provides all the following properties: anonymous authentication, Backward unlinkability, subjective blacklisting, fast authentication speeds, rate-limited anonymous connections, revocation auditability (where users can verify whether they have been blacklisted), and also addresses the Sybil attack to make its deployment practical In Nymble, 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.

2.3 Modules Description

- Admin Module
- User Module

Admin Module

Login:

In this module maintain the admin login details. Admin is used unique user name and password. They are only can access in this web application and we can create different access are through this web application.

Users

I'd creation:

In this module a new user can enter personal details to create an profile, like First name , Last name , Gender , Date of birth ,Mail id , Password , Confirm password, Add Photos and Age etc.

Login

User get unique username and password after creating an id. User easy to view the other user and can follow the favor user in this application.

Home Page

The user can use a social network straight a way by login by using the home page.

Profile

A profile is made up of a user details like name, date of birth, gender, mail id, password, age etc,. The user can also edit and change the profile as he/she wants.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, June 2022
Impact Factor: 6.252

III. CONCLUSION

We have 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. 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.

REFERANCES

[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]. 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.

[3]. 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.

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

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