BLOCK CHAIN- SECURE ONLINE CHAT NETWORK FROM SPAM BOT

M. Manikandan[1], A. Balaji[2]

[1] Student of Department of Information Technology, Meenakshi College of Engineering, Chennai, Tamil Nadu, India
[2] Student of Department of Information Technology, Meenakshi College of Engineering, Chennai, Tamil Nadu, India

---***---

Abstract - This paper addresses the development of a live chat messaging network that detects and blocks spam bot text messages using advanced algorithms. By preventing spam bots and hackers from infiltrating the system, the goal is to provide users with a secure and private chat environment. Using a combination of machine learning algorithms and natural language processing techniques, the proposed system assesses the content of incoming messages and detects probable spam. With the rapid rise of online communication channels, the issue of spam and unwanted messages has become a serious concern. Hackers and spammers employ automated bots to transmit unwanted and malicious emails to unsuspecting users. As a result, developing a system capable of recognizing and preventing spam bots is crucial.

Key Words: Chat, Message, Chatroom, Communication Online, spamming, Spam Bot.

1. INTRODUCTION

The following goals could be addressed while developing an online chat application that provides a safe and secure environment for users to communicate while also protecting their chat information from spam bots and hackers.

Strong security measures should be in place to prevent unauthorized access, hacking attempts, and spam attacks. Secure login authentication, data encryption, firewalls, and spam filters are examples of such features. The development team should update the application on a regular basis to repair any security vulnerabilities or faults that spammers or hackers may exploit. Online chatting has become an essential aspect of communication in today's digital network lifestyle.

People utilize numerous online chat systems to stay connected with their friends, family, coworkers, and clients, whether for personal or professional purposes.

Here are some general guidelines for internet chatting: Keep your wording and tone in mind. It's critical to be aware of your words and tone when conversing online. Use good language and spelling, and avoid using slang or abbreviations that the other person may not understand.
Also, keep your tone nice and respectful, and avoid employing sarcasm or humor that could be misconstrued.

2. REPORT ANALYSIS

2.1 Use caution when using language and tone

It's vital to remember while speaking online that written communication can be readily misunderstood. As a result, it is crucial to be careful with your words and tone.

Use appropriate grammar and spelling, and stay away from acronyms and slang that the other person might not understand. Additionally, be careful to speak in a polite and professional manner and refrain from employing sarcasm or inappropriate humor.

2.2 Don't divulge private information

Sharing personal information should be done with caution because online chat rooms are not always secure. Don't divulge private details like your address, phone number, or financials. Be cautious of those who want this information and report any suspicious activity to the platform’s customer support team.

2.3 Show consideration for other people's time

It's crucial to show consideration for other people's time when chatting online. If it's not an emergency, avoid sending texts at night or in the early morning. Additionally, be patient and refrain from sending successive messages if the other person is preoccupied or doesn't react right away.

2.4 Be safe

It's crucial to secure your personal information and use caution when conversing online. Be careful when giving out private information like your address or phone number, and stay away from face-to-face meetings unless you feel at ease and have taken the necessary safety precautions.

2.5 Be mindful of your online presence

It's crucial to be mindful of your online presence when conversing online. This includes the information you post on your profile, such as your username and profile photo. Make sure your online presence is appropriate for the platform you're using and represents the image you want to project.

2.6 Have patience

It's crucial to have patience when conversing online. The other person might not always reply right away and could need some time to formulate a well-thought-out response. Give them the time they need to answer without pressing them to do so.

2.7 Pay attention to your timing

When speaking online, it's crucial to pay attention to your time. Sending communications at times when the recipient may be busy, such as at work or late at night, should be avoided. Additionally, if you are in a different time zone, be mindful of the difference and modify your messaging as necessary.

2.8 Steer clear of spam

Sending unwanted or unsolicited messages to other users is known as spamming. When conversing online, it's crucial to avoid spamming because it can be annoying and cause the other person to block or report you.

3. PROPOSED SYSTEM

Safe online conversation Users of social networks could gain a variety of advantages, including stronger social ties and better mental health. The proliferation of incorrect information, cyber bullying, online predators, addiction, and privacy invasion are just a few of the threats and issues that need to be handled. Social network operators ought to follow best practices to reduce these dangers and encourage the appropriate use of internet resources.

Client connections can be made after the server has been launched. A chat room login is an option for the user. to develop a chat program that enables users to converse with one another over a networked server. This website looks for spam and automatically blocks unwanted messages and links. In the chat room, users may see the status of other users, including whether they are online or not.

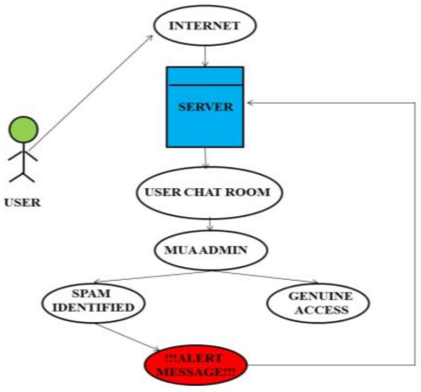

Figure 1: Use case Diagram for Proposed system

4. LIST OF MODULES

4.1 User Interface/Authentication

Users can be actual people or any kind of computer programmed, application, service, or software agent that communicates either directly or indirectly with a physical object or a system. There are two different categories of end users here.

- Trusted Authority
- MUA Administrator

4.1.1 Trusted Authority

Verifying user input is the initial stage in the login checking procedure. This is accomplished by comparing the user's credentials with those stored in the database or user management system. To prevent unauthorized access to the user's credentials, all interactions between the client and server throughout the login process should be encrypted using HTTPS (SSL/TLS).

4.1.2 MUA Administrator

As an administrator, you ought to use a robust and distinctive password for your login information. There may be a combination of capital and lowercase letters, numerals, and special characters in this. The login system should only be accessible to authorized individuals. Setting up user roles and access controls will enable this.

4.2. Behavioral Identify

To understand what the user is discussing, start by reading the chat. Look for terms and phrases that could provide you with information about the subject. After reading the entire conversation, look for any trends in the user's talk. Are they talking about a certain good or service? Are they requesting a lot of information on a particular subject?

4.3 MUA Algorithm

A communication process is made more simple and effective when MUA algorithms are removed. Users can converse without having to sort through pointless or spammy communications, which can enhance the general effectiveness and quality of conversation. Users can work more efficiently by reducing the number of spam bots, which frees up time and effort that would otherwise be used to filter out undesirable messages. This may result in more productive and laser-focused work.

4.4 Spam Detection

Although detecting spam bots during live message transmission can be difficult, there are a number of methods that can be utilized to spot and prevent suspected spam bots.

You can use machine learning techniques to train a spam filter to recognize spam by teaching it to recognize frequent spam terms and patterns. The MUA administrators are in charge of keeping an eye on the chat area to make sure that any spam messages that the filters missed are swiftly deleted. Spammers frequently create new accounts to avoid being blacklisted by filters and bans. You can detect users who are more likely to be spammers with the aid of a MUA system.

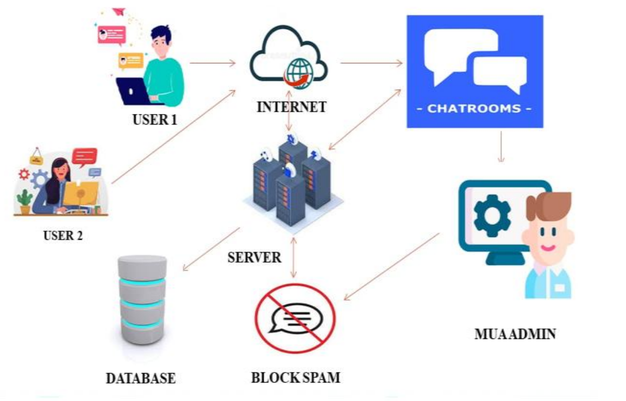

Figure 2: Block diagram of spam bot

5. STEPS FOR PROCESS OF MUA ADMIN ALGORITHM:

Step: 1 - Monitor the performance of a single webpage or sequence of web pages.

Step: 2 - Monitor critical page workflows and test applications before launch.

Step: 3-Track unauthorized content changes. Step:4- Three level of security for user data

Step: 5- It's shows the live user in the chat rooms and shows joined user and left user in the live room.

Step: 6- MUA Algorithm run in the server itself.

Input: UID, Udate, Utime, Umsg, n,UNW, Up, Th UID : User ID, Udate : User Date of access, Utime: User Time of access, Umsg : User chat, n: no.of users, UNW: unwanted msg, Up = User pattern, Threshold. Step:6.1- Start

Step: 6.2- User Login

Step: 6.3- UNW = 0

Step: 6.4- For UID = 1;UID<=n;UID++ Track Udate, Utime, Umsg

Step: 6.5- If UID.Umsg = Up UNW = UNW +1

Step: 6.6- If UNW >Th Block the user

Step: 6.7- Stop

Step: 7-MUA Algorithm analysis each and every chats in live room.

Step: 8-MUA Admin has stores user chats in the server to find the unwanted message and links in the live room.

Step: 9- Remove spam bot or user who sends unwanted messages and links automatically.

Step: 10- Block that user interface and unregister from the access list.

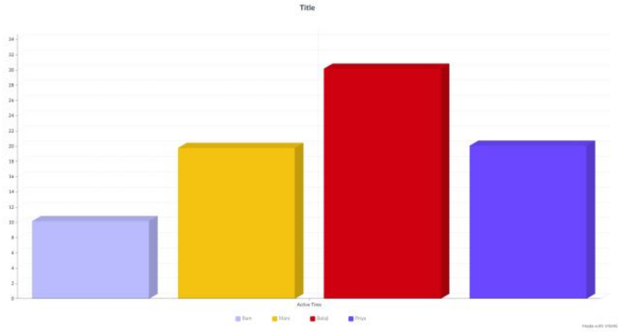

Chart -1: User Active Time

6. CONCLUSIONS

Online safe chat social networks have the ability to offer users a number of advantages, such as a growth in social connections and a betterment of mental health. The proliferation of misleading information, cyber bullying, online predators, addiction, and privacy invasion are a few of the threats and issues that need to be addressed. Social network providers should put best practices in place to reduce these hazards and encourage ethical usage of digital spaces. The suggested technique offers a practical means of locating and preventing spam bot text messages in chat messaging systems.

The study of social networks for safe online discussion emphasizes the significance of weighing the advantages and disadvantages of using these systems. While they have many advantages, like better mental health, more social connections, and better learning possibilities, there are also a number of difficulties and potential concerns that need to be taken into consideration. Social network providers must take the necessary precautions to safeguard their users from cyber bullying, online predators, the propagation of false information, addiction, and invasion of privacy if they are to keep these platforms secure and useful for their users.

7. REFERENCES

[1] Stefano Cresci, Roberto Di Pietro., "Social Fingerprinting – Detection Of Spam bot," Twitter spam account deduction, pp. 1-7,2022.

[2] H. Liu et al., "Uncovering deception in social media," Social Network Analysis and Mining, vol. 4, no. 1, pp. 1–2, 2021.

[3] G. Stringhini, M. Egele, C. Kruegel, and G. Vigna, "Poultry markets: on the underground economy of Twitter followers," in Online Social Networks. ACM, 2021, pp. 1–6.

[4] G. Stringhini, G. Wang, M. Egele, C. Kruegel, G. Vigna, H. Zheng, and B. Y. Zhao, "Follow the green: growth and dynamics in Twitter follower markets," in Internet Measurement Conference (IMC). ACM, 2021.

[5] C. Lee, I. Sohn and W. Lee, "Eavesdropping Detection in BB84 Quantum Key Distribution Protocols," in IEEE Transactions on Network and Service Management, April 2022.

[6] J. Señor, J. Portilla and G. Mujica, "Analysis of the NTRU Post-Quantum Cryptographic Scheme in Constrained IoT Edge Devices," in IEEE Internet of Things Journal, March 2022.

[7] Suhyeon Jeon, JeonghoKwak, Jihwan P. Choi," Cross-Layer Encryption of CFB_AES-TURBO for Advanced Satellite Data Transmission Security" IEEE Trans. Aero and Elec. Syst ., Dec 2021.

[8] N. Alshaer, A. Moawad and T. Ismail, "Reliability and Security Analysis of an Entanglement-Based QKD Protocol in a Dynamic Ground-to-UAV FSO Communications System," in IEEE Access, vol.

[9] H. A. Al-Mohammed et al., "Machine Learning Techniques for Detecting Attackers During Quantum Key Distribution in IoT Networks With Application to Railway Scenarios," in IEEE Access, vol. 9, pp. 136994-137004, October 2021

[10] X. Lu, Z. Wu, Y. Wu, Q. Wang and Y. Yin, "ATMChain: Blockchain-Based Solution to Security Problems in Air Traffic Management," 2021 IEEE/AIAA 40th Digital Avionics Systems Conference (DASC), November 2021.

[11] M. Q. Vu, T. V. Pham, N. T. Dang and A. T. Pham, "Design and Performance of Relay-Assisted Satellite Free-Space Optical Quantum Key Distribution Systems," in IEEE Access, vol. 8, pp. 122498-122510, July 2020.

[12] I. Mustafa et al., "A Lightweight Post-Quantum Lattice-Based RSA for Secure Communications," in IEEE 11 Access, vol. 8, pp. 99273-99285, May 2020.

[13] D. Huang et al., "Quantum Key Distribution Over Double-Layer Quantum Satellite Networks," in IEEE Access, vol. 8, pp. 16087-16098, January 2020.

[14] T. M. Fernández-Caramès and P. Fraga-Lamas, "Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks," in IEEE Access, vol. 8, pp. 21091-21116, January 2020.

[15] Z. Sun, C. Wu, S. Zheng and C. Zhang, "Efficient Multiparty Quantum Key Agreement With a Single dd -Level Quantum System Secure Against Collusive Attack," in IEEE Access, vol. 7, pp. 102377-102385, July 2019.

[16] A. Aguado et al., "The Engineering of Software-Defined Quantum Key Distribution Networks," in IEEE Communications Magazine, vol. 57, no. 7, pp. 20-26, July 2019,

[17] W. Lu, T. Liang, K. An and H. Yang, "Secure Beamforming and Artificial Noise Algorithms in Cognitive Satellite-Terrestrial Networks With Multiple Eavesdroppers," in IEEE Access, vol. 6, pp. 65760-65771, October 2018.

[18] S. Krendelev and P. Sazonova, "Parametric Hash Function Resistantto Attack by Quantum Computer". In Proc. Federated Conference onComputer Science and Information Systems, Poznan, Poland, Sep. 2018.

[19] Bedington, R., Arrazola, J.M. & Ling, A. Progress in satellite quantum key distribution. npj Quantum Inf 3, July 2018.

[20] Korzh, B., Lim, C., Houlmann, R. et al. Provably secure and practical quantum key distribution over 307 km of optical fibre. Nature Photon 9, 163–168 February 2018.