

Detection of Cyberbullying Spam Mails

Naveenkumar R¹, Dr.A.R.Jayasudha²

¹Student, ²Professor,

Department of MCA, Hindusthan College of Engineering and Technology,
Coimbatore, India.

***Corresponding Author**

E-mail Id: - sudhahindusthan.backup@gmail.com

ABSTRACT

Cyberbullying is a serious problem that affects many young people, and social networking sites are a common platform for this behavior. The use of technology as a medium for bullying has increased in recent years, and this underscores the need for research to develop intelligent systems that can automatically detect and prevent potentially harmful messages. The work on constructing and annotating a corpus of Dutch social media posts with fine-grained cyberbullying-related text categories is an important step in addressing this issue. Being able to identify specific types of cyberbullying behavior, such as insults and threats, can help in the development of targeted prevention and intervention strategies. Furthermore, the identification of specific participants in cyberbullying conversations, such as the harasser, victim, or bystander, can enhance the analysis of human interactions and provide valuable insights into the factors that contribute to this behavior. By understanding these dynamics, researchers can develop more effective prevention and intervention strategies to combat cyberbullying.

Keywords: Spam Mails, Python, MySQL, MODULE DESCRIPTION

OBJECTIVE

E mail is a service that enables electronic message transmission via the internet. It provides a quick, affordable, and effective way to disseminate information among people. Thus the mail process will be referred as mail over internet. Mail refers to the process of communicating, interacting and/or exchanging messages over the Internet. It involves two or more individuals that communicate through a mail-enabled service or software. Mail may be delivered through text, verbal, communication. Terrorist activities communicate over application and mail programs over internet. It also uses these mail applications over the internet for getting their message to younger generation and making all of type's terrorists. The mail monitor system is an important application that could allow for

secure mails along with terrorism related mail detection that helps track down spread of terrorist networks and locate the activities using IP addresses

EXISTING SYSTEM

There is a need for automated tools that can assist in the detection of suspicious chat activity. These tools typically use machine learning algorithms to analyze chat logs and identify patterns of behavior that are indicative of malicious intent, such as the use of specific keywords or phrases. In addition, many chat services employ moderators who monitor conversations in real-time and can quickly intervene if they detect any inappropriate behavior. However, given the vast number of online chat rooms and the constantly evolving tactics of malicious actors, it remains a significant challenge to ensure the safety

and security of individuals who use these platforms.

PROPOSED SYSTEM

- The proposed system aims to automatically analyze online text sources from specific discussion forums and classify them into different categories, distinguishing between legal and illegal content. The system would rely on a set of suspicious keywords predetermined by the admin, which would be used to identify potentially problematic content.
- If any content containing these keywords is detected, the system would automatically block the offending message, preventing it from being viewed by other users. Additionally, the system would flag the sender's email address as suspicious, which could prompt the admin to investigate further and potentially report the user to the appropriate authorities.
- Overall, this system appears to be designed to help the admin manage the content of the discussion forums and ensure that they remain free from illegal or harmful activity. However, it's worth noting that any automated system like this may have limitations and could potentially flag legitimate content as suspicious, so it's important for the admin to carefully review and evaluate any content that is flagged by the system.

ADVANTAGES OF PROPOSED SYSTEM

- If the proposed system is designed to monitor emails and identify suspicious chats, it could potentially involve analyzing the content of emails for specific keywords or phrases that are known to be associated with illegal or harmful activities. The system might also use other techniques, such as natural language processing or machine learning algorithms, to identify patterns of behavior or language that are indicative of suspicious activity.

- Once a suspicious chat is identified, the system could alert the admin and potentially block the offending user or take other actions to prevent further harm. It's worth noting, however, that monitoring emails in this way could raise privacy concerns, so it's important for the system to be designed and implemented in a way that respects users' privacy rights and complies with any relevant laws and regulations.

- This system is also designed to detect and block users who send illegal emails or engage in other harmful activity, it could potentially involve using a combination of automated and manual processes to identify and take action against offenders.

- For example, the system might analyze the content of emails for specific keywords or patterns of behavior that are associated with illegal activity. When suspicious activity is detected, the system could automatically block the offending user and alert the admin to the issue. The admin could then manually review the evidence and determine whether to report the user to the appropriate authorities.

- In addition, the system could use a variety of technical measures to help protect users' privacy and security. For example, it could encrypt user data to prevent unauthorized access, use multi-factor authentication to verify users' identities, or implement other security protocols to prevent hacking or other attacks.

SYSTEM SPECIFICATION

HARDWARE SPECIFICATION

PROCESSOR	: Intel CELERON
RAM	: 8GB
HARD DISK DRIVE	: 250GB

SOFTWARE SPECIFICATION

OPERATING SYSTEM	: Windows 11
FRONTEND	: HTML, CSS
DATABASE	: MYSQL

BACKEND : PHP
SOFTWARE :
WAMP SERVER
CLIENT : ANY
BROWSER

ABOUT FRONT END

PYTHON

Python is an interpreter, object-oriented, high-level programming language that is known for its simplicity and ease of use. Its dynamic semantics and built-in data structures make it an attractive choice for rapid application development and scripting. Python also supports modularity and code reuse through its modules and packages, and the Python interpreter and extensive standard library are available free of charge for all major platforms. Additionally, Python's debugging capabilities make it easy to catch errors and exceptions in code, both through the use of a source level debugger and by adding print statements to the source code.

ABOUT BACK END

MYSQL

MySQL is a powerful and widely used relational database management system that allows for efficient storage, organization, and retrieval of large amounts of data. It is particularly popular for use in web applications due to its speed, reliability, and scalability. MySQL also offers a variety of advanced features, such as support for transactions, triggers, and stored procedures, which make it a powerful tool for building complex systems. MySQL is supported on all major platforms, including Windows, Linux, and macOS, and can be easily integrated with a variety of programming languages, including Python, PHP, and Java. Additionally, the fact that MySQL is open source and available under the GNU General Public License makes it an attractive option for developers who want to avoid expensive licensing fees associated with proprietary database

system.

MODULE DESCRIPTION

ADMIN MODULE

1.View User

- Once a user has registered and provided their details, such as their name, email address, and other relevant information, these details can be stored in a database. When the user logs in to the system using their username and password, the system can retrieve their details from the database and display them on the user's dashboard.

- The details of the user can also be used by the admin to verify the user's identity and ensure that they are authorized to access the system. The admin can view the details of all registered users in the system and make any necessary changes or updates to the user's profile.

2. Add Keyword

- The admin can add keywords to the database to help identify illegal or suspicious activity. These keywords can be added manually by the admin or through an automated process that uses data mining algorithms to analyze email conversations and identify suspicious keywords.

- The system should also be regularly monitored and updated to ensure that it is detecting the most relevant keywords and patterns.

- These techniques can help the system to better understand the context and meaning of words used in email conversations, and makes more accurate decisions about whether a keyword is suspicious or not.

3. View Suspicious Attacker

- Once the keyword is identified, the system can generate an alert or notification to the admin and/or the user, informing them of the suspicious activity. The notification can include details about the chat, such as the date and time of the conversation, the sender and recipient of

the message, and the content of the message.

- It's important to ensure that notifications are generated quickly and accurately, so that appropriate action can be taken to prevent any illegal or malicious activity. Notifications should also be accompanied by detailed instructions on what action should be taken next, such as contacting law enforcement or blocking the sender of the suspicious message.

4. Block Attacker

- If an attacker is identified as sending spam or malicious messages through the system, the system can block them from accessing the system or sending further messages.
- The system can use various techniques such as IP blocking, user banning, or content filtering. IP blocking involves blocking the IP address of the attacker, which prevents them from accessing the system from that IP address. User banning involves blocking the user account of the attacker, which prevents them from logging in to the system and sending further messages. Content filtering involves analyzing the content of messages sent by the attacker and blocking any messages that contain suspicious keywords or content.

AUTHORITY MODULE

1. Authority intimidation

- If suspicious activity is identified through the system, such as the use of a suspicious keyword in a chat, the relevant authorities should be notified. This can include law enforcement agencies, intelligence agencies, or other relevant authorities depending on the nature of the activity.
- Once the authorities are notified, they can take the necessary actions to investigate the activity and take appropriate measures to prevent any illegal or malicious activity. This can include

blocking the user account, conducting a more thorough investigation into the activity, and potentially taking legal action against the perpetrator.

- It's important to ensure that any notifications sent to the authorities are accurate and include as much detail as possible about the suspicious activity. This can include details about the user account, the content of the chat, and any other relevant information that may assist in the investigation.

2. View Spammer and ID detection

- The IP address can be used to identify the network and internet service provider (ISP) that the spammer used to send the message. The ISP can then be contacted to identify the account holder associated with the IP address. However, this may not always lead to the actual spammer, as the account holder may not be the one who sent the spam message.
- It is important to report any spam messages to the appropriate authorities, who can then take appropriate measures to investigate and prevent further spamming.

DATAFLOW DIAGRAM

LEVEL 0

User block: This component would handle the creation of new user accounts, as well as user login and blocking. When a new user registers, their information would be stored in a database, which could then be used to authenticate them when they log in. The user block would also provide a mechanism for blocking users who engage in inappropriate behavior, such as sending spam emails or engaging in harassment.

Admin block: This component would be used by system administrators to set up and manage the spam detection system. It would allow admins to define keywords and other criteria that the system could use to identify potentially problematic emails. The admin block would also provide a way for admins to view user accounts and

emails, in order to identify and address any issues that arise

Authority block: This component would be used by law enforcement or other authorities to investigate and address illegal activity on the platform. It would provide a way for authorized users to review flagged emails and block user accounts that are engaging in illegal or harmful behavior.

Database: All of the components in the system would be linked to a central database, which would store information about user accounts, emails, keywords, and other relevant data. This data could be used to identify patterns and trends in user behavior, as well as to track down and address specific instances of spam or other harmful activity.

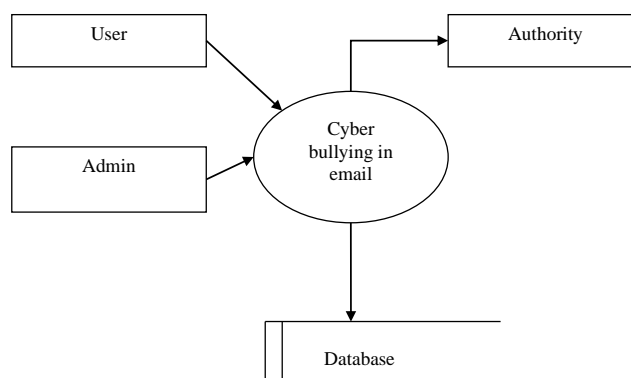


Fig.1:-Level 0 DFD

LEVEL 1

- Users would start by registering for an account on the system. This would involve providing some basic information, such as their name, email address, and a password. Once the user account is created, they would be able to log in and access the email sending functionality.
- Once logged in, users would be able to compose and send emails to other users on the system. As you mentioned, the system would check the content of the email against a list of keywords that have been defined by the system admin. If the email contains any of the keywords, it would be flagged as potentially problematic and marked as spam.

- The spam detection functionality would be managed by the system admin. They would be able to create and manage the list of keywords that the system should be looking for in emails. This would help to ensure that any illegal or inappropriate messages are caught and flagged.
- If an email is flagged as spam, the system would generate an alert or notification to the authority side of the system. This would allow authorized users to review the email and determine whether it is illegal or inappropriate. If necessary, the sender's account could be blocked to prevent them from sending further spam emails.

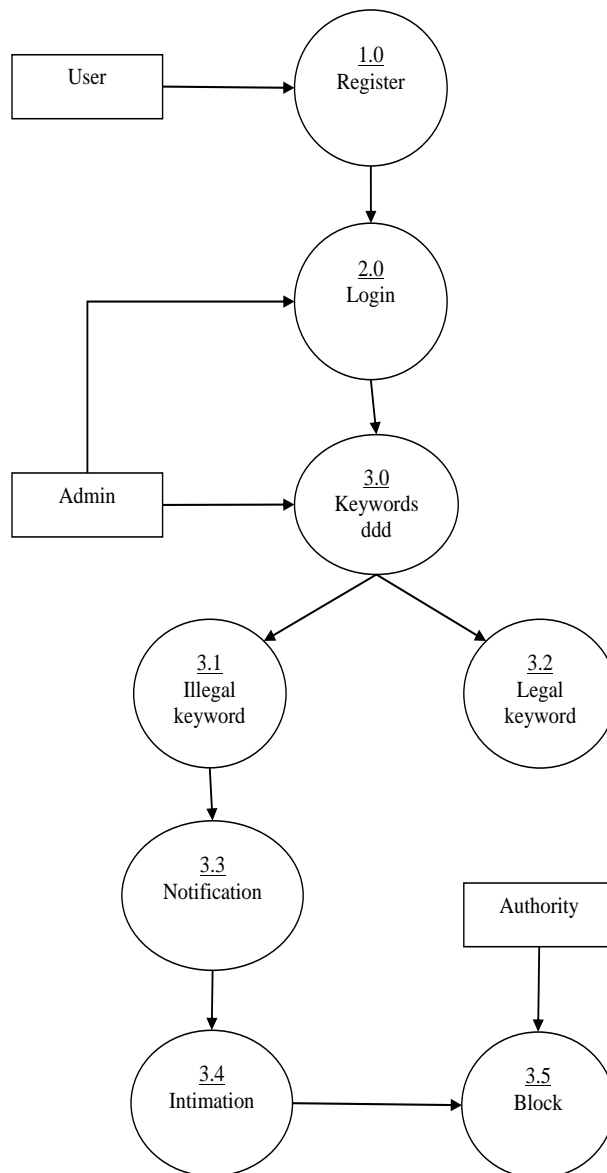


Fig.2:-Level 1 DFD

ENTITY RELATIONSHIP DIAGRAM

- The admin would maintain the IDs of users or keywords that are not allowed to send emails through the system. The keywords could be checked against the content of the message to determine if it matches any of the blocked terms. If a match is found, the message would be blocked from being sent.
- On the other hand, the user message block would contain the user's

requirements when composing a message, such as their name, email address, and the content of the message itself. This information would be displayed to the recipient when they receive the message.

- To prevent spam from being sent through the system, the system would likely use some form of spam filter to analyze the content of the message and determine whether it is legitimate or not.

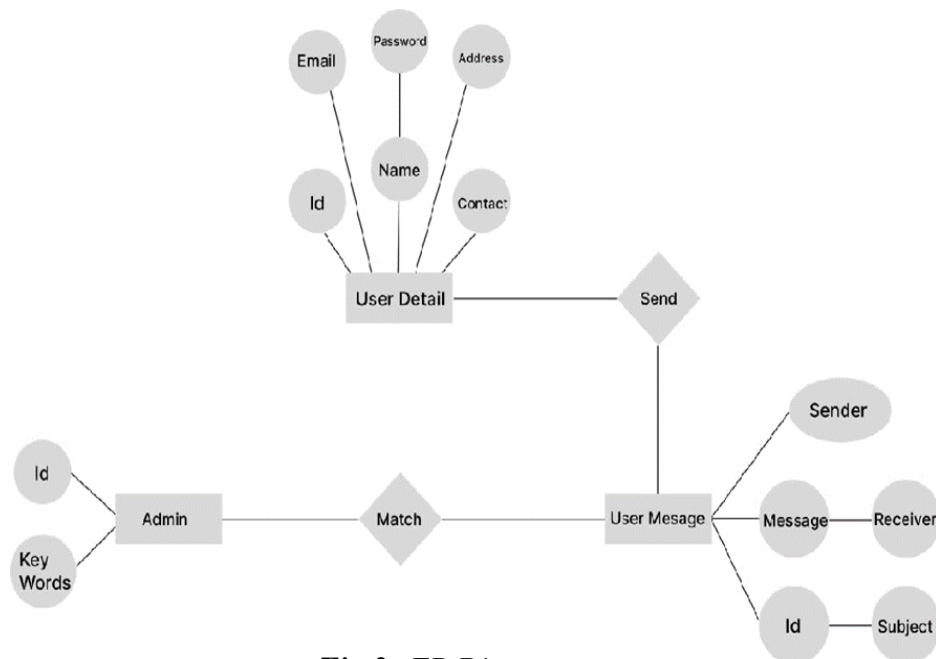


Fig.3:-ER Diagram

INPUT DESIGN

- Registering for an account typically involves providing some personal information, such as your name, email address, and a password.

Name	<input type="text"/>
Contact	<input type="text"/>
Email	<input type="text"/>
Address	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password"/>
<input type="button" value="Register"/>	

Fig.4:-New Register

OUTPUT DESIGN

When implemented as a form and re-entered into the system as an input, some

of the external outputs are intended to be turnaround outputs.

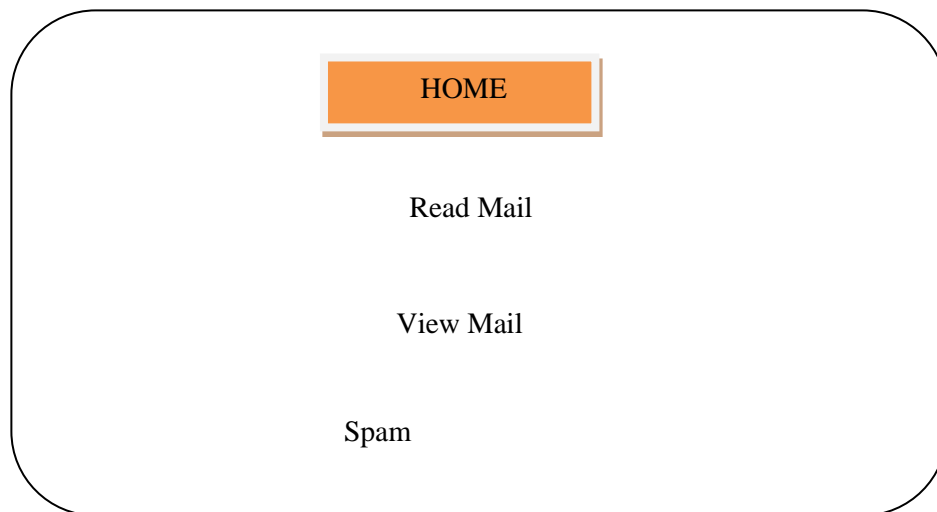


Fig.5:- Output Page

- If a user receives a message that is detected as spam, the messaging platform or email service may move it to a spam folder or label it as spam. Some platforms

may also provide users with the ability to report spam messages or block the sender of the spam message.



Fig.6:- View Mails

- If system detects that a user has been sending spam messages, they may take actions to prevent that user from continuing to send spam. Depending on the severity of the issue and the platform's

policies, this could include temporarily or permanently blocking the user's account.

- If a user's account is blocked for sending spam messages, they may not be able to access the messaging platform or email service until the issue is resolved.

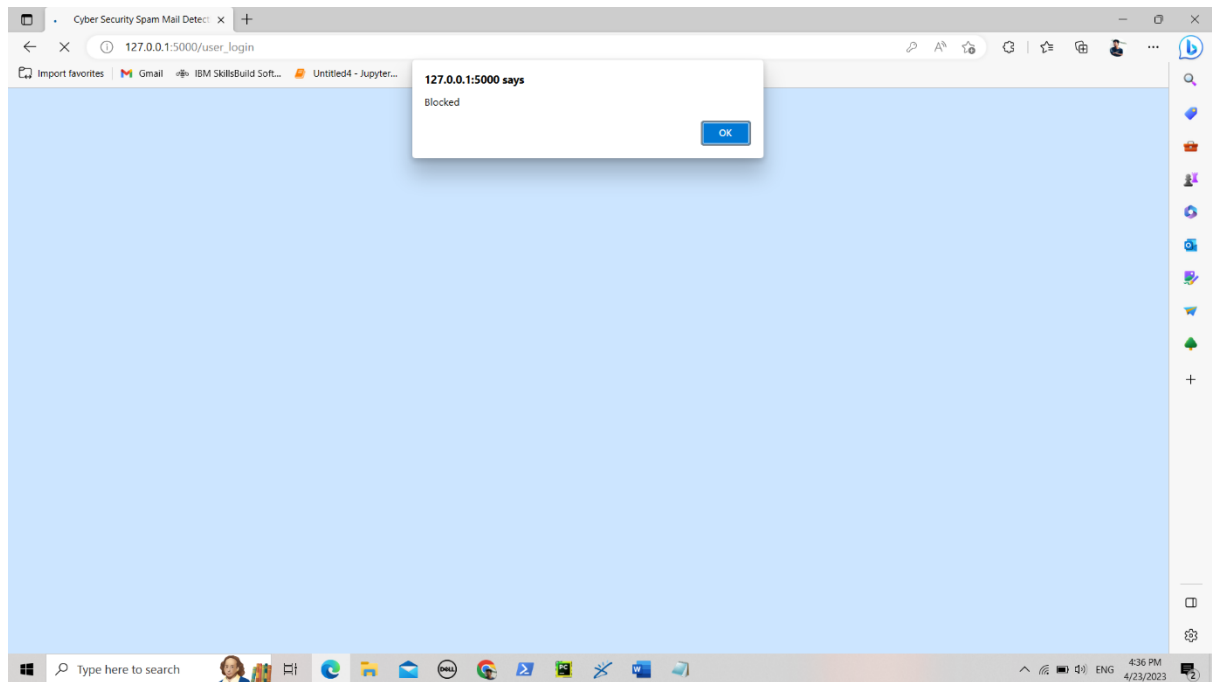


Fig.7:- Blocked Message

SOFTWARE TESTING

Unit Testing:

- To test the user login functionality, a unit test could check whether the email field contains the required format and
-

structure, such as a valid email address with a "@domain.com" suffix.

- The test could also check whether the email and password fields are not blank or null, as these are typically required fields for user login.

Test condition id	Test Id	Test condition	Test Description	Test data	ExpectedResult	Initial Result
TC_LF_01	TC_LF_1	Check whether the Email textbox is blank	Email textbox should not be blank	Blank	System Did not accept the blank value	Pass

TC_ LF_01	TC_ LF_1	User email should be alphabet or numbers or combination of both	User can enter the required email	naveen@123	System accept	pass
TC_ LF_01	TC_ LF_2	Check whether the password textbox is blank	Password textbox should not be blank	blank	System did not accept the blank value	pass
TC_ LF_01	TC_ LF_2	Username should be alphabet or numbers or combination of both	User can enter the required username	naveen	System accept	pass

Table 1:-User Login form

Fig.8:- User Page

Validation Testing

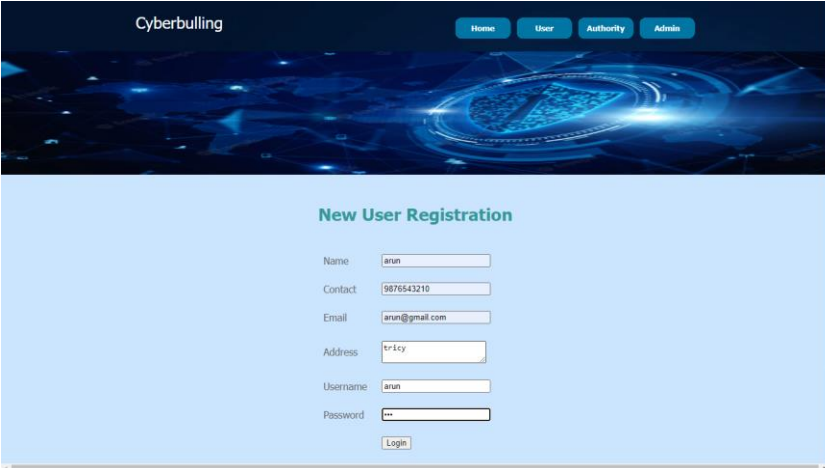
- The contact field should only contain ten numbers. A validation check could be implemented to ensure that the input contains exactly ten digits, and does not include any other characters or symbols.
- And the email field should contain a valid email address format, including the "@" symbol and a domain suffix.

- Other should not be empty or null. A validation check could be implemented to ensure that the input contains at least one character, and does not consist only of whitespace characters.
- This can help to prevent errors or issues that could arise from invalid or incorrect user inputs.

Test condition id	Test Id	Test condition	Test Description	Test data	ExpectedResult	Initial Result
TC_LF_02	TC_LF_1	Check whether the Name textbox is blank	Name textbox should not be blank	Blank	System Did not accept the blank value	Pass
TC_LF_02	TC_LF_1	User should be alphabet only	User can enter the required name should be string	Naveen12	System did not accept numeric value in name	pass
TC_LF_02	TC_LF_2	User should be numeric only	User can enter the required contact only in number	1122336655449988	System did not accept the more than ten number	pass
TC_LF_02	TC_LF_2	User should be numeric only	User can enter the required contact only in number	6369249851	System accept	pass
TC_LF_02	TC_LF_3	Check whether the Email textbox is blank	Email textbox should not be blank	Blank	System Did not accept the blank value	Pass

TC_ LF_02	TC_ LF_3	User email should be alphabet or number or both	User can enter the required email	naveen@123	System accept	pass
TC_ LF_02	TC_ LF_4	Check whether the Name textbox is blank	Name textbox should not be blank	Blank	System Did not accept the blank value	Pass
TC_ LF_02	TC_ LF_4	Username should be alphabet or numbers or both	User can enter the required name should be both	Naveen12	System accept	pass
TC_ LF_02	TC_ LF_5	Check whether the password textbox is blank	Password textbox should not be blank	blank	System did not accept the blank value	pass
TC_ LF_02	TC_ LF_5	Username should be alphabet or number or both	User can enter the required username	naveen	System accept	pass

Table 2:-User Registration



The screenshot shows a web application interface for 'Cyberbullying'. At the top, there's a dark blue header with the title 'Cyberbullying' and four navigation buttons: 'Home', 'User', 'Authority', and 'Admin'. Below the header, the main content area is light blue and features a 'New User Registration' form. The form includes input fields for 'Name' (filled with 'arun'), 'Contact' (filled with '9876543210'), 'Email' (filled with 'arun@gmail.com'), 'Address' (filled with 'tricy'), 'Username' (filled with 'arun'), and 'Password' (filled with '***'). A 'Login' button is positioned at the bottom of the form.

Fig.9:-New User Page

SYSTEM IMPLEMENTATION

- When the admin logs in with their username and password, they will be directed to the admin dashboard where they can view various options and functionalities related to monitoring and managing the mail system.
- To verify the registered users and their chats with the keyword added, the admin will have access to the user database and the chat logs. The admin can search for specific keywords in the chat logs and view the messages exchanged by the users containing those keywords
- The admin can also view the profiles of registered users to gather more information about them, such as their personal details, contact information, and chat history. This will help the admin to identify any suspicious activities or behavior patterns of the users.
- In case any suspicious activity is identified, the admin can take necessary actions such as blocking the attacker, notifying the user, and generating reports on the suspicious activity. The admin can also add new keywords to the database to improve the monitoring process and identify any potential threats.
- When the admin identifies an attacker with spam, they can take necessary actions to block the attacker from the system. This can be done by adding the attacker's information to a blacklist, which will prevent them from accessing the mail system and sending spam messages in the future.
- Blocking the attacker will help to prevent further spam messages and maintain the security and integrity of the mail system. Additionally, the admin can generate reports on the blocked attackers to track the number of attacks and take necessary measures to improve the system's security.
- The authorities to be notified when suspicious activities related to terrorism or other criminal activities are identified on the internet. If the mail system has been set up to monitor suspicious keywords and chat content related to such activities, and if any suspicious activity is identified, the admin can notify the authorities and provide them with relevant information such as the user ID, chat content, and IP address of the user.

- The authorities can then take appropriate actions to investigate and prevent any potential terrorist or criminal activities. This may include blocking the user ID from accessing the internet and taking necessary legal actions against the user.

CONCLUSION AND FUTURE ENHANCEMENT

- Social networking websites provide cutting-edge methods of connection and communication, but they also present new privacy and security concerns. In this essay, we provided a quick overview of social networking websites, summarized their taxonomy, and emphasized important privacy and security concerns while providing some vital anti-threat tactics in light of the websites' potential future.
- According to our analysis, the development of new technology in general and social networking sites in particular will lead to increased security concerns that could give bad actors, key loggers, Trojan horses, phishing, spies, viruses, and attackers new chances. Government officials, intelligence agencies, and information security experts must create new technologies that protect against and respond to anticipated risks and attacks in the future.
- It is also capable of safely manipulating the vast amount of data present on social media networks.

SCOPE FOR FUTURE ENHANCEMENT

- In the future, we can analysis how much spammer over internet. The database

approach of developing the system has helped in reducing redundancy of data and improving the consistency of data in the system. This system is flexible, user friendly. The system satisfies the client requirements specified.

BIBLIOGRAPHY REFERENCES

1. Matthes, E. (2023). *Python crash course*. no starch press.
2. Barry, P. (2016). *Head first Python: A brain-friendly guide*. " O'Reilly Media, Inc."
3. Prajna, M., Venugopal, V., Srivatsa, K., Suma, M. N., & Sudhindra, K. R. (2022, December). Terrestrial Communication Link Computation. In *2022 Fourth International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT)* (pp. 1-4). IEEE.

WEB REFERENCES

1. https://www.researchgate.net/publication/336800562_Credit_Card_Fraud_Detection_using_Machine_Learning_and_Data_Science
2. https://pats.cs.cf.ac.uk/@archive_file?p=1859&n=final&f=1-report.pdf
3. <https://www.ijrte.org/wp-content/uploads/papers/v10i2/B62580710221.pdf>
4. <https://pdf.sciencedirectassets.com/280203/1-s2.0-S1877050920X00032/1-s2.0-S187705092030065X/main.pdf>
5. <https://ijcsmc.com/docs/papers/April2021/V10I4202112.pdf>