WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Email Alert System On WhatsApp

Mr. Sanjay Jagtap[1], Somnath Dahiphale[2], Kunal Dukare[3], Ajinkya Adhav[4] , Sarthak Jadhav[5], Shivam Nangare[6]

[1] Associate Professor Of Computer Engineering, JSPM's Bhivarabai Sawant Polytechnic, Pune, Maharashtra, India
[2,3,4,5,6] Students Of Computer Engineering, JSPM's Bhivarabai Sawant Polytechnic, Pune, Maharashtra, India

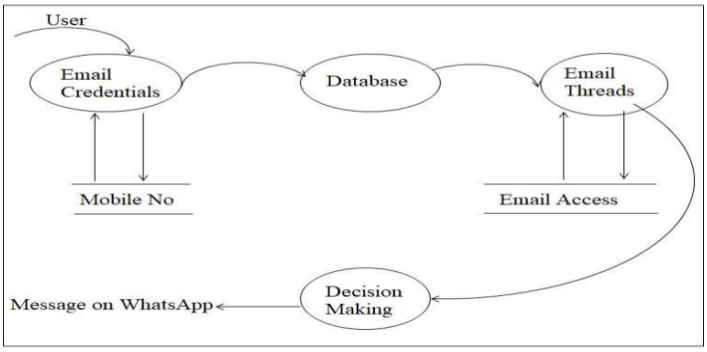
ABSTRACT :

When dealing with matters pertaining to official business, the most effective means of communication is email. Even though there are many alternative channels of communication available, the use of email continues to rise. In today's world, when the number of emails sent and received is constantly rising, the use of email management software has become an absolute necessity. Over fifty-five percent of all emails are considered to be spam. This indicates that spams are a waste of time and effort for email users, without bringing anything of value to the conversation. The primary focus of this research is on the various methods for recognizing emails arrived and they are unread through the concept of machine learning. In addition, this project provides a comprehensive way to forward the meta data of the arrived email in the in box by using the interactive thread system on the user's registered Whatspp number

Keywords: Gmail Host, WhatsApp, MAIL API, Multi threads

1. INTRODUCTION :

For the vast majority of people who use the internet, using email as their primary method of professional communication has quickly become the norm. In the recent past, there has been a rise in the number of people using email, which has led to an increase in the number of difficulties that are produced by spam emails. The practice of sending large numbers of unsolicited messages in bulk is referred to as spam or junk email. On the other hand, emails that are meaningful but have an opposite tendency are referred to as "Ham." A typical email subscriber receives between 40 and 50 messages each day on average. Every year, spammers bring in an estimated $3.5 million USD from their activities, causing financial harm to recipients on both the individual and the institutional level. As a consequence of this, the users invest a considerable amount of their working time in responding to these emails. According to reports, spam accounts for more than fifty percent of the traffic on email servers and is responsible for the transmission of a large number of uninvited and unwanted bulk emails. They reduce productivity by using user resources while producing little of value in return. The purpose of the marketing purposes that are intended to unfold malevolent criminal acts such as identity theft, financial disturbances, stealing sensitive information, and reputational damage that is carried out by spammers that disseminate spam has this objective. Email management and the categorization of spam emails are key necessities for enterprises in order for them to boost their production and reduce the financial losses they incur as a result of decreased output.



2. STRUCTURAL DESIGN.

1. The User Interface :

- *What they provide:*
  - Web/Mobile Dashboard
  - User Authentication (Login/Register)

- Sometimes, extra things like:
  - A code from their phone (like a secret handshake).
  - A Two factor Authentication (like a special key).
- *What they get:*
  - Instant Email Alerts on WhatsApp. (the system).

2. Backend Server :

- Manages logic for sending emails & WhatsApp messages
- Database operations
- **API handling**

3.Third Party API 's :

- Email API (SMTP, SendGrid, Gmail API)
- WhatsApp API (Twilio, Meta, WhatsApp Business API)

4. The Database :

- This is where all the user information is stored.
- It's super secure, like a locked vault.
- Email Logs
- Alert Preferences

Security is Key:

- **API Key Authentication** – A unique key assigned to each user/system for secure API access.
- **OAuth 2.0 Token** – A dynamic access token that expires after a certain time for better security.
- **Encryption Key** – Used to encrypt and decrypt sensitive email data.
  - JWT (JSON Web Token) – A token-based authentication system for verifying user identity. API Key Authentication – A unique key assigned to each user/system for secure API access.
  - **OAuth 2.0 Toke**n – A dynamic access token that expires after a certain time for better security.
  - **Encryption Key** – Used to encrypt and decrypt sensitive email data.

✅ **JWT (JSON Web Token**) – A token-based authentication system for verifying user identity.

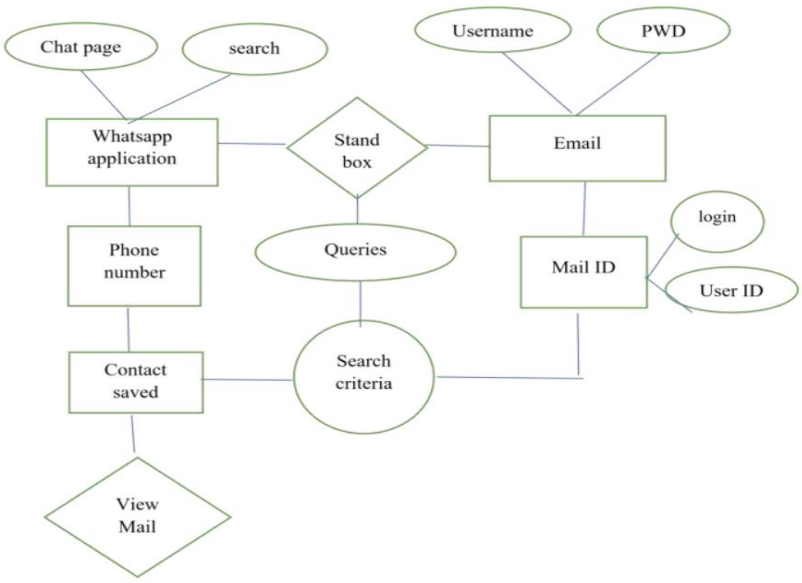
PROBLEM DEFINATION

To ease the process of email handling through interactive multi-thread to read the emails from the Gmail host and send the notifications on WhatsApp with meta metadata of the emails using decision making technic

SCOPE OF THE PROJECT

DeskAlerts:

With the Deskalerts Email Alerts Module, you can send desktop alerts as emails. Notify thousands of employees with email alerts simultaneously alongside other types of alerts, all in just one click and within one to two seconds. The Deskalerts email alert module increases the chances that your internal messages will be seen by the intended audience, even if employees are not in front of their computers or do not have access to the mobile app at the time. Additionally, these messages will be stored in employees' email history, which is crucial if your company has a policy requiring important communications to be documented in email form.



Lansweeper:

Email notifications enable you to remain informed about critical updates and emergencies related to your network, such as significant software modifications and errors occurring in servers or workstations. You have the option to configure your email alerts to disseminate information to the appropriate individuals as it arises or to send them on a predetermined schedule. This functionality allows you and your organization to proactively manage potential network issues, such as computers nearing disk space limits, systems lacking antivirus protection, or printers with low toner levels. Lansweeper can send two types of email alerts: A) Report Alerts and B) Event Log Alerts. When set up correctly, report alerts will notify you whenever a report yields results. You simply need to select the reports for which you wish to receive alerts and add them to the Email Reports list. If a report generates one or more results after execution, Lansweeper will automatically send an email to and designated email address or group, or it can copy the results to a preconfigured directory. The alert will include the report's results in an Excel, HTML, or CSV format. The frequency of these emails is customizable, ranging from every minute to once a month. Event log alerts provide immediate notifications whenever a specified Windows event is detected. You can choose the events that are relevant to you from a list and ensure that Lansweeper scans for these event types. By default, Lansweeper scans only for error events to prevent an overwhelming influx of event logs from cluttering your database. To avoid receiving an email for every single event log, you can easily adjust the criteria that an event must meet to trigger an alert. When Lansweeper identifies an event that satisfies these criteria, an email is sent to a designated mailing group. Unlike report alerts these emails are dispatched immediately.

WORKING AND PROCESSES :

The above diagram indicates an overview of the proposed model designed to send the WhatsApp notification for the received emails. The steps that are carried out in this process are elaborated on in the below-mentioned points.

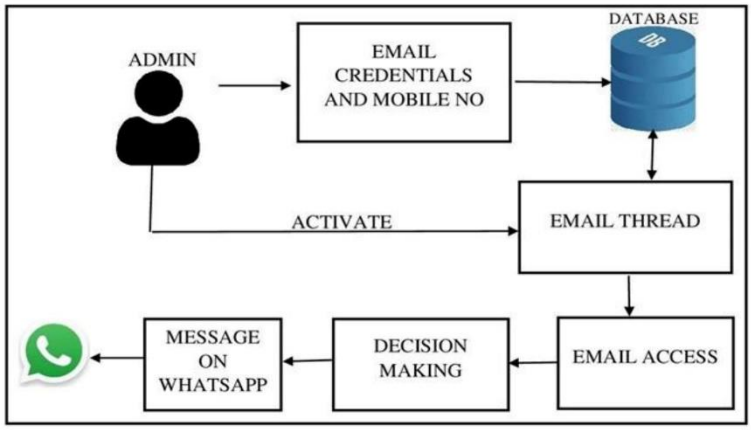
Step 1: Generating a Gmail Security Key –

A security key serves as a form of authentication designed to safeguard your Google Account. You have the option to utilize the integrated key available on your mobile device or purchase a physical key from the Google Store or an authorized retailer. These physical keys resemble thumb drives equipped offer protection for your account similar to how a traditional key secures your home.

Employing a security key as a supplementary method for 2-Step Verification can facilitate account recovery in the event that you misplace your phone or need to reset it. Additionally, security keys play a crucial role in preventing phishing attempts and confirming the authenticity of the sign-in URL prior to logging in.

A security key can complement other 2-Step Verification methods, such as backup codes, Google prompts, or your phone number. For further information on 2-Step Verification, please follow these steps:

- Access your Google Admin console.
- Navigate to Menu > Security > Access and data control.
- To implement the setting for all users, keep the top organizational unit selected.
- Choose the setting for less secure applications to generate the security keys.
- Click Save.



Step 2: Email Thread and Decision-Making –

Prior to activating the email thread, it is essential to configure the security key and specify the email address for which the model will be activated. Once the email thread is initiated, it will automatically access the email to extract pertinent information such as the sender, subject, and date. By utilizing IMAP and SMTP protocols, we can establish a connection to the user's email account to facilitate the sending and receiving of messages. The Python email API will be employed for this purpose. After gathering the information from all incoming emails during that session, the data will be organized into a structured string format, complete with a serial number as part of the message string.

Step 3: Sending Messages via WhatsApp:

This phase employs the Pywhatkit library, a Python library renowned for its user-friendly features. It requires no additional setup, making it one of the most widely used libraries for automating tasks on WhatsApp and YouTube. The library is regularly updated with new functionalities and bug fixes. The

constructed message string will be forwarded to the Pywhatkit function, along with the recipient's mobile number, to ensure the message is delivered to the end user, who is also the owner of the email address

LITERATURE REVIEWS :

A few ponders have investigated the integration of moment informing stages with conventional e-mail caution frameworks to upgrade communication effectiveness. Inquire about demonstrates that whereas emails are broadly utilized for notices, they regularly endure from deferred reaction times, spam sifting issues, and client absentmindedness (Gupta & Sharma, 2019). To address these impediments, ponders have inspected the utilize of WhatsApp-based cautions, which offer higher engagement rates and real-time conveyance (Patel & Kumar, 2021). In any case, challenges such as API limitations, information security concerns, and security dangers stay noteworthy boundaries to appropriation (Chen & Zhou, 2020). Later progressions in AI-driven sifting and encryption procedures point to progress the unwavering quality and security of these coordinates frameworks (Lee & Kim, 2023). Advance investigate is required to create more secure and adaptable WhatsApp-based mail alarm arrangements whereas keeping up client protection and compliance with informing stage controls.

4. CASE STUDY :

Speedier Communication & Reaction Time :
A corporate IT helpdesk coordinates WhatsApp alarms for basic emails with respect to server downtimes and security breaches.

Higher Engagement & Examined Rate:
A college sent exam plan and result notices through WhatsApp rather than mail. Understudies checked WhatsApp 3x more as often as possible than emails, driving to way better mindfulness and less missed exams.

Decreased E-mail Over-burden & Spam Sifting Issues:
A clinic utilized an email-to-WhatsApp alarm framework for basic lab test comes about to dodge delays caused by e-mail spam channels.
Critical cautions bypassed inbox clutter, guaranteeing patients and specialists gotten opportune upgrades.

Made strides Client Encounter & Fulfillment
An e-commerce commerce executed WhatsApp alarms for arrange affirmations and conveyance upgrades.
Clients gotten real-time overhauls, lessening bolster calls by 40% and moving forward believe within the benefit

REQUIREMENT ANALYSIS

Here requirement analysis are done based on following points
Base paper for Email Alerts On Whatsapp
System Design:

- The System of Email Alert On Whatsapp is designed by using the following hardware and software

Hardware Specification:

- CPU : Core i5
- RAM : 8 GB
- HDD : 500 GB

Software Specification:

- Coding Language : Python
- Development Kit : Python SDK
- Development IDE : Spyder
- Front End : Tkinter

5. CONCLUSION :

Email is the most efficient form of contact when discussing issues related to government business. Email usage is still growing, despite the abundance of other viable communication avenues. With the amount of emails sent and received in the world increasing every day, email management software is now a must-have. It is estimated that more than 55% of emails are spam. This suggests that, rather than adding anything worthwhile to the discussion, spams are a time and effort waster for email users. This study's main focus is on the different approaches of using machine learning to identify emails that have arrived but have not yet been read. Furthermore, this project offers a thorough method of leveraging the interactive thread system on the user's registered Whatspp number to convey the meta data of the arrived email in the inbox.

6. REFERENCES :

1. "EMAIL ALERTS ON WHATSApp" by V. Abinaya and Shobika J.
Published in the EPRA International Journal of Research and Development (IJRD), May 2023.
This paper explores the concept of integrating email notifications directly into WhatsApp to enhance convenience and efficiency. The authors discuss the benefits, implementation process, and potential improvements in productivity and communication through such integration.

2. "A WhatsApp-Based Email Notifier" by Robert Poenaru.
Published on ResearchGate, November 2024.
This study presents the development of a system that integrates email notifications into WhatsApp, aiming to provide users with real-time alerts and improve responsiveness to important emails.

3. "Development of Email Notification System Based on User Criteria" by K. Lappanitchayakul.
Published in the International Research Journal of Engineering and Technology (IRJET), July 2022.
This research focuses on creating an email and SMS-based notification system to detect abnormal network conditions, offering insights into integrating email alerts with messaging platforms like WhatsApp.

4. "EMAIL ALERTS ON WHATSApp" by N. Neelima.
Published in the International Research Journal of Modernization in Engineering, Technology and Science (IRJMETS), March 2023.
This paper discusses the development of an automation tool using Python and Twilio to read and write emails from WhatsApp, enhancing user flexibility and productivity.