
SMTP Playground: A secure privacy-preserving web and mobile application for automation of sending and scheduling bulk emails to multiple receivers.

Tom Jose Oorasala, Ritesh Kumar Shukla, Sunkari Serena, Jayavignesh Thyagarajan

School of Electronics Engineering, Vellore Institute of Technology, Chennai, TamilNadu.

Abstract.

This paper proposes a web and mobile application named "SMTP Playground" to automate the process of sending bulk emails after extracting details of the potential receiver email address from an input file in the format of excel or comma-separated value (CSV). Unlike other automation scripting, this work also can send scheduled emails and encrypted emails to ensure privacy apart from the basic services provided by other email service providers in the market. This proposed Simple Mail Transfer Protocol (SMTP) Playground application provides a user-friendly interface and achieves the objectives.

Keywords— SMTP, E-Mail, End-to-End Encryption, Automation, Bulk Mails, Schedule Mails.

1. INTRODUCTION

A Mailing server is computer software that allows users to send emails to the ones who have registered with the server. It allows them to send text and data such as pictures, videos, and MP3s. However, there are some restrictions on the size of the attachments, which can be adjusted according to the server. This paper aims to develop a mailing system that will replace traditional email clients (such as Gmail and Outlook) [4]. The app's development is being done using Python and JavaScript. The following are some of the features incorporated are:

1. Notification Alert
2. End to End Encryption
3. Excel Sheet Batch Processing
4. Schedule Emails

SMTP (SIMPLE MAIL TRANSFER PROTOCOL): This is an application that web servers use for sending, receiving, and relaying incoming mail between email senders [3]. As soon as you compose an email and hit send, this is one of the most important stops on its journey to the inbox, and it delivers its message securely to the recipient. It's not uncommon to see SMTP servers on the Internet, but their function is highly specialized in handling and delivering email outbound [4]. It's a protocol that's part of the application layer.

IMAP (INTERNET MESSAGE ACCESS PROTOCOL): This protocol operates at the application layer that allows email users to deliver and receive messages over a distant mail server. The contemporary model of IMAP is described through RFC 3501. IMAP listens on 143 whilst IMAP over SSL/TLS makes use of 993 by default [1]. An email patron makes use of one or extra of some of the email retrieval protocols to retrieve messages from an email server that shops the messages withinside the email box of the recipient. A person can send emails to and obtain emails from quite a few email servers. In assessment to a few customers and servers that favor using vendor-specific, proprietary protocols, almost all protocols consisting of POP3(Post Office Protocol 3) and IMAP2 are supported, permitting many specific email customers to get right of entry to those servers, and permitting those customers for use with many different servers as well. This feature of IMAP operation permits more than one customer to manipulate the equal mailbox [2].

FERNET ENCRYPTION: Fernet system uses industry best practices and adopts symmetric encryption/decryption. It also authenticates the message, allowing the recipient to determine whether or not the message has been tampered with since it was transmitted. Fernet is part of the cryptography library. To encrypt and decrypt data, a secret key is required, which must be shared by everyone who needs to transmit encrypted or receive decrypted data. Because anyone with the key can read and create encrypted messages, it must be kept secret from others. As a result, a secure way to distribute the key is a necessity. The same key could be used many times and instances [5-8].

2. RELATED WORK

There has been a study on the importance of encrypted mail. Since a lot of third-party applications can be logged in via a Google account, emails sent through Gmail are vulnerable. Hence, encryption is very necessary for the same. Around 360 billion emails are sent daily. There have been concerns about the security of the emails. Currently, the majority of email service providers prefer PGP3 and S/MIME2 standards for public encryption of keys. Both need a user's client to maintain his/her private key, and the public keys of the email senders and receivers [9]. Certain research papers have also highlighted the problems in encrypted mail. There have always been concerns about the circumstances if the keys reach the wrong hands. Some of the services like automatically adding meeting schedules through email won't be functional anymore as the system cannot read a receiver's emails. There will be difficulties for the system to categorize spam mails as everything is encrypted [10]. Few 3rd party applications are pre-existing in the market. Prevail mail, Proton mail are some of the examples. However, most of the existing services are paid or advertisement based which usually redirects the user to multiple fishy sites. Also, these 3rd party websites provide services either only in sending bulk emails or just sending encrypted mails.

3. FLOWCHART/ALGORITHM

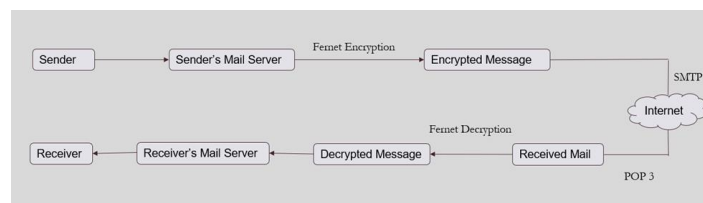


Fig.1 Dataflow of sending an e-mail

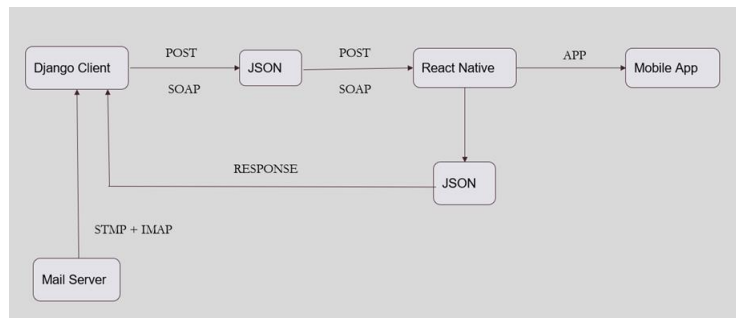


Fig.2 Dataflow between the mailing server, Django client, and the Mobile App

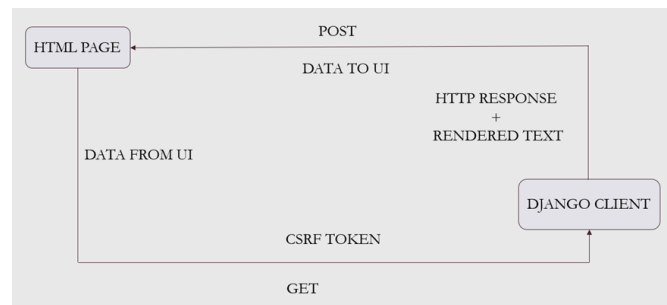


Fig.3 Dataflow between website and app.

Fig.2 and Fig3 shows, when a user composes a message or an email, it's normally done with the help of email clients.

4. SIMULATION/IMPLEMENTATION

Django is used to develop the website and the REST APIs. The biggest reason for using Django is the use of Python Language. Python language has lots of tools for SMTP and IMAP. It makes it easier for us to send emails and read emails. Also, python has some great tools for encryption and decryption which are highly secure. These modules are used in 2-factor authentications. There is a secret key that is stored in secret.key. The key is then loaded and used for encryption and decryption.

- 1) Pandas is used to run bulk mails.
- 2) SMTP server is set on.
- 3) Excel is then taken from the HTML input.
- 4) The email is parsed through the Pandas library.
- 5) An iterator runs through the email columns and sends emails to each address.

Scheduling emails is another interesting function incorporated inside the project. This feature enables users to schedule emails together and the e-mail with the given content will be sent at the given time. A server continuously monitors the time once the desired time is reached, the iterator stops monitoring and sends the mail [11]. React Native is used for the development of the Android Application. The REST API generated is used for communication between Django and React Native. The data is collected and sent through GET and POST requests of Rest API. React native is preferred over Flutter because it has a

4

scope to develop a desktop application in the future through electron module. The Contributed Code is available here: <https://github.com/riteshshukla04/SMTP-PlayGround> (Publicly Accessible).

5. RESULTS/INFERENCES

Fig. 5 is the web interface to send emails. The decrypted emails received by the user are shown in Fig. 6.

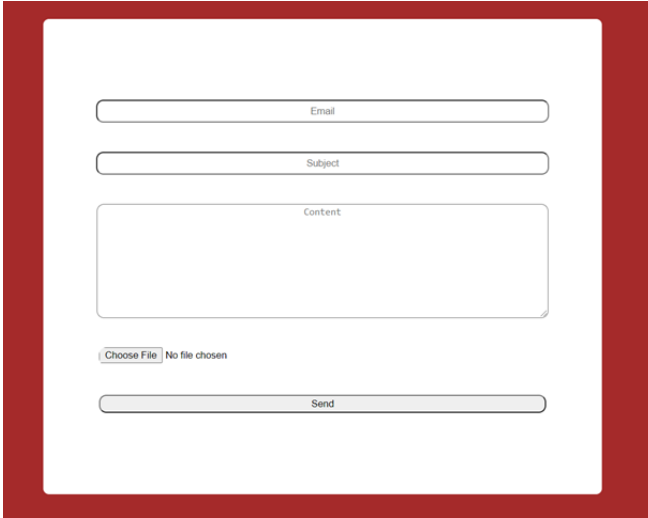
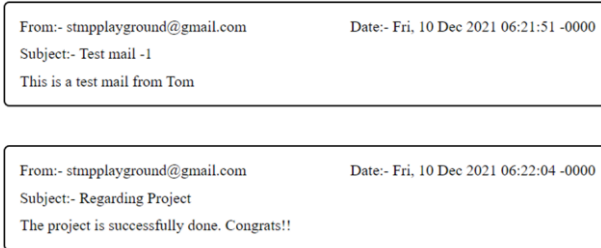


Fig.5 Web App Interface to send mails.



From:- stmpplayground@gmail.com Date:- Fri, 10 Dec 2021 06:21:51 -0000
Subject:- Test mail -1
This is a test mail from Tom

From:- stmpplayground@gmail.com Date:- Fri, 10 Dec 2021 06:22:04 -0000
Subject:- Regarding Project
The project is successfully done. Congrats!!

Fig.6 Mail sent and received on WebApp. The email is decrypted.



Regarding Project inbox

stmpplayground@gmail.com
to me

11:52 AM (7 minutes ago) ☆ ↶ ⋮

gAAAAABhsvIMS23yRbFPKH4YYYZmiCOSvS1mdYpSIIIG6HkV4SNqpeBA1qk7UyOabgZhmaETI-RAhcZ9fby_Woa9nA/GxJpSkZn-oPXwV0IIEK543bV4JU-O_NGM9u1



Fig.7 (1) shows how the email would look to a user when they use Gmail to read the encrypted mail. (2) Encrypted mail received in Gmail App.

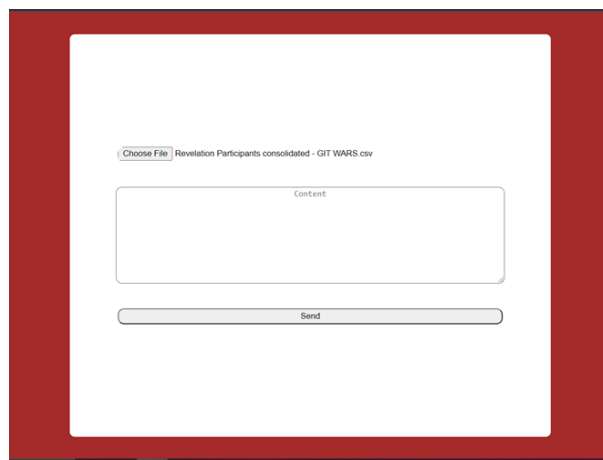


Fig.10 Interface for sending Bulk Mails

6. CONCLUSION

SMTP is the most convenient way for transmission to send messages via emails to recipients all over the globe. Sending emails in bulk is only possible through SMTP servers since it's a cost-effective way of sending emails to multiple receivers at the same time [11]. The SMTP connection is unrestricted and can be used to connect to any system. It is also beneficial to have a designated server to manage the outgoing emails in organizations. The amount of time and energy saved by using this system to send bulk emails is highly significant. For example, suppose a user has to send personalized emails to 500 users with the same content in the body, and assuming sending each email takes 10 seconds on average, it will take more than 1 hour to send them all. While using our system it just takes about 40 seconds, thereby saving the hassle of repeatedly composing new emails and the time spent in doing so.

7. FUTURE WORK

There is a large scope of UI improvements in the project. The UI can be more user-friendly and attractive. The UI should not only focus on looks but also the user experience. Future work involves hosting this website on premium hosting services like AWS or Digital Ocean. The second issue is that POP3 can't be used to read emails. This is due to the strict google security policy. Using POP3 to read mails would be faster, and also messages can be read

even if the user is offline. The end-to-end encryption security can be improved by increasing the length of the secret key. Randomizing and replacing keys regularly will reduce the chances of key misuse. To make the encryption more secure, more powerful, and robust, advanced encryption algorithms like AES 256 can be adopted.

8. REFERENCES

- [1] Javatpoint.com, “Internet Message Access Protocol”, 2021. [Online]. Available: <https://www.javatpoint.com/imap-protocol> [Accessed 23- Feb- 2022].
- [2] Rhoton J. Programmer's guide to internet mail: SMTP, POP, IMAP, and LDAP. *Digital Press*; 2000.
- [3] sendgrid.com, “What is an SMTP server” ,2019. [Online]. Available: <https://sendgrid.com/blog/what-is-an-smtp-server/> [Accessed 22- Feb- 2022]
- [4] Riabov VV. “SMTP (Simple Mail Transfer Protocol)”, River College. 2005.
- [5] Zadka M. “Cryptography”, InDevOps in Python Apress, Berkeley, CA. pp. 95-110, 2019
- [6] Schwenk J, Brinkmann M, Poddebniak D, Müller J, Somorovsky J, Schinzel S., “Mitigation of attacks on email end-to-end encryption”. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security pp. 1647-1664, 2020
- [7] Jain A, De P. Enhancing Database Security for Facial Recognition using Fernet Encryption Approach. In 2021 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA) 2021 Dec 2 (pp. 748-753). IEEE
- [8] Ferguson SJ, Hebels R. Computers for librarians: An introduction to the electronic library. Elsevier; 2003 Aug 1.
- [9] M. D. Ryan., “Enhanced certificate transparency and end-to-end encrypted mail”. In Network and Distributed System Security Symposium (NDSS), Feb. 2014.
- [10] Yu J, Cheval V, Ryan M. “Challenges with End-to-End Email Encryption.” In: Springer Reference (2014).
- [11] Sukhija V., “Sending Email”, InPowerShell Fast Track Apress, Berkeley, CA, 2022, pp. 65-69.