Smart India Hackathon 2017

Ministry Category : **Indian Space Research Organisation (ISRO)**

Problem Code : **#ISR1**

Problem Statement : **Storing emails on mailbox server in encrypted format accessible only to owner of the email**

Current AICTE Application No. : 1-3328528908

Team Leader Name : **Anup Kumar Panwar**

IDEA

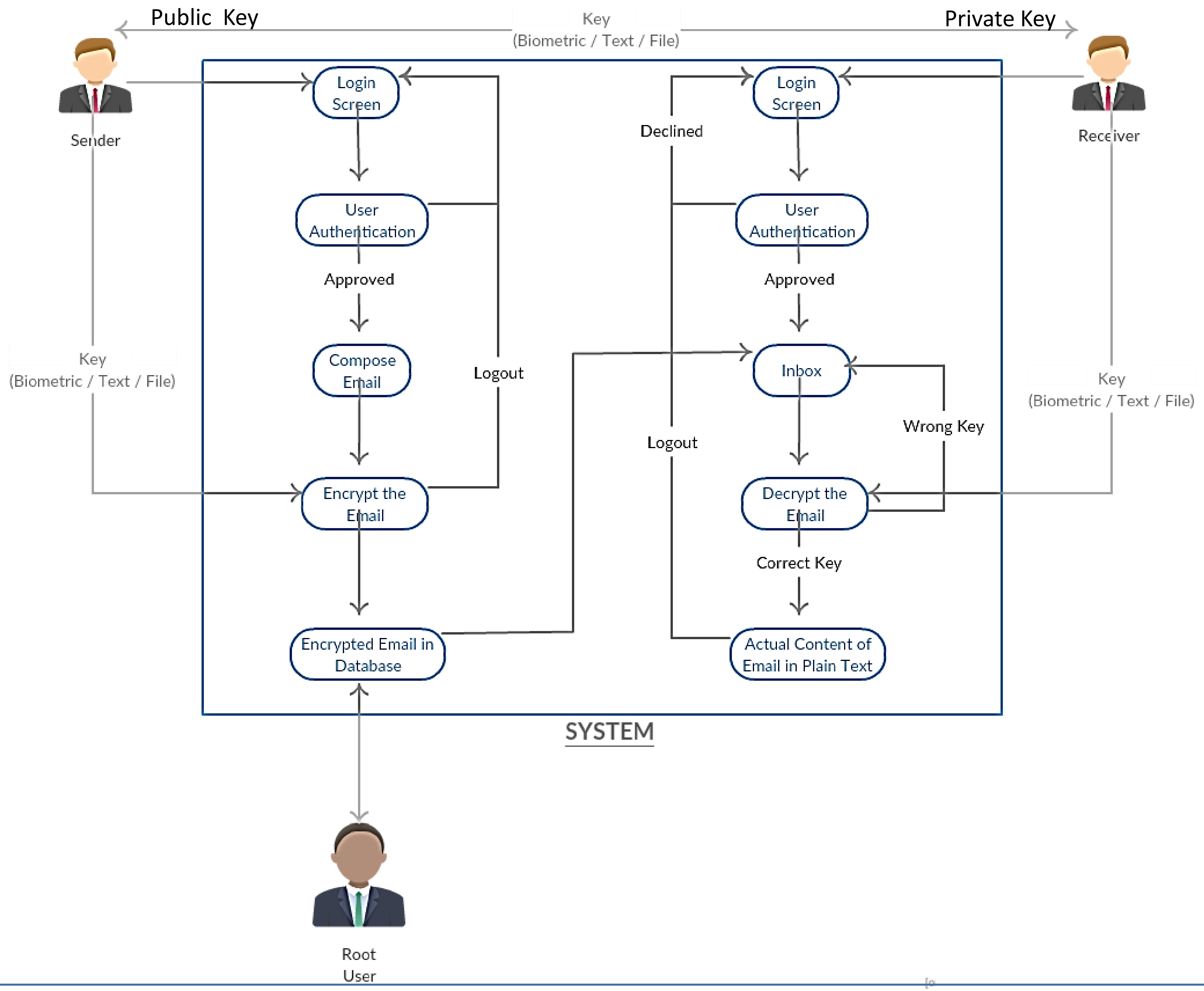
Our idea is to develop a SECURED & ENCRYPTED EMAIL SERVICE. Normally Email services provide STORAGE LEVEL ENCRYPTION which are decrypted on-the-fly and that too with a SINGLE KEY. So, we have tackled the drawbacks in this ON-THE-FLY DECRYPTION and SINGLE KEY approach:-

1. Our approach is based on Asymmetric Encryption; We will be utilizing biometrics (namely finger prints) of the sender and the receiver to encrypt the emails content.
2. The finger print will be used to generate a PRIVATE TOKEN and a PUBLIC HASH.
3. A RANDOM SALT will be generated under MD5 ENCRYPTION ALGORITHM and SERVER TIMESTAMP;
4. The PUBLIC KEY(I.E., FINGER PRINT HASH) + SALT will be used to generate an INITIALIZATION VECTOR (IV) that will again undergo MD5 ENCRYPTION;
5. Then this INITIALIZATION VECTOR will be used to encrypt the email content using AES 128 BIT ENCRYPTION TECHNIQUE;
6. This Encrypted content will be BASE64 ENCODED and stored in the database. (NOTE : The private key is NEVER STORED anywhere in any form. It will be provided by the receiver at the real time for content decryption.)
7. The recipient of the email will see the content of the email in encrypted form which no one can understand. To read the actual content he has to provide his FINGER PRINTS. This decryption is temporary and at the VIEW LEVEL ONLY . Once the user has read the actual content, as soon as he redirects from the web page. The temporary decryption will vanish and the email will remain in encrypted format. (NOTE : the email is never decrypted at STORAGE LEVEL.)
8. Moreover the sender of the email will get a notification if number of wrong password attempts exceeds a preset value(say 3).Then he gets an option to delete the email permanently from the server (Even from the receiver's inbox for the sake of security).
9. Not only biometrics but the user also gets an option to encrypt the email with a string or use a file as a key using SYMMETRIC ENCRYPTION in a similar way with an added benefit of using different keys for each email. Biometric encryption is our primary focus due to it higher security and convenience.

Technology Stack

Angular.js, jQuery, PHP, MySQL DB, Mcrypt, AJAX, OpenSSL, Asymmetric Encryption, MD5 Encryption Algorithm, AES 128 bit Encryption Algorithm, PHP Mailer, APACHE server, WAMP/LAMP, Ionic Framework, ng-Cordova, Android Studio + SDK version 23, Node.js, HTML, CSS, Material Design Light (MDL), JavaScript

USE CASE

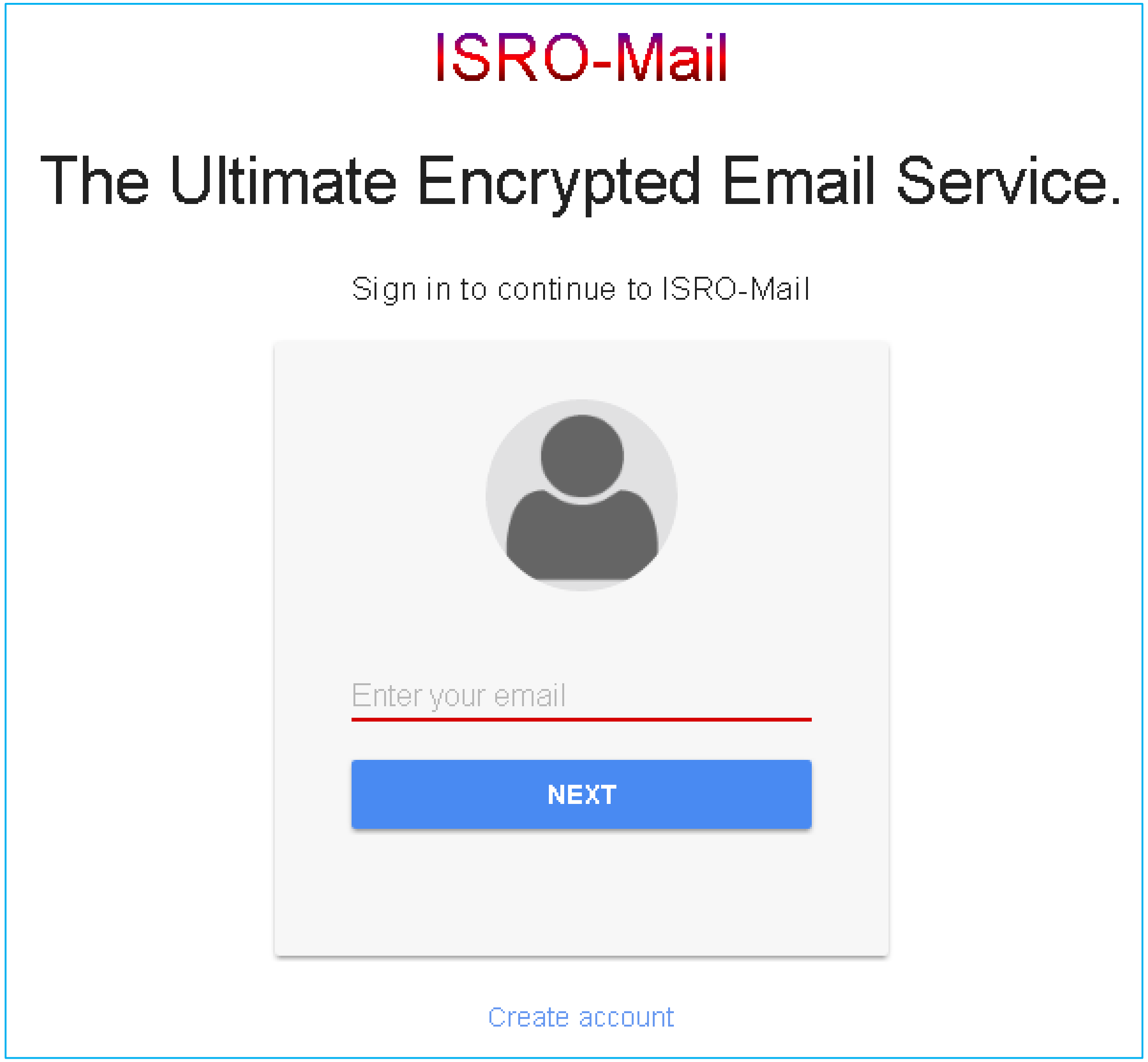


DEPENDENCIES

Android Device with Finger Print Scanner and Minimum SDK version 23, Internet Connection, A computer with Biometric Scanner

Some Work in Progress

LOGIN



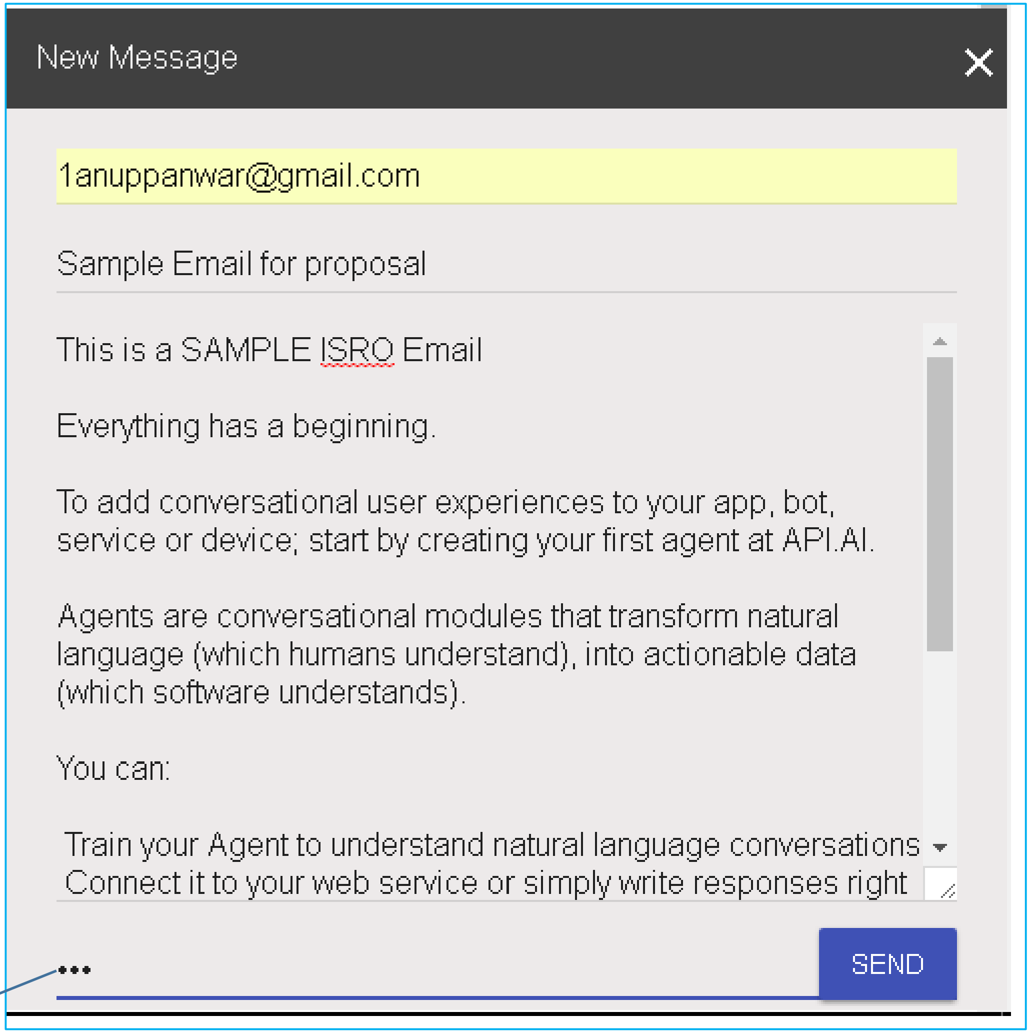
ISRO-Mail

The Ultimate Encrypted Email Service.

Sign in to continue to ISRO-Mail

Enter your email

COMPOSE EMAIL



New Message

1anuppanwar@gmail.com

Sample Email for proposal

This is a SAMPLE ISRO Email

Everything has a beginning.

To add conversational user experiences to your app, bot, service or device; start by creating your first agent at API.AI.

Agents are conversational modules that transform natural language (which humans understand), into actionable data (which software understands).

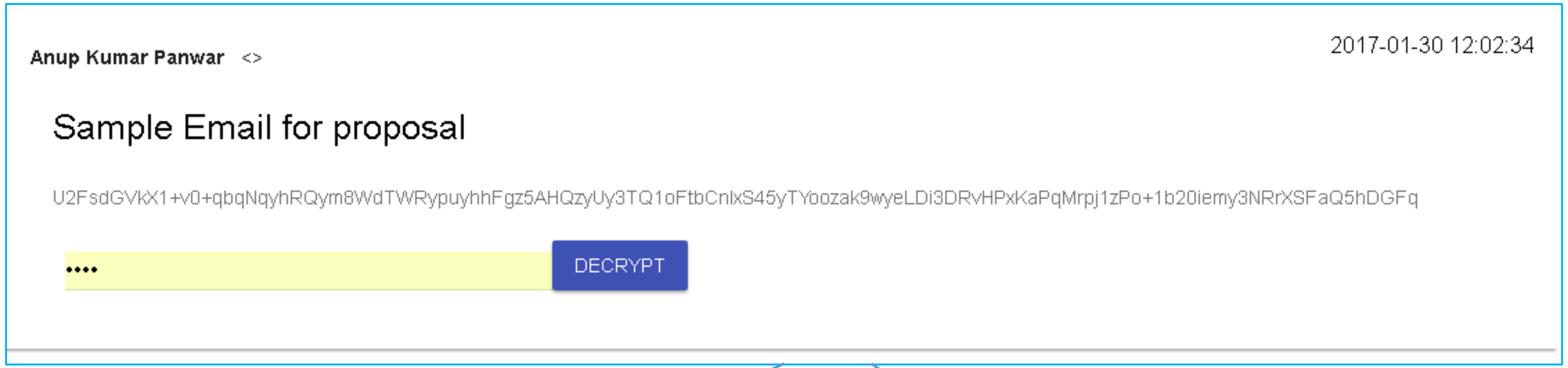
You can:

Train your Agent to understand natural language conversations
Connect it to your web service or simply write responses right

•••

STRING | FILE | FINGER PRINT

INBOX



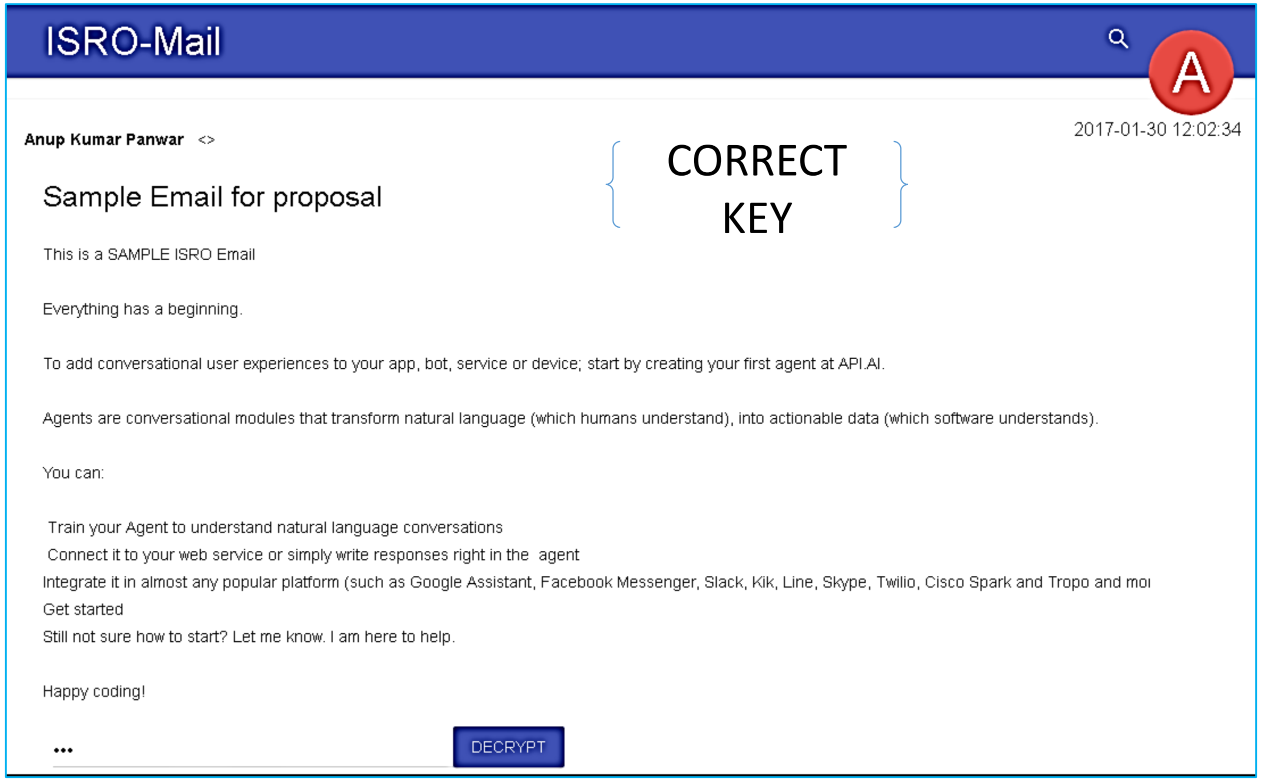
Anup Kumar Panwar <>

2017-01-30 12:02:34

Sample Email for proposal

U2FsdGVkX1+v0+qbqNqyhRQym8WdTWRypuyhhFgz5AHQzyUy3TQ1oFtbCnlxS45yTYoozak9wyeLDi3DRvHPxKaPqMrpj1zPo+1b20iemy3NRrXSFaQ5hDGFq

••••



CORRECT KEY

Anup Kumar Panwar <>

2017-01-30 12:02:34

Sample Email for proposal

This is a SAMPLE ISRO Email

Everything has a beginning.

To add conversational user experiences to your app, bot, service or device; start by creating your first agent at API.AI.

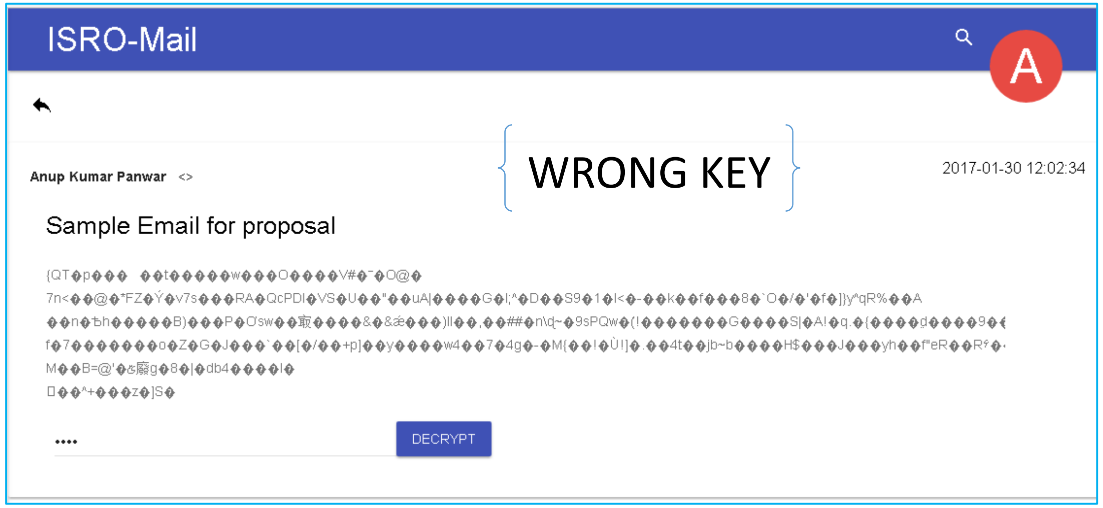
Agents are conversational modules that transform natural language (which humans understand), into actionable data (which software understands).

You can:

Train your Agent to understand natural language conversations
Connect it to your web service or simply write responses right in the agent
Integrate it in almost any popular platform (such as Google Assistant, Facebook Messenger, Slack, Kik, Line, Skype, Twilio, Cisco Spark and Tropo and moı
Get started
Still not sure how to start? Let me know. I am here to help.

Happy coding!

•••



WRONG KEY

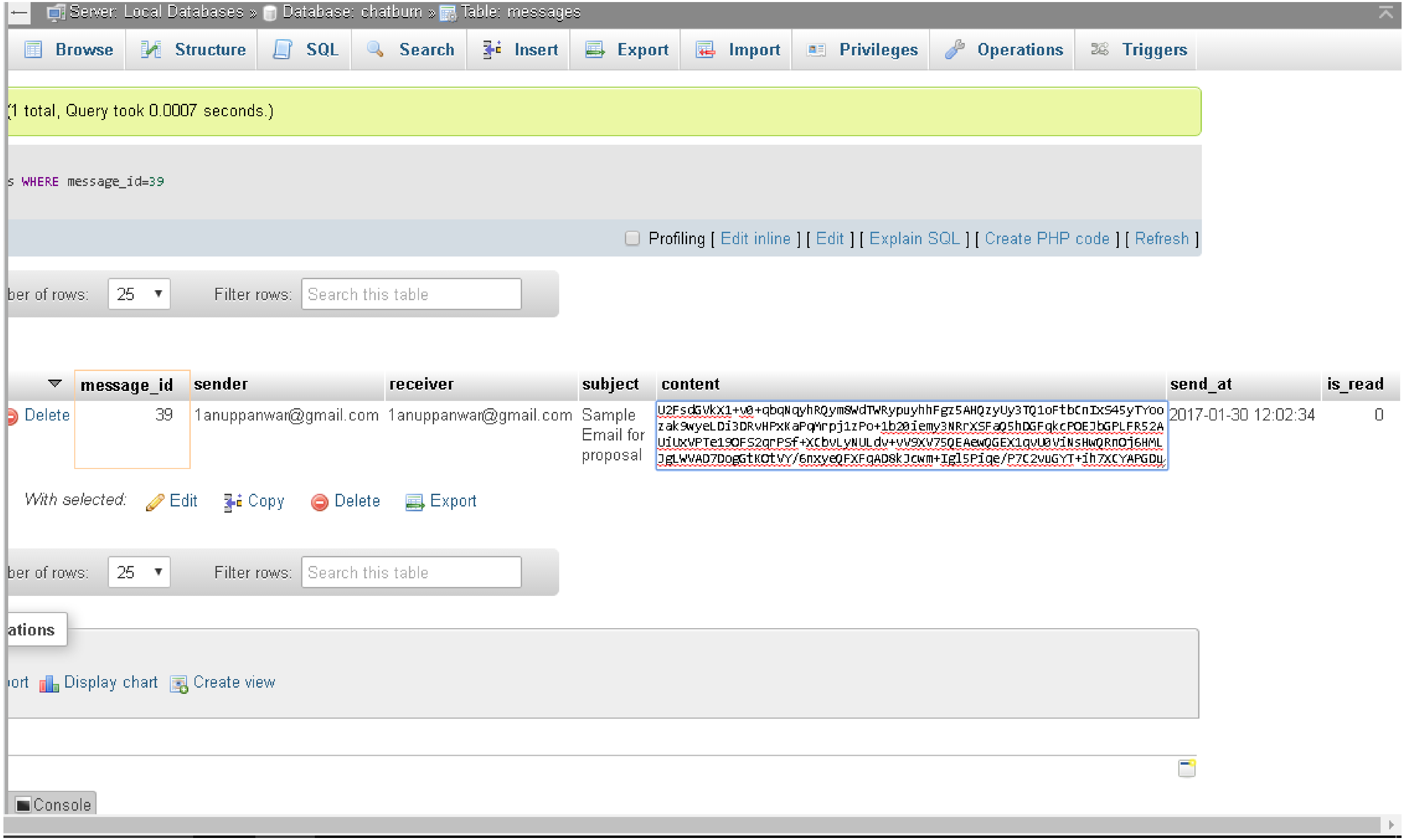
Anup Kumar Panwar <>

2017-01-30 12:02:34

Sample Email for proposal

```
{QT�p���  ��t������w����O�����V#�¯�O@�
7n<��@�*FZ�Ý�v7s���RA�QcPDI�VS�U��"��uA|����G�l;^�D��S9�1�l<�-��k��f����8�`O�/�'�f�]}y^qR%��A
��n�ƀh�����B)���P�O'sw�������&�&æ���)ll��,��##�n\q~�9sPQw�(!�������G����S|�A!�q.�{����d�����9�
f�7��������o�Z�G�J���`��[�/��+p]��y����w4��7�4g�-�M{��!�Ù!]�.��4t��jb~b����H$���J���yh��f"eR��R�·
M��B=@'�ಕ廢g�8�|�db4����l�
□��^+���z�]S�
```

••••


Server: Local Databases » Database: chatbum » Table: messages
Browse
Structure
SQL
Search
Insert
Export
Import
Privileges
Operations
Triggers

(1 total, Query took 0.0007 seconds.)

```
s WHERE message_id=39
```

□ Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]
ber of rows: 25
Filter rows: Search this table

	message_id	sender	receiver	subject	content	send_at	is_read
Delete	39	1anuppanwar@gmail.com	1anuppanwar@gmail.com	Sample Email for proposal	U2FsdGVkX1+v0+qbqNqyhRQym8WdTWRypuyhhFgz5AHQzyUy3TQ1oFtbCnIxS45yTYoozak9wyeLDi3DRvHPxKaPqMrpj1zPo+1b20iemy3NRrXSFaQ5hDGFqkcPOEJbGPLFR52AUiUxVPTe19OFS2qrPSf+XCbvLyNULdv+VV9XV75QEAewQGEX1qvU0ViNsHwQRnOj6HMLJgLWVAD7DogGtKOtVY/6nxyeQFXFqAD8kJcwm+Igl5Piqe/P7C2vuGYT+ih7XCYAPGDu	2017-01-30 12:02:34	0

With selected: Edit Copy Delete Export
ber of rows: 25
Filter rows: Search this table
ations
ort Display chart Create view
Console

{ HOW IS APPEARS TO THE ROOT USER }

More coming soon…