

Communicate Securely by using Python with TKinter

Rakesh.D¹ Dinesh Kumar.G² Janaharajan .N .D³ Vigneshwaran.A⁴ Ritheesh Kumar.V⁵

^{1,2,3,4,5}UG Scholar

^{1,2,3,4,5}Department of Information Technology

^{1,2,3,4,5}S. A. Engineering College, Chennai, Tamil Nadu, India

Abstract— Secure your information by encoding the messages. Message encoding and decoding is the process to first convert the original text to the random and meaningless text called cipher text. This process is called encoding. Decoding is the process to convert that cipher text to the original text. This process is also called the Encryption-Decryption process.

Keywords: Surveillance cameras, Computer Vision, monitoring, Human Prediction.

I. INTRODUCTION

Web application(or web app) is a application software that runs on a web server. Web applications are accessed by the user through a web browser with an active network connection. These applications are programmed using a client-server modeled structure-the user (“client”) is provided services through an off-site server that is hosted by a third party. Here we are going to build an chat application to communicate securely by using Python with tKinter.

II. MOTIVATION & SCOPE OF THE PROJECT

To communicate securely over internet. It is necessary to protect our data from third person while communication. Secure applications for:

- Army secrets
- Business Communication

III. EXISTING SYSTEM

A. Advantages

- We are able to protect our data by using the technique encoding and decoding.
- It is cost free.
- It is easy to handle.

B. Disadvantages

- However it is secure, Present day transactions are considered to be “un-trusted” in terms of security, i.e. they are relatively easy to be hacked.
- We have to consider the transfer the large amount of data through the network will give errors while transferring.
- Nevertheless, sensitive data transfer is to be carried out even if there is lack of an alternative.

IV. PROPOSED SYSTEM

The proposed system should have the following features. The transactions should take place in a secured format between various clients in the network. It provides flexibility to the user to transfer the data through the network very easily by compressing the large amount of file.

It should also identify the user and provide the communication according to the prescribed level of security

with transfer of the file requested and run the required process at the server if necessary.

A. Overcoming the drawbacks of Existing System

Network security in the existing system is the motivation factor for a new system with higher-level security standards for the information exchange.

In this system the data will be send through the network as a encrypted file.

The user who received the file will do the operations like decryption and decompress in their level of hierarchy etc.

The decryption will be possible when the sender sends the authentication code along with the file only visible to the appropriate receiver.

V. SYSTEM ARCHITECTURE

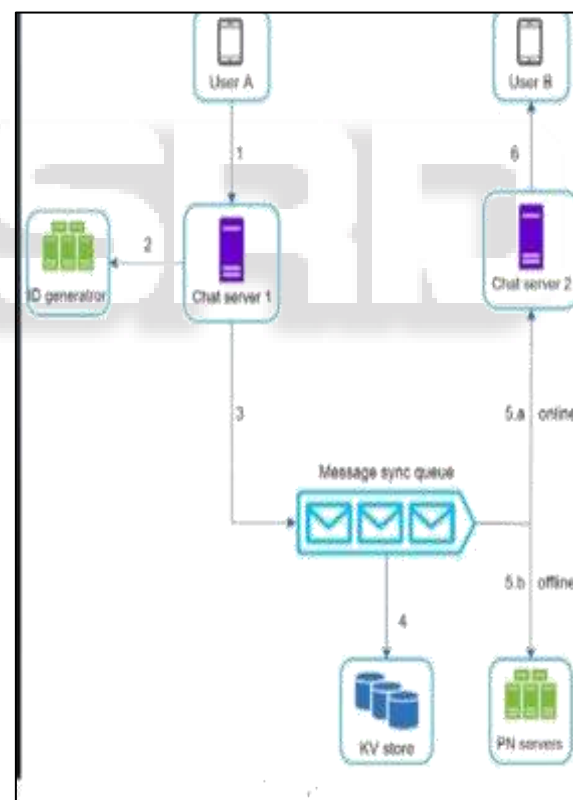


Fig. 1: System Architecture

VI. MODULES OF THE SYSTEM

- (1) Stenography
- (2) Base 64
- (3) Data compression

1) Stenography

Steganography is the method of hiding secret data in any image/audio/video. In a nutshell, the main motive of steganography is to hide the intended information within

any image/audio/video that doesn't appear to be secret just by looking at it.

2) Base 64

The base64 module is used to encode and decode data. First, the strings are converted into byte-like objects and then encoded using the base64 module. The below example shows the implementation of encoding strings isn't base64 characters.

3) Data Compression

The data can be archived, compressed using the modules like zlib, gzip, bz2,lzma,zipfile and tarfile. To use the respective module, you need to import the module first.

VII. CONCLUSION

We have learned a lot from this project on how to develop Web Application and publishing it in real time, using Web Services. As mentioned this application will be more secure than other existing applications.

REFERENCES

- [1] Molly McKinney (19 November 1998). ""Sell a Couch or Make a New Friend: Broadcast Provides Potential Mind Games and Hookups." The Wooster Voice, November 19, 1998, p.8". Retrieved 2 July 2019.
- [2] "The 'Security Digest' Archives (TM): TCP-IP Distribution List for February 1989". securitydigest.org. Archived from the original on 8 December 2017. Retrieved 6 May 2018.
- [3] "CompuServe Innovator Resigns After 25 Years", The Columbus Dispatch, 11 May 1996, p. 2F.
- [4] Mike Pramik, "Wired and Inspired", The Columbus Dispatch, (Business page), 12 November 2000.
- [5] "IRC Chatiquette – Chat Etiquette". Livinginternet.com. 28 November 1995. Retrieved 19 January 2012.