# Fog Based Three-Layer Architecture for Privacy Preserving

**Ashwini Jilla, K. C. Sreedhar**

***Abstract*****:** ***Fog computing is one of the most latest technology used by the cloud providers to safe guard the user data and service provider's data servers. Fog computing acts as mediator between hardware and remote servers or cloud servers. Cloud computing still has the lot of vulnerabilities. Privacy to the users data is main issue in the present cloud computing. Whenever users uploads data into cloud server then user will lose their right on their own data because users don't know about, what cloud providers do with users data, they can sell the users data for their own profit without knowing to users. Fog computing provides lot of services like operation of computer, storage and networking services between users and cloud computing data centers. With the networking services users can lose their data privacy or leakage without knowing to user. Because public clouds are not secure enough and users doesn't know where data is storing in cloud servers. Breaking the data into small parts can lead to loss of data and which it can create way to attackers to steal data. Even data might be changed instated of one data with another. Intelligence can be applied in the fog computing technology to use of computing resources and security reasons. Applying multiple layers of security features by using kubernets can improve better service to user and user's data can be safe from the attackers. Whenever user lost connection with the server kubernets establishes reconnection between user and server. RSA256 encryption is applied to users data with this we can provide better security between cloud server and users***.

***Keywords:*** ***Cloud Computing, RSA, Kubernet, Fog Computing***

## I. INTRODUCTION

Fog computing is a term made by Cisco that alludes to stretching out distributed computing to the edge of an endeavor&#39;s system. Otherwise called Edge Computing or misting, mist processing encourages the activity of register, stockpiling and systems administration benefits between end gadgets and distributed computing server farms. Mist registering works by sending mist hubs all through your system. Gadgets from controllers, switches, switches, and camcorders can go about as haze hubs. At the point when an IoT gadget creates information this would then be able to be broke down by means of one of these hubs without being sent right back to the cloud. Haze is a sort of cloud that contacts the ground. Mist structures when the air close to the ground cools enough to transform its water fume into fluid water or ice. There are a wide range of sorts of mist, as well. Ice mist structures when the air close to the ground is sufficiently cold to transform the water in mist into ice gems. Cloud computing collects and stores large amount data in it. Which can make difficulties to manage data sufficiently without making any kind of errors in it. This results without nature of the got content. The effects of fog handling on circulated figuring and huge data structures may move. Regardless, an average viewpoint is a limitation in definite substance assignment, an issue that has been taken care of with the development of estimations that attempt to improve accuracy. haze arranging contains a control plane and a data plane. For example, on the data plane, fog enrolling enables handling organizations to live at the edge of the framework rather than servers in a server ranch. Diverged from disseminated processing, fog enrolling stresses closeness to end-customers and client focuses (for instance operational costs, security draws near, resource misuse), thick geological movement and setting care (for what concerns computational and IoT resources), dormancy diminishing and spine information move limit venture achieve better Quality of Service and live stream mining, realizing unmatched users can feel better and secure while it is in like manner fit to be used in Assisted Living circumstances. Kubernetes characterizes a lot of building squares (&quot;natives&quot;), which all in all give components that convey, keep up, and scale applications dependent on CPU, memory or custom measurements. Kubernetes is inexactly coupled and extensible to meet various remaining tasks at hand. This extensibility is given in enormous part by the Kubernetes API, which is utilized by inside segments just as expansions and holders that sudden spike in demand for Kubernetes. The stage applies its authority over figure and capacity assets by characterizing assets as Objects, which would then be able to be overseen thusly. A Kubernetes administration is a lot of cases that cooperate, for example, one level of a multi-level application. The arrangement of cases that comprise a help are characterized by a name selector. Kubernetes gives two methods of administration revelation, utilizing natural factors or utilizing Kubernetes DNS. Administration disclosure appoints a steady IP address and DNS name to the administration, and burden adjusts traffic in a cooperative way to arrange associations of that IP address among the units coordinating the selector (even as disappointments cause the cases to move from machine to machine). Generally Kubernetes was appropriate just for stateless administrations. Be that as it may, numerous applications have a database, which requires diligence, which prompts the production of persevering stockpiling for Kubernetes. Actualizing steady stockpiling for compartments is one of the top difficulties of Kubernetes chairmen, DevOps and cloud engineers.

**Revised Manuscript Received on June 15, 2020.**
***** Correspondence Author

**Ashwini Jilla**, Department of Computer Science and Engineering, Sreenidhi Institute of Science and Technology, Yamnampet, Ghatkesar, Hyderabad, India. E-mail:ashwinijilla5@gmail.com

**Mr.K.C.Sreedhar** , Asst Professor Department of Computer Science and Engineering, Sreenidhi Institute of Science and technology, Yamnampet, Ghatkersar, Hyderabad, India. E-mail: simplykakarla@gmail.com

Holders might be transient, however increasingly more of their information isn&#39;t, so one needs to guarantee the information&#39;s endurance if there should be an occurrence of compartment end or equipment disappointment. Kubernetes can uncover a holder utilizing the DNS name or utilizing their own IP address. On the off chance that traffic to a holder is high, Kubernetes can stack adjust and disperse the system traffic with the goal that the organization is steady. Kubernetes allows you to store and oversee touchy data, for example, passwords, OAuth tokens, and SSH keys. You can convey and refresh insider facts and application setup without modifying your holder pictures, and without uncovering privileged insights in your stack arrangement.

## II. EXISTING PROCEDURE

In the existing system Hash Solomon Code splits the documents into three parts small parts stores in user system, fog server and remaining part will store in server. But they used only 64bit encryption. This encryption is vulnerable for attackers. Attackers can easily break this encryption in very small amount of time. Users are storing their data files in public clouds, these public clouds can’t provide that much security to users data files.

### A. An Efficient Public Auditing Protocol with Novel Dynamic Structure for Cloud Data

Henceforth, numerous analysts have dedicated themselves to the structure of examining conventions coordinated at re-appropriated information. In this paper, we propose an efficient open evaluating convention with worldwide and inspecting square less verification just as clump examining, where information elements are significantly most efficiently upheld than is the situation with the best in class. Indicative system assaults, which are outside and natural to Internet clients, compromise cloud information. Programmers may recover and take cloud clients&#39; information or even degenerate and erase the information, decimating its confidentiality, honesty, and accessibility. The gadgets used to speak with the TPA can be telephones, PCs, tablets, and so forth. The final component is the TPA, which is a dependable outsider between the CSP and the DO. The doubly connected data table (DLIT) is a two-dimensional information structure utilized by the TPA to store information data concerning reviewing, contrasting from the one-dimensional Index Hash Table (IHT). The proposed evaluating convention can be separated into two stages: the arrangement stage and the check stage. The previous stage is answerable for some readiness works and contains three calculations: KeyGen, Filepro2C, and Filepro2T. The last contains three calculations also: ChalGen, ProofGen, and Verify Proof. Sufficient hypothetical verification shows the security of our convention. Broad numerical investigation and trial correlation results could be utilized to approve the exhibition of our convention, making it significantly all the more persuading.

### B. A Privacy-Preserving and Copy-Deterrence Content-Based Image Retrieval Scheme

Cloud servers contains large amount of data with huge number of users information. The attacker always tries to break security levels to steal information from the cloud server. If any vulnerable found in the servers the attackers turn that server into attacker’s server to use as their own server. The current accessible encryption plots for the most part consider that the inquiry clients are completely dependable. This isn&#39;t really valid in true applications. The watermarked pictures are sent to the picture client. At the point when an illicit duplicate of the picture is discovered, the unlawful question client who caused the unlawful circulation to can be followed by the watermark extraction. However, this water mark model setting aside parcel of effort to locate the illicit works and devouring more assets and individual is have to discover the unlawful duplicates. The inquiry efficiency despite everything stays to be the primary issue. It requires high computational multifaceted nature and subsequently is relied upon to be finished by the cloud server. In general, the picture highlights are secure against Cipher text- just Attack model.

### C. Fog-Based Computing and Storage Offloading for Data Synchronization in IOT

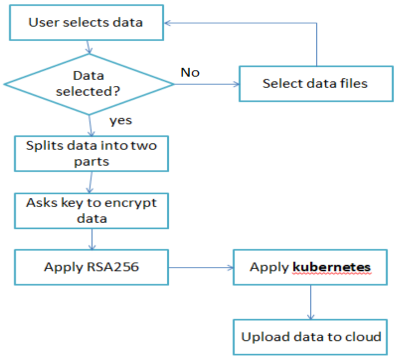
IoT devices send the sum of their data to the cloud, by then data security transforms into an unprecedented issue. By offloading some segment of preparing and limit work to the fog servers, the data security can be guaranteed. Also, to decrease the correspondence cost and reduce the inertness, we plan a differential synchronization count. For the gigantic accumulating breaking point and figuring limit of disseminated registering, it can offer IoT devices with offloading organizations. Their fundamental weight is that they for the most part move the entire record regardless, when a little change occurs. Unmistakably, this kind of synchronization realizes dreary correspondence and inertness when the customers as frequently as conceivable alter the data. This condition can be improved in our building in light of the fact that just one out of each odd time of change will be synchronized to the cloud. We conceivably move the last structure when the proportion of data set aside in the fog server shows up at the edge. By offloading some part of the figuring and limit work to the fog servers, the data security can be guaranteed. What&#39;s more, to reduce the correspondence cost and diminish torpidity, we arranged a differential synchronization estimation. There is a run of the mill wonder that the new record is regularly barely novel according to the past interpretation by one time of modification. To deal with this issue, past examinations focused on the most capable strategy to lessen the proportion of new data. Differential synchronization gives a feasible course of action, anyway it fabricates the exceptional job needing to be done on the customers&#39; contraptions and the cloud server.

## III. PROPOSED SYSTEM

Proposing a kubernets to fog computing which can handle all types of networks. In the proposed system user uploads data file to cloud but the application splits file into two parts and first part stores in computer and another part store in cloud. Later it applies RSA256 bit encryption on user data files. Here comes kubernets into action, once file starts uploading to server it finds ip address and host name of system.

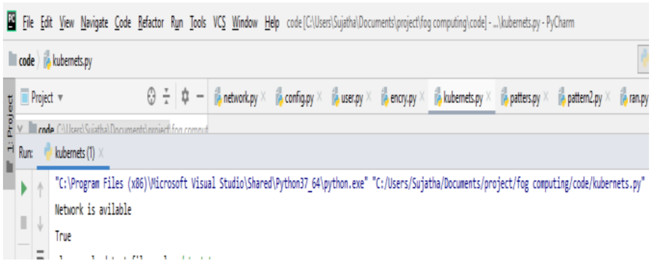
If connection got down then kubernets tries to reconnect automatically to user automatically. In this way user doesn't lose their data files or it doesn't allow any data leaks from the network. It handles complete network connections from user to server until session ends. Once file uploaded to server then it stores in it and encrypts complete file in RSA256 bit. Which gives more secure to user and users doesn't lose their files.

## IV. DESIGN AND MYTHOLOGY



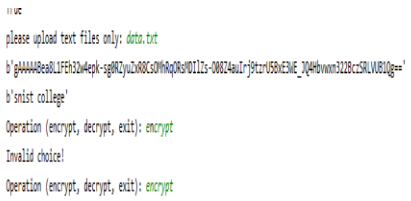
## V. RESULT

### Checks for internet:


File Edit View Navigate Code Refactor Run Tools VCS Window Help code [C:\Users\Sujatha\Documents\project\fog computing\code] - ...\kubernets.py - PyCharm
code
kubernets.py
Project
network.py
config.py
user.py
encry.py
kubernets.py
patters.py
pattern2.py
ran.py
1: Project
Run:
kubernets (1)

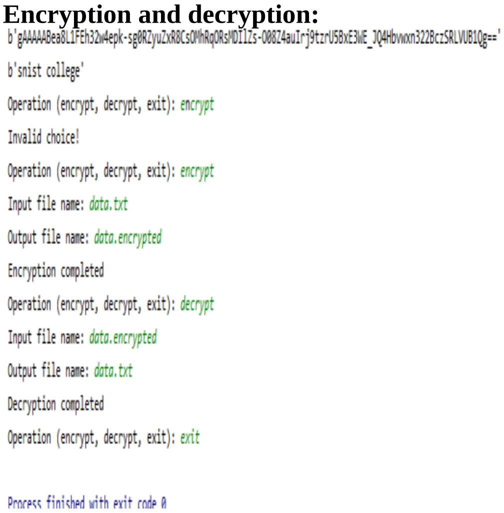
```
"C:\Program Files (x86)\Microsoft Visual Studio\Shared\Python37_64\python.exe" "C:/Users/Sujatha/Documents/project/fog computing/code/kubernets.py"
Network is avilable
True
```

### File uploading:



```
True
please upload text files only: data.txt
b'gAAAAABea8L1FEh32w4epk-sg0RZyuZxR8CsOMhRqORsMDIlZs-O08Z4auIrj9tzrU5BxE3WE_JQ4Hbvwxn322BczSRLVUB1Qg=='
b'snist college'
Operation (encrypt, decrypt, exit): encrypt
Invalid choice!
Operation (encrypt, decrypt, exit): encrypt
```

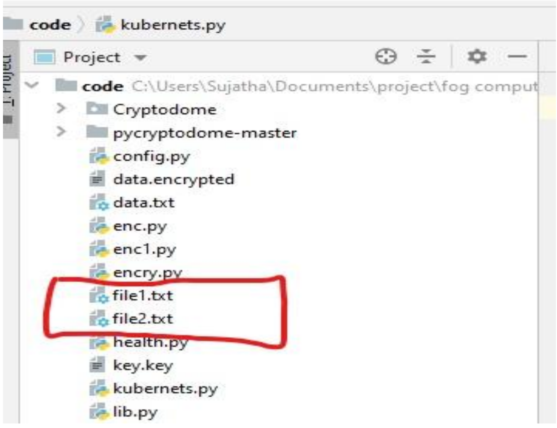
### Encryption and decryption:



```
b'gAAAAABea8L1FEh32w4epk-sg0RZyuZxR8CsOMhRqORsMDIlZs-O08Z4auIrj9tzrU5BxE3WE_JQ4Hbvwxn322BczSRLVUB1Qg=='
b'snist college'
Operation (encrypt, decrypt, exit): encrypt
Invalid choice!
Operation (encrypt, decrypt, exit): encrypt
Input file name: data.txt
Output file name: data.encrypted
Encryption completed
Operation (encrypt, decrypt, exit): decrypt
Input file name: data.encrypted
Output file name: data.txt
Decryption completed
Operation (encrypt, decrypt, exit): exit


Process finished with exit code 0
```

### Fog computing file splitting:



## VI. CONCLUSION

Kubernets provides better security to fog computing in every aspects. RSA256 bit encryption will give security to user's data file. With this encryption it will be very hard to break the encryption levels. Kubernets works with based on IP address, if it doesn't find any IP address then it will search for domain. It required constant internet, if user lost internet connection then it will try to reconnect to server. If server lost connection with client then kubernet will finds nearest hop to connect back to client.

## REFERENCES

1. Tian Wang, Jiyuan Zhou, Xinlei Chen , Guojun Wang , Anfeng Liu , and Yang Liu, "A Three-Layer Privacy Preserving Cloud Storage Scheme Based on Computational Intelligence in Fog Computing" , IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTATIONAL INTELLIGENCE, VOL. 2, NO. 1, FEBRUARY 2018
2. Zhihua Xia, Member, IEEE, Xinhui Wang, Liangao Zhang, Zhan Qin, Member, IEEE, Xingming Sun, Senior Member, IEEE, and Kui Ren, "A Privacy-preserving and Copy-deterrence Content-based Image Retrieval Scheme in Cloud Computing" , IEEE TRANSCATION ON INFORMATION FORENSIC AND SECURITY, VOL. , NO. , SEPTEMBER
3. Jian Shen, Jun Shen, Xiaofeng Chen, Senior Member, IEEE, Xinyi Huang, and Willy Susilo, "An Efficient Public Auditing Protocol With Novel Dynamic Structure for Cloud Data" , IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 12, NO. 10, OCTOBER 2017.
4. Tian Wang, Jiyuan Zhou, Anfeng Liu, Md Zakirul Alam Bhuiyan, Guojun Wang, Weijia Jia, Senior Member, "Fog-based Computing and Storage Offloading for Data Synchronization in IoT" IEEE Internet of Things Journal VOL. 14, NO. 8, AUGUST 2015.
5. Quang duy la, mao V.ngo, Tony Q.S. quek, "enabling intelligence in fog computing to achieve energy and latency reduction", Digital communication and netwokds 5.
6. Thanh Dat Dang, Doan Hoang," A data protection model for fog computing", 2017 Second International Conference on Fog and Mobile Edge Computing (FMEC).
7. Vladimir Marbukh," Towards Fog Network Utility Maximization (FoNUM) for Managing Fog Computing Resources", 2019 IEEE international conference on fog computing (ICFC).
8. Sejin chun, sangjin, seungmin seo, sungkwang eom, kooik jung and kyong-ho lee," A Pub/SubBased fog computing architecture for internet of vehicles", 2016 IEEE 8th international conference on cloud computing technology and science.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

## AUTHORS PROFILE:

**Ashwini Jills** pursuing Master’s Degree in computer Science & Engineering from Sreenidhi Institute of Science and Technology, Hyderabad. She has completed her B. Tech Degree from KMIT Hyderabad. She also published few papers in reputed journals **.**

**Mr.K.C.Sreedhar** is currently working as Asst Professor in Sreenidhi Institute of Science and Technology, Hyderabad. He is currently pursuing his PhD from VIT University, Vellore. His research interests include Data Mining, Cloud Computing, and Web Mining.

*Retrieval Number: E1010069520/2020©BEIESP*
*DOI: 10.35940/ijeat.E1010.069520*

*Published By:*
*Blue Eyes Intelligence Engineering*
*& Sciences Publication*