Cross-VM Network Channel Attacks and Countermeasures within Cloud Computing Environments

Cloud servers provides heavy computation resources and storage at cheaper cost so all users migrating their social and business data to 3rd party cloud servers. Data stored at cloud servers will be away from user control and can be misuse by cloud servers in various ways such as data tamper by internal employees or attackers who can hack VM (virtual machine) to divert traffic to different IP or send huge request to other VM to crash VM resources. In all this attack scenarios user data will be at risk.

In propose paper author performing cross-VM attack and then providing solution to those attack. All cloud servers will utilize virtual machines to handle request from millions of users as this VM are software defined resources which will be created and destroyed based on number of user’s request. If more request arrived then more VM will be created and upon completing task VM will be destroyed to free resources.

Sometime attacker can attack one VM and this VM can divert traffic to other VM IP and can send huge request to crash that VM. In propose work author introducing Monitor Node which will monitor all VM’s and if any VM sending huge packet or diverting request to other VM then that monitor will detect and drop such attack request to save user data.

Following are the resources used by author to monitor VM

VM-Monitor/Controller: Responsible for executing the services of management software that are needed for functioning of cloud platform.

Compute: Compute nodes execute virtual machine instances in cloud. KVM is used as a hypervisor in this node. This node is also responsible for providing firewall services. One can deploy more than one compute node in a setup.

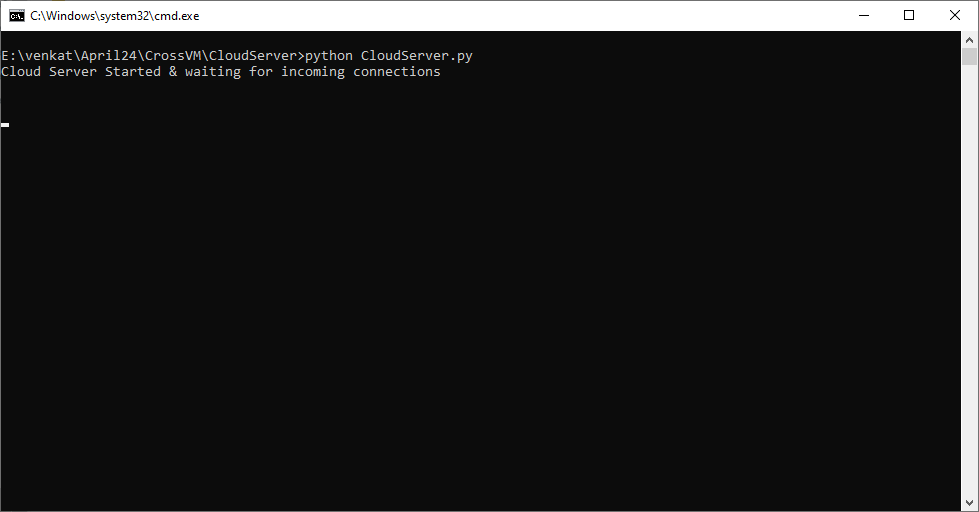
Network: The responsibilities of network nodes ensure the creation of virtual networks needed by the customers to create public or private networks. It connects their virtual machines with the external networks, i.e. the Internet.

To implement this project, we have designed following modules

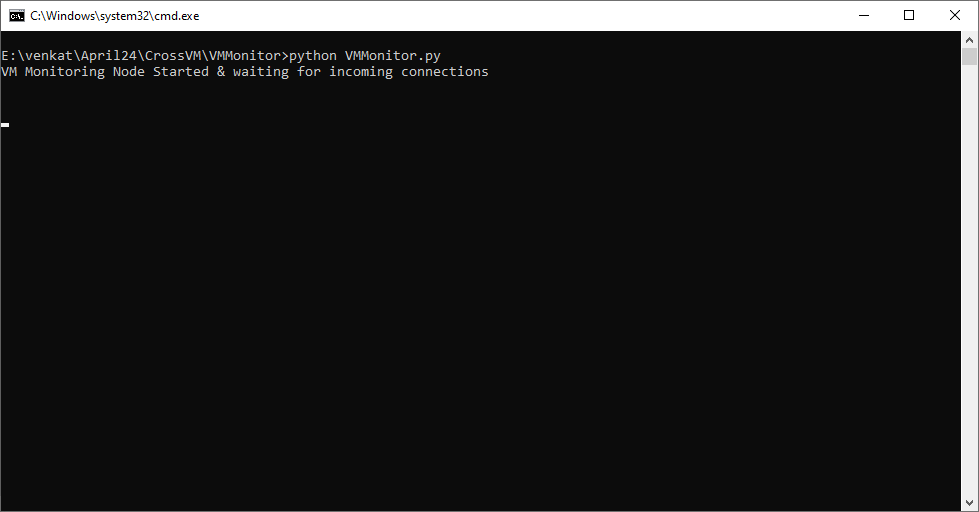
1. Cloud Server: use to receive and store data from servers and for each request cloud will create and destroy VM as THREADS.
2. VM-Monitor Node: this is a controller node which will monitor each VM behaviour and if request diverting or sending huge packet data then VM will be detected as attack. Here there is no external attacker so we will upload huge file size which will be detected by monitor
3. User/simulation node: here user will upload or download files from cloud.

SCREEN SHOTS

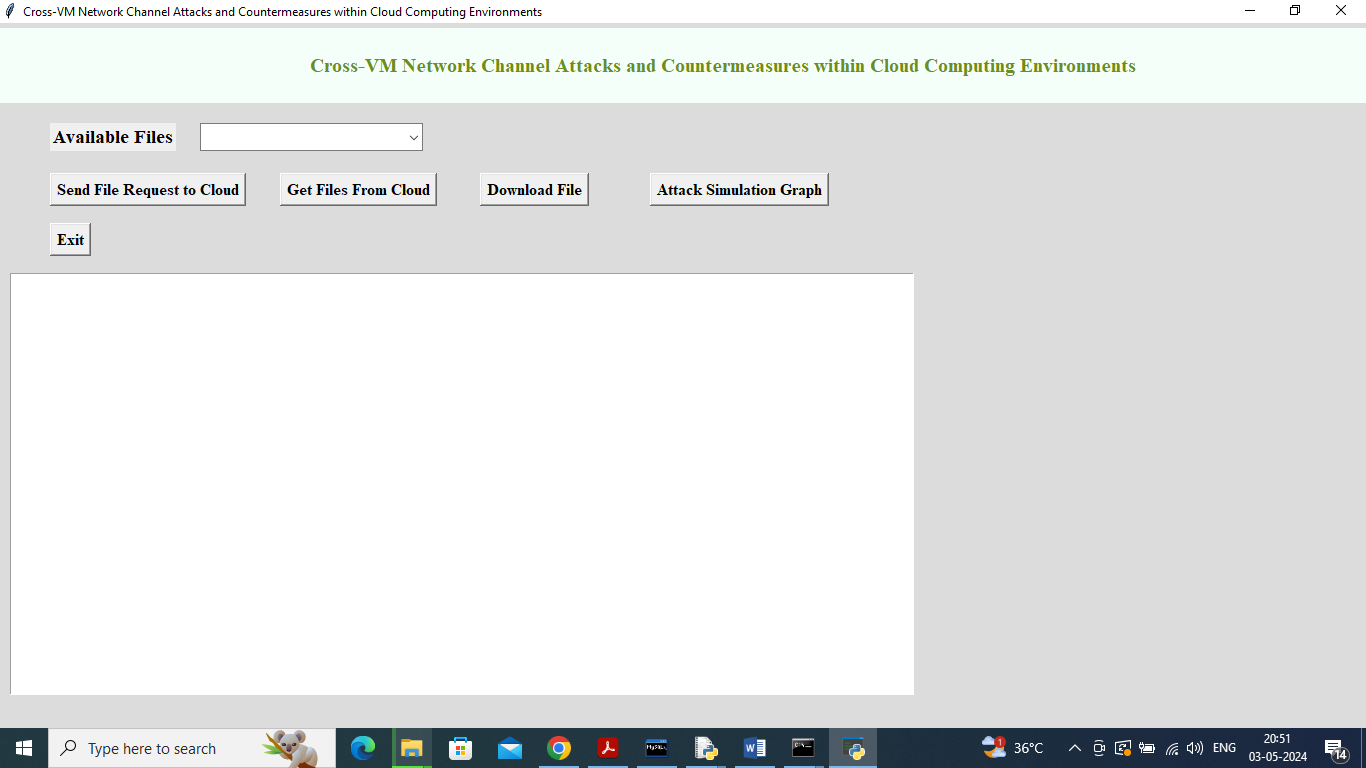
To run project first double, click on ‘runServer.bat’ file from ‘Cloud Server’ folder to get below screen



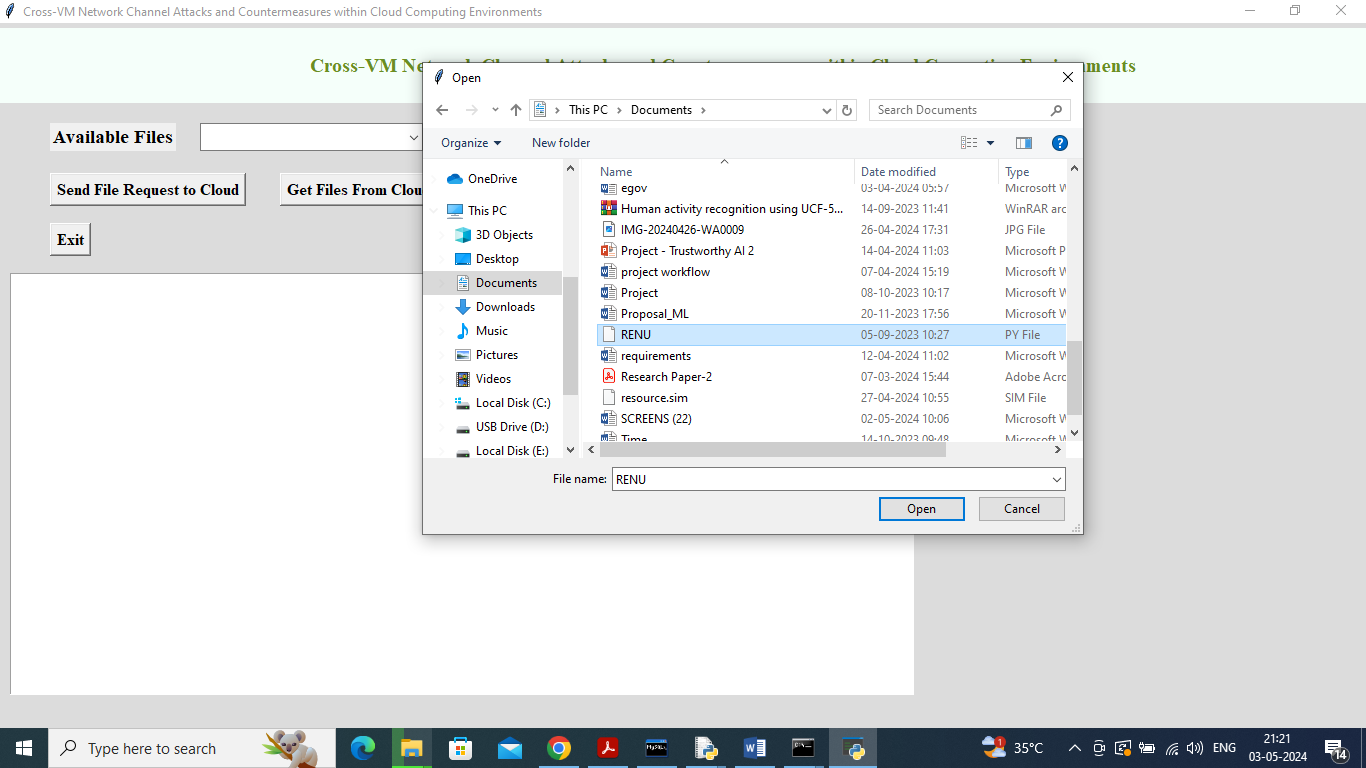
In above screen Cloud Server started and let it running and now double click on ‘runMonitor.bat’ file from ‘VM Monitor’ folder to start monitor and get below screen



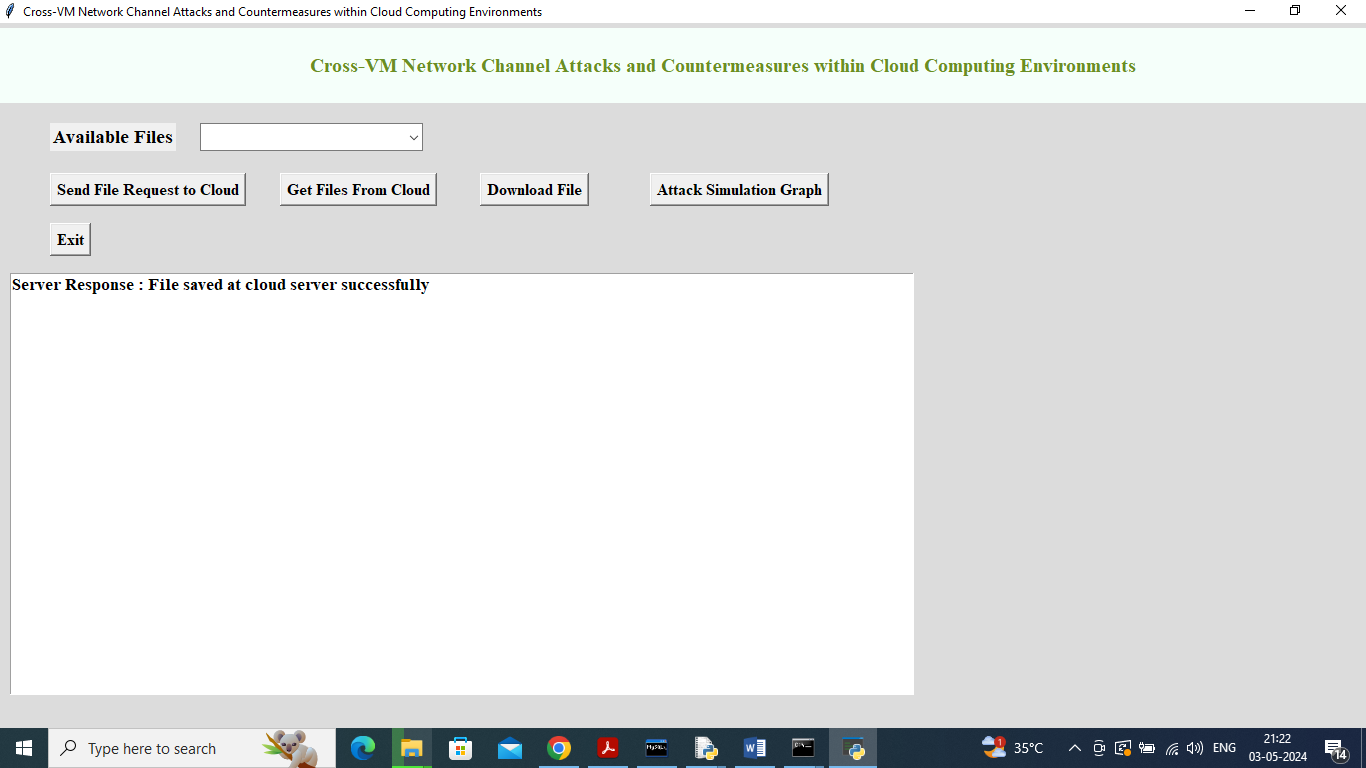
In above screen Monitor started and let it running and now double click on ‘run.bat’ file from ‘Simulation Node’ folder to start simulation and get below screen



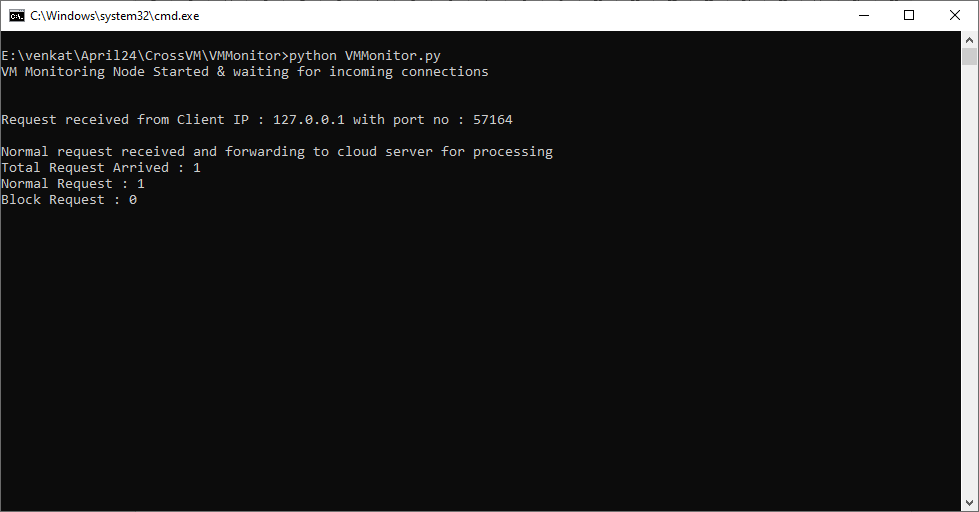
In above screen cloud user as simulation screen started and now click on ‘Send Request to Cloud’ button to send file to cloud and get below page



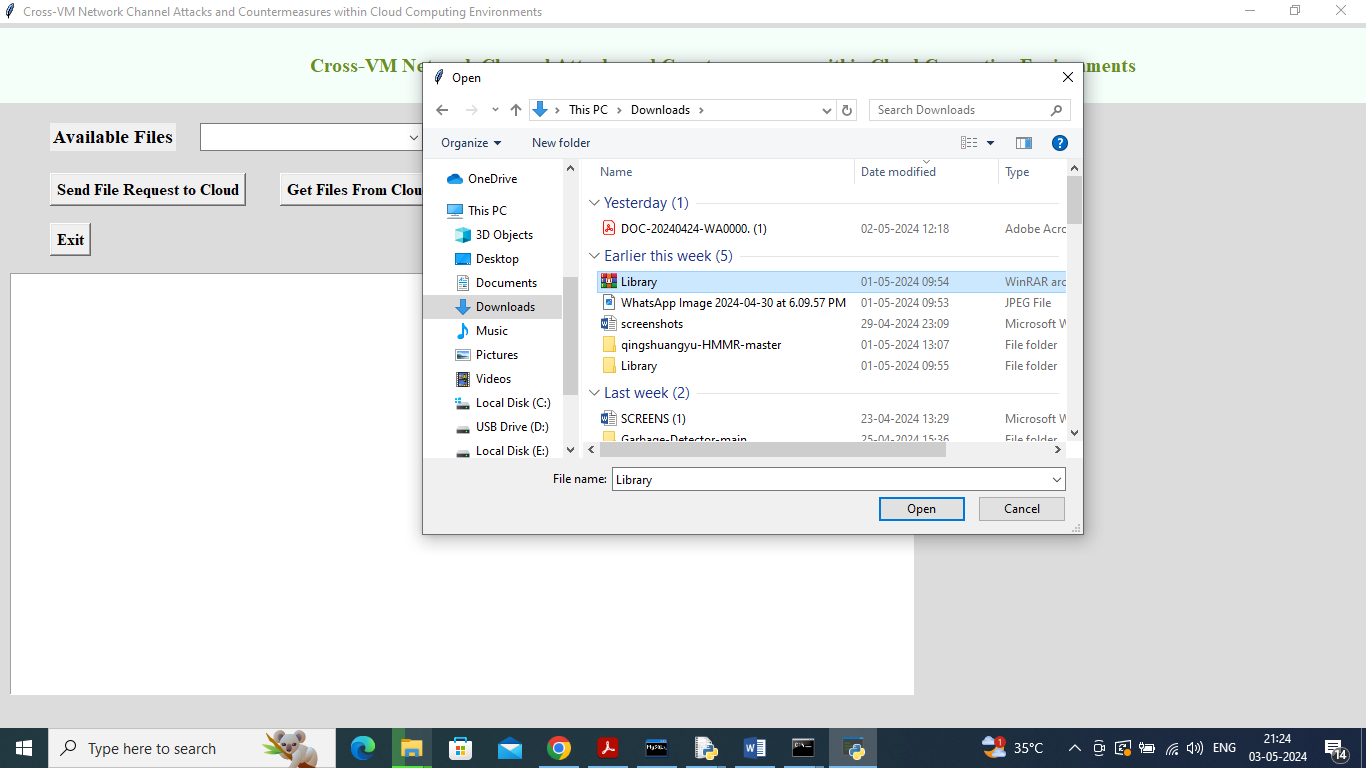
In above screen selecting and uploading a file and then click on ‘Open’ button send file to cloud which will monitor by VM and then will get below output



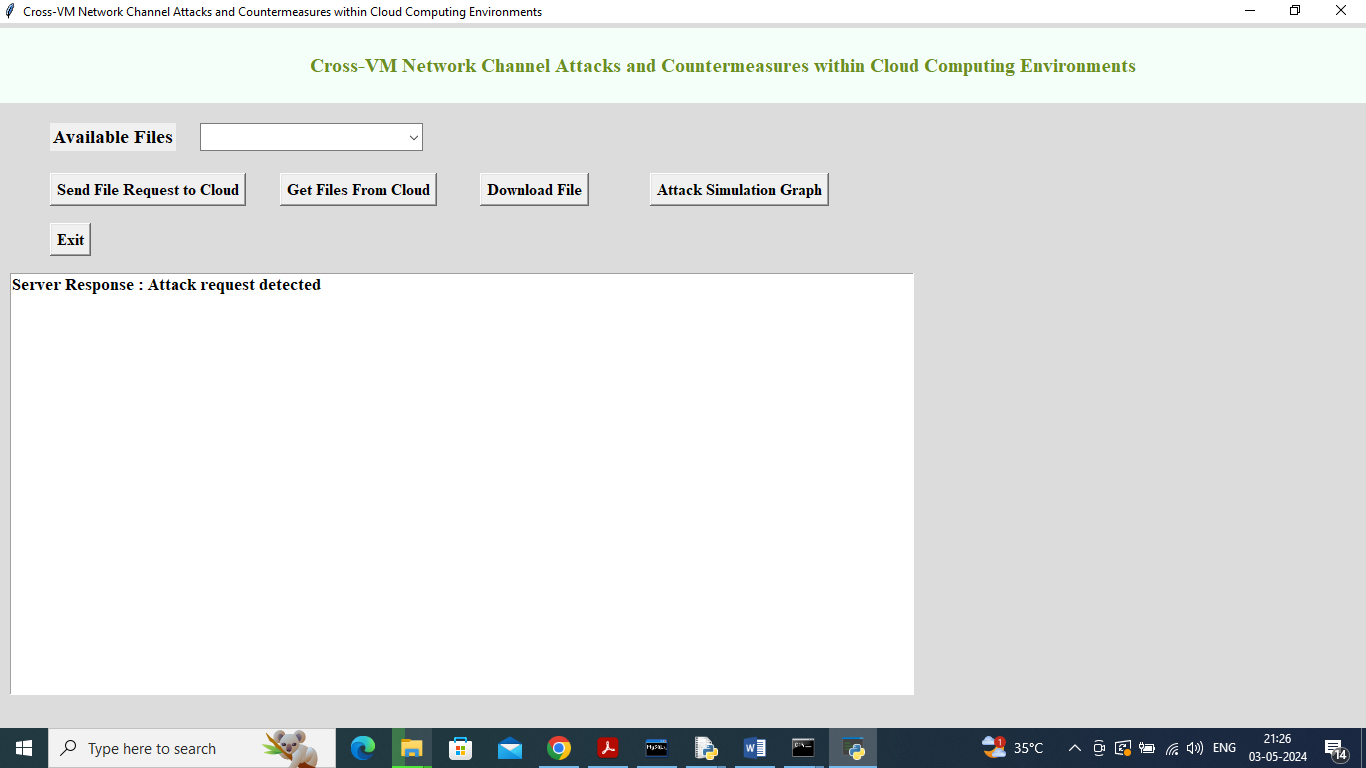
In above screen we got response from cloud as file saved successfully and below is the monitor response



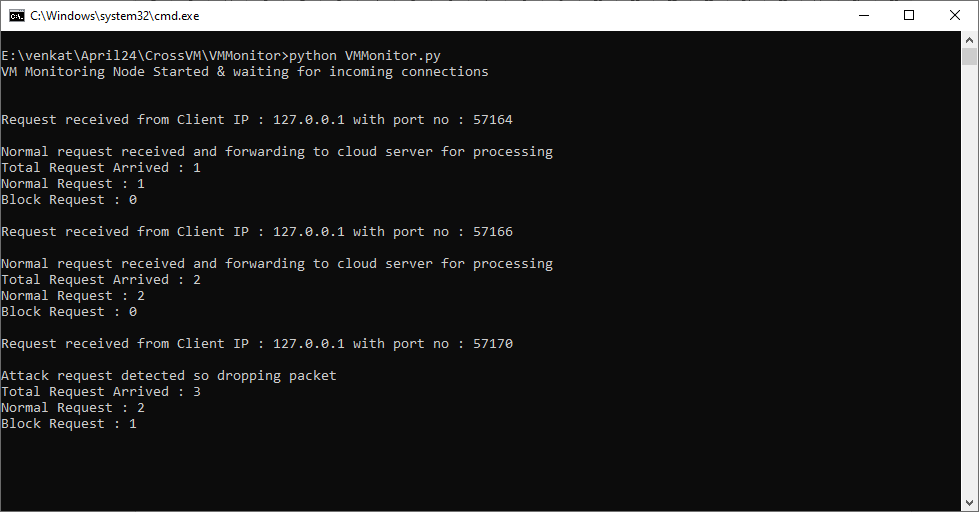
In above screen Monitor consider request as normal and Block count is 0 and now upload another file



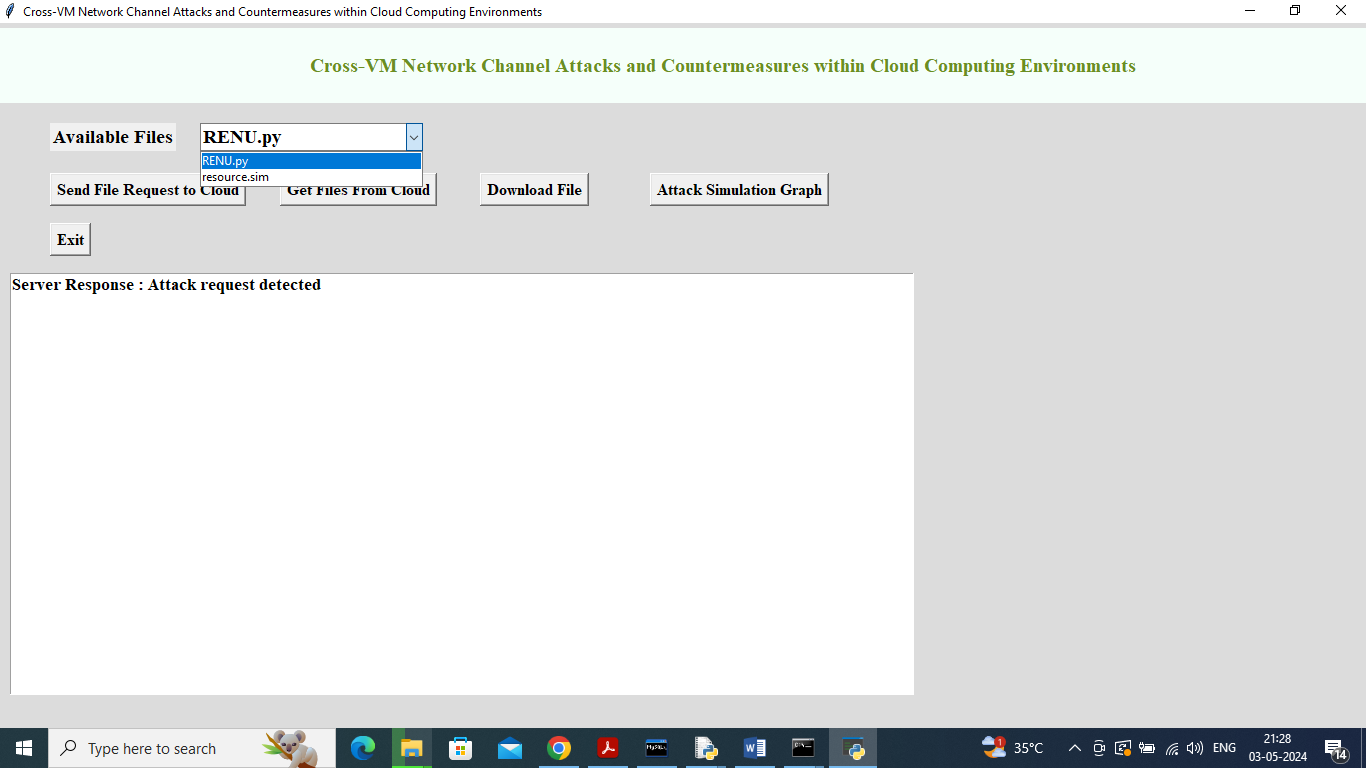
In above screen uploading huge zip file intentionally to crash cloud server and this will monitor by VM monitor and drop the request and get below output



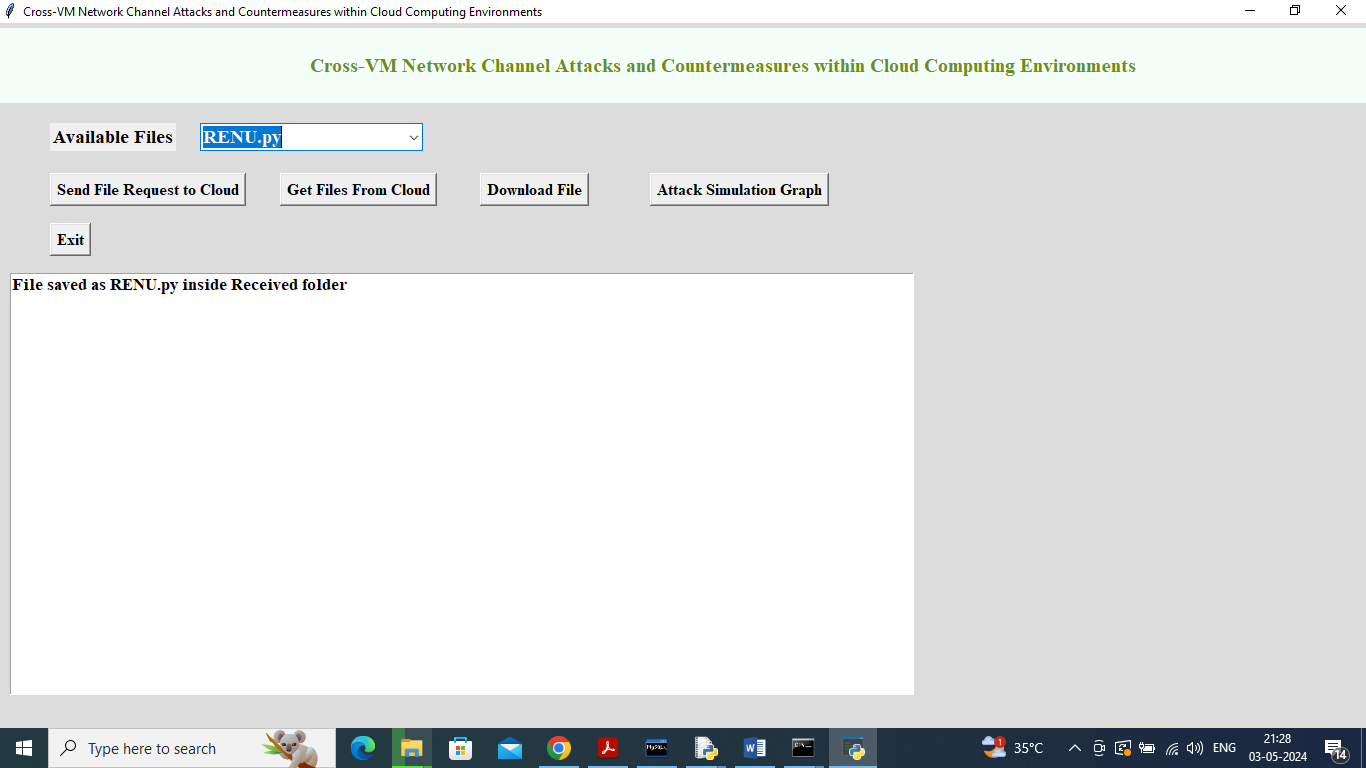
In above screen cloud monitor detected request as ATTAACK and then drop that request to save user data and below is the monitor response



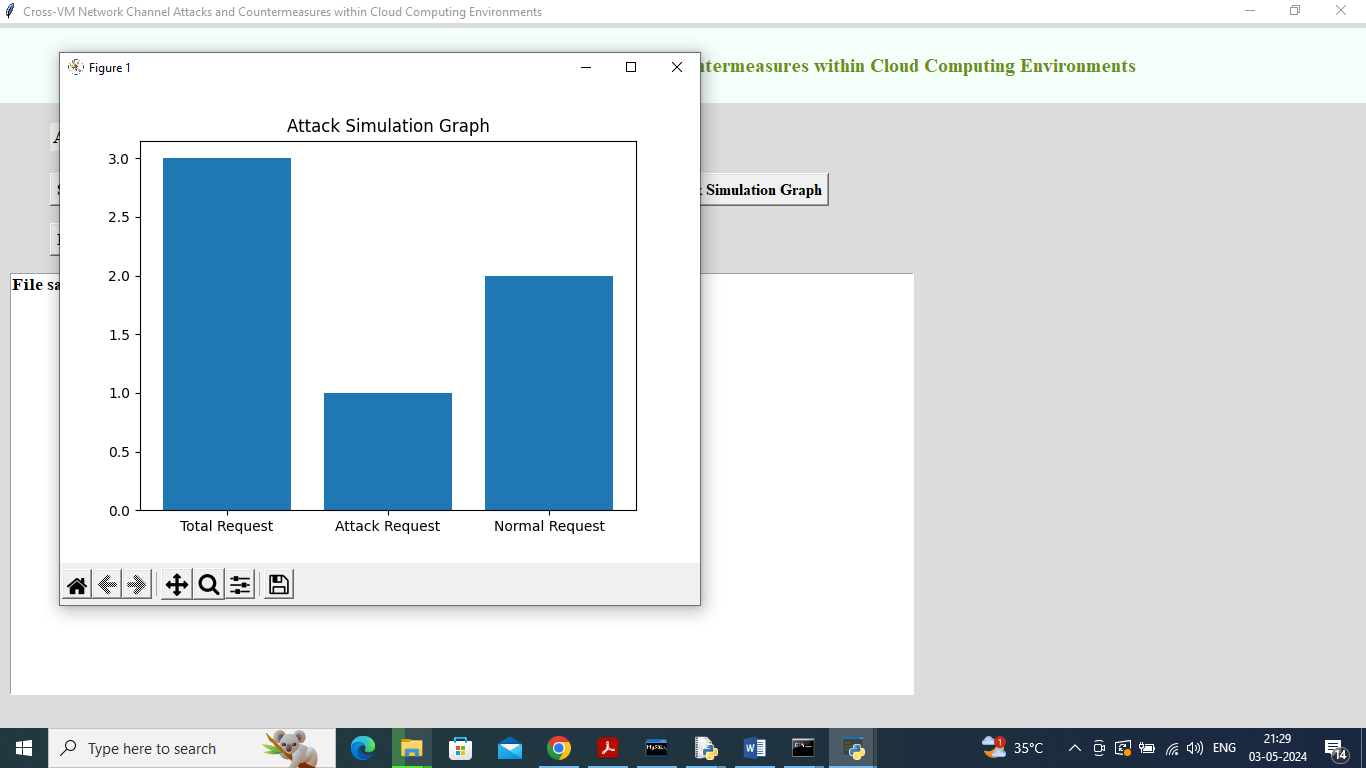
In above screen monitor saying 2 Normal requests arrived and 1 attack request arrived and in below screen click on ‘Get Files from Cloud’ button to get below page



In above screen can get all file list from cloud and user can selected desired file and then click on ‘Download File’ button to get below output



In above screen can see file downloaded and saved inside Received folder and now click on ‘Attack Simulation Graph’ button to get below graph



In above graph x-axis represents total, attack and normal request type and y-axis represents count and in above graph can see how many request MONITORS received and how many are normal and attacks.