# Securing Android Phones against Potential Thefts: AhMyth Android RAT

[1]Raigen Joseph Tomy, [2]Jeena Thomas, [3]Noel Jacob, [4]Ms.Lisha Varghese

[1, 2, 3] P G Scholar, Amal Jyothi College of Engineering, Kanjirappally, 686518

[4]Assistant Professor, Amal Jyothi College of Engineering, Kanjirappally, 686518

[1]raigenjosephtomy@mca.ajce.in, [2]jeenathomas@mca.ajce.in, [3]noeljacob@mca.ajce.in, [4]lishavarghese@amaljyothi.ac.in

***Abstract—Android Smartphones have become an everyday companion for the modern man. Day by day, new improved versions of phones are being introduced into the market. Everyone who owns a smartphone adds more personal data on it daily. Therefore there is a bigger need to secure these devices. Even though various methods have been adopted to secure the phones, a full-scale process is not yet found. We are aiming to develop a system where the user himself can access his phone remotely when it is lost. The proposed system obtains GPS location, photograph and audio recording of surroundings using Client-Server Methodology. AhMyth Android RAT, a Remote Administration Tool (RAT) is used to acquire these data securely from the target system. The device will be installed with a payload injected application which will act as a backdoor. We can access and retrieve data from the target device after establishing the session. Data transfer is done using Port Forwarding and VPN technologies regardless of the location of the device. A visual representation of device location and other data received is displayed on the GUI interface provided by AhMyth. Users can locate their phones using the received data and GPS.***

***Keywords: Remote Administration Tool, Port Forwarding, Virtual Private Networks, Backdoor tracking, GPS, Payload***

## I. INTRODUCTION

In our modern lifestyle smartphones have become an unavoidable factor. Smartphones changed our way of using fixed land lines for communication. Most of the smartphones are using Android Operating System. The most modern features allows group voice calls, video conferencing and text messages. It also provides facilities like data storage, image capture, voice recording, internet access, GPS services and much more. The data stored on the phone includes a lot of important information and that includes confidential company documents also.

Because of its small-size Smartphone robbery is a common crime in our society. Half a million phones were reported stolen in 2018. Carelessness is another reason where phone goes missing. Most of these could have been avoided if we took precautions for such an incident.

In this current scenario, there is a need for individuals to come up with a working solution for such an event. Here we are aiming to create a method that allows users to secure their phones themselves to a certain extent. In the proposed system, we are using AhMyth Android RAT (Remote Administration Tool) to access our phone through a backdoor application. RAT allows users to access target systems using backdoors. These backdoors enable users to retrieve data from the infected device. After the payload injected application is installed on the target system, the user can access the device from AhMyth Desktop application. Information like location, photograph and audio record can be taken along with contact list, file system, and SMS log. Whenever there arises a need to locate the phone, the user can do it by accessing the backdoor.

We are using OpenVPN to transfer data between server and client so that the connection can be established across multiple networks. Here target phone acts as the client and the server is kept at the user's end. Port-Forwarding technology is used to redirect our data towards the server. Server can access the victim by listening to the port number of the backdoor application. When the session is active the data will be passed from victim to the VPN server and from there to user. Using this method the connection can be established between user and target system irrespective of their network types.

## PORT FORWARDING

Port forwarding is the method of redirecting a communication request from a single combination of address and port number to another while the data is passed through a network gateway.

### REMOTE ADMINISTRATION TOOL

A remote administrative tool is a program that allows the user to connect to other computer systems via internet with or without the consent of the owner. These programs are usually used by hackers to gain access to unauthorized networks or computers. AhMyth Android RAT is a remote administration tool used to connect to infected android devices through a backdoor. A payload is injected in the target system to create the backdoor.

### AHMYTH ANDROID RAT

AhMyth is an exploitation tool which operates on client-server architecture that is used to gain access to an android phone by using a payload installed on the target system. Location, file system, images, sound record, contacts and SMS details can be retrieved by GUI interface of AhMyth. It is also used to track real time location of the target system.

### VIRTUAL PRIVATE NETWORK

VPN is an extension of private networks which enables devices on public network to connect and transfer data across the private servers. OpenVPN is used to set up a VPN Server which acts as a bridge between the AhMyth Server and the client. Using this the server and client can be connected from anywhere around the world irrespective of the IP address of the server.

### BACKDOOR ATTACK

Backdoor attack is attacking strategy used by most of the hackers. Initially it creates a backdoor application on the target system. This backdoor is hidden and it collects necessary data and returns to the server whenever a request is pushed. This method is used by authorized and unauthorized users across the world to gain access and exploit various network resources.

### GLOBAL POSITIONING SYSTEM

GPS is a satellite navigation system that uses radio signals to pinpoint the location and time of the device. It calculates the distance and time between satellites and device to formulate the global location of the device.

## II. LITERATURE REVIEW

Rupal D. Bhatt[1], Dr. D.B. Choksi[1] mentioned that remote administration is used for improving efficiency in maintaining and managing computer systems across communication networks in a cost-less manner. Modern remote access tools support flexible features for controlling remote systems through a wide range of attractive features. Different remote administration tools are found in the market and it is difficult to choose appropriate tools to meet the needs. It contains a comparative study of selected popular remote administration tools such as Graphical User Interface (GUI) oriented tools, Command-Line Interface (CLI) tools to help users in making appropriate selection of suitable tools. Web-based GUI tools, Console based tools, Windows Management Instrumentation tools, etc. considering various popular remote access software tools.

NidhiVerma[2], Monika kashyap[2] points that the port forwarding or port mapping is an application of network address translation (NAT) that redirects a communication request from one address and port number to another while the packets are traveling through a network gateway, such as a router. It allows remote computers to connect to a specific computer within a private LAN. IoT allows connection with devices using the internet among the ability to gather and exchange data. These devices are usually attached to micro-controllers like Arduino, sensors, actuators and internet connectivity. Analysis of the scale of the network in terms of the number of connected nodes through port forwarding and limitations, if any can also form a part of future considerations.

Vancea Florin[3], Vancea Codruta[3] states that port forwarding is generally used to collectively expose services available on remote machines to clients running on the local machine. TCP services are easy to forward using SSH, at least as long as the details of the transported protocol are transparent. It describes a Java client or server pair that may be used in almost the environment to forward a UDP dialog in a TCP connection. The tool is tested for SNMP traffic with multiple targets and multiple clients. There are many scenarios where traffic should arrive at the transport level between two hosts on different networks even if normally no traffic can (or should) traverse the internetwork from the first host to the second one. A reasonable example would be remote telnet access from a client on the network behind a firewall to a network-enabled simple device placed on network B, behind another firewall. It specifies a method to build an additional layer over TCP that can tunnel and proxy UDP traffic. The tool can be useful, but in the wrong hands, it may be a security hazard, not by itself but by exploiting weak configuration setups.

Ahmed A. Jaha[4], Fathi Ben Shatwan[4], and Majdi Ashibani[4] pointed that VPN is a way to provide secure communication between members of a group through use of public telecommunication infrastructure which maintains privacy through the use of a tunnelling protocol. VPN is divided as Secure or Trusted VPNs, Client-based or Web-based VPNs, Customer Edge-based or Provider Edge-based VPNs, or Outsourced or In-house VPNs. The main purpose of a VPN is to give enterprises the same capabilities, or even better, as in private networks, but at a much lower cost. There are basically two types of VPNs, remote access VPN and site-to-site VPN. Site to site VPN is further divided into intranet VPN and extranet VPN.

Shan Jing[5], Runyuan Sun[5], Qi Qi[5], Qun Li[5] proposed that the demand for remote access to the campus network becomes more and more diversified. So, it is important to build a secure and efficient network architecture. It is necessary to be considered to ensure a safe, efficient and low-cost access to these information systems in the long-distance mobile office. Remote access requirements, the design and deploy of multi-campus network VPN security interconnection scheme, has a certain practical significance. Scheme of comprehensive application of IPSec VPN, L2TP over IPSec VPN and firewall technology that improve the safety of campus network interconnection and enhance the accessing experience of users outside the campus to access the resource in remote. The successful implementation of the project can provide effective reference of multi-campus network interconnection for other colleges, universities and enterprise.

## III. PROBLEM DEFINITION

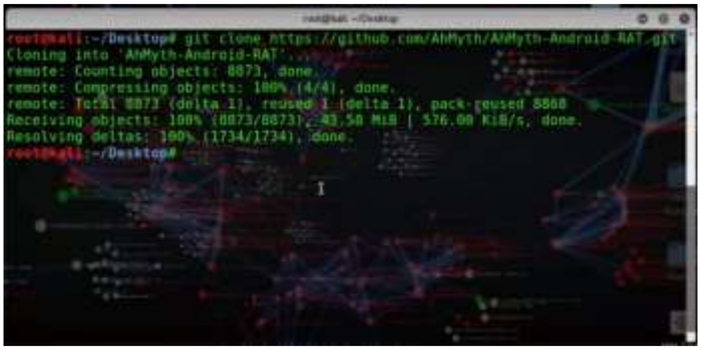
Step 1: Configuring AhMyth Android RAT in Microsoft Windows 10

In order to configure AhMyth on Windows we have to make sure that the system holds some prerequisites, which are:

1. Electron(to start the app)
2. Java (to generate apk backdoor)
3. Electron-builder and Electron-packer(to interact with the App)
4. NodeJs and Npm for interaction with the AhMyth app

After installing necessary environments and programs we have to clone AhMyth files from github. We can do this by opening git bash in windows 10:

**git clone https://github.com/AhMyth/AhMyth-Android-RAT.git**



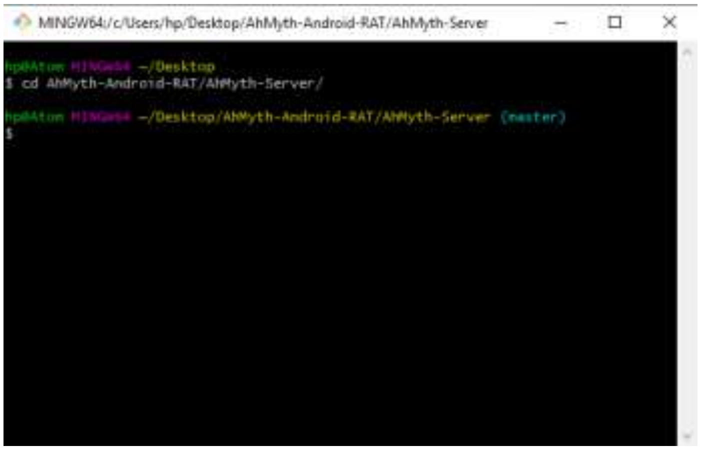
```
root@kali:~/Desktop# git clone https://github.com/AhMyth/AhMyth-Android-RAT.git
Cloning into 'AhMyth-Android-RAT'...
remote: Counting objects: 8873, done.
remote: Compressing objects: 100% (4/4), done.
remote: Total 8873 (delta 1), reused 1 (delta 1), pack-reused 8868
Receiving objects: 100% (8873/8873), 43.50 MiB | 576.00 KiB/s, done.
Resolving deltas: 100% (1734/1734), done.
root@kali:~/Desktop#
```

Fig 4.1

Step 2: Now change the directory to AhMyth Server

The module contains two sections: client and server. The app should be started with the server in order to start the session. Now change the folder to AhMyth-Server. Type the following command:

**$ cd AhMyth-Android-RAT/AhMyth-Server/**



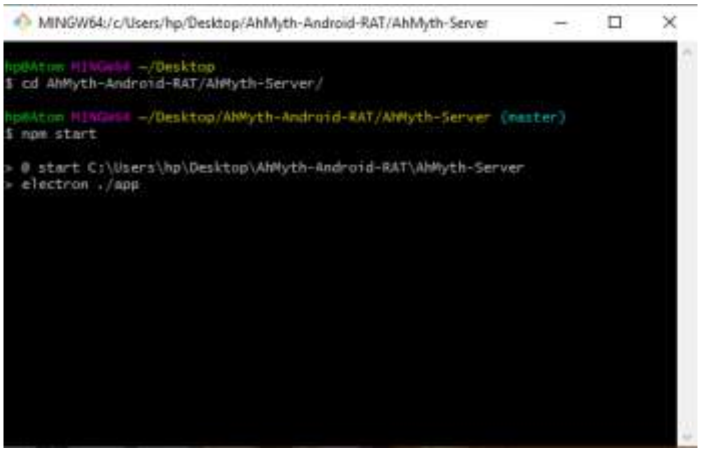
```
MINGW64:/c/Users/hp/Desktop/AhMyth-Android-RAT/AhMyth-Server

hp@Atom MINGW64 ~/Desktop
$ cd AhMyth-Android-RAT/AhMyth-Server/

hp@Atom MINGW64 ~/Desktop/AhMyth-Android-RAT/AhMyth-Server (master)
$
```

Fig 4.2

Step 3: Run AhMyth Android RAT

The previous command changed the directory to the AhMyth server. Now it’s time to launch the tool. Run it by the command:

**$npm start**



```
MINGW64:/c/Users/hp/Desktop/AhMyth-Android-RAT/AhMyth-Server

hp@Atom MINGW64 ~/Desktop
$ cd AhMyth-Android-RAT/AhMyth-Server/

hp@Atom MINGW64 ~/Desktop/AhMyth-Android-RAT/AhMyth-Server (master)
$ npm start

> @ start C:\Users\hp\Desktop\AhMyth-Android-RAT\AhMyth-Server
> electron ./app
```

Fig 4.3

The npm command will start the electron to launch the app

Step 4: Setting up OpenVPN connection

In order to set up the VPN network we need to perform the following steps:

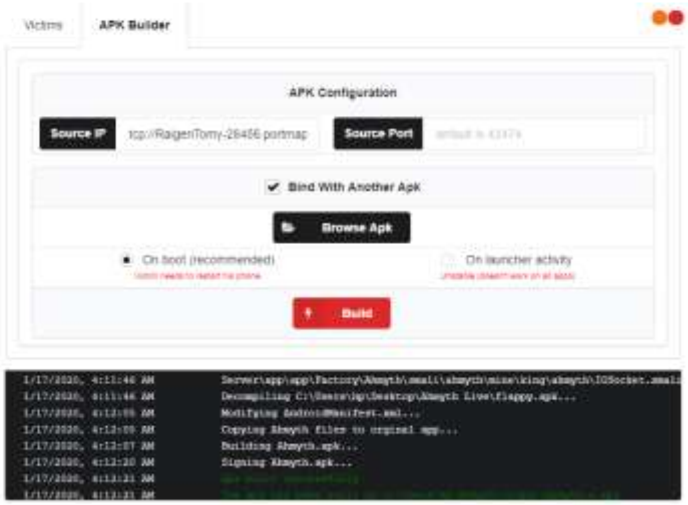
1. Install the OpenVPN client in the windows system.
2. After that create a new configuration file and a new mapping rule in https://portmap.io website. Download the configuration file and place it inside the config folder in OpenVPN folder

   **C:\Program Files\OpenVPN\config\**

   Start the OpenVPN from the bottom tray and connect the new configuration.

Step 5: Creating AhMyth Payload infected apk file

From here on we will be interacting with the AhMyth GUI. We will create a backdoor in an app and install the apk file in the target phone. To inject the payload insert the port number and IP address you got when you created the configuration file in portmap.io website. Select on-boot option and hit build. The payload will be injected into the apk file and backdoor will be created.



Source IP: tcp://RaigenTomy-28456.portmap
Source Port: default is 42474

☑ Bind With Another Apk

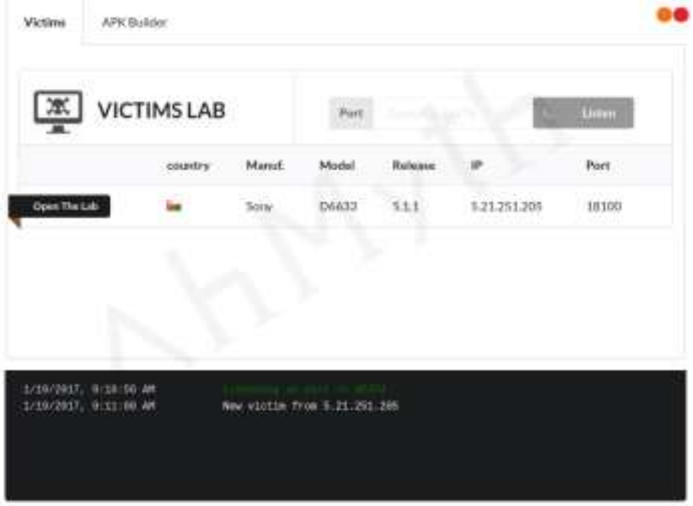
● On boot (recommended)
○ On launcher activity

```
1/17/2020, 4:11:46 AM        Server\app\app\Factory\Ahmyth\smali\ahmyth\mine\king\ahmyth\IOSocket.smali
1/17/2020, 4:11:46 AM        Decompiling C:\Users\hp\Desktop\Ahmyth Live\flappy.apk...
1/17/2020, 4:12:05 AM        Modifying AndroidManifest.xml...
1/17/2020, 4:12:05 AM        Copying Ahmyth files to orginal app...
1/17/2020, 4:12:07 AM        Building Ahmyth.apk...
1/17/2020, 4:12:20 AM        Signing Ahmyth.apk...
1/17/2020, 4:13:21 AM        [illegible]
1/17/2020, 4:13:21 AM        [illegible]
```

Fig 4.4

Step 6: Installing the apk file in your phone
The next step is to install the infected apk file and reboot the system. By doing so we will be creating a backdoor in our android phone to be accessed from the AhMyth server.

Step 7: Listening to your phone
Now open Victims lab in AhMyth and since we used the default port 42474 just click on the listen button to start listening.



| | country | Manuf. | Model | Release | IP | Port |
|---|---|---|---|---|---|---|
| Open The Lab | | Sony | D6633 | 5.1.1 | 5.21.251.205 | 18100 |

```
1/19/2017, 9:10:56 AM        [illegible]
1/19/2017, 9:11:00 AM        New victim from 5.21.251.205
```

Fig 4.5

Now the tool searches for clients and returns a list of devices where our payload is installed. When your phone is listed click on 'Open the lab' to access data of the phone.

Step 8: Go through various options to access data from phone
There are various options that AhMyth allows like, GPS location, camera image capture, voice record, contacts list, file manager and even sending SMS remotely.

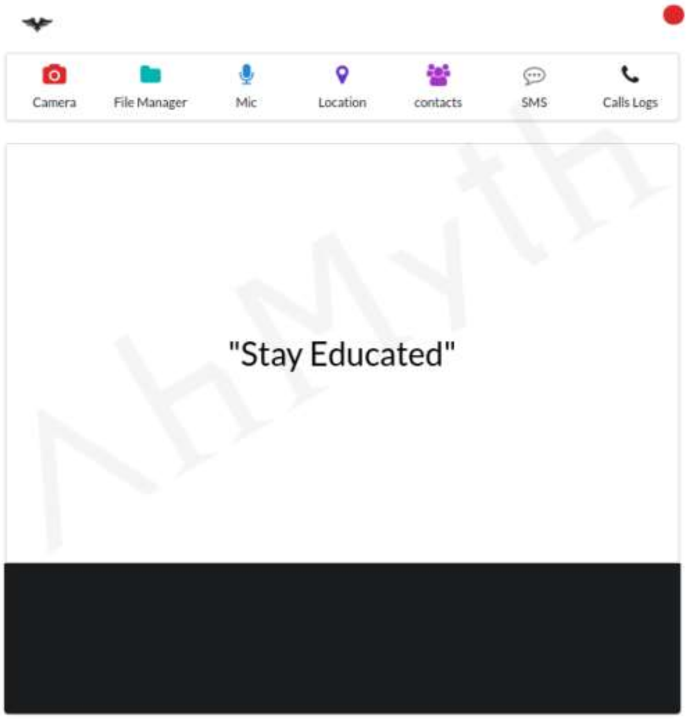


Fig 4.6

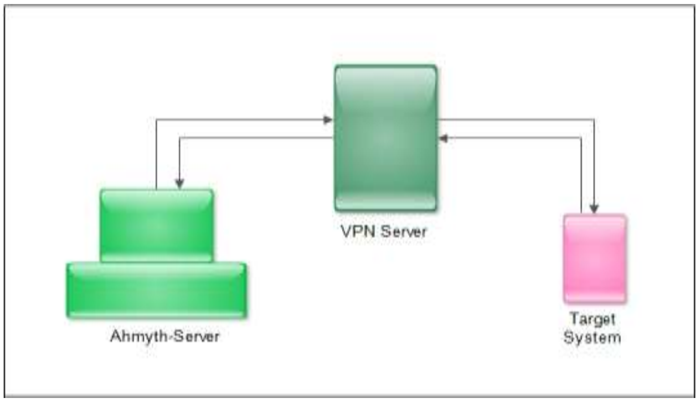


Fig 4.7 Diagram of connection : Target System to server

## IV. IMPLEMENTATION

AhMyth RAT allows us to monitor android device remotely from our computer system. We can access the phone any time after the payload has been activated in the system. The use of OpenVPN in this module enables us to access the android device from any network connection. This whole module is created to maintain a remote administration on your android device. If a scenario occurs that your device is lost, we can track it using this system. The exact GPS location will be provided together with photograph and audio record. If it is a case of theft, we can use this information to find out the criminals.

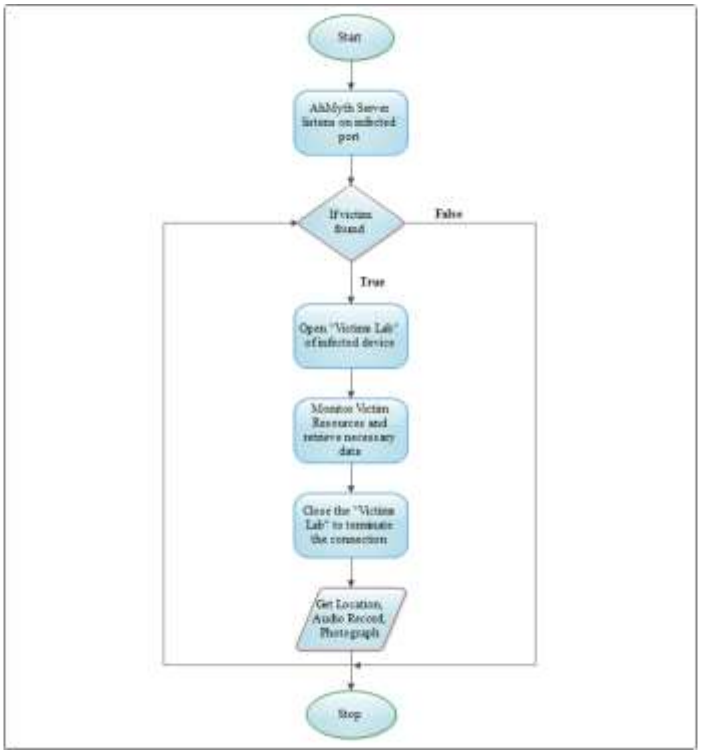
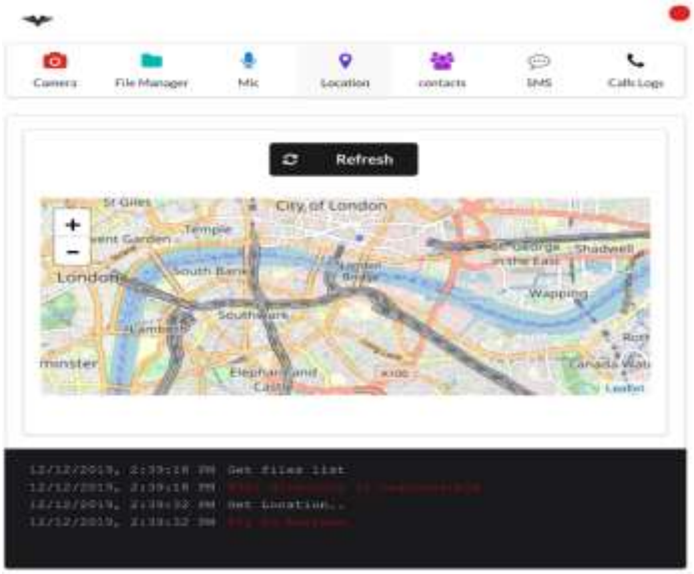

Start
AhMyth Server listens on infected port
If victim found
False
True
Open "Victim Lab" of infected device
Monitor Victim Resources and retrieve necessary data
Close the "Victim Lab" to terminate the connection
Get Location, Audio Record, Photograph
Stop

Fig 5.1 Working FlowChart



```
12/12/2019, 2:39:18 PM  Get files list
12/12/2019, 2:39:18 PM  [illegible]
12/12/2019, 2:39:32 PM  Get Location..
12/12/2019, 2:39:32 PM  [illegible]
```

Fig 5.2 GPS location

## V. RESULT

The AhMyth Android RAT accesses an android device through the installed backdoor. After the session is started it retrieves live GPS location, image and audio record. By using this data we can easily locate our phone if it is lost.

## VI. CONCLUSION

Nowadays losing our mobile phone will be very painful and problematic. So we can take early precautions by installing a backdoor to secure our phone from such a situation. AhMyth Android RAT is used to manipulate this backdoor and gain access to the phone when it is lost. By using the VPN networks for connectivity we enables the AhMyth-Server to connect to any network. The VPN server acts as a bridge between the server and client, thus removing the problems related to the static IP address. The location of the client and server is not an issue in such a scenario. The administrative system developed here is very useful in locating your phone when it is lost. Such a type of precaution is needed and will be very useful.

## REFERENCES

[1] Rupal D. Bhatt, Dr. D.B. Choksi: A Comparative Evaluation of Remote Administration Tools, International Journal of Advanced Research in Computer Science, Volume 4, No. 4, March-April 2013

[2] NidhiVerma, Monika kashyap: Extending Port Forwarding Concept to IOT, International Conference on Advances in Computing, Communication Control and Networking (ICACCCN2018)

[3] Vancea Florin, Vancea Codruta: Portable UDP port forwarding in user space

[4] Ahmed A. Jaha, Fathi Ben Shatwan, and Majdi Ashibani: Proper Virtual Private Network (VPN) Solution, The Second International Conference on Next Generation Mobile Applications, Services, and Technologies

[5] Shan Jing, Runyuan Sun, Qi Qi, Qun Li: Study on VPN solution based on multi-campus network, 2016 8th International Conference on Information Technology in Medicine and Education

[6] Afshan Mulla, Jaypal Baviskar, Amol Baviskar and Aniket Bhovad: GPS Assisted Standard Positioning Service for Navigation and Tracking: Review & Implementation, 2015 International Conference on Pervasive Computing (ICPC)

[7] Praveen Likhar, Ravi Shankar Yadav and Keshava Rao M: SECURING IEEE 802.11G WLAN USING OPENVPN AND ITS IMPACT ANALYSIS, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011

[8] Rathod Mahesh Pandurang, Dr. Deepak C. Karia: Performance Measurement of WEP and WPA2 on WLAN Using OpenVPN, International Conference on Nascent Technologies in the Engineering Field (ICNTE-2015)

[9] Patrick Butler, Adam Rhodes, and Ragib Hasan MANTICORE: Masking All Network Traffic via IP Concealment with OpenVPN Relaying to EC2, IEEE Fifth International Conference on Cloud Computing

[10] Irfaan Coonjah, Pierre Clarel Catherine, K. M. S. Soyjaudah: Performance Evaluation and Analysis of Layer 3 Tunneling between OpenSSH and OpenVPN in a Wide Area Network Environment

[11] Huaqing MAO, Li ZHU, Hang Qin: A comparative research on SSL VPN and IPSec VPN

[12] Daoyuan Wu, Debin Gao, Rocky K. C. Chang, En He, Eric K. T. Cheng, and Robert H. Deng: Understanding Open Ports in Android Applications: Discovery, Diagnosis, and Security Assessment,https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_06B-5_Wu_paper.pdf

[13] Byongkwon Lee, Joongnam Jeon: An Embedded Router for Internet Communication Among Private Networks,https://ieeexplore.ieee.org/document/4237579

[14] Onkar Mule, Nihal Shaikh, Pratik Shinde, Amit Wagaskar, Prof. Sneha Ramteke: Remote Access of Android Smartphone, Onkar Mule et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (2), 2016, 711-714

[15] Jay Novak, Jonathan Stribley, Kenneth Meagher, and J. Alex Halderman: Absolute Pwnage: A Short Paper About the Security Risks of Remote Administration Tools,15th International Financial Cryptography Conference, January 2011

[16] R. Manikandasamy: Remote Desktop Connection Using Mobile Phone, International Journal of Science, Engineering and Technology Research (IJSETR) Volume 2, Issue 8, August 2013

[17] Ganaa D. Ernest, Abeo Apasiba Timothy, Gerald Kpangkpar: The Use of Remote Access Tools by System Administrators Today and their Effectiveness: Case Study of Remote Desktop, Virtual Network Computing and Secure Android App, International Journal of Computer Applications (0975 – 8887) Volume 136 – No.10, February 2016