# AUTOMATIC DETECTION AND PREVENTION OF VIRUS IN MOBILE ENVIRONMENT

R.Priya
Department of Computer Science and Engineering,
Pondicherry Engineering College,
Puducherry, India.

**Abstract—Mobile phone becomes an essential device for everyone due to the need and drastic growth of technology. Mobile phones have truly transformed the mode of communications. It becomes the basic requirement of life. It is very difficult to imagine the live without a mobile phone as most of the work is done using mobile phones. They are not just narrowed only for communication purpose by using mobile phone one can able to access internet, send SMS, MMS, chat and share images, files via Bluetooth. The malicious virus, worms can also spread from one mobile to another by using operational or human behavior. The severe impact of malicious virus and worms may leads to lack of user privacy, eavesdropping, draining of battery charges. Moreover, it may track the user location using GPS technology or jams the server and spreads spam messages. In this paper, the developed application detects and deletes the virus that has been send via SMS finally the relevant patches is installed into the mobile to prevent from severe damage.**

**Keywords-**Mobile Network; Mobile phone Virus; Worms; Data leakage

## I. INTRODUCTION

The growth of mobile phone drastically increases day by day when compared to past decade. Over a period of time mobiles were used for the purpose for calling and sending text messages. But, now due to the technological advancement there exists many mobile apps for making the daily works simpler such as e-banking, e-booking, e-shopping, e-marketing, e-billing etc. This occurs due to the improvement and growth of internet as well as the smartphones.

As the technology grows higher and higher their vulnerabilities and threats also grows simultaneously. If a mobile phone is affected by virus it causes severe damage to the user which includes leakage of privacy information, leakage of data, draining of battery charges.

## II. OBJECTIVE

The prime objective of the paper is to prevent the mobile from folder virus and to restrain the virus propagation using the android application. And so, the mobile can be prevented from virus and related patches will be downloaded based on the severity of the virus.

## III. EXISTING SYSTEM

In the existing approaches, viruses and malwares can spread from computer networks into mobile networks with the speedy progress of smart cell phone users. In a mobile network, viruses and malwares can cause many severe impact such as lack of privacy, draining of battery charge and eavesdropping. The preventive methods were introduced in costly mobile phones. Since many people are using mobile phones with low cost. So the people prefer to buy moderate cost mobile rather than high cost mobile. So mainly attacker focus on these low cost mobile because of they didn’t have any antivirus software to detect and prevent the mobile from virus infection. Hence, these viruses were easily infected in the mobile and they will spread to more number of users during communication.

## IV. PROPOSED SYSTEM

The proposed system involves creation of folder virus and it is propagated through SMS. The virus will be send to other user mobiles via SMS. When the user opens the SMS the virus will be exploited and spreads to their mobile phones. To protect the mobile phones from folder virus an android application is built to destroy the virus and to download the patches from the server also provides automatic alert to the user virus found and deleted. Thereby, the mobile phone is protected from severe impact.

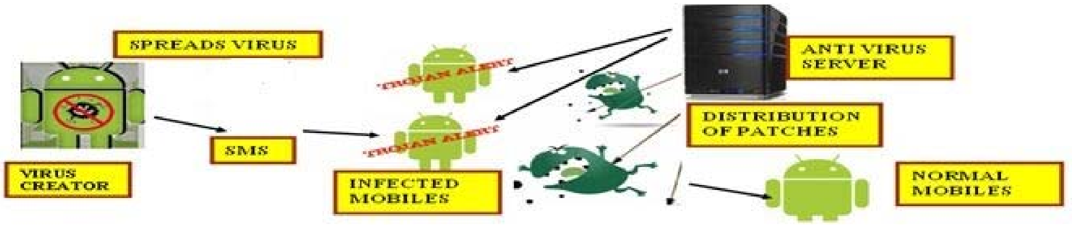


Figure 1. Architecture Diagram

### A. *Algorithm and Design*

The algorithm and design for the proposed system are as follows:

#### 1) *Algorithm*

The virus propagation algorithm involves operational behavior and mobile behavior. The operational behavior involves the propagation of virus through the user security and awareness pattern. The mobile behavior involves the propagation of the virus through Bluetooth. The user who are all aware of the mobile virus propagation through SMS may secure their phones from virus by not opening the SMS.

#### 2) *Flow Chart*

The flowchart provides the basic outline view of the proposed work.

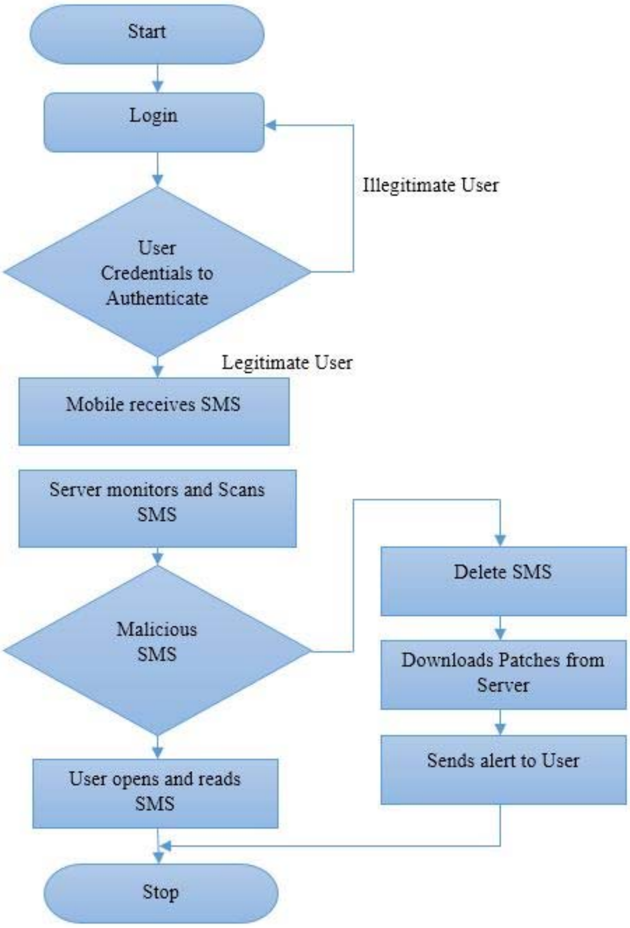


Figure 2. Flowchart Diagram

## V. METHODOLOGY

The modules involved in this paper are as follows:

**Login:** It contains account creation which includes the basic information of the user such as username, password, and IP address. The user has to sign up or sign in for account activation inorder to get the application stored in the mobile phone.

**Scanning:** If the mobile phone receives any links via SMS it scans the link automatically through the server.

**Delivery of Patch:** If the link contains any malicious virus it automatically deletes the virus and equivalent patch will be downloaded and installed to the mobile phone. An alert will be sent to the user that the virus

## VI. IMPLEMENTATION

The scenario is as follows:

### *A) Scenario of this Paper*

**Scenario 1: Mobile client**

- The mobile client consists of user registration details to enter the user credentials.
- The user who registered with this app can alone download and install this application into their mobile phone.

**Scenario 2: Server**

- It is a server side application.
- The server communicates with client via GPRS technology.
- It does not allow the unauthorized user.
- The legitimate user who registered with this application alone observed by the server inorder to detect the malicious links that are received via SMS to the user.

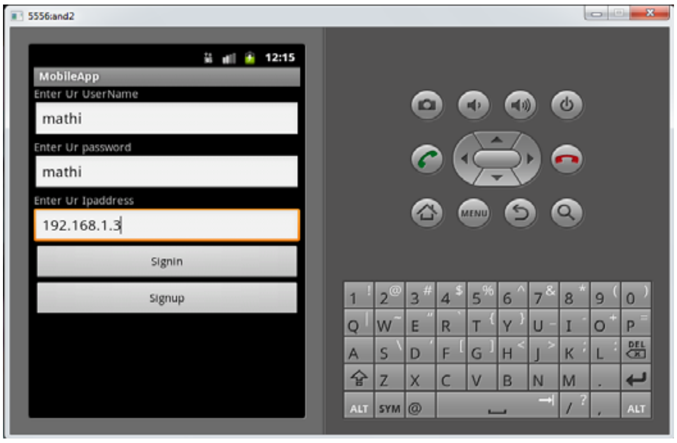
**Scenario 3: Automatic detection of virus**

- The attacker spreads the virus file to other users via mobile phone.
- The server analyze the file if malicious behavior is found it automatically deletes the virus.
- The patch that are downloaded from server will removes the malicious files.

**Scenario 4: Delivery of patches**

- The server provides patches in order to destroy the virus.
- After deleting the virus from the user mobile phone the application sends an alert to the user after destroying the virus.

## VII. RESULTS



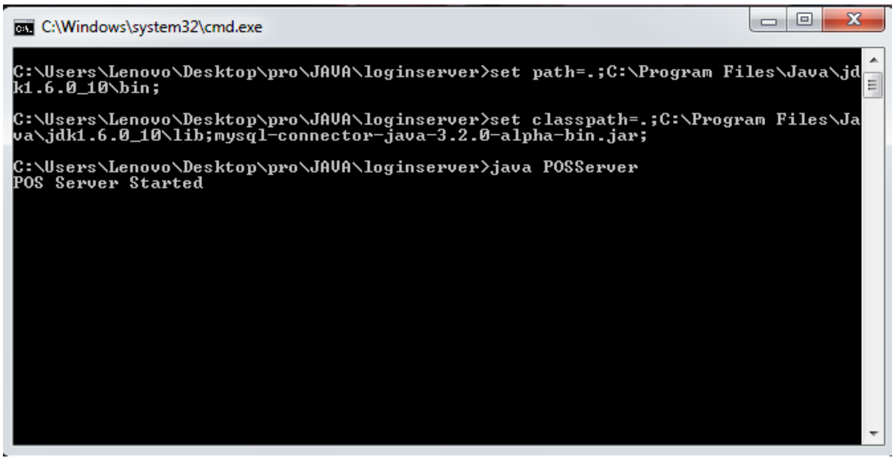
MobileApp

Enter Ur UserName: mathi

Enter Ur password: mathi

Enter Ur Ipaddress: 192.168.1.3

Figure 3. Mobile client



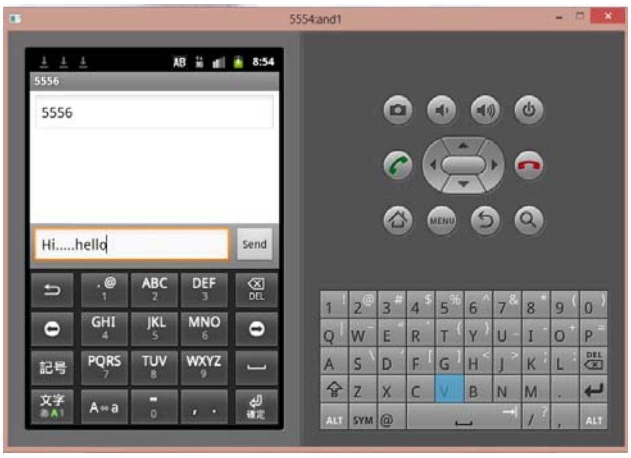
C:\Windows\system32\cmd.exe

```
C:\Users\Lenovo\Desktop\pro\JAVA\loginserver>set path=.;C:\Program Files\Java\jd
k1.6.0_10\bin;

C:\Users\Lenovo\Desktop\pro\JAVA\loginserver>set classpath=.;C:\Program Files\Ja
va\jdk1.6.0_10\lib;mysql-connector-java-3.2.0-alpha-bin.jar;

C:\Users\Lenovo\Desktop\pro\JAVA\loginserver>java POSServer
POS Server Started
```

Figure 4. Initiating server



5554:and1

8:54

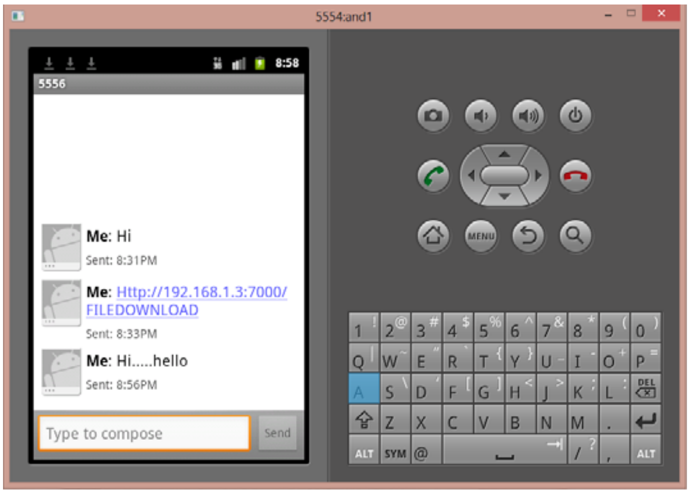
5556

5556

Hi.....hello

Send

Figure 5. Initializing device for communication



5554:and1

8:58

5556

Me: Hi
Sent: 8:31PM

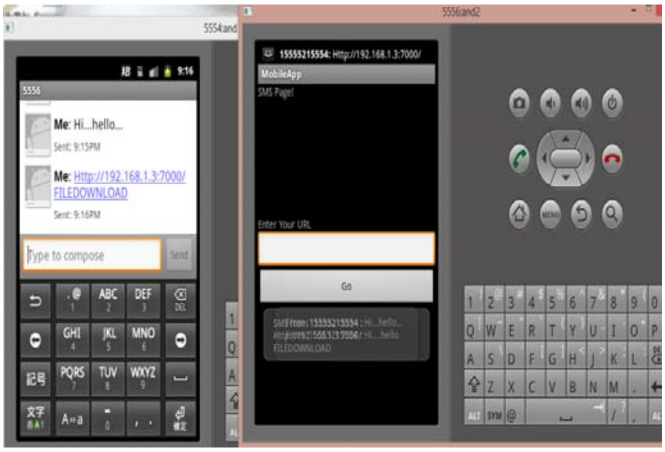
Me: Http://192.168.1.3:7000/FILEDOWNLOAD
Sent: 8:33PM

Me: Hi.....hello
Sent: 8:56PM

Type to compose

Send

Figure 6. Sending the message and URL



9:16

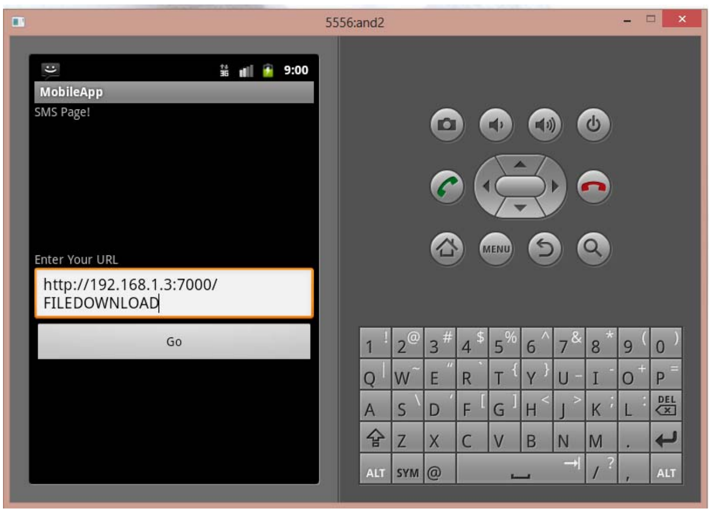
Me: Hi...hello...
Sent: 9:15PM

Me: Http://192.168.1.3:7000/FILEDOWNLOAD
Sent: 9:16PM

15555215554: Http://192.168.1.3:7000/

SMS from: 15555215554 : Hi...hello... Http://192.168.1.3:7000/ Hi....hello FILEDOWNLOAD

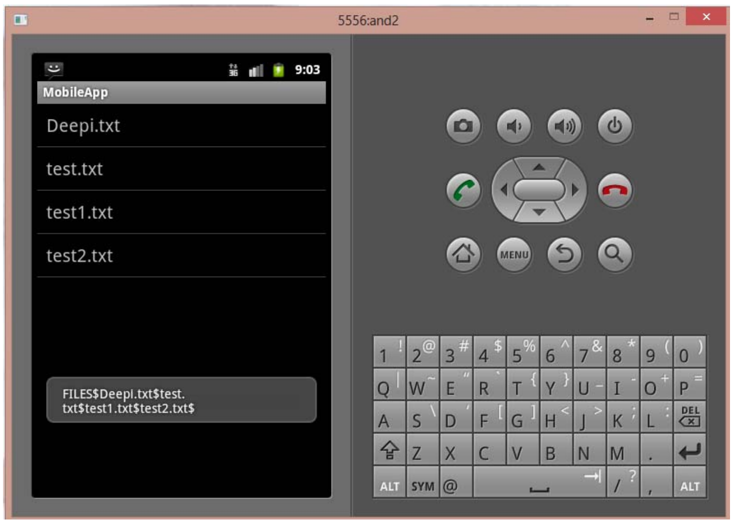
Figure 7. Receiving the message and URL



9:00

http://192.168.1.3:7000/FILEDOWNLOAD

Figure 8. Checking the URL



9:03

Deepi.txt

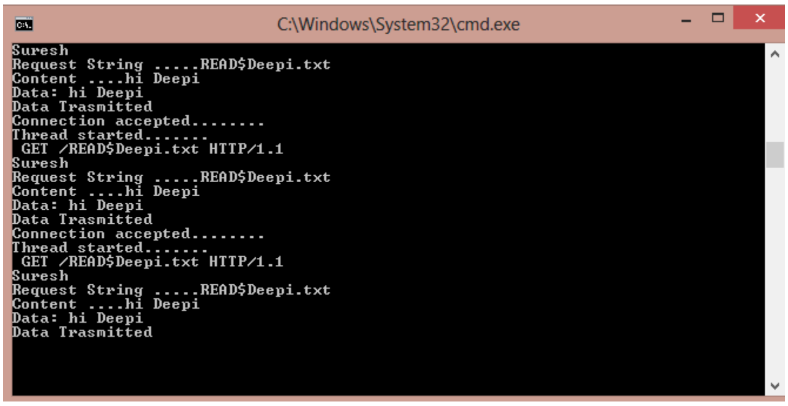
test.txt

test1.txt

test2.txt

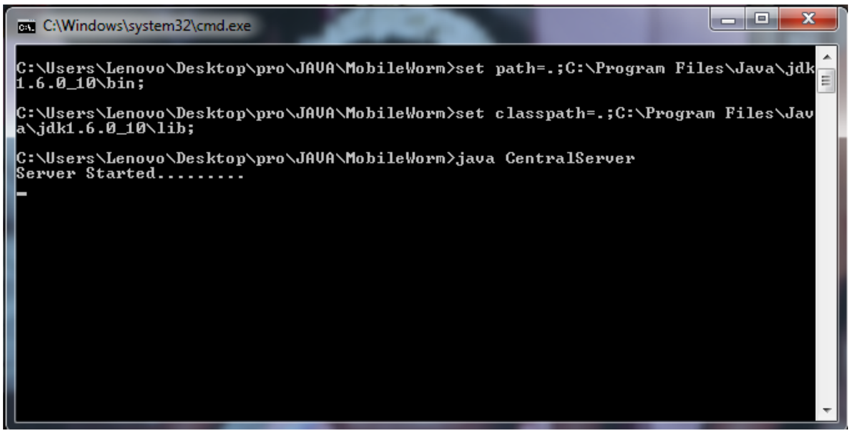
FILES$Deepi.txt$test.txt$test1.txt$test2.txt$

Figure 9. Displaying list of files



```
Suresh
Request String .....READ$Deepi.txt
Content ....hi Deepi
Data: hi Deepi
Data Trasmitted
Connection accepted........
Thread started.......
 GET /READ$Deepi.txt HTTP/1.1
Suresh
Request String .....READ$Deepi.txt
Content ....hi Deepi
Data: hi Deepi
Data Trasmitted
Connection accepted........
Thread started.......
 GET /READ$Deepi.txt HTTP/1.1
Suresh
Request String .....READ$Deepi.txt
Content ....hi Deepi
Data: hi Deepi
Data Trasmitted
```

Figure 10.  Transmitted files

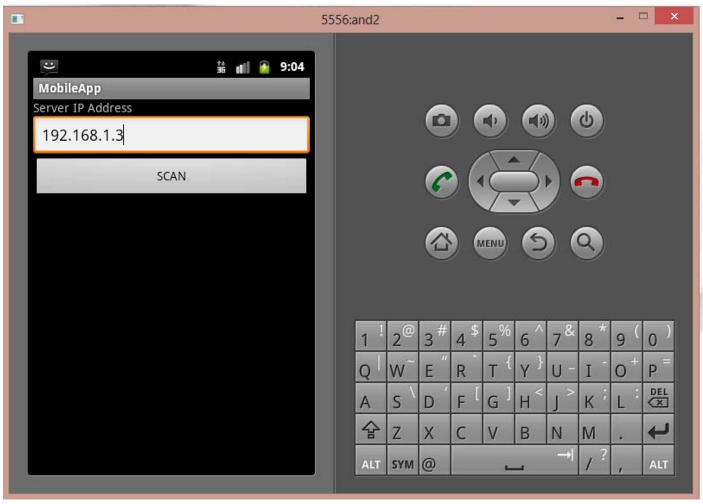


```
C:\Users\Lenovo\Desktop\pro\JAVA\MobileWorm>set path=.;C:\Program Files\Java\jdk
1.6.0_10\bin;

C:\Users\Lenovo\Desktop\pro\JAVA\MobileWorm>set classpath=.;C:\Program Files\Jav
a\jdk1.6.0_10\lib;

C:\Users\Lenovo\Desktop\pro\JAVA\MobileWorm>java CentralServer
Server Started.........
_
```

Figure 11.  Central server started



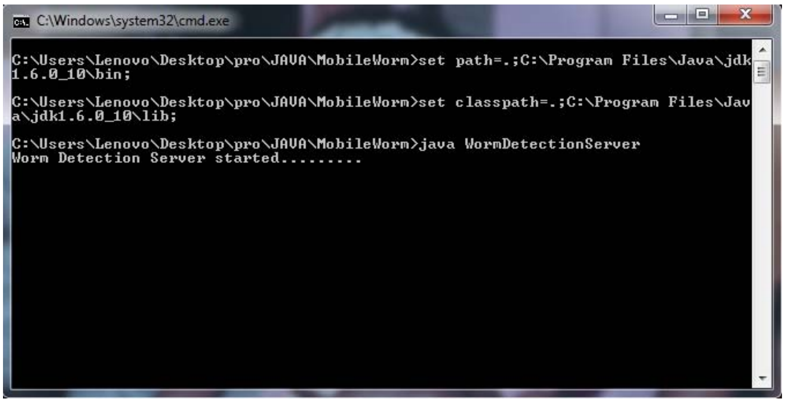
MobileApp

Server IP Address

192.168.1.3

SCAN

Figure 12.  Scanning the URL

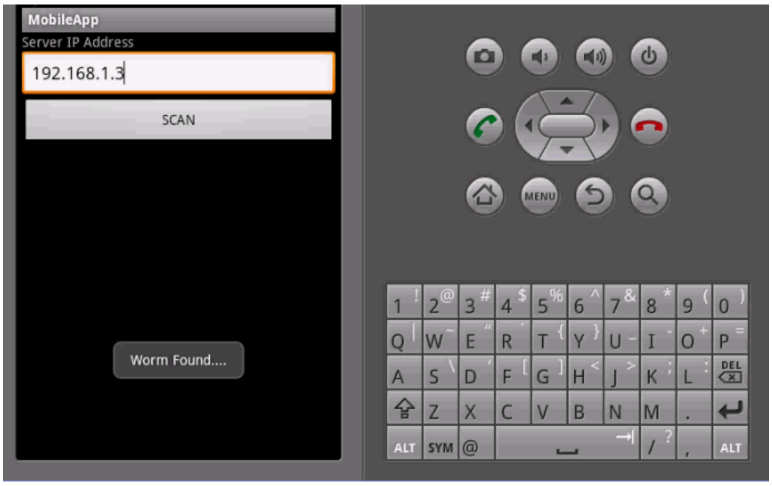


```
C:\Users\Lenovo\Desktop\pro\JAVA\MobileWorm>set path=.;C:\Program Files\Java\jdk
1.6.0_10\bin;

C:\Users\Lenovo\Desktop\pro\JAVA\MobileWorm>set classpath=.;C:\Program Files\Jav
a\jdk1.6.0_10\lib;

C:\Users\Lenovo\Desktop\pro\JAVA\MobileWorm>java WormDetectionServer
Worm Detection Server started.........
```

Figure 13.  Worm detection server started


MobileApp

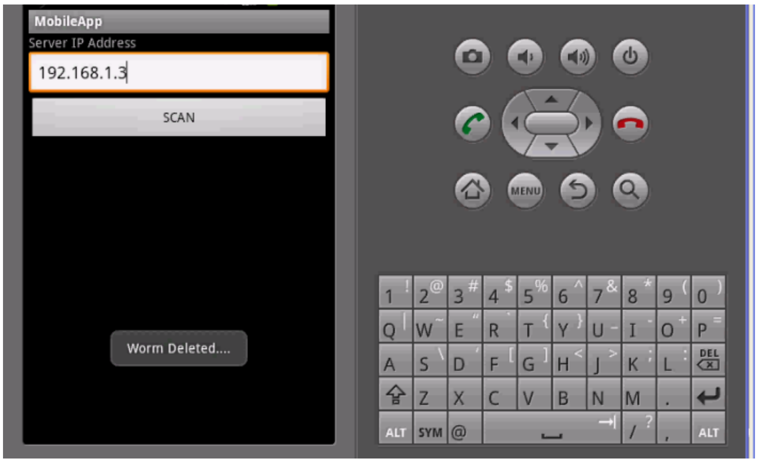
Server IP Address

192.168.1.3

SCAN

Worm Found....

Figure 14.  Application detect the worm


MobileApp

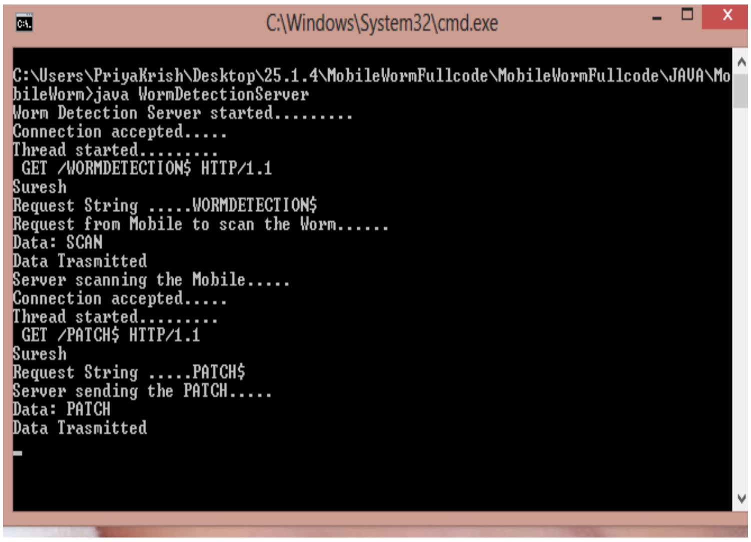
Server IP Address

192.168.1.3

SCAN

Worm Deleted....

Figure 15.  Application deletes the worm



```
C:\Users\PriyaKrish\Desktop\25.1.4\MobileWormFullcode\MobileWormFullcode\JAVA\Mo
bileWorm>java WormDetectionServer
Worm Detection Server started.........
Connection accepted.....
Thread started.........
 GET /WORMDETECTION$ HTTP/1.1
Suresh
Request String .....WORMDETECTION$
Request from Mobile to scan the Worm......
Data: SCAN
Data Trasmitted
Server scanning the Mobile.....
Connection accepted.....
Thread started.........
 GET /PATCH$ HTTP/1.1
Suresh
Request String .....PATCH$
Server sending the PATCH.....
Data: PATCH
Data Trasmitted
_
```

Figure 16. Delivery of patch

## ACKNOWLEDGMENT

I would like to thank all my faculties for their constant encouragement and valuable guidance. I would express my sincere gratitude to my parents for their blessings and support.

## REFERENCES

[1] S. Cheng, W.C. Ao, P. Chen, and K. Chen, (2011) “On Modeling Malware Propagation in Generalized Social Networks,” IEEE Comm. Letters, Vol. 15, No. 1, pp. 25-27.

[2] S. Bansal, J. Read, B. Pourbohloul, and L.A. Meyers, (2010) “The Dynamic Nature of Contact Networks in Infectious Disease Epidemilogy,” J. Biological Dynamics, Vol. 4, No. 5, pp. 478-489.

[3] P. De, Y. Liu, and S.K. Das, (2009) “An Epidemic Theoretic Framework for Vulnerability Analysis of Broadcast Protocols in Wireless Sensor Networks,” IEEE Trans. Mobile Computing, Vol. 8, No. 3, pp. 413-425.

[4] P. Wang, M.C. Gonzalez, C.A. Hidalgo, and A.-L. Barabasi, (2009) “Understanding the Spreading Patterns of Mobile Phone Viruses,” Science, Vol. 324, No. 5930, pp. 1071-107

[5] D.-H. Shi, B. Lin, H.-S. Chiang, and M.-H. Shih, (2008) “Security Aspects of Mobile Phone Virus: A Critical Survey,” Industrial Management and Data System, Vol. 108, No. 4, pp. 478-494.

[6] M.E.J. Newman, (2002) “The Spread of Epidemic Disease on Networks,” Physical Rev. E, Vol. 66, No. 1, pp. 01612.

[7] R. Pastor-Satorras and A. Vespignani, (2001) “Epidemic Spreading in Scale-Free Networks,” Physical Rev. Letters, Vol. 86, No. 14, pp. 3200-3203.

## Author

R.Priya pursuing her M.Tech (Information Security) in Computer Science and Engineering from Pondicherry Engineering College, Puducherry. She completed her B.Tech degree in Information Technology from Sri Ganesh College of Engineering and Technology, Puducherry. Her research interest are Information Security and Computer Networks.