I J C T A, 9(2) 2016, pp. 1267-1272

Secure Offline/Online Device to Device Communication

Amreen Ayesha[*] **and Augustian Isaac R.**[**]

ABSTRACT

In this study, in day to day life to communicate social networks with their friends, family, and community to access the cloud service based application on mobile devices. In Device to Device communication can download popular content such as videos or any other applications in offline can reduce the workload on the mobile network infrastructure. While transferring the application in the client base and share substantial measure of data, the aggressor's simple to assault the channel. Many social network websites can process the informal communication locales attempt to keep those abuses, yet numerous assailants are still ready to defeat those security countermeasures by utilizing distinctive methods. This paper mainly upgrade the social-mindful methodology for streamlining D2D correspondence lessening the Bandwidth utilization, Network activity and Server load, enhancing the information utility by neighbourhood sharing keeping up the security and protection concerns.

Keywords: communication; infrastructure; bandwidth; security;

I. INTRODUCTION

Person to person communication sites, for example, Facebook, Twitter and MySpace have been becoming quickly inside of the previous couple of years with now more than two billions clients. Verging on each PC proficient individual has no less than one interpersonal organization record and they spend a lot of their time on informal communities every day. Interpersonal organizations can be depicted as web applications that permit clients to make their semi-open profile a profile that some data is open and some is private, speak with the individuals who are their associations (companions), and fabricate an online group. It depends on social connections among clients. The vast majority join interpersonal organizations to share their data and stay in touch with individuals they know. The principle highlight of informal organizations is a companion discoverer that permits interpersonal organization clients to look for individuals that they know and afterward develop their own particular online group.

In numerous long range informal communication destinations, clients utilize their genuine name to speak to their records. Along these lines, their character is presented openly to other informal organization clients, and additionally others in the online world. Likewise, informal community client's record can be filed via web crawler and typically showed up in the top rank of the indexed lists. For this situation, if aggressors know the name of the casualties, they can without much of a stretch quest for casualty's profile, or they can look through long range interpersonal communication locales to acquire new casualties. Aside from the straightforward utilization of genuine name as record name, there are likewise different systems that can be utilized to uncover informal organization client's namelessness.

II. EXISTING SYSTEM

In a current framework capacity to proceed with these communications at whatever time, anyplace consistently is rapidly getting to be normal spot, and clients on present day cell phones hope to get to

[*] (M.tech), Computer Science and Engineering, SRM University, Chennai, India, *E-mail: ayesha1.success@gmail.com*

[**] M.E, (Ph.d), Asst. Professor, Computer Science and Engineering, SRM University, Chennai, India, *E-mail: Augustianisaac.r@rmp.srmuniv.ac.in*

interpersonal organizations as well as trade rich media substance, for example, video, sound, and pictures, for an upgraded client experience. It is accounted for that 93% of Android PDA clients in India use informal organizations on their advanced mobile phones and regularly this is the motivation behind why they buy PDAs in any case. We watch that the fundamental need (main driver) of dependably on connectedness comes from the presumption that current portable social versatile applications, for example, portable Facebook application, expect dependably on network. The issue of ideally pre-fetching online networking content from online networking suppliers to versatile clients is more perplexing than it appears at first look.

Because of this consistently expanding interest for remote get to, a gigantic measure of information is flowing over today's remote systems. This expansion sought after is straining current cell frameworks most of the movement in cell relates to the download of mainstream substance, for example, recordings or versatile applications.

All the client solicitations are prepared in server side. For instance: Watsapp, Facebook brings about a huge number of download solicitations every day, of which 20% of the solicitations are copy which originates from close vicinities. This raises the Server load and Network movement in extraordinary way.

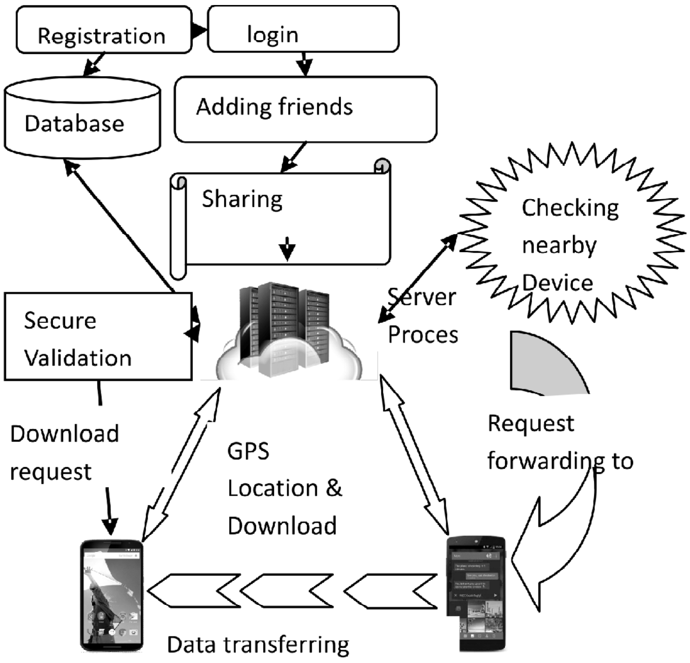
III. PROBLEM DEFINITION

The problem that we have in hand which should be dealt now is the following.

- High data usage for downloading content though Online SN.
- High Network traffic and Bandwidth usage.
- Overload on servers.
- High battery usage.
- Duplicate requests.

IV. PROPOSED SYSTEM

We propose an Online/Offline Social Networking application which uses the P2P correspondence, when the asked for substance is accessible with neighbourhood by utilizing the areas of all clients and builds up a protected information association utilizing Bluetooth for nearby get to. OSN clients can post their Text, Image and Video to open or companions. On the off chance that client needs to see the post, it ought to be downloaded from OSN Server or get from the adjacent gadget if accessible. Server constantly keeps up all clients download history and current GPS of all OSN clients. In the event that a solicitation emerges to the server, it turns upward for the close-by gadgets and if accessible it looks for the client asked for substance. In the event that the substance is accessible server triggers the both the neighbouring gadgets and start a distributed method of correspondence, Here we utilize Bluetooth as P2P correspondence and the asked for substance will be conveyed to the destination gadget in disconnected from the net mode.



V. ARCHITECTURE DIAGRAM

VI. MODULES

- Social Networking Web Application.
- Sharing Posts with Access Control.
- Review/Like, Posts/View through Android Application.
- Downloading/Transferring of Data via P2P

(A) Social Networking Web Application

In this module, the OSN web application is work as social network interaction application in which new client can enrol for the administrations. The enlistment fields are accepted client can login with his accreditations. The client's can set Cover picture, Profile photographs and can include companions. The companion solicitation will be dispatched to end client account and will be promptly accessible once he signed in. He can acknowledge/reject the companion demand. The companion rundown is appeared in the right board and can have the capacity to visit with the beneficiary private way.

(B) Sharing Posts with Access Control

In this Module, The client's (users) can post a few News, Images, Videos and some other data. These posts can be imparted to companions with access control. The mutual posts can be seen by companions in the event that they have appropriate access control once they login. Companions can answer to the posts with a few remarks and like/abhorrence the posts.

(C) Reviews/Likes, Posts/Views through Android Application

In this Module, clients initially need to introduce the OSN application in their Android telephone and client need to login with their legitimate record. After login server can ready to keep up their gps position of the client and Bluetooth MAC location and IMEI. The Server monitors every one of the clients gps organizes and the downloaded record substance if a download demand ascends from the client. An administration string will be keep running in android application which consistently overhauls the gps directions to the server if any change happens. The gps position is implied just if there a change advised which diminishes the correspondence overhead between the customer and server. The server will be in a push mode at whatever point a post is activated to the android cell phone. Our Image pressure method empowers the client to see packed picture without obscure and diminish the information utilization. All the post can be seen in android and web application.

(D) Downloading/Transferring of Data via P2P

On the off chance that any of the user need to see the post e.g. (Video/Image) the solicitation is sent OSN Server which will turn upward for the adjacent gadgets. In the event that there is one or more gadgets in close closeness, the server will check for the authentic download solicitations of each adjacent client for substance. In the event that the substance is accessible with any of the client, server triggers both the adjacent gadgets (Content requester, Content dispatcher) in back end Service Thread that officially running in the cell phones to start a Bluetooth correspondence. Here we took care of both matched and in addition unpaired gadgets and this is through pre sharing of Bluetooth ids by server to neighboring gadgets. After effective Bluetooth introduction the substance will be exchanged from source versatile to destination portable. The protection of the whole client is held by having pseudo personalities for every one of the interchanges. The clients don't know about distributed correspondence that is going on in the back end, consequently guaranteeing the security.

```
U=user
If((user==registered)&& (user>=5times))
Encrypt the data using RSA(Accept the user)
If(Authorized user==user)
(
Check nearby device availability
If (Device==Available)
(
Request forwarding device
If (Accept the device)
{
Send the message and download the data and Check the ACK
}
}
Else
{
Reject the connectivity
}
```

ALOGORITHM:SECURE DOWNLOAD DEVICE TO DEVICE COMMUNICATION

VII. SOFTWARE AND HARDWARE REQUIREMENTS

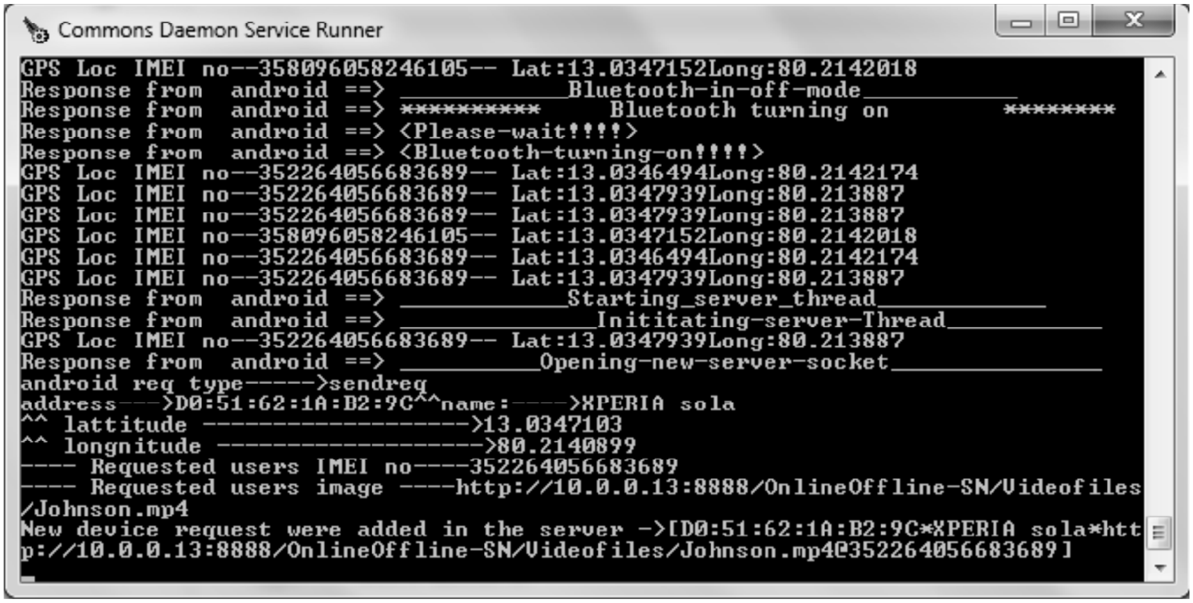
Serial No	*Experimental Setup*	
	Support Needed	*Specification*
1	Number of system	5
2	Accessing Time	30 minutes
3	Protocol Needed	IPv4
4	Total RAM size	1024MB
5	Software Tools	JDK 1.6, Tomcat (JSP, Servlet)
6	Database	Mysql 5.0
7	OS	Android

VIII. EXPERIMENTAL RESULTS

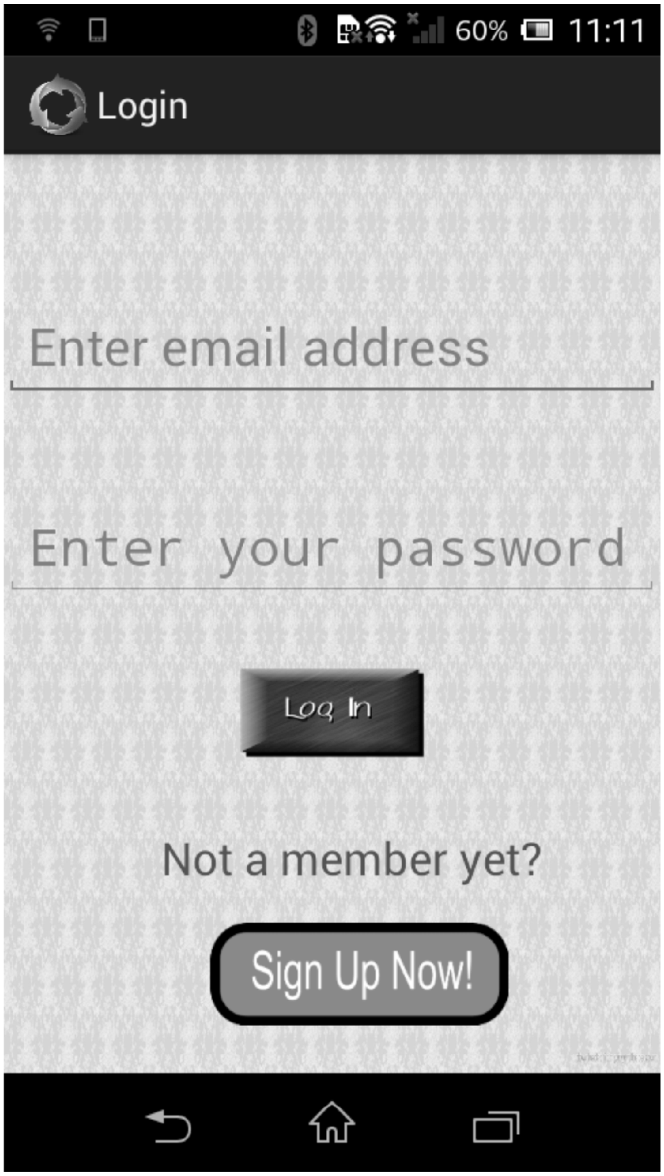
The above screenshots illustrates how using multimedia file download and file transfer is done in such a way that offline downloading of the files is facilitated.

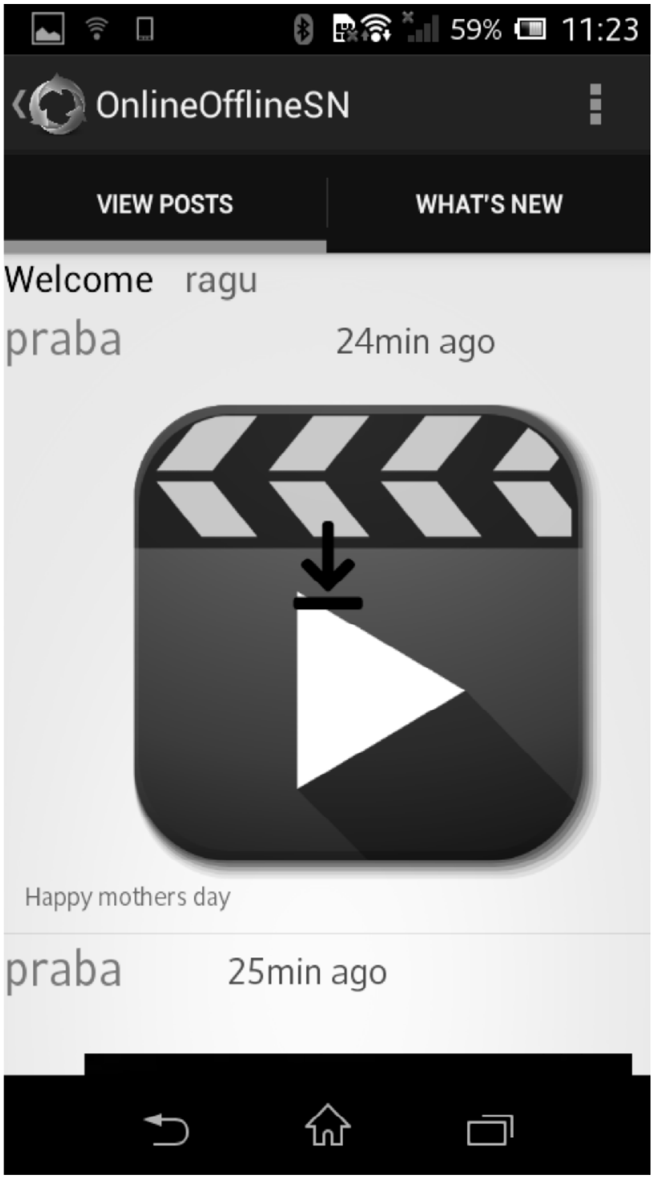
IX. CONCLUSION

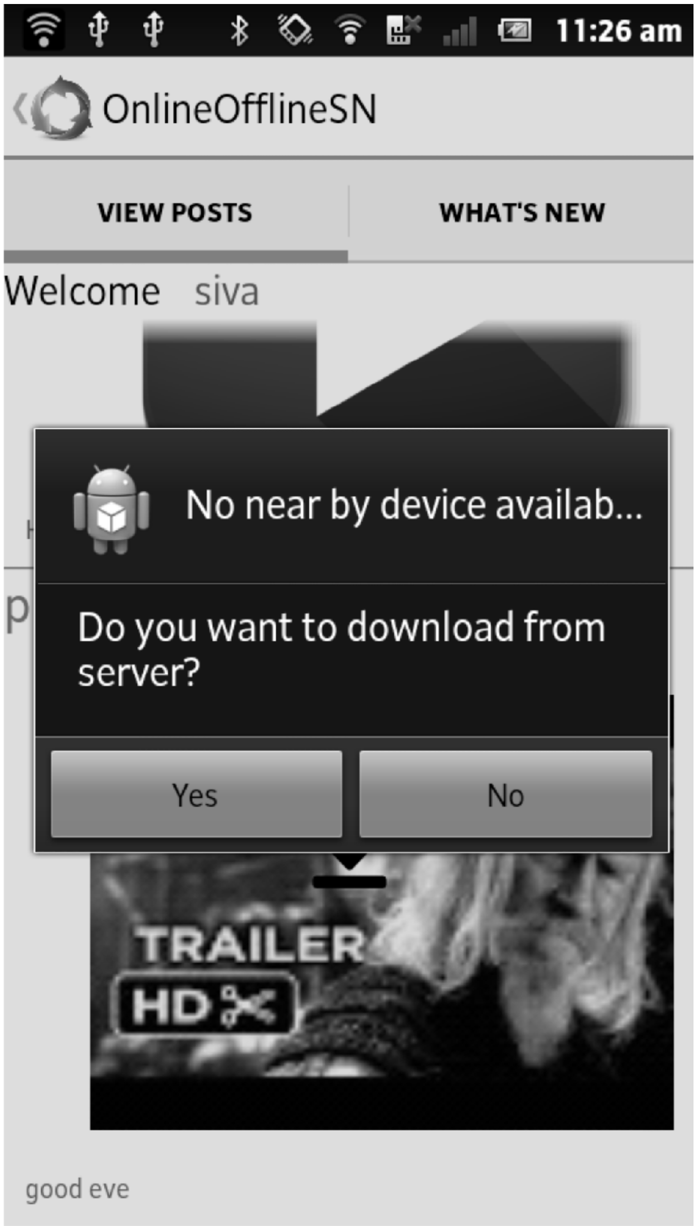
Using cloud services in mobile applications, we are communicating from one person to other. The device to device communication is used to download content from various videos, which reduces workload in the mobile network architecture. By sharing the data measure, it is easy for the aggressor to deduce the data in the channel. Informal communication is used by the social media communication networks, which are often tracked by various assailants. The D2D corresponding is used to reduce bandwidth utilization, network activity and server load. The security and neighbour concerns are used for security and protection concerns.



```
GPS Loc IMEI no--358096058246105-- Lat:13.0347152Long:80.2142018
Response from  android ==> ____________Bluetooth-in-off-mode___________
Response from  android ==> **********     Bluetooth turning on       ********
Response from  android ==> <Please-wait!!!!>
Response from  android ==> <Bluetooth-turning-on!!!!>
GPS Loc IMEI no--352264056683689-- Lat:13.0346494Long:80.2142174
GPS Loc IMEI no--352264056683689-- Lat:13.0347939Long:80.213887
GPS Loc IMEI no--352264056683689-- Lat:13.0347939Long:80.213887
GPS Loc IMEI no--358096058246105-- Lat:13.0347152Long:80.2142018
GPS Loc IMEI no--352264056683689-- Lat:13.0346494Long:80.2142174
GPS Loc IMEI no--352264056683689-- Lat:13.0347939Long:80.213887
Response from  android ==> ____________Starting_server_thread____________
Response from  android ==> ______________Inititating-server-Thread___________
GPS Loc IMEI no--352264056683689-- Lat:13.0347939Long:80.213887
Response from  android ==> __________Opening-new-server-socket_______________
android req type----->sendreq
address--->D0:51:62:1A:B2:9C^^name:---->XPERIA sola
^^ lattitude ------------------->13.0347103
^^ longnitude ------------------->80.2140899
---- Requested users IMEI no----352264056683689
---- Requested users image ----http://10.0.0.13:8888/OnlineOffline-SN/Videofiles
/Johnson.mp4
New device request were added in the server ->[D0:51:62:1A:B2:9C*XPERIA sola*htt
p://10.0.0.13:8888/OnlineOffline-SN/Videofiles/Johnson.mp4@352264056683689]
```







Welcome siva

No near by device availab...

Do you want to download from server?

good eve

REFERENCES

[1] M. Cagalj, S. Capkun, and J.P. Hubaux, “Key agreement in peer-to-peer wireless networks,” in Proc. IEEE (Special Issue on Cryptography and Security), 2006.

[2] A. Asadi and V. Mancuso, “Energy efficient opportunistic uplink packet forwarding in hybrid wireless networks,” in Proceedings of the fourth international conference on future energy systems, ACM pp. 261-262, 2013.

[3] K. Doppler, M. Rinne, C. Wijting, C.B. Ribeiro, and K. Hugl, “Deviceto-device communication as an underlay to LTE-advanced networks,” *IEEE Communications Magazine*, Vol. 47, No. 12, pp. 42-49, 2009.

[4] K. Doppler, M. Rinne, C. Wijting, C.B. Ribeiro, and K. Hugl, “Deviceto-device communication as an underlay to LTE-advanced networks,” *IEEE Communications Magazine*, Vol. 47, No. 12, pp. 42-49, 2009.

[5] C. Yu, K. Doppler, C.B. Ribeiro, and O. Tirkkonen, “Resource sharing optimization for device-to-device communication underlaying cellular networks,” *IEEE Trans. Wireless Commun.*, Vol. 10, No. 8, pp. 2752-2763, 2011.

[6] C. Yu, O. Tirkkonen, K. Doppler, and C. Ribeiro, “Power optimization ofdevice-to-device communication underlaying cellular communication,”in Proc. IEEE ICC, pp. 1-5, 2009.