Wifi AP Based Secure Data Sharing Among Smartphones And Computer System

Miss. Rachana N. Sawade
Student of M.E: Information Technology
P.R.M.I.T&R, Badnera
Amravati, India
rachanas56@gmail.com

Prof. P. V. Dudhe
Assistant Professor: Information Technology
P.R.M.I.T&R, Badnera
Amravati, India
preeti.dudhe@rediffmail.com

Abstract—Smartphones operate independently of each other, using only local computing, sensing, networking, and storage capabilities and functions provided by remote Internet services. It is generally difficult or expensive for one smartphone to share data and computing resources with another. Coordinating smartphone data and computing would allow mobile applications to utilize the capabilities of an entire smartphone cloud while avoiding global network bottlenecks. In many cases, processing mobile data in-place and transferring it directly between smartphones would be more efficient and less susceptible to network limitations than offloading data and processing to remote servers. The main objective of this paper is to introduce a methodology to provide flexible media content sharing by exploiting collaborative amongst WiFi devices via the temporarily-established links over the local server which is based on heterogeneous mobile which is having different mobile platform, users connected to the server like computer System via Wi-Fi. The realized prototype devices altogether show improved sharing performance by supporting two-times more concurrent devices at target media quality when compared with conventional non-collaborative. In this the client and local server will upload or retrieve the data in authenticated and in confidential manner. The proposed method is based on sending/receiving data between client server via Wi-Fi connection without the need of taking any service from mobile service provider and without the use of internet connection.

Keywords- *Network, Heterogeneous Mobile, Data Integrity, Authentication, Confidentiality*

*****

I. Introduction

Mobile phones are unquestionably the fastest-spreading and most widely adopted personal computing technology in history. Not only have cellular subscription rates jumped from 1 out of 5 people to 1 out of every 2 people worldwide over the last five years, but more phones were sold alone than the total number of PCs and laptops in use today. Moreover, with their small size and the convenience they offer for continuous personal and professional connectivity, cell phones are widely considered an essential accompaniment to life beyond the home. Yet despite the mobile phone's rapid adoption for voice and text communication, they have remained relatively underutilized for data-oriented productivity tasks. Thus in our research, we are exploring how mobile phones ever-increasing accessibility, storage and computing capabilities can be leveraged to promote efficiency in the workplace, particularly when workers are away from their desks.

It would be hard to imagine a world without wireless applications and services. Around the globe, mobile services are playing increasingly important roles in many facets of our society. Just a decade ago, mobile considered primarily of basic voice communication. Today, we depend on mobile services not only for communication, but also for education, entertainment, healthcare, location and m-commerce.

There is an opportunity to harness the collective sensing, storage, and computational capabilities of multiple networked phones to create a distributed infrastructure that can support a wealth of new applications. These computational resources and data are largely underutilized in today's mobile applications. Using these resources, applications could conveniently use the combined data and computational abilities of an entire network of Smartphone have to generate useful results for clients both outside and within the mobile network. Mobile services have also made significant inroads into developing nations, by improving the quality of life for many of their citizens [1].

Using mobile offers advantages over using traditional hardware such as computational access to multimedia and data without large network transfers, more efficient access to data stored on other mobile devices, and distributed ownership and maintenance of hardware. Such a concept inevitably gives rise to many concerns, including access-control, privacy, and mobile resource conservation. At the same time, this concept may create many opportunities for interesting new applications and for more resource-efficient versions of existing applications. Some of major requirements of secure data sharing in the server are as follows. Firstly the data owner should be able to specify a group of users that are allowed to view his or her data. Any member within the group should be able to gain access to the data anytime, anywhere without the data owner's intervention. No-one, other than the data owner and the members of the group, should gain access to the data, including the Service Provider. The data owner should be able to add new users to the group. The data owner should also be able to revoke access rights against any member of the group over his or her shared data. No member of the group should be allowed to revoke rights or join new users to the group [2].

A more scalable way to support multimedia sharing from mobile devices is to host files on phones and distribute queries and summarization tasks across many nodes, eliminating the need for each user to upload large files to and retrieve files from remote services. Instead, large transfers could be performed directly within local networks. For data transmission systems a number of alternative wireless technologies have been proposed, such as infrared ,ultrasound, Wireless LAN, Radio Frequency Identification , Bluetooth, wireless sensor networks [3][4].

Wi-Fi based data transmission systems have gained more attention, mainly for their widespread deployment and low cost. We discuss the growing need for data sharing among heterogeneous mobile devices and the benefits of data sharing via the local server. We list the requirements of data sharing in the server followed by the traditional approach to sharing data.

II. Literature Review

In the past few years, several different approaches to collaborative sharing of data using different devices have been proposed this section will explore some of the research approaches.

Mr. Bhoopesh kumawat Sudhendra Pal Singh Chandra Prakash Verma[5], The main objective of this paper is to introduce a methodology to provide instant Messaging Service over the intranet which is addressed to android based smartphone and tablet users connected over intranet via Wi-Fi. The proposed method is based on sending/receiving messages in intranet through intranet server via Wi-Fi connection without the need of taking any service from mobile service provider and without the use of internet connection.

Priya Mehrotra, Tanshi Pradhan and Payal Jain[6],The main objective of this paper is to introduce a methodology to provide instant Messaging Service over the intranet which is addressed to android based smartphone and tablet users connected over intranet via Wi-Fi. The proposed method is based on sending/receiving messages in intranet through intranet server via Wi-Fi connection without the need of taking any service from mobile service provider and without the use of internet connection. In this paper, we shall be discussing the pros and cons of BlueStacksApp Player which has been designed to enable Android applications to run on Windows PC. We will show or discuss this by using Bluestacks software which will provide an efficient and fast way to perform instant messaging which will further increase the performance. With IM, you can keep a list of people you interact with. You can IM with anyone on your buddy list or contact list as long as that person is online. You type messages to each other into a small window that shows up on both of your screens.

Rushabh Balpande, Chetan Dusane, Khushboo Kashyap, Nandkumar Patil Prof. Sunita Patil[7]The proposes a system that can be used for communication between peoples located at different places using a chat application which is secure and it uses client server architecture to connect peer-to-peer networks. The system is proposed for an organization in which the administrator can communicate with the project leader and programmer. The administrator which acts as server can keep track of the login time and logout time of the employee which acts as a client. The proposed system uses Node.js technology also known Node and it is a server-side JavaScript environment. Node.js is based on single as well as multiple thread by thread execution. The proposed system uses CompuP2P uses peer-to-peer networks for sharing of computing resources. The proposed system uses Collaborative Locality-aware Overlay Service (CLOSER), an architecture whose aims is to lessen the usages of expensive international links by exploiting traffic locality. It also includes the privacy module that may arouse the user interest and encourage them to switch to the new architecture. The proposed method based on sending/receiving messages in intranet through intranet server via Wi- Fi connection without the need of taking any service from mobile service provider and without the use of internet connections.

Hayoung Yoon, Student Member, IEEE and JongWon Kim, Senior Member[8], This paper, proposed DOMS (Decentralized collaborative Media content Streaming) that realizes flexible media content sharing by exploiting collaborative segment-based streaming amongst WiFi devices via the temporarily-established direct links. They implement the DOMS prototype devices with embedded computing machines and verify its performance under several realistic experimental configurations. The realized prototype supporting two-times more concurrent devices at target media quality when compared with conventional non-collaborative (i.e., client-server) streaming In home networks, it has been challenging to provide flexible and scalable media content sharing among heterogeneous consumer electronic devices. Upcoming industrial standard WiFi-Direct will prompt the popular WiFi-equipped devices to establish instant ad-hoc peer-to peer (i.e., direct) connectivity

III. System Anlysis And Design

A. System Analysis

The entire project is basically based on the client server model, request handling. So in order to proceed with the project development it is quit necessary to have a background of how the client server approach function. The following section describes the necessary concepts of client server model.

a) Client Server Model

The most common model for distributing a system is the client server model. The model is fairly simple to explain.

Initially when a server is started up its first opens up a particular port through which client can access it. It then sits downs and waits until somebody attempts to connect it. This connection takes place using so called sockets.

- Server
- Client

Server

Server is used for handling multiple connections sequentially. Clients have to queue up and they are handled one by one. If there are number of clients requesting at a same time ,then a parallel connection is made. We can handle number of connections using the threads. Each time the connection is established ,a new thread is created and connection is given to that thread. The server thread then continues accepting new connections. Because creating threads is an expensive process threads are usually kept in a pool. When a thread finished its job, it is kept alive until a new request has arrived it can handle.

Client

For the client to connect it must know the server IP address or hostname or port name to connect to. Once connection is establish the client and server can exchange messages. Depending on the distributed system a client may connect to multiple servers. One server to access the database, one for file services, another for e-mail for example.

b) Secured Data Communication Channel

Based on IDC survey (International Data Corporation) the security and vulnerability market should exceed revenue of $4.4 billion by the end of 2013, with a climbing annual growth rate resulting in a compound annual growth rate (CAGR) of

10.8%. This study shows that products that reduce within the security and vulnerability management market will remain in high demand.

There are no flawlessly secure channels in the real world. Channel is a media through which data is travels. There are only ways are present to convert insecure channels into less insecure. In the encryption the plan is to implement symmetric key encryption technique which uses same key for the encryption and for decryption. And this key is generated by the user and going to send the key to only trusted party which are going to update our information based on some emergency situation like medical problem.

c) Requirements:

Every security system must provide a bundle of security functions that can assure the secrecy of the system. These functions are usually referred to as the goals of the security system. These goals can be listed under the following five main categories (Earle, 2005):

- Authentication: The process of proving one's identity. This means that before sending and receiving data using the system, the receiver and sender identity should be verified.
- Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver. Usually this function is how most people identify a secure system. It means that only the authenticated people are able to interpret the message content and no one else.
- Integrity: Assuring the receiver that the received message has not been altered in any way from the original. The basic form of integrity is packet check sum in IPv4 packets.
- Non-repudiation: A mechanism to prove that the sender really sent this message. Means that neither the sender nor the receiver can falsely deny that they have sent a certain message.
- Service Reliability and Availability: Since secure systems usually get attacked by intruders, which may affect their availability and type of service to their users. Such systems provide a way to grant their users the quality of service they expect.

B. System Design

1) Proposed System Modules:

a) Proposed System Module for Client

- New User Registration.
- Client Login
- Upload Plain/Encrypted data file on server.
- Key Generation.
- Sending key.
- Download Plain/Encrypted data file from server.

b) Proposed System Module for Server

- Database

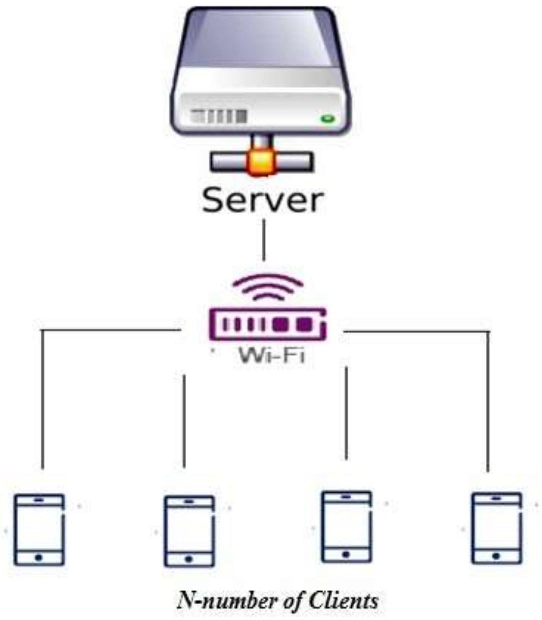

Figure 1. General architecture diagram

2) Proposed System

In this paper, we propose an system that allows Smartphone users to send and receive data or the file over via Wi-Fi which requires neither any internet connectivity nor any service from the mobile service providers as shown in figure 1. The motivation is to allow the Smartphone users using any platform to communicate for sharing the data without paying any internet data charges.

IV. Implementation

In this paper, we implement system that allows Smartphone users to send and receive data or the file over the server via Wi-Fi which requires neither any internet connectivity nor any service from the mobile service provider's .Smartphone users can communicate through the service which is developed and deployed on the server. This service allows users to communicate with each other via Wi -Fi network without using any internet connectivity. When a user wants to send a data or the file to another user, a request goes to the server and now it is the responsibility of the server to deliver the data or file to the receiving party successfully.

Proposed architecture basically consists of client and server module which may include the following steps

- First of all server program runs on server machine.
- Then client program runs on mobile device and send a request to connect with server.
- Once the client is successfully connected, it will allow the user to communicate w other the active users to the client.
- Client can view the list of all users and can communicate with them

We have merge the two algorithms which provides security for sharing the data or the files. That algorithms are Advanced Encryption Standard and Message digests (MD5).The main purpose of using this algorithm is to provide security.

For integrity of data, we have used Checksum MD-5 code while storing and accessing the file. Checksum MD-5 code is used to provide intrusion tolerance for data servers.

Performance analysis shows that the proposed scheme is highly efficient and resilient against data modification hit on data.

Authentication is operation of verify the truth of an entity or genuine user. This might involve confirming the identity of a software program or person. Here we will provide user id and password for validation of legitimate user. Confidentiality is a set of rules that limits access or places limitations on certain types of information. To maintain confidentiality of data there will be provision for encryption of data using cryptography tool.

In the encryption the plan is to implement AES symmetric key encryption technique which uses same key for the encryption and for decryption. And this key is generated by the user and going to send the key to only trusted party who are going to used the data.

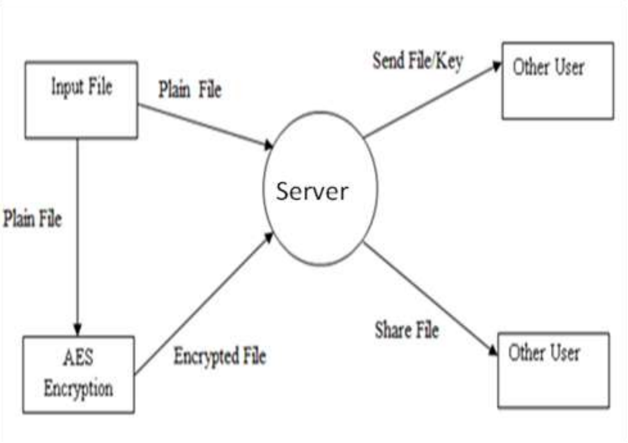

Figure 2. Data flow Diagram for input file

V. CONCULSION

This paper presents an idea to develop a service for the users; this service will be deployed on the server of any organization that allows smartphone user to send and receive data within an organization at free of cost. This communication does not need to interact with mobile service provider or no need to take any data plan. Internet connectivity is also not required. So this way it reduces the cost of communication and increases the communication between various devices which gives compatibility between the users which provide an efficient communication by increasing its performance. It can be downloaded free of cost, so it is economical also.

ACKNOWLEDGMENT

I would like to wish to the Head of the Department of Information Technology& my guide Prof. P. V. Dudhe madam for the encouragement& support, which lead to enhancement of the paper work.

.

REFERENCES

[1] Ian F. Akyildiz, TommasoMelodia, and Kaushik R. Chowdhury. "A survey on data sharing in wireless Computer Networks", International conference on network computing, Volume 3, pages 921–960, Nov 2006..

[2] Huang R, Gui X, Zawel, "A. Enterprise need for public and private wireless LANs. Wireless/Mobile Enterprise Commerce", The Yankee Group, 2nd International Conference on Computer Engineering and Technology (ICCET 2010). Vol. 7, pp. v7- 700 – v7-707, 2010

[3] Sen Zhang1, Wendong Xiao1, Baoqiang Zhang2, Boon Hee Soong3 "Wireless Indoor Localization for Heterogeneous Mobile Devices", IEEE 978-1-4673-1697-2/$31.00 ©2012.P.C.

[4] Sanjay P. Ahuja and Jack R. Myers, "A survey on wireless grid computing". International Journal of Computer Science and Security (IJCSS), Volume (5): Issue (1): 2011,pp12-15

[5] Mr. Bhoopesh kumawat Sudhendra Pal Singh Chandra Prakash Verma, "Intranet Based Messaging Service on Android Smartphones and Tablets", International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, ISSN: 2277 128X Issue 7, July 2013.

[6] Priya Mehrotra, Tanshi Pradhan, and Payal Jain, "Instant Messaging Service on Android Smartphones and Personal Computers", International Journal of Information and Computation Technology.ISSN 0974-2239 Volume 4, Number 3 (2014), pp. 265-272

[7] Rushabh Balpande, Chetan Dusane, Khushboo Kashyap, Nandkumar Patil Prof. Sunita Patil "CLIENT SERVER BASED SECURE CHAT APPLICATION USING PEER-TO-PEERNETWORK ARCHITECTURE" International Journal of Emerging Trend in Engineering and Basic Sciences (IJEEBS) ISSN (Online) 2349-6967 Volume 2 , Issue 1(Jan-Feb 2015), PP223-230

[8] Hayoung Yoon, Student Member, IEEE and JongWon Kim, Senior Member, "Collaborative Streaming-based Media Content Sharing in WiFi-enabled Home Networks", IEEE 0098 3063/10/$20.00 © 2010

.