CMD: Call, Message and Data transfer by Proper Utilization of Available Range

Himanshu Kolhe[1] Akshay Deshmukh[2] Suraj Kapse[3] Gaurav Dhakane[4] Sphurti Deshmukh[5]
[1,2,3,4,5]Jawahar Education Society's, Institute of Technology, Management & Research, Gowardhan, Nashik

Abstract— Today, we Surrounded by wireless connectivity where everyone prefers to be online without a bundle of wires. Communication through mobile phones comes at a certain expense. The proposed system will reduce this expenses at a certain level and make this communication a cost-free communication. The purpose of this project is to make use of available resources for providing efficient free voice calls, without using service provider. The co-workers of an organization, colleagues or staff members can communicate with each other by using the range of router, but without internet. No burden on institute or organization as infrastructure cost is reduced. This system can prove as the best alternative for existing intercom system.

Key words: VOIP, Android, Wi-Fi peer to peer, Router, Socket, TCP, Privacy, AES algorithm, Encryption, Decryption, Private Key

I. INTRODUCTION

Wide development of electronic devices such as mobiles, I-pads, tabs, etc which is known as smart devices now a day's; along with the implementation of sensors which are available at low cost have proved to be beneficial for improving the quality the message transfer and reception. Remote mobile message transmission and reception is growing trend towards Digital india. In Communication has developed from a simple mobile-phone to an extended technological smart-phone thus increasing the functionality and user interactivity. Due to its increasing portability and simplicity, it can be seen today in everyone's pocket. Thus providing users with cheaper and smarter phones has become a lucrative business for many manufacturers.

With the increasing expectations for Cell-phone devices, there is an increase in the number of service providers too. But the cheaper service providers usually win over the costlier ones.

Service providers that have already earned a name are still expanding further and further to earn recognition throughout the globe. With the worldwide communication between people through mobile phones increasing daily, it is necessary to reduce the costs of data transmission for texts, voice or video.

The concept behind Project is to avoid interruption in calls and to make it possible for long distance transmission and at a higher efficiency. This concept being very useful and productive has made a mark in the field of data transmission. There has been increasing demands to have cheap communication within a fixed range, like an office, in a building or a township. The recent advancements in The mobile phone technology have incorporated the features of accessing Wi-Fi from a very small device. The presence of Wi-Fi in the latest mobiles allows the user to access internet with the help of a Wi-Fi router. Exploiting the entire bandwidth of 2.4ghz for making voice calls between devices, it eliminates the need of using the service provider's bandwidth. Hence voice calls, messaging and videoCalls can be made at zero cost. Almost all of the recent launches of phones comes with Wi-Fi. The number of people using Wi-Fi devices is increasing day-by-day.

Our proposed model would eliminate the use of service providers and would provide zero cost communication for short distance.

The base idea is unifying voice and data onto a single network infrastructure by digitizing the voice signals, convert them into IP packets and send them through an IP network together with the data information.[be expert at the attacks and also expert at escaping the intrusion attack.

In this paper we will be designing a system known as "CMD : Call, Message and Data transfer by proper utilization of available range". We will firstly identify he problems related to the design of privacy protection and then the solutions will be provided. So that we understand it without any problem we will start with the basic structure so that we can understand all the possible privacy schemes. After understanding the privacy scheme we will give an improved solution to the privacy scheme observer by us. In AES algorithm, the keys will be generated between the client and theserver. The data will be encrypted using the key generated and the decryption process will also be done be using the same key. The key will not be stored on the cloud. It will be with the respective client and the server. Once the communication starts between the server and the client the exchange of the data done will also be in the encrypted form. For that purpose also the key will be generated. In short 2 keys will be generated i.e. First key for authentication purpose and the second key for the purpose of the safety of the data exchange done between the client and the server.

II. SYSTEM MODEL

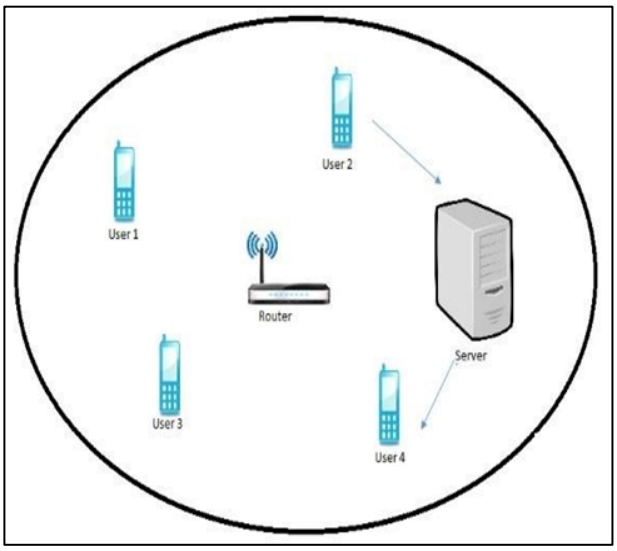

Fig. 1:

We would first like to elaborate our paper "CMD". Medicare consists of 7 different modules. The modules are as follows.

1) Caller Module
2) Router Module
3) Receiver Module

A. Caller Module:

Wi-Fi enabled cell phone with Android operating system opens an application and it receives the list of users. Reachable users are shown by green bubble. Other names are shown by red bubble which indicates unreachable users. User selects the name of callee. He is provided with facility to identify the callee as per the selection of department, designation. Once he is connected to the callee, he can start voice communication Algorithms Used.

B. Router Module:

Sending the list of reachable user is the first task when any user opens an application. Here server and router together take decision of users' reachability. Server pings a list of users categorized under above parameters. Accepting the request from caller and placing a call is another responsibility of this module. On demand of user, server has to refresh the list of Available users.

C. Receiver Module:

This module allows receiver to receive call. Retrieving the voice file when router intimates about voice file.

D. System Flow:

Firstly User enters into the router area if user is authenticated then user will get connected to router. Server assign IP if user is new. Uer can able to communicate with another user which resides in same area of roter ,if user is not available for communication with whom first user wants to communicate the user will wait for second user.

After successful connection between client and server client can communicate with server via call, message or he can easily transmit files.

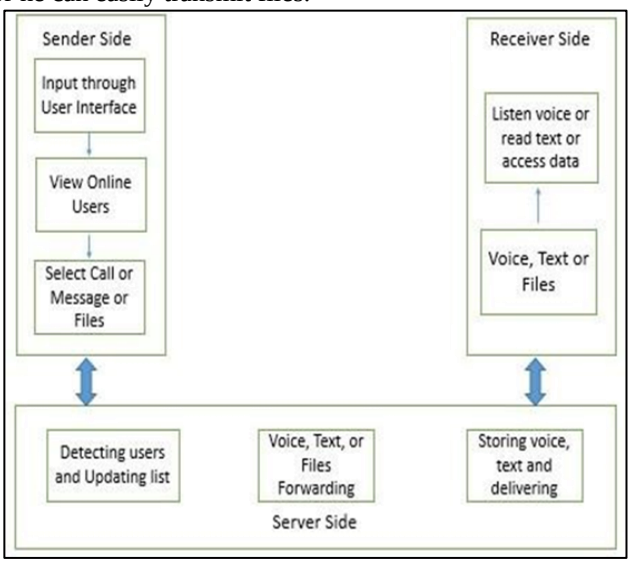

Fig. 2:

III. Implementation

A. Web Socket:

Websocket is a computer communications protocol, providing full-duplex communication channels over a single TCP connection. The websocket protocol was standardized by the IETF as RFC 6455 in 2011, and the websocket API in Web IDL is being standardized by the W3C. Websocket is designed to be implemented in web browsers and web servers, but it can be used by any client or server application. The websocket Protocol is an independent TCP-based protocol. Its only relationship to HTTP is that its handshake is interpreted by HTTP servers as an Upgrade request.[1] The websocket protocol enables interaction between a browser and a web server with lower overheads, facilitating real-time data transfer from and to the server. This is made possible by providing a standardized way for the server to send content to the browser without being solicited by the client, and allowing for messages to be passed back and forth while keeping the connection open. In this way, a two-way (bi-directional) ongoing conversation can take place between a browser and the server. The communications are done over TCP port number 80 (or 443 in the case of TLS-encrypted connections), which is of benefit for those environments which block non-web Internet connections using a firewall. Similar two-way browser-server communications have been achieved in non-standardized ways using stopgap technologies suchas Comet.

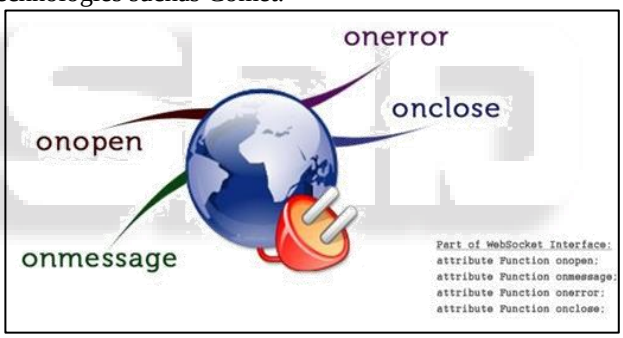

Fig. 3: Web Socket

Fig. 4: Data Transfer

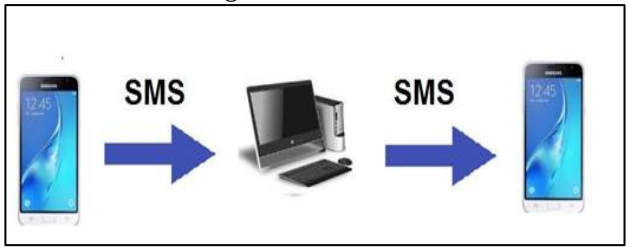

Fig. 5: Message

B. Working:

When user will open the app the wifi of the mobile device is turned on automatically. The mobile device is connected to the proper router and then user need to create his profile by

entering his name and register to the app. After creating the profile user will see the online user list. The users which are active on the same time will be shown in the list. User need to click on the name of the user and will open the chat window. User can send text messages to the another user. There is an option of file attachment from where user can select the file to be send. There is an option of call where user will get the list of active users.

C. AES (Advanced Encryption Standard)

AES stands for Advanced Encryption Standard. This algorithm is a symmetric encryption algorithm. The two cryptographers Joan Daemen and Vincent Rijmen developed this algorithm. This algorithm was designed to be effective on both hardware and software and block length of 128 bits is supported and also key length of 128, 192, and 256 bits is supported.

The AES algorithm consists of 2 parts i.e. Encryption and decryption. Encryption means conversion of the pain text into cipher text. This cipher text is the text which is in unreadable format. And decryption is the reverse process of encryption. This process converts the cipher text into plain text which is again in readable format.

1) Encryption:

Input: String to be encrypted Output: Encrypted value
Steps:
Begin:

Get the instance of the Cipher class i.e. Java.crypto.cipher
Step 1:
Generate the dynamic key
Step 2:

Using Base 64 encoder to encode the bytes of the given String and get the encrypted value. Return encrypted value.
End

2) Decryption:

Input: String to be decrypted Output: Decrypted value
Output: Decrypted value
Steps: Begin:
Get the instance of the Cipher class i.e. Java.crypto.cipher
Step 1:
Generate the dynamic key Step 2:
Using Base 64 decoder to decode the bytes of the given String and get the decrypted value. Return decrypted value.
End

D. Mathematical Model for AES Algorithm:

Homomorphic Encryption henc (.) This gives 2 encrypted messages:
Henc(m1+m2)= henc(M1)*henc(M2)
*: Corresponds to operation in Cipher Text M1: Message 1
M2: Message 2

It can encrypt the message under Range [r1, r2]

Receiver can decrypt the message with the privacy key corresponding to the range [r1, r2]
Encryption Anonenc (id,pp,m)
Pp : System Parameter
M:message
Id :identity
Input: M 2 M
Output: C= (C1, C2, C3)
With r= H3(mj j s) C1= gr C2=s_H2(e(H,(id),y)r) Where,
S: random element from m
Decryption
Algorithm performed by decryptor:
(c,Skid) Input: cskid Compute
C2_ H2 (e (Skid: (1)) =s c3 _ H4(s) =m
Success Case:
1) Successful login.
2) Successful Communication between patient and doctor.
Failure Case:
1) Login Failed.
2) Patient not in the range of Wi-Fi.

E. FTP Algorithm:

FTP Protocol is used to transfer the computer files between client and server on a computer network

The reports made by doctors or the previous history of reports can be send to patient or doctor by using FTP protocol.

IV. SCREEN SHOTS

A. Registration:

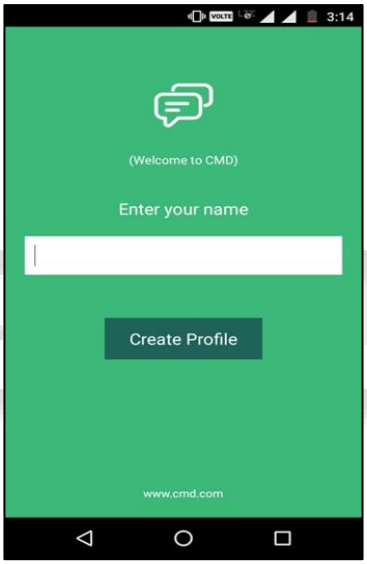

Fig. 6:

B. User List:

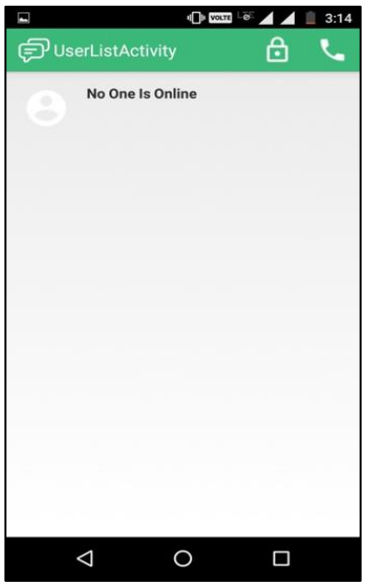

Fig. 7:

C. Online User List:

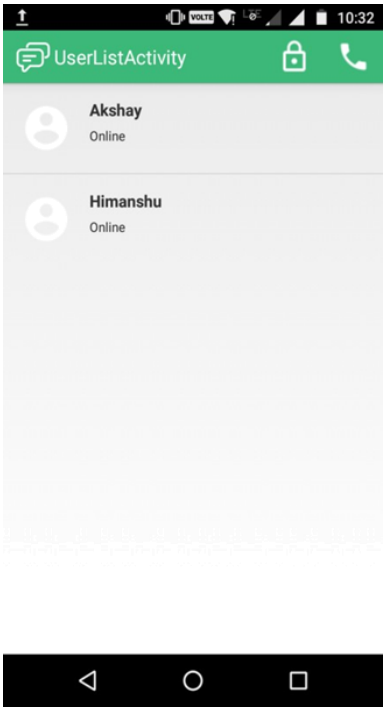

Fig. 8:

D. Server Logs:

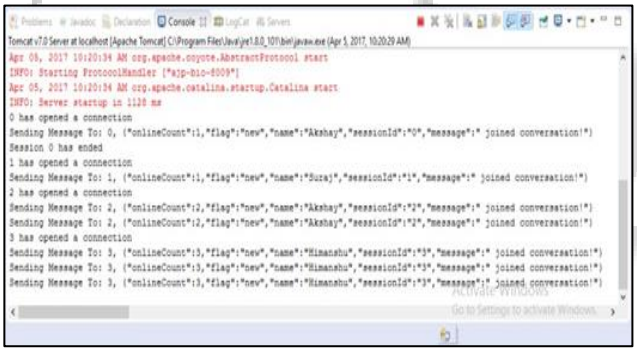

Fig. 9:

V. CONCLUSION

In this paper, we designed a "CMD" application which is a health monitoring system, which we can use to protect the privacy of the clients and also so that we can protect the intellectual property of the providers.

REFERENCES

[1] Yazdi, Nazi Tabatabaei, and Chan Huah Yong. "A poten-tial way for efficient information sharing based on mobile text messaging." Green and Ubiquitous Technology (GUT), 2012 International Conference on. IEEE, 2012.
[2] Chavan, Ramesh, and M. Sabnees. "Secured mobile mes-saging."Computing, Electronics and Electrical Technologies (IC-CEET), 2012 International Conference on. IEEE, 2012.
[3] Neetesh Saxena,Narendra S. Chaudhai "An Approach for SMS Security using Authentication Functions" , Industrial Electronics and Applications (ICIEA), 2012 7th IEEE Confer-ence on (0975 – 8887),Singapore, Digital Object Identifi-er: 10.1109/ICIEA.2012.6360809
[4] Goel, Utkarsh, Kanika Shah, and Mohammed Abdul Qadeer. "The personal SMS gateway." Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on. IEEE, 2011.
[5] Husodo, Ario Yudo, and Rinaldi Munir. "Arithmetic cod-ing modification to compress SMS." Electrical Engineering and Informatics (ICEEI), 2011 International Conference on. IEEE, 2011.
[6] Liu, Jun, Haifeng Ke, and Gaoyan Zhang. "Real-time smsfiltering system based on bm algorithm." Management and Service Science (MASS), 2010 International Conference on. IEEE, 2010.
[7] Shah, Sumiran, et al. "Zip it up SMS "A path breaking model in the field of mobile messaging"." Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE Internation-al Conference on. Vol. 4. IEEE, 2010.
[8] Shirali-Shahreza, Mohammad, and Sajad Shirali-Shahreza. "Sending pictures by SMS." Advanced Communication Technol-ogy, 2009. ICACT 2009. 11th International Conference on. Vol. 1. IEEE, 2009.
[9] Wang, Xibo, and Yanting Yang. "Method and Implementa-tion of Sending and Receiving Mobile Phone Messag-es." Computer Science-Technology and Applications, 2009. IFC-STA'09. International Forum on. Vol. 1. IEEE, 2009.
[10] Mohammad, M. A., and A. Norhayati. "A short message service for campus wide information deliv-ery." Telecommunication Technology, 2003. NCTT 2003 Proceed- ings. 4th National Conference on. IEEE, 2003.
[11] https://globaljournals.org/GJCST_Volume12/3- Voice-Calls-between-Wireless.pdf.
[12] http://www.technologyreview.com/news/402970/voic e-over-wifi-the-great-disrupter/
[13] Android real-time audio communications over local available: http://iteamserver.iteam.upv.es/revista/2012/4_ITEAM_2 012.pdf
[14] https://developer.android.com/reference/android.html
[15] AAC-ELD based Audio Communication on Android available:Http://www.iis.fraunhofer.de/content/dam/iis/de/dokumen te/amm/wp/AAC-ELD%20Android%20Application%20Bulletin.pdf
[16] Android real-time audio communications over local available: http://iteamserver.iteam.upv.es/revista/2012/4_ITEAM_2 012.pdf
[17] Mjsip home page – available: http://www.mjsip.org/index.html
[18] http://stackoverflow.com/questions/9883136/working-with-sip-and-voip
[19] RTP: A Transport Protocol for Real-Time Applications - available: http://tools.ietf.org/pdf/rfc3550.pdf
[20] C. Chafe and M. Gurevich, \Network Time Delay and Ensemble Accuracy:Effects of Latency, Asymmetry," in The 117th AESConv., October 2004,Preprint 6208.
[21] A. Spanias, T. Painter, and V. Atti, Audio Signal Processing and Coding,Wiley-Interscience, 2007

