Global Journals LaTeX JournalKaleidoscope™

Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

Secure Voip Call on Android Platform

saruchi kukkar [1]

[1] Lovely Professional University

Received: 11 December 2011 Accepted: 5 January 2012 Published: 15 January 2012

Abstract

In the Secure voice call, the human voice shall be digitized by the Android APIs and the VOIP packets will travel over the SIP layer. The digitization process also includes the encryption phase wherein secure call technique is used in order to generate unique keys every time a call handshake is done. During the Secure Call key exchange, the caller party sends a Secure Call hello packet. Once that packet is positively acknowledged by the recipient party the handshake happens successfully and the call packets get encrypted. Using Secure call, digitized voice data is transformed into cipher text form on third generation GSM data or GPRS servers in android platform which results in a better encrypted voice speed and clarity.

Index terms—

1 Introduction

OIP works by converting analog voice signal into digitized data packets. The packets are sent out across the internet the same way as any other IP packets, using the internet's TCP/IP protocol The Internet is a notoriously insecure network. Anything send across internet can be easily snooped upon. This is of particular concern when highly confidential information, such as corporate data and credit card numbers, is transmitted across the Internet. Another related concern is that it can be difficult to know whether the person sending the information is really who he says is he.

Despite of the advantages of implementing VOIP there is a main drawback of using this technology that is the security issues. Since it will be connected to the Internet and use many of the same hardware and software components. VOIP becomes vulnerable to different types of attacks such as Man in the middle attack, Denial of service or Eavesdropping.

Several ways have been developed to solve these problems. At the heart of them is Encryption, it is technique of altering information so to anyone other than the intended recipient it will look like meaningless garble. When the recipient gets the information, it needs to be decrypted that is, turned back into the original message by the recipient, and only by the recipient. In the Encrypted IP voice call this digitized voice data is transformed into Ciphertext form using encryption techniques. Hence, the encrypted voice call is very secured as compared to VOIP.

2 II.

Objectives 1) Users will be able to communicate effectively, speedily and most importantly, securely, there by enhancing the privacy and confidentiality of mobile communication.

Author : Assistant Professor Lovely Professional University. E-mail : ganpati.saruchi@gmail.com

2) Implementing voice encryption on third generation GSM data or GPRS servers which would in turn result in a better encrypted voice speed and clarity.

3) The configuration and usage of proxy server (SIP / Asterisk) through defining call routing and handset registration mechanisms. 4) It will enable the users to communicate with each other in an encrypted fashion III.

3 Research design

Research design specifies the logical structure of a research project and the plan will be followed in its execution.

Suppose A want to communicate with B through secured voice communication. A and B must have android based mobile handsets with J2ME (proposed) application installed on it which is responsible for encrypted voice communication. 1. The mobile handsets need to be registered at SIP server. 2. When A calls B the application installed on mobile handsets will convert it into encrypted data. 3. The encrypted data will travel through GPRS channels. 4. The SIP server will route the call to the registered recipient B. 5. The application installed on B handset will perform the decryption process. In the proposed work GPRS mode will be used

Step2: There would be 1 SIP server (Asterisk) and minimum 2 Android handsets. The handsets need to be registered at SIP server.

Step3: The SIP server of callcentric.com are used. SIP client is configured on both the Android handsets.

Step4: The Android application which will be developed needs to be installed on all the handsets which are registered in the SIP server and wish to communicate with each other using encrypted IP voice communication.

Step 5: The dialler will launch the Android application on his/her handset and dial the receiver's number. The dialling interface will be developed for the Android application. Once the call is made, the request will go the SIP server wherein the recipient's number will be checked and the call will be routed on its handset

Step 6: Once the recipient receives the call through the same Android application and the dialler starts the conversation, all the digitized voice data will first be encrypted on the dialler's handset by the application and then sent to the SIP server for routing to the recipient's handset. Logically, every handset will be assigned a numeric no. in the SIP server during configuration through which it will become identifiable.

Step7: The digitized voice data will travel in an encrypted fashion through the GPRS medium.

IV.

4 Technical workflow of the application

1) The caller handset uses Secure Call application to initiate the VOIP call to the recipient. 2) When the call is made, the caller handset also sends the logical number of both caller and receiver via GPRS which is cross-verified at the call centric server for genuineness. 3) Once the genuineness of both the numbers is verified the analog voice signals are digitized using the SIP stack APIs which is PJSIP used in application. SIP stack APIs are a collection of packages and functions used for the transmission of voice over IP using SIP protocol. 4) Once the call is established successfully, the caller sends "Hello Packet" in order to exchange the secure key with the recipient. The caller sends the(D D D D)

Year "Hello Packets" a couple of times. When the recipient sends the acknowledgement for the hello packet, the secure key exchange is accomplished successfully. When the secure key is exchanges, the call packets become encrypted. 5) Before the call is connected, the sender and recipient parties have to register themselves with the call centric server in order to attain a logical number which is also added in the SIP client on Android in order to synchronize with the server so that the SIP account gets activated.

6) Once the SIP account is activated the SIP call session is established using SIP stack which is the collection of APIs and the encryption is performed using ZRTP. SIP stack is written in C language. 7) There are two different projects in the application.

One project consists of the full SIP stack integration and the another deals with the Android interface design and the SIP client development.

5 Fig. 2 : Workflow of application

This application shall work on both Wi-Fi and GPRS as the communication medium and requires that we have high-bandwidth network speed. The secured communication can only occur dynamically if the sender and recipient devices are equipped with this application. Otherwise, the call would be insecure which essentially means that there would not be any Secure Call key exchange and intruder would able to decode the VOIP packets and can listen to the conversation on a media player.

V.

Significance 1) This can benefit the users to communicate with each other through digitized voice data which is free from any noise or interference in comparison to its analog variant and carries more clarity.

2) The best part of this communication will be it can be done from geographically any independent location.

3) It will enable the users to communicate with each other in an encrypted fashion which will enhance the security and confidentiality of the communication. 4) The most significant part is it support the newest generation of the mobile handset called SmartPhones which run on an advanced hardware and latest mobile operating system from Google called Android.(D D D D)

VI.

6 Implementation a) Secure Call application

The implementation of Secure Call application is done by developing several components and then joining them together. Every component signifies a specific functionality in the application. i.

7 Configuration of SIP client

This application utilizes the configuration parameters of the SIP server. Services of existing SIP servers are used. Since the development and maintenance of SIP services is a costly affair, so 3 rd party services from Callcentric.com has taken.

Additionally, as most of the SIP servers are Linux-based, configuring the SIP server also requires assignment of the dynamic IP address to the Linux server which requires high-end network configuration on Linux. And even if it is successful in that configuration, it is practically infeasible to achieve good call clarity and speed because the servers need a high bandwidth internet speed which is only applicable if we take 3 rd party services.

8 Fig. 3 : SIP Account Configuration

In the SIP account configuration, as in Fig. **??** the generic details are mentioned after which the user shall be assigned a logical number which would essentially be the telephone number of the device.

Volume XII Issue XII Version I Android SIP client named Saruchi and Logical no. 17772438110 has been created. Tap the icon to make it Active as shown in Fig. **??**. Once the account is active, the VOIP calls shall be made and received from that account only.

ii.

9 Dialler Application

In this component, once the SIP account is registered, the user will be able to dial the number of another Android SIP user through a custom-made touch-pad. In order to develop the custom touch-pad, different images of the numbers have created in the application and have used then as resources. After the user has typed the correct numbers as in Fig. **??** the Android APIs will initiate a call to the SIP recipient registered on the server. If the call is made to an invalid recipient, it will be handled by the IVR of call centric server.

iii.

10 Digitization of Voice Call

When the call is connected, the human voice shall be digitized by the Android APIs and the VOIP packets will travel over the SIP layer. Once the genuineness of both the numbers is verified the analog voice signals are digitized using the SIP stack APIs which is PJSIP used in our application. SIP stack APIs are a collection of packages and functions used for the transmission of voice over IP using SIP protocol iv.

11 Encryption Phase

The digitization process also includes the encryption phase wherein we use secure call technique in order to generate unique keys every time a call handshake is done. During the Secure Call key exchange, the caller party sends a Secure Call hello packet. Once that packet is positively acknowledged by the recipient party the handshake happens successfully and the call packets get encrypted.

i.

The Secure Call protocol does not rely on a public key infrastructure or on certification authorities, In fact ephimeral Diffie-Hellman keys are generated on each session establishment: this allows to bypass the complexity of creating and maintaining a complex third trusted party. ii.

These keys will contribute to the generation of the session key and parameters for SRTP sessions, along with previously shared secrets: this gives protection against Man-in-the-Middle attacks, assuming the attacker was not present in the first session between the two endpoints. iii.

To ensure that the attacker is indeed not present in the first session (when no shared secrets exist), the Short Authentication String method is used: the two endpoint compare a value by reading it aloud. In case the two values match, then no Man-in-the-Middle attack has been performed. preceding sessions (if any): this creates a new shared secret, from which all key material can be derived by means of one-way functions. v.

Keying material is destroyed at the end of each session, thus this protocol offers perfect forward secrecy.

v.

12 Demonstration

The encryption of packets could be successfully shown through their decoding using a packet sniffing tool in which we shall sniff the VOIP packets on an IP address by connecting the Android device via Wi-Fi on a shared network which has a public IP address. After sniffing the packets, try to decode them in order to hear the voice. The packet sniffing cannot occur in the GPRS network because we do not have an access point to can the packets. vi.

13 Installing Application on

[1]

[1] © 2012 Global Journals Inc. (US)Global Journal of Computer Science and Technology

1

Figure 1: Figure 1 :

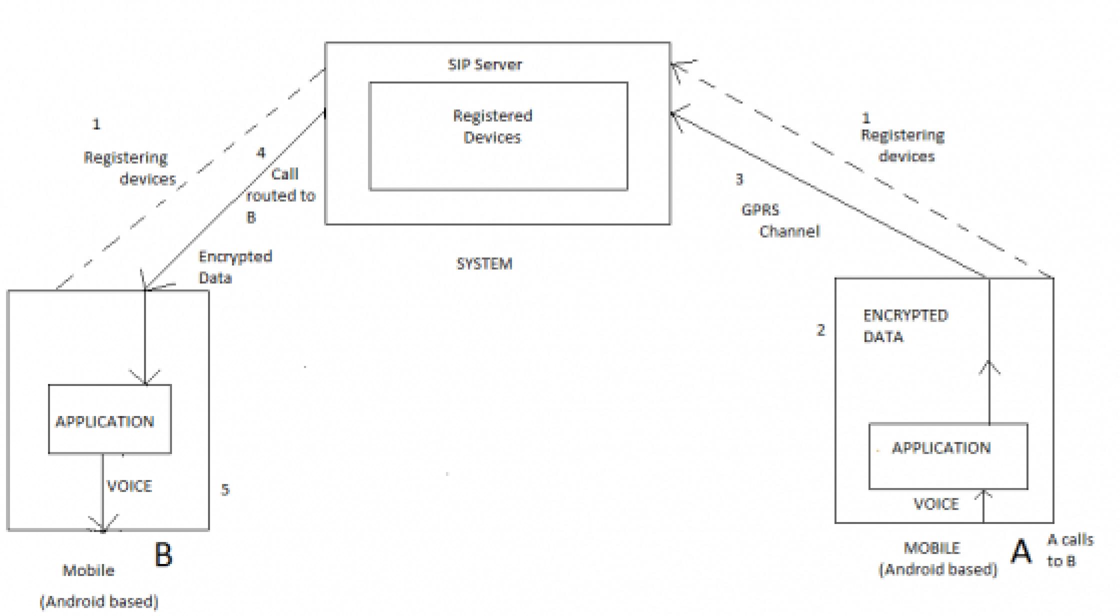
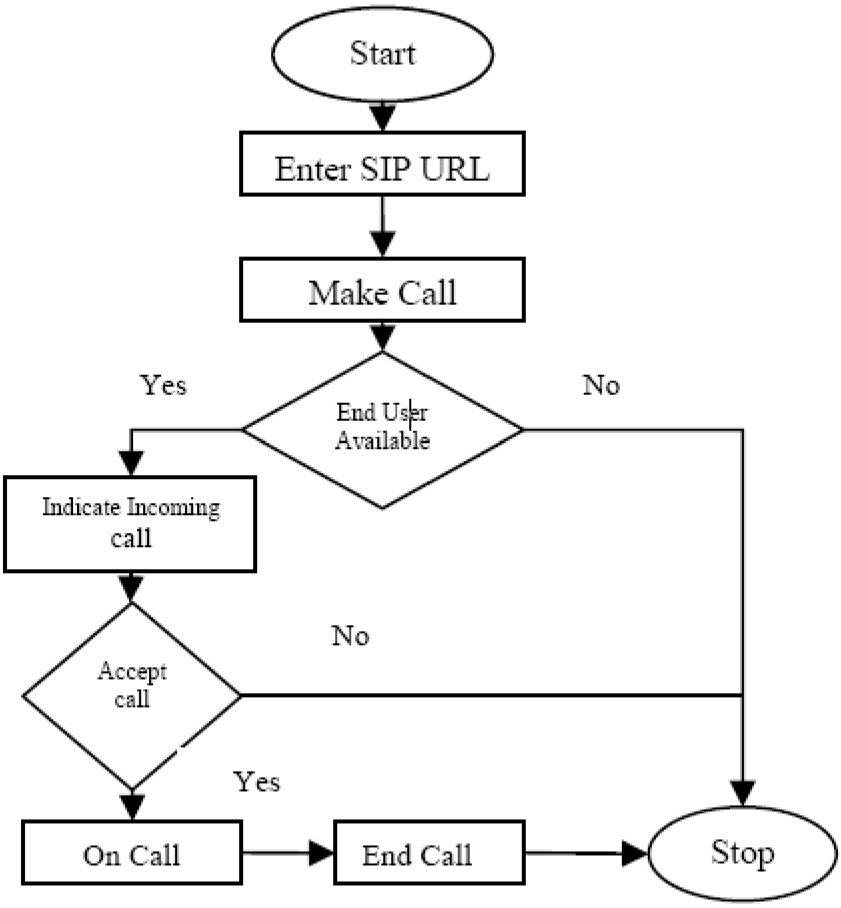
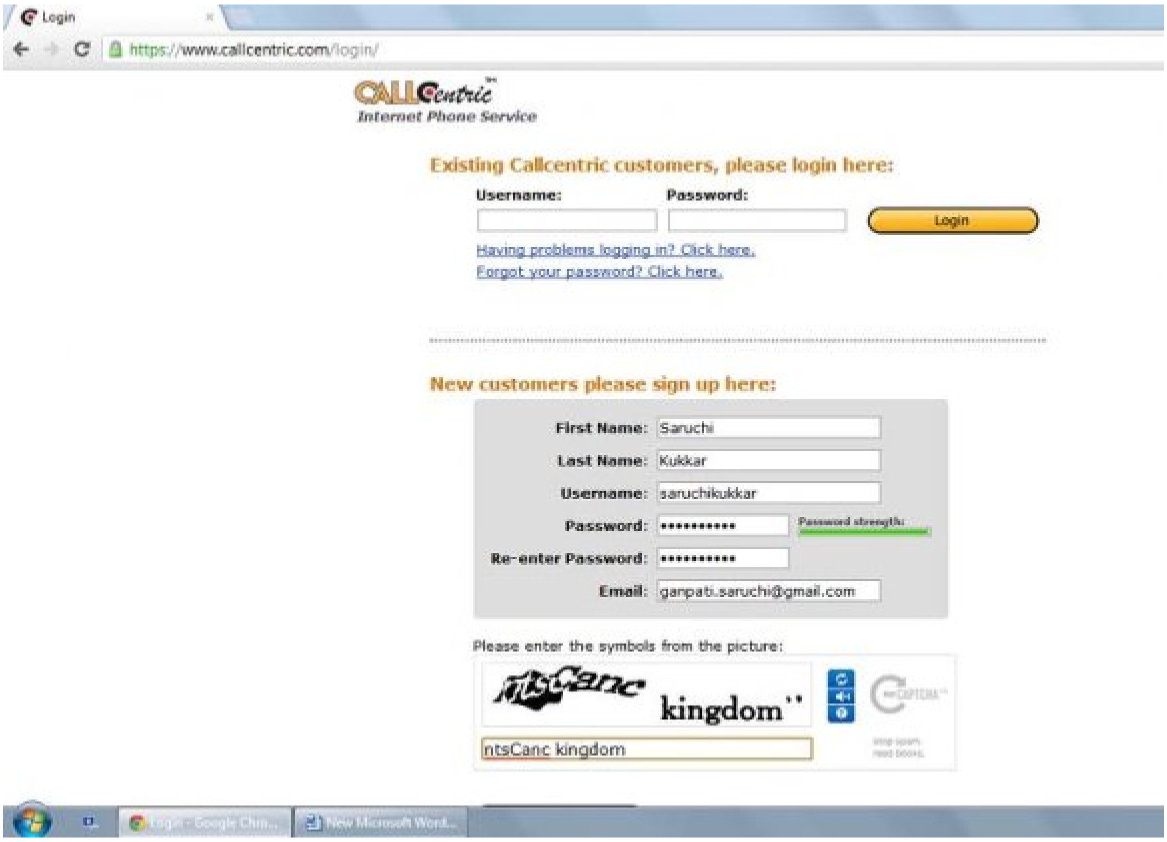
456


Figure 2: Fig. 4 :Fig. 5 :Fig. 6 :



78

Figure 3: Fig. 7 :Fig. 8 :



Existing Callcentric customers, please login here:

Username:

Password:

Having problems logging in? Click here.

Forgot your password? Click here.

New customers please sign up here:

First Name: Saruchi

Last Name: Kukkar

Username: saruchikukkar

Password: •••••••••••

Password strength:

Re-enter Password: •••••••••••

Email: ganpati.saruchi@gmail.com

Please enter the symbols from the picture:

ntsCanc kingdom

Figure 4:

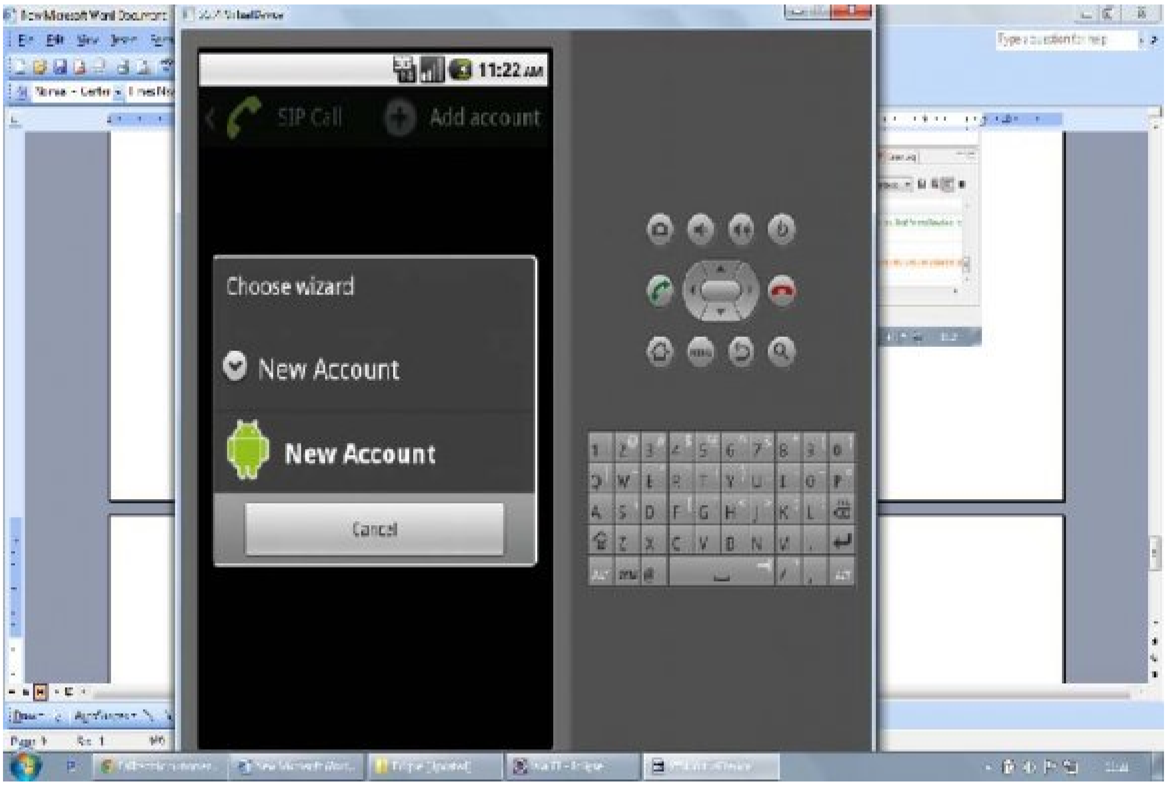
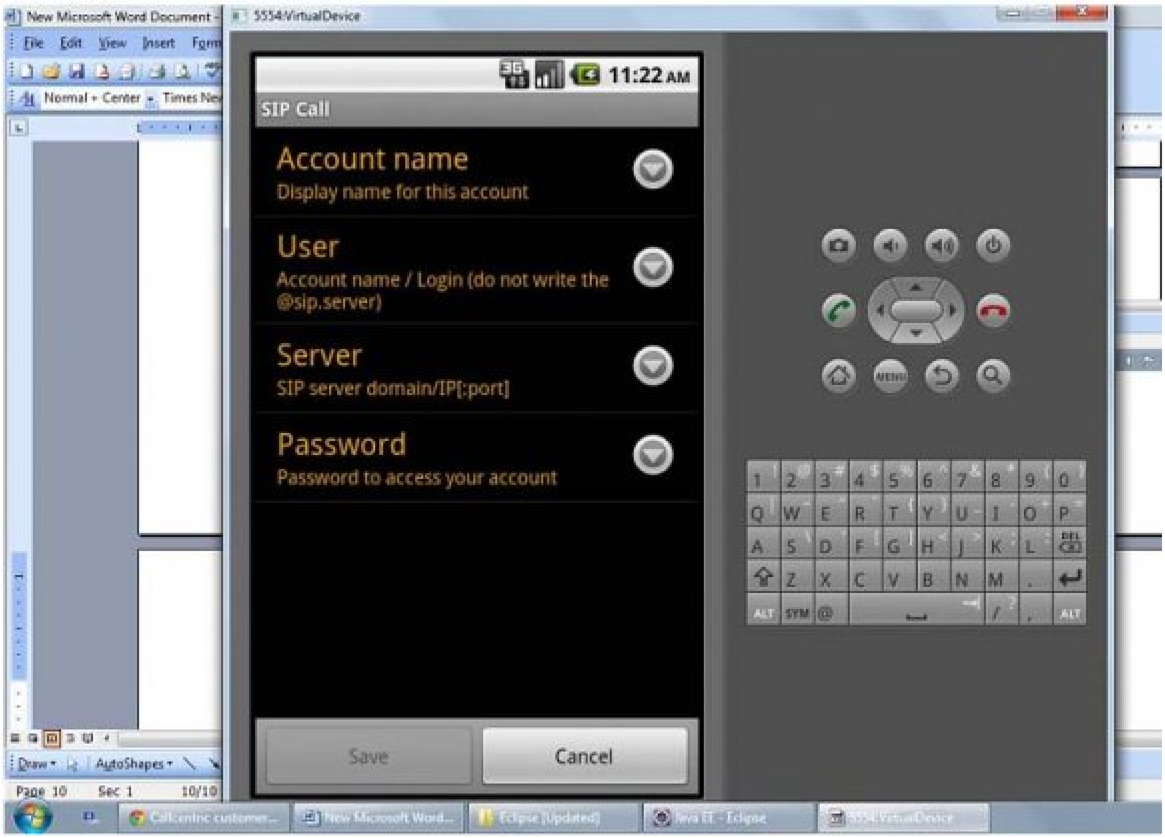


Figure 5:



SIP Call

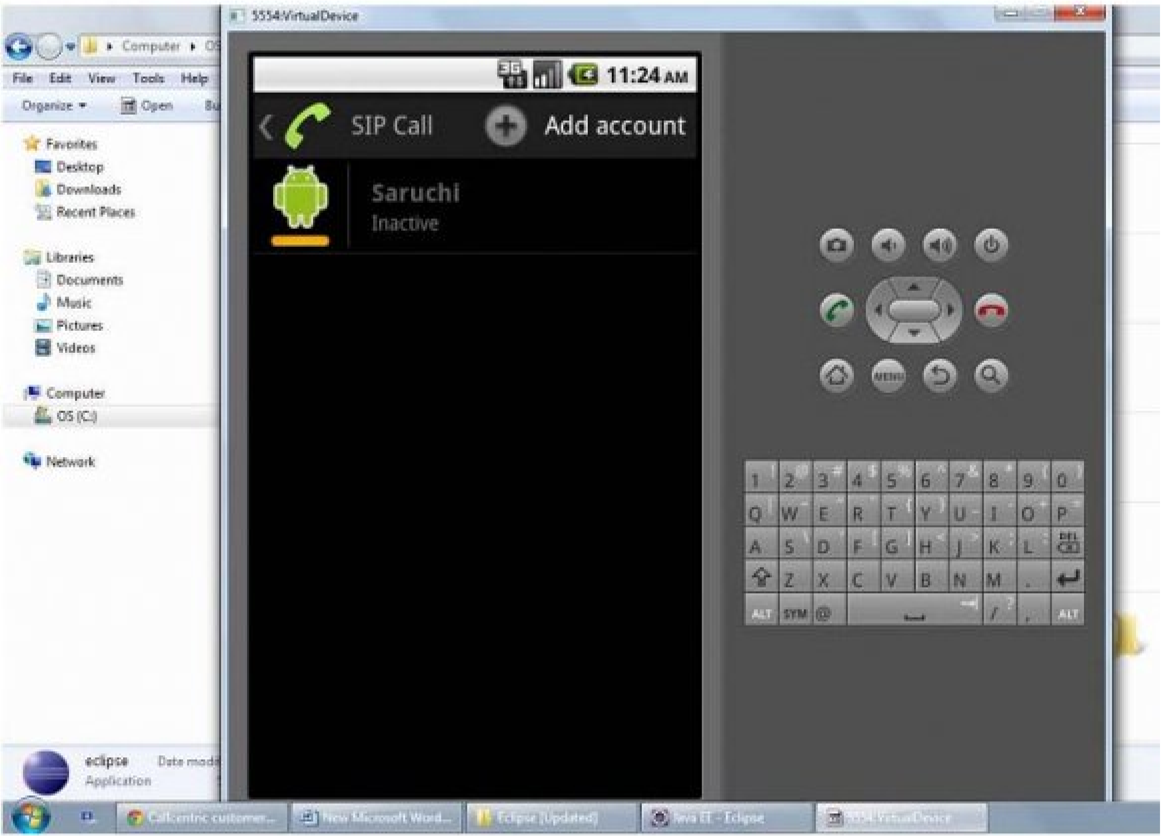
Account name
Display name for this account

User
Account name / Login (do not write the @sip.server)

Server
SIP server domain/IP[:port]

Password
Password to access your account

Figure 6:



SIP Call

Add account

Saruchi
Inactive

Figure 7:

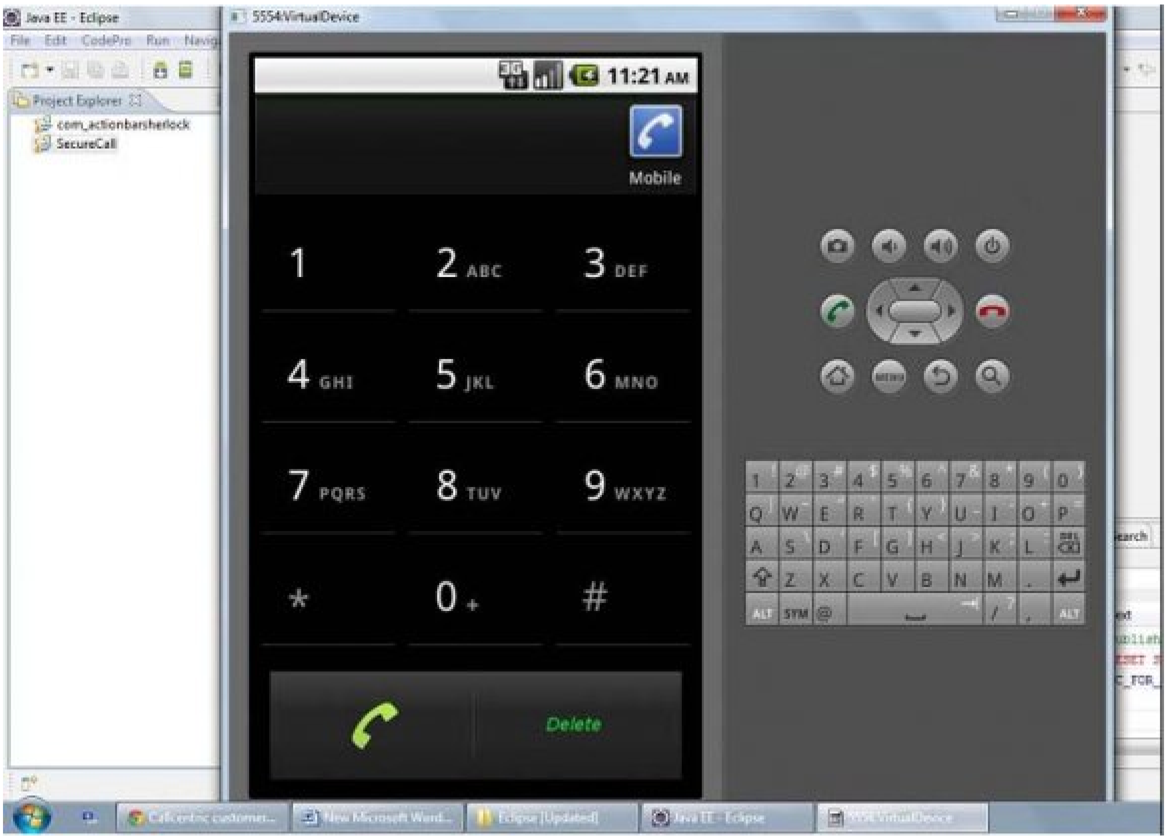


Figure 8:

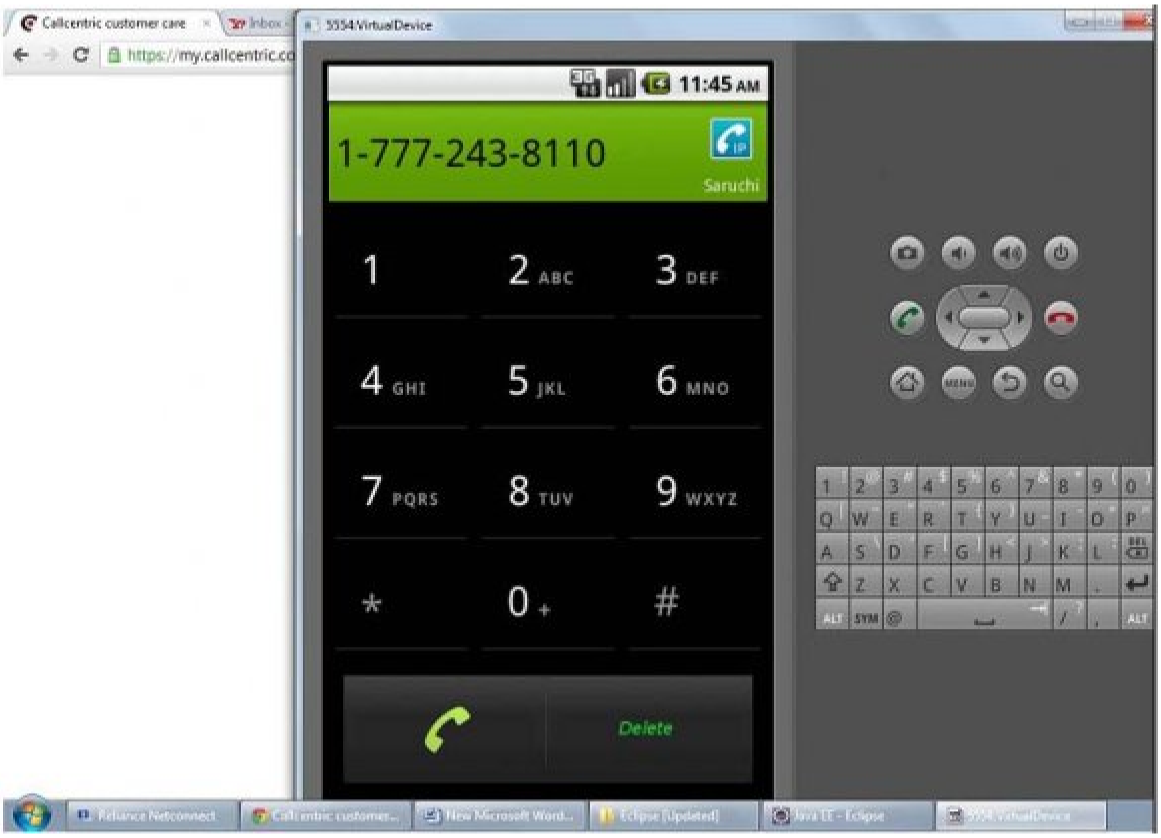


Figure 9:

Figure 10:

[Mcnair et al. ()] , J Mcnair , I F Akyildiz , M Bender . for IMT-2000. 2000. (An Intersystem Handoff Technique)

[Abbasi et al. ()] ‘A Comparative study of the SIP and IAX VOIP protocols’. T Abbasi , S Prasad , N Seddigh , I Lambadaris . *Proc.of Canadian Conference on Electrical and Computer Engineering*, (.of Canadian Conference on Electrical and Computer Engineering) 2005.

[Montoro and Casilari ()] ‘A Comparative Study of VOIP Standards with Asterisk’. Pablo Montoro , Eduardo Casilari . *Fourth International Conference on Digital Telecommunications-IEEE*, 2009.

[Angelos and Keromytis ()] ‘A Comprehensive Survey of Voice over IP Security Research’. D Angelos , Keromytis . *A Mobile Service Architecture for improving Availability and Continuity* Shahniza,Kamal Bashah, Tore Jonvik & Do van Thanh (ed.) 2011. 2010. IEEE.

[Wang et al. ()] *A Distributed Key-Changing Mechanism for Secure Voice Over IP (VOIP) Service*, Chia-Hui Wang , Mei-Wen Li , Wanjiun Lian . 2003. IEEE.

[Zourzouvillys and Rescorla ()] ‘An Introduction to Standards-Based VOIP: SIP, RTP, and Friends’. T Zourzouvillys , Rescorla . *Internet Computing* 2009. IEEE.

[Van Meggelen et al. ()] *Asterisk: The Future of Telephony*, J Van Meggelen , J Smith , L Madsen . 2007. O’Reilly Media.

[Lin and Lin ()] *Channel allocation for GPRS*, Phone Lin , Yi-Bing Lin . 2001. IEEE.

[Mohammed et al. ()] *Encrypted Voice Calls with IP enabled Wireless Phones over GSM/ CDMA/ WiFi Networks*, A Mohammed , Robin Qadeer , Sarvat Kasana , Sayeed . 2009. Computer Engineering and Technology

[Regis and Bates ()] ‘General Packet Radio Services’. J Regis , Bates . `http://www.callcentric.com/31. http://www.developer.android.com/` *Tata McGraw Hill* 2002. 29.

[Dimarzio ()] *McGraw Hill Year mobile Communication*, J F Dimarzio . 2009. New Delhi. (Android A programmers guide)

[Stallings ()] *Network Security and Cryptography, Pearson Education*, W Stallings . 2007. New Delhi.

[Shen ()] ‘Performance of VOIP over GPRS’. Q Shen . *Advanced Information Networking and Applications 17th International Conference, 17. Goode, AT&T Labs and Weston*, 2003. 2002. (Voice over Internet protocol (VOIP). IEEE)

[Yeob Yeun ()] ‘Practical Implementations for Securing VOIP Enabled Mobile Devices’. *Third International Conference on Network and System Security -IEEE*, Chan Yeob Yeun, Salman Mohammed Al-Marzouqi (ed.) 2009.

[Lella ()] *Privacy Of Encrypted Voice-Over-IP*, Tuneesh Lella , Riccardo . 2007. IEEE.

[Proc. IEEE INFOCOM] *Proc. IEEE INFOCOM*, (IEEE INFOCOM)

[Shan and Jiang ()] ‘Research on Security Mechanisms of SIP-based VOIP System’. Liancheng Shan , Ning Jiang . *Ninth International Conference on Hybrid Intelligent Systems-IEEE*, 2009.

[Kuhn et al. ()] *Security Considerations for Voice Over IP Systems*, D R Kuhn , T J Walsh , S Fries . 2005. Gaithersburg, MD USA. National Institute of Standards and Technology

[Si et al. ()] ‘Security mechanisms for SIP-based multimedia communication infrastructure’. D F Si , Q Long , X H Han , W Zou . *IEEE Conf. on Comm, Circuits and Systems (ICCCAS)*, 2002.

[Seurre et al. ()] Emmanuel Seurre , Patrick Savelli , Pierre-Jean Pietri . *GPRS for mobile Internet*, 2003. (Artech House)

[Rosenberg et al. ()] *SIP: Session Initiation Protocol*, J Rosenberg , H Schulzrinne , G Camarillo , A Johnston , J Peterson , R Sparks , M Handley , E Schooler . 2002. (Internet Engineering Task Force (IETF)

[Tian et al. ()] *Study of SIP Protocol Through VOIP Solution of Asterisk*, Lu Tian , Nicolas Dailly , Qiao Qiao , Jihua Lu1 , Jiannan Zhang , Jing Guo , Ji’ao Zhang . 2010. IEEE.

[Liu and Lo ()] ‘The study of the SIP for the VOIP’. Chung-Hsin Liu , Chun-Lin Lo . *Fifth International Joint Conference on INC, IMS and IDC*, 2009.

[Thermos and Takanen ()] P Thermos , A Takanen . *Securing VOIP Networks: Threats, Vulnerabilities, and Countermeasures*, 2007. Addison-Wesley Professional USA.

[Mohammed et al. ()] *Voice Communication over GGSN/SGSN*, Ahmad Ali Habeeb ; Mohammed , A Qadeer , Shamshir Ahmad . 2007. IEEE.

[Kalden ()] *Wireless Internet access based on GPRS*, R Kalden , Meirick , Meyerm . 2002. IEEE.