Instant Messaging privacy in the clouds

Lizbeth Granda Paredes
Departamento de Computação, Universidad Federal de São Carlos, São Carlos, São Paulo, Brazil., lizgrand18@gmail.com

Sergio Donizetti Zorzo
Departamento de Computação, Universidade Federal de São Carlos, São Carlos, São Paulo, Brazil., zorzo@dc.ufscar.br

Instant Messaging privacy in the clouds

Lizbeth N. Granda Paredes
Department of Computer – UFSCar
Universidade Federal de São Carlos
São Carlos – SP. Brazil
lizgrand18@gmail.com

Sérgio Donizetti Zorzo
Department of Computer – UFSCar
Universidade Federal de São Carlos
São Carlos – SP. Brazil
zorzo@dc.ufscar.br

ABSTRACT

Instant messaging are applications that allow spontaneous communication between two or more people, enabling the relationship between them regardless of the distance that separates them. Also, social network like Facebook used to maintain contact current or old friends, to publish and view photos, to allow a closer relationship between the contacts and private instant messaging is including in its structure. Instant messaging applications are placed in the cloud to facilitate the access to users from any workstation resulting in better cooperation and exchange of information between users. Since the instant messenger needs an internet connection, there are disadvantages of privacy and security, given the risk that messages are sent to be read by strangers. This paper proposes the inclusion of a privacy mechanism to protect information sent or received and allow the personalization according to the user preferences in instant messaging in the cloud.

Keywords

Cloud computing, privacy, preferences, instant messaging.

INTRODUCTION

Instant messaging (IM) applications like Gtalk, MSN or Yahoo are used by a lot of people of all ages not only for social bounds but also for collaborative works in companies or educational institutions. The use of instant messaging brings a number of benefits that improve communication between users. Instant messaging allows measuring the availability of colleagues and adjusts the communications between them, providing faster responses and greater interaction among peers (Patil, S. and Kobsa, A., 2010).

The functionality of instant messaging where the goal is to enable real-time conversation has been improving communication and interaction among users, becoming a working tool and a form of personal communication. The instant messaging, unlike other media, significantly improves the speed, the ease and effectiveness of communication between people.

Currently most IM provider are adapting their services to the clouds, to get easier and faster to more users, releasing user from installing the application on each workstation and allowing the use of the application regardless of operating system where the user is found (Chen, R. et al., 2009)(Ramirez, M. and Kennedy, R., 2011). Google is a one of the companies that put their different services in the cloud and in the case of its instant messaging, Gtalk, was no exception, which embedded in the e-mail service. At first, Gtalk only allowed communication by text messages, but the function of video communication was added.

However, to allow easier communication to increase risk related to privacy and security of information sent and received for users, the online visibility of a particular user can lead to distraction and interruptions caused by inappropriate messages or the conversation between users can be invaded or accessed by third parties with or without permissions of the user.

The privacy is a concern in people's lives. For them it is important that the information being sent or received is not accessed by unauthorized or malicious people. The issue of privacy must be related to the theme of personalization, because the context of privacy is not equal for all people. So, (Kobsa, A., 2002) suggests the use of personalization techniques to ensure the protection of user information as the use of techniques for the creation of privacy policies that allow the user to customize the availability of information and ensure their protection.

Cloud computing enables the use of these types of applications placed on the internet facilitating users' tasks and the access to these applications. The user sends and receives information through the cloud, with a full availability of applications in the cloud. However, the large amount of information sent to the cloud can be obtained by other users. For that, it seeks to offer instant messaging services in the cloud with guarantees of protection for users' information.

The paper is organized as follow: Section II discusses the concepts of instant messaging describing the main features of this term. Existing instant messaging are presented with their features and limitations. It also presents the privacy policies used in instant messaging. Section III presents the definition of an architecture that proposes the insertion of a privacy mechanism, describing the tasks of their modules integrating the mechanism. Section IV describes the implementation of the proposal, defining the components to be used. Finally, Section V presents the conclusions.

INSTANT MESSAGING AND POLICIES PRIVACY

A. Instant Messaging

Instant messaging are applications that allow instant communication between two or more distant people, using any device such as laptop, cell phones, etc. connected to a network. The main purpose of instant messaging is to allow the sending and receiving messages between users. Such applications can be used in different settings, since a family or friendly environment to a work or educational environment.

Interesting features are present in the most instant messaging, such as providing relevant information on the availability of users in real time and allowing a personalization space of message where the user can detail his current status (Chung, D. and Nam, C.S., 2007)(Santos, R.P.D., 2009). The several instant messaging are based on different protocols and have some different characteristics. However, according to (Yan, G. et al., 2008), the general structure of all user communication system in the network can be represented by Figure 1, where the server is the place where all the functionality of the system is provided.

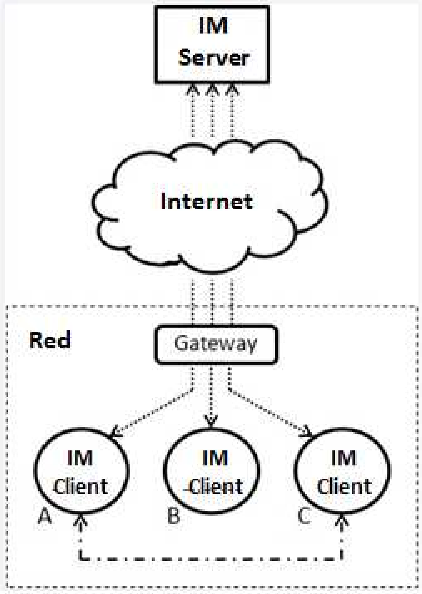


Figure 1 General Structure of instant messaging system (Cancian, M.H. 2009)

The first instant messaging mIRC was created in 1995, which was an application offered by Microsoft using the IRC protocol (Internet Relay Chat) to send messages, games and works between two people or a group of people. The mIRC was developed taking into account different features such as file transfer, multi-server connections, IPv6, SSL encrypted, oral messages, notifications, messages logging, among other. mIRC also had a powerful scripting language allowing users to process different tasks in addition to chatting, such as multimedia playback or gaming network communication[1].

[1] http://www.mirc.com/

After the instant messaging mIRC, ICQ emerged with the objective of providing communication through the internet, with features like messaging, video conferencing, voice chat, and present integration with social networks. ICQ uses a communications protocol called OSCAR. And ICQ users are identified by a registration number, called UIN (Universal Internet Number).

MSN Messenger emerged in 1999 and became the most innovative and popular among users instant messaging. This messenger serves the same purpose of providing communication between users in real time. However, the most impressive was the integration with e-mail service Hotmail (Trigo, V. and Martin, A.C.). Since 2005 this IM was renamed, and now it is called Windows Live Messenger, which in addition to the messaging service, provides a range of service like Photo Gallery, Movie Marker, Mail, Writer and Windows Live Mesh. Windows Live Messenger lets you make call from PC to phones. It also allows to send messages to contacts that are not connected, who will receive the message when they connect. It offers a number of games and applications which can be accessed through the chat window. At first, this instant messaging offered the feature of “shared folders” for the computers with hard drivers using NTFS file format. Now, this feature was eliminated, replaced by the Windows Live SkyDrive.

Instant messaging service from Google, called Gtalk, was released in 2005 and used the interoperability protocol Jabber/XMPP. This service is available from Gmail users and allows sharing messages between users in real time, update status and transfer files instantly[2]. Currently, Gtalk allows voice communication, using Jingle protocol that offers free calls from one PC to another, audio conferencing and integration with Gmail. The conversations are stored in the history of the user’s Gmail page. It presents integration with Google’s social network, called Orkut. Its disadvantages are: it allows massive shipping information and as encryption from end to end is not used, conversations can be easily accessed by others.

Yahoo presents their instant messaging, called Yahoo Instant Messaging, which provides easy communication between users. Like instant messaging listed above, it offers other features such as file transfer, photo sharing, calls from PC to PC, the use of instant messaging with friends on other networks, in addition to message exchange. Yahoo Messenger has a stealth feature which allows the user to choose which friends you want to see you connected, disconnected or unavailable[3].

Pidgin is a multi-platform instant messaging client that allows connecting to multiple networks and accounts simultaneously. Pidgin allows recording of conversations, replacing the names of contacts, transferring files. It offers simultaneous connection to Google Talk, AIM, MSN, Yahoo, among others.

Social networks like Facebook and Google +, are applications used in Internet, which have included in their structures the use of instant messaging, to allow their users so better communication and closer ties with their contacts.

Facebook, the social network more known and used, was created by Mark Zuckerberg, founded in 200, to communicate and connect with people with some type of relationship or common interests. Currently, this social network has over 350 million active users[4]. Facebook is updated every day, improving and providing new activities to its structure, according to the use of the user. One activity that included was instant messaging. This option was included thinking about giving users the option of sending private messaging to your contacts instead of writing on the wall of them and other to read.

Google+ is the social network created by the company Google in 2011. This social network includes Circles, Interests and Messages. Google+ for being other application of Google includes social services such as Google Profiles and Google Buzz, and integrates instant messaging service, Gtalk[5].

Instant messaging in the cloud can offer this service in a fast way to users, and can be accessed by the user at any time no matter where he is. The Cloud Computing aims at facilitating the use of such applications providing an easy access without wasting time on installation or configurations issues.

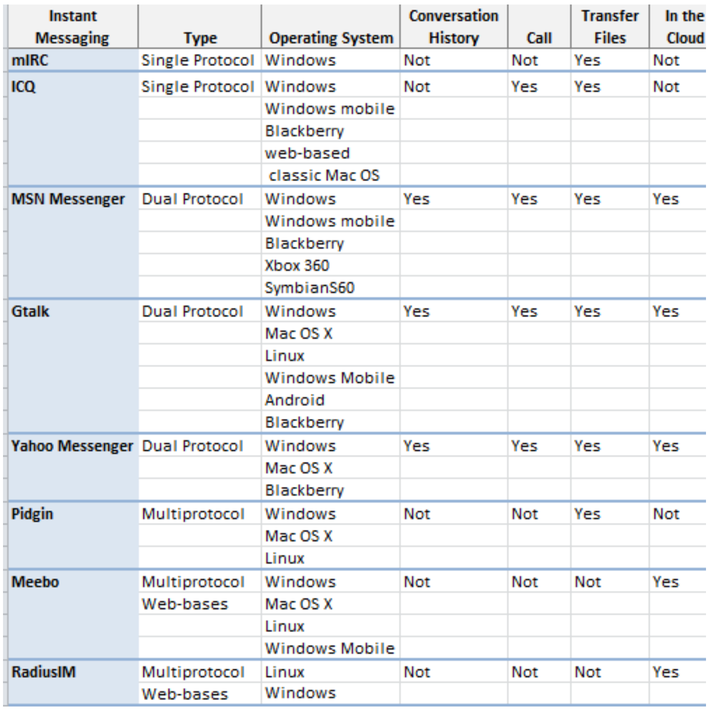
To provide ease of use for its users, some instant messaging described above sent their services for the cloud. As is the case with Google’ Gtalk, MSN Messenger from Windows or Yahoo Messenger from Yahoo, which were introduced in service e-mail from their suppliers, freeing users to install the messenger locked in each workstation.

There are multiplatform IM clients like Pidgin, such as Meebo and RadiusIM, which unlike Pidgin, uses the cloud to reach users and be accessed online from anywhere workstation. It allows access to different messenger like Gtalk, Yahoo or

[2] http://www.google.com/talk/
[3] http://pe.messenger.yahoo.com/
[4] https://www.facebook.com/
[5] https://plus.google.com/

MSN Messenger. The advantage of this service is that you can group all the contacts without login account by account, you only need to access the application through an internet connection, and then everything works in the cloud.

The Table 1 presents the best known IM applications with their characteristics. It allows a comparison between the applications presented. Most instant messenger are applications for Windows, however there are users who use other operating systems. A good point about cloud computing is that no matter what operating system is used, applications in the cloud come regardless of the operational system.



Instant Messaging	Type	Operating System	Conversation History	Call	Transfer Files	In the Cloud
mIRC	Single Protocol	Windows	Not	Not	Yes	Not
ICQ	Single Protocol	Windows	Not	Yes	Yes	Not
		Windows mobile				
		Blackberry				
		web-based				
		classic Mac OS				
MSN Messenger	Dual Protocol	Windows	Yes	Yes	Yes	Yes
		Windows mobile				
		Blackberry				
		Xbox 360				
		SymbianS60				
Gtalk	Dual Protocol	Windows	Yes	Yes	Yes	Yes
		Mac OS X				
		Linux				
		Windows Mobile				
		Android				
		Blackberry				
Yahoo Messenger	Dual Protocol	Windows	Yes	Yes	Yes	Yes
		Mac OS X				
		Blackberry				
Pidgin	Multiprotocol	Windows	Not	Not	Yes	Not
		Mac OS X				
		Linux				
Meebo	Multiprotocol	Windows	Not	Not	Not	Yes
	Web-bases	Mac OS X				
		Linux				
		Windows Mobile				
RadiusIM	Multiprotocol	Linux	Not	Not	Not	Yes
	Web-bases	Windows				

Table 1 Characteristics of existing IM

B.Privacy Policies

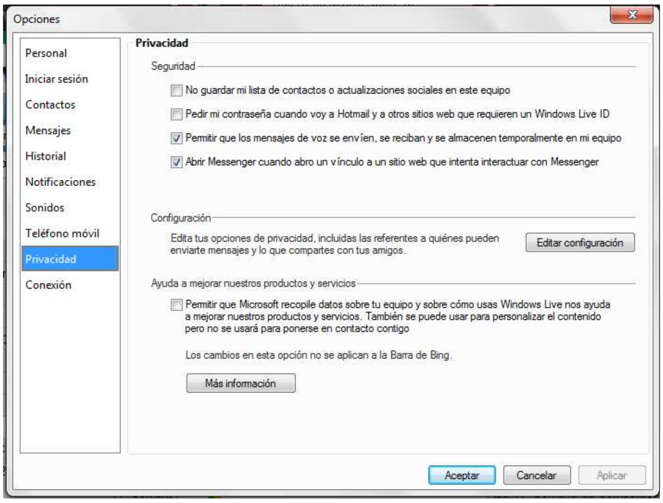
Instant messaging services offer users different privacy policies with respect to personal information of its users. For example, the privacy policies on the Google services, including Gtalk, are based on five principles:

- Use the information to provide users with valuable products and services.
- Develop practices and products that reflect strong privacy standards.
- Compile transparent personal information.
- Give users meaningful alternatives to protect the privacy.
- Responsibly monitor the stored information.

If the user wants to register any Google Service, it is necessary to provide personal information, which is combined with other Google Services or Third parties. Google sends cookies to the user's computer. The cookies include storage of user preferences, search results, but also include advertising services cookies. When the user accesses the services of Google, their servers store other information like web request, IP address, browser language, date and time of application, etc.[6]

The Windows Live Messenger lets the user choose some options for privacy and security. It gives the user control to decide whether their contacts must be saved in the computer, ask or not the password to the Hotmail service, to decide whether their conversations must be stored in the computer, as shown in Figure 2. In the figure 2 we can see that the user is a Spanish people and her options for privacy and security was "allows to send the voice message…." and "open the messenger when …"

[6] http://www.google.com/intl/es/privacy/privacy-policy.html



Privacidad

Seguridad

- ☐ No guardar mi lista de contactos o actualizaciones sociales en este equipo
- ☐ Pedir mi contraseña cuando voy a Hotmail y a otros sitios web que requieren un Windows Live ID
- ☑ Permitir que los mensajes de voz se envíen, se reciban y se almacenen temporalmente en mi equipo
- ☑ Abrir Messenger cuando abro un vínculo a un sitio web que intenta interactuar con Messenger

Configuración

Edita tus opciones de privacidad, incluidas las referentes a quiénes pueden enviarte mensajes y lo que compartes con tus amigos.

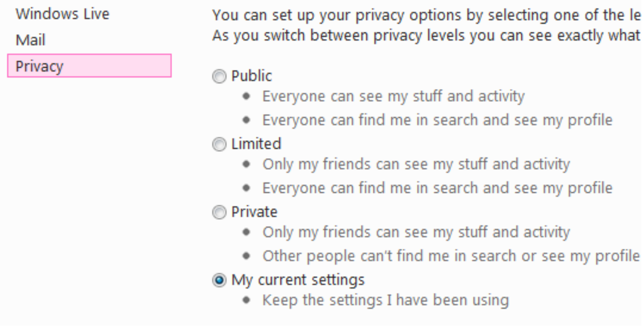
Ayuda a mejorar nuestros productos y servicios

- ☐ Permitir que Microsoft recopile datos sobre tu equipo y sobre cómo usas Windows Live nos ayuda a mejorar nuestros productos y servicios. También se puede usar para personalizar el contenido pero no se usará para ponerse en contacto contigo

Los cambios en esta opción no se aplican a la Barra de Bing.

Figure 2 Privacy Options of Windows Live Messenger

It also allows setting additional privacy options by selecting one of the levels for each functionality offered by Windows Live. Figure 3 and Figure 4 show some of privacy options to configure Windows Live.



You can set up your privacy options by selecting one of the le
As you switch between privacy levels you can see exactly what

○ Public
- Everyone can see my stuff and activity
- Everyone can find me in search and see my profile

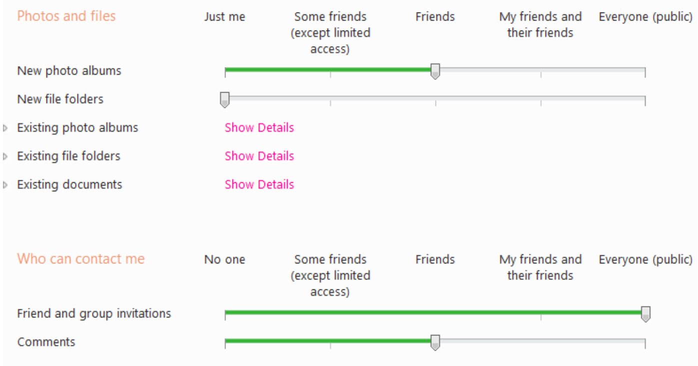
○ Limited
- Only my friends can see my stuff and activity
- Everyone can find me in search and see my profile

○ Private
- Only my friends can see my stuff and activity
- Other people can't find me in search or see my profile

● My current settings
- Keep the settings I have been using

Figure 3 Configuration of privacy user

In the Figure 3 it is possible to set the privacy option as public, limited, private or my currents setting. The last one was the option of this user shown in the Figure 3. In the Figure 4 it is possible to configure the privacy levels of the "Photos and Files" and "Who can contact me". The Figure 4 shows the user options in these categories.



Photos and files	Just me	Some friends (except limited access)	Friends	My friends and their friends	Everyone (public)
New photo albums			●		
New file folders	●				
Existing photo albums	Show Details				
Existing file folders	Show Details				
Existing documents	Show Details				

Who can contact me	No one	Some friends (except limited access)	Friends	My friends and their friends	Everyone (public)
Friend and group invitations					●
Comments			●		

Figure 4 Configuration of privacy levels

Yahoo Messenger collects personal information from users when they register and when the use Yahoo services. Records personal data such as name, email address, sex, occupation, personal interests, etc. For payment related services, register address, income, social reason. Yahoo uses this information for advertising, customizing the content according the user, studying and investigating, make reports.

Facebook offers its users the ease in locating friends and in making decisions to establish friendships. It offers protection options to information, depending on the decisions of these users (Young, A.L. and Quan-Haase A., 2009). Facebook lets you choose the privacy of status updates, photos and selecting the type of contacts you can see, as shown in figure 5.

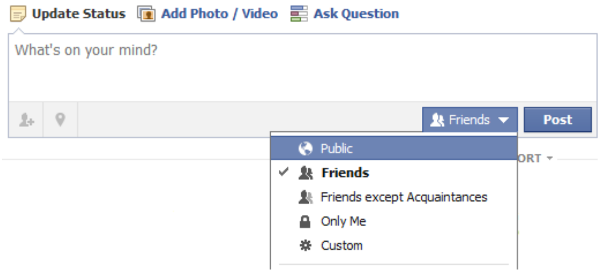
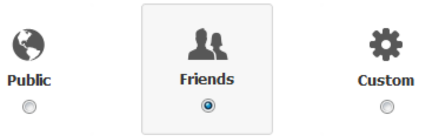


Figure 5 Control Privacy in the Post of Facebook

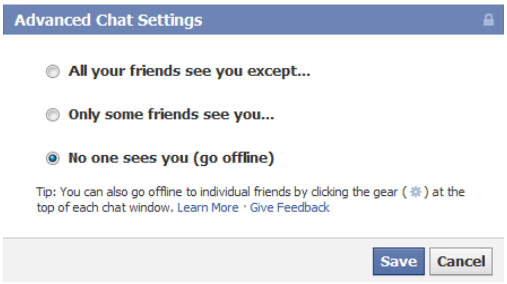
The figure 6 shows the options that Facebook provides to configure the privacy of users: public, friends and custom. The best options are friends and custom. In the option “friends”, the user profile can be seen by all their contacts considered friends. The option “custom” allows the user to specific in more detail what contacts might view his profile.



Public ○ Friends ● Custom ○

Figure 6 Control Default Privacy of Facebook

However, the privacy setting on Facebook are presented for all the functionality of the social network, including instant messaging, as shown in Figure 7. It offers no specific privacy protections for instant messaging.



Advanced Chat Settings

○ All your friends see you except...

○ Only some friends see you...

● No one sees you (go offline)

Tip: You can also go offline to individual friends by clicking the gear (✲) at the top of each chat window. Learn More · Give Feedback

Figure 7 Advanced Chat Settings of Facebook

PRIVACY MECHANISM OF THE INSTANT MESSAGING IN THE CLOUDS

Manipulated information in instant messaging applications in the cloud may present risks of information or identity theft, infiltration, unauthorized access, etc. As seen in the previous section, the user information stored in some cases is combined by the providers of these services with other services or third parties, such as for advertising. Due to that the insertion of a privacy mechanism for the protection of the information of the user is proposed, using these applications, giving them control to personalize and decide what information should be stored.

We investigated different jobs is also intended to provide users with options for protection of information sent over the Internet. As in (Bertino E. et al., 2009) that attempts to control user authentication in the cloud through a heterogeneous identities' Manager and using the protocol AgZKPK - *Aggregate Zero Knowledge Proofs of Knowledge*. Also, in (Pearson S.S. et al., 2009) that provides a mechanism of protection using obfuscation techniques. But many of the jobs found are not even focused on cloud computing, or interfere with the customization of user profiles, or increase costs of installation of any necessary equipment or involved only in some aspect of the protection of information.

This mechanism is focused on three issues: secrecy, anonymity and isolation, considered in the context of privacy (Fischer-Hübner, S., 2001) (Wright, T., 2004). The main objective of this mechanism is to ensure the privacy of user, giving the user privacy setting in each of these points. The idea is to ensure access permissions for data, authentication, to protect the information when it is being sent through cryptographic processes, and in turn allow the user to select options according to their privacy preferences and level of trust for the application.

The privacy mechanism proposed is implemented by the architecture described in two parts. The client part is the first part and it is the instant messaging environment. The user submits requisitions to the server from the client part. The second part is the server; which is the privacy mechanism for processing the respective configurations requested by the user. In this proposed architecture, the privacy mechanism is divided into three modules, according to the three points mentioned above: (i) the identity module, (ii) the confidentiality module and (iii) the preferences module. The communication between the client and server is through remote procedure calls.

All architecture placed in the cloud needs to use a cloud provider, which can be accessed by any user at any time. The proposed architecture is illustrated in the Figure 8.

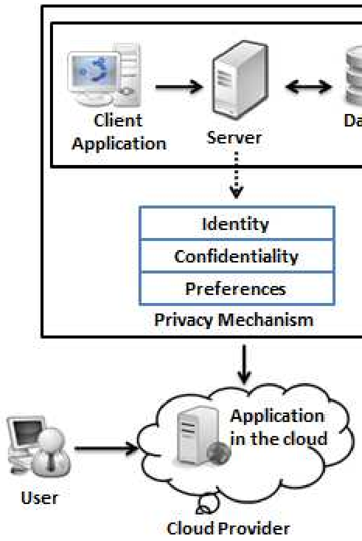


Figure 8 Architecture of privacy mechanism

A. Identity Module

The Identity module is concerned with anonymity, which objective is the protection of identity of user using the instant messaging in the cloud. This module takes care of authentication, access control and user identification. In the first use of each user needs to perform authentication for continue the sequence settings in the following two modules.

Once the user performs the registration application, the user must to do access control and identify them, preventing access to malicious people to steal the identity or misusing the information of any user. The verification of identity is also based on proof of additional information required by the server. In this module the user decides that personal information can be shown or if he prefers to pass as anonymous for some contacts.

B. Confidentiality Module

The Confidentiality Module is concerned with secrecy, which objective is ensuring the preservation and protection of information submitted by a user of the instant messaging in the cloud. This module provides protection of information that is sent and received by the user, which is accomplished through the generation of public and privates keys, and encryption of the message to be sent.

Once the user passed by the identity module, the user is in the IM interface. It begins with the definition of the private key for which can be done using a cryptographic protocol session to ensure safety. When the user starts to send message to any of their contacts, making the definitions of the public key and the information being sent is conducted to a cryptographic process.

C. Preferences Module

The Preferences Module is concerned with isolation, which objective is the availability of the user compared to the others, the desire to store the messages sent to another user. All these characteristics depend on the preferences and user confidence. In this module to perform the privacy setting based on the preferences and the degree of confidence with this type of application.

The settings of this module apply to the presence of a particular user in this application, the way the user wants to be seen by others users, the user's location and the other characteristics. Preferences are set once the user passed for the registration process, which are stored and will be met by privacy mechanism. However, the preferences can also modify at any other time.

The sequence diagram illustrated in Figure 9 describes the use of the proposed architecture, showing the user interaction with the three modules that are part of privacy mechanism. The requisitions made to each of the modules are through the client application.

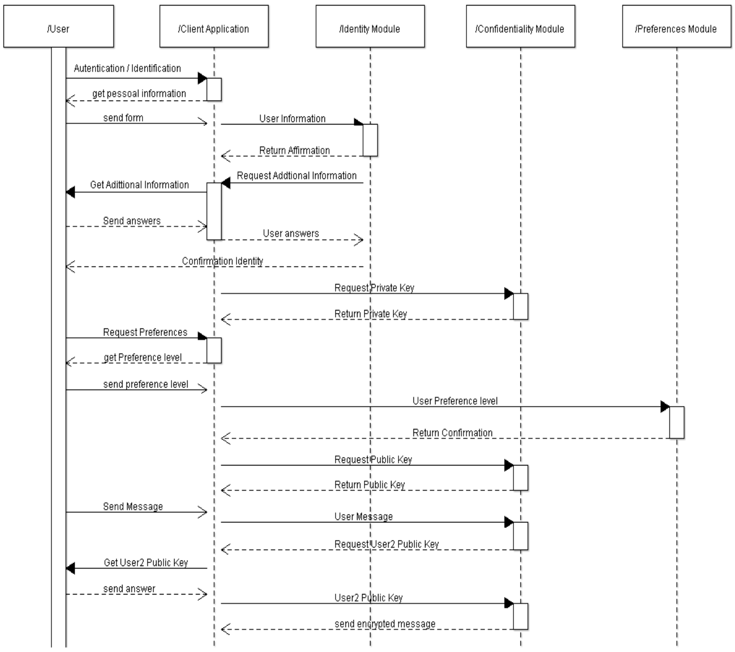


Figure 9 Sequence Diagram

IMPLEMENTATION

To validate the proposal, which will be called "Prisma", will go to use the Eclipse tool library with Google, called Google Web Toolkit (GWT), which facilitates the creation layer and the communication with the server is through remote procedure calls. We're going to use a template like instant messaging Gtalk Google, which makes use of different libraries that help in the implementation of the application.

The template follows the Model-View-Controller architecture. The model represents the objects on which the application operates. In this case, there are the user, the contact list and the message. The view presents the windows requires rendering the instant messaging, such as the main windows for the instant messaging, the windows for the chat with the contact, the windows for the contact list and the window for the privacy options. The controller implements communication with the server and manages model objects to be rendered in the view. Also help in communication with the privacy mechanism, because instant messaging functionality will be located on the server using asynchronous interfaces for calls on the client.

The figure 10 shows a diagram GWT with the organization both on client and server. The definition of the classes and interfaces related for communication between the client and the server side. On the client creates two interfaces, one synchronous call "ControlePrisma" where are placed the methods, and one asynchronous call "ControlePrismaAsync" to call the service from the client side. On the server side is created a class called "ControlePrismaImpl" where is implemented the code of each method and the connection to the database.

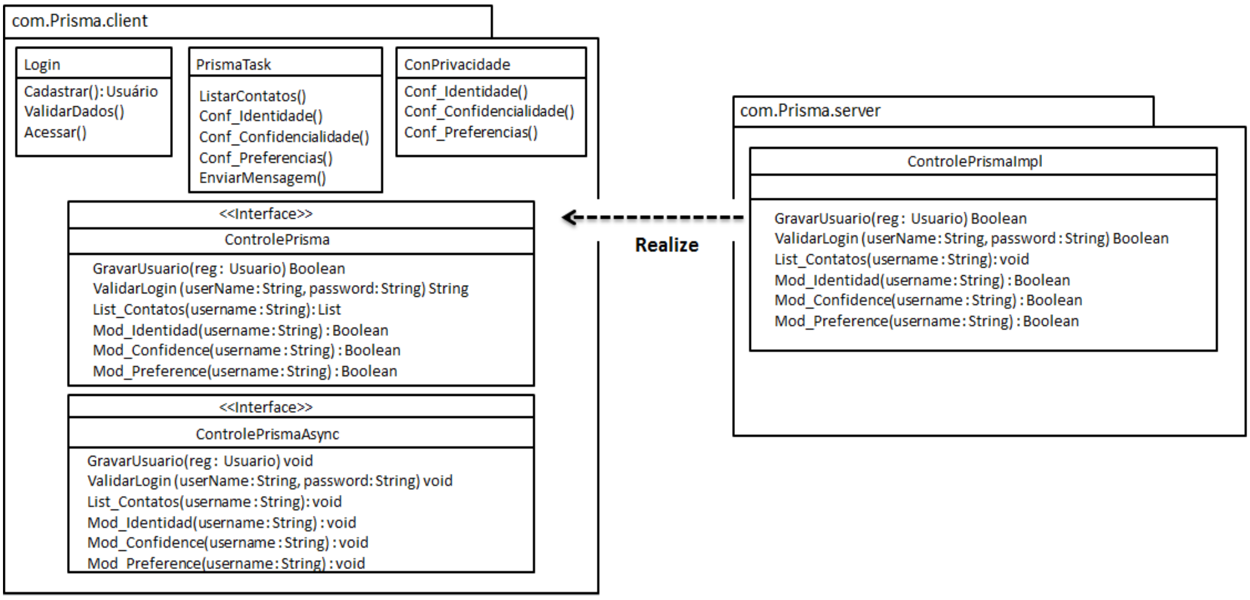

com.Prisma.client
Login
Cadastrar():Usuário
ValidarDados()
Acessar()
PrismaTask
ListarContatos()
Conf_Identidade()
Conf_Confidencialidade()
Conf_Preferencias()
EnviarMensagem()
ConPrivacidade
Conf_Identidade()
Conf_Confidencialidade()
Conf_Preferencias()
<<Interface>>
ControlePrisma
GravarUsuario(reg: Usuario) Boolean
ValidarLogin (userName:String, password:String) String
List_Contatos(username:String):List
Mod_Identidad(username:String) :Boolean
Mod_Confidence(username:String) :Boolean
Mod_Preference(username:String) :Boolean
<<Interface>>
ControlePrismaAsync
GravarUsuario(reg: Usuario) void
ValidarLogin (userName:String, password:String) void
List_Contatos(username:String):void
Mod_Identidad(username:String) :void
Mod_Confidence(username:String) :void
Mod_Preference(username:String) :void
Realize
com.Prisma.server
ControlePrismaImpl
GravarUsuario(reg: Usuario) Boolean
ValidarLogin (userName:String, password:String) Boolean
List_Contatos(username:String):void
Mod_Identidad(username:String) :Boolean
Mod_Confidence(username:String) :Boolean
Mod_Preference(username:String) :Boolean

Figure 10 GWT Diagram

Once the application, it is placed in the cloud using the Google platform, called Google App Engine, which allow easy installation of the application in the cloud.

CONCLUSIONS

Instant messaging applications bring many benefits for communication between people. Place these applications in the cloud for easy access and interaction, so that different providers of such services are sending their applications to the cloud.

The processed information in IM applications in cloud computing environments can be accessed by any user, so there is the risk that the information is stolen and still used for other purposes.

There are mechanisms that attempt to solve such problems, however in trying to interfere in customizing user profiles.

This paper presents the architecture of privacy mechanism, to ensure the protection of identity information and user personalization possibilities with the preferences of each user.

Privacy assured in this proposal broke the secrecy, anonymity and isolation, which are important points in the theme of the privacy. This proposal is an option for resolve the privacy, request addressed by this work.

REFERENCES

1. Patil, S. and Kobsa, A. (2010), “Enhacing privacy management support in instant messaging”.
2. Chen, R. and Kraemer, K. and Sharma, P. (2009), “Google: The world first information utility?”, Business and Information System Engineering.
3. Ramirez, M. and Kennedy, R. (2011), “Communication in the cloud: Skype, Google Talk, and Google voice”.
4. Kobsa, Alfred (2002), “Personalized hypermedia and international privacy”, Commun. ACM, New York, USA.
5. Chung, D. and Nam, C.S. (2007), “An analysis of the variables predicting instant messenger use,” New Media Society.
6. Santos, R.P.D. (2009), “Iteraction with wikis in through instant messaging,” Master Thesis, ICMC/USP, São Carlos – SP.
7. Yan, G., Xiao, Z. and Eidenbenz, S. (2008), “Catching instant messaing worms with change-point detection techniques.”, Berkeley, CA, USA.
8. Cancian, M.H. (2009), “Uma proposta de guia de referência para provedores de software como serviço”.
9. mIRC Site. http://www.mirc.com/.
10. Trigo, V. and Martin, A.C., “Windows Live Messenger”, Anaya Multimedia, Spain.
11. Gtalk Site, http://www.google.com/talk/
12. Yahoo Site, http://pe.messenger.yahoo.com/
13. Privacy Policies of Google http://www.google.com/intl/es/privacy/privacy-policy.html
14. Fischer-Hübner, S. (2001), “IT-Security and Privacy: Design and use of privacy-enhancing security mechanisms”, Springer-Verlang.
15. Wright, T. (2004), “Security, Privacy, and Anonymity”, ACM, New York, USA.
16. Young Alyson L. and Quan-Haase A. (2009), “Information Relevation and Internet Privacy Concerns on Social Network Sites: A Case Study of Facebook”, ACM, Pennsylvania, USA.
17. Bertino, E., Paci, F., Ferrini, R. and Shang, N., “Privacy-preserving Digital Identity Management for Cloud Computing”, IEEE Data Eng. Bull., 2009.
18. Pearson, S., Shen, Y. and Mowbray, M., “A Privacy Manager for Cloud Computing”, Springer-Verlag, Berlin, Heidelberg, 2009.