Middle-East Journal of Scientific Research 21 (7): 1136-1140, 2014
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2014.21.07.21579

# Implementation of Instant Messaging Toolfor Security Forces

*Thepfusatuo Albert and S. Chakravarthi*

Saveetha University, Saveethanagar, Thandalam, Chennai-602105, India

**Abstract:** Instant Messaging (IM) is a type of communications service over the Internet that enables individuals to exchange text messages and track availability of a list of users in real-time. The existing instant messaging technology does not provide built-in support for security feature as proposed idea. And also in Battle Field Management System the most commonly used as means of communication is Walky-Talky, which we feel is much unsecured. In this paper we propose a secured instant messaging system using identity-based cryptosystems which provide a strong authentication and secured communication for both IM client to IM server and IM client to IM client.Identity-based cryptography is a type of public-key cryptography in which a publicly known string representing an individual or organization is used as public key. The public key string can be IP address, domain name or email address.

**Key words:** Identity-based signature · Identity-based encryption · Identity-based key issuing · Instant messaging · Bilinear pairings · Combat vehicle research development & establishment

## INTRODUCTION

**General Introduction:** Instant Messaging enable individual to exchange text messages and track availability of a list of users in real-time. IM worms and securecommunication are two safety issues of instant messaging system. Most of the existing system give more scalability priority than that of security service. Instant messaging communication can be done in following manner IM client to IM server and IM client to IM client with the following properties of security areas:Authentication, Integrity, Non-Repudiation, Integrity and confidentiality. There are some existing IM systems that only provide confidentiality service, for instance Kikuchi et al. some uses TLS/SSL to establish a secure connection employing digital certificate. However it increases the privacy concerns. And certificate management is complex and costly [1]. In this paper we propose identity-Based cryptosystem, a secure instant messaging system for Battle field Management system, which can provide strong authentication and secure communication for both instant messaging client to instant messaging server and instant messaging client to instant messaging client. Mostly used communication for Battle field Management is that of Walky-Talky which we prove it as more unsecure. Propose a secure IM system by using identity-based cryptosystems. The system consists of a group of private key generators (PKGs), which generate the master key according to secure distributed key generation protocol to avoid key agreement problem. In propose an identity-based cryptosystems, the public key of an entity can be easily calculated from his identity information(e.g. e-mail address, IP address, IM account, etc.),and private key is generated by a trusted third party named as private key generator (PKG),which is transferred via a secure channel from the PKG to the client [2].

**Dentity-Based Cryptosystem:** Identity-Based Cryptosystem is various cryptography combinations of keys used by cryptographic group of community. Identity-based cryptography is a type of public-key cryptography in which a publicly known string representing an individual or organization is used as public key. The public key string can be IP address, domain name or email address. Identity-Based system allows any party to generate a public key from a known identity value. Trusted third party, called private key

**Correspondding Author:** Thepfusatuo Albert, Saveetha University, Saveethanagar, Thandalam, Chennai-602105, India.

generator (PKG) generates the private key. To operate the PKG first publish a master key and retain the master private key. A user submits his identity ID to the PKG. The PKG computes the user's public key and user gets his private key which is returned by PKG [3].

**Identity-Based Encryption:** It is a type of public key encryption in which the public key of a user is some unique information about the identity of the user, for instance e-mail id, IP address and IM account etc., which was proposed by Adishamir in 1984.

**Identity-Based Decryption:** Identity-Based decryption is computed by the PKG based on the ID associated with the receiver and secret master key. Once the private decryption key from the PKG, the receiver uses it together with the element $r_p$ and bilinear map to compute the secret message key, which is then used to decrypt the original senders' message [4-5].

**Identity-Based Signature:** Identity-based signature depends on the assumption that secret keys are secured absolutely. If a secret key is exposed, secret key have to be reissued. Thus limiting the impact key exposure of secret key in Identity-Based signature is an important task.

**System Analysis**

**Existing System:** The existing IM technology does not provide built-in support security features. Most of the existing IM services were design giving scalability priority over security. Some IM employs TSL/SSL to establish a secure connection between client and a server by digital certificate. However TLS/SSL will increase privacy concern. Some only provide confidentiality service e.g. Kikuchi. And in Battle field management system most commonly used is walky-Talky, which we feel is very unsecure [6].

**Disadvantage of Existing System:** There are various disadvantages in the existing. Some of them are as follows:

- Giving more scalability priority over security.
- There is no built in support (like confidentiality, integrity, authentication and non-repudiation).

**Proposed System:** We propose a secure IM system by using Identity-Based Cryptosystem, which can provide strong authentication and secure communication for both IM client to IM client and IM client to IM server. Secure communications includes the Properties of: Authentication, Integrity, Non-Repudiation, Integrity and confidentiality. For secure and confidentiality proposedDeffie-Hellman protocol suitable for Instant Messaging system. Identity-Based public key cryptography (cryptosystem) was proposed which was first introduced by Shamir.

In an identity-based cryptosystems, the public key of an entity can be easily computed from his identity information for e.g. e-mail address, IP address, IM account, etc. and the corresponding private key is generated by a trusted third party named as private key generator (PKG), the private key is transferred from the PKG to the user through a secure channel. The system consists of a group of private key generators (PKGs), which generate the master key according to secure distributed key generation protocol to avoid key escrow problem. IM service provider functions as a registration authority,answers for authenticating user information and signing authenticated users' information to PKGs.

**Advantage of Proposed System:** The Main advantages of using the proposed IM system are as follows:

- Gives more priority on security than scalability.
- IM system support security features like Integrity, Authentication, Non-repudiation and Confidentiality etc. by using Identity-Based Cryptosystem.
- Generation of private key on request is very secure.
- In an identity-based cryptosystems, the public key of an entity can be easily computed from his identity information for e.g. IP address, domain name or email address.

**System Specification**

**Technologies Used:** .NETas a set of software technology of Microsoft for rapidly building and integrating XML Theb services, Microsoft Windows-based application and Theb solution [7].

**Visual Studio Platform:** Microsoft Visual Studio is an integrated development environment (IDE) from Microsoft. Microsoft Visual Studio platform includes a code editor supporting IntelliSense code as well as refactoring code. Other tools include form designer for building GUI applications, web designer and database designer of schema. Plug-ins are accepted that enhance

functionality at almostevery level-including support and adding new toolsets like editors and visual designers for domain-specific languages or toolsets for other aspects of the software development lifecycle (like that of the Team Foundation Server client: Team Explorer). Microsoft Visual Studio supports various different languages by means of services language that allows debugger and code editor to support (to varying degrees) nearly any language of programming language service exists. Support for other languages such as Ruby, M and Python are among other available throughlanguage programming service separately installed. Visual studio also exists as an individual language specific version which provides more limited language services to the user: Microsoft VB, Visual C# and Visual C++ etc [8-9].

**Brief to C#.NET:** C# is built on the syntax and semantics of C++, allowing C programmer to take advantageous of .NET. The development team is lead by Anders Hejlsberg. The most recent version is C# 5.0 released in August 15, 2012. It was a language built intended for simple, general purpose, modern and object-oriented language. The language was built for intention to develop software components.

**Microsoft SQL Server R2:** Microsoft SQL Server is a relational DBMS. It is a software product whose function is to store and it retrievedata's as requested application software, be it on same computer or running on other computer across a network. SQL Server includes better features lie compression, which helps in improving scalability. SQL Server 2008 R2 adds certain features to SQL Server 2008 including a master data management system branded as Master Data and a master data entities and hierarchies.

**System Design**

**Input Design:** The input design is the link between the system and the user. It comprises of Text, Video and audio Messaging. After successful login user can have a life chat in form Text, video and Audio. User need to have his/her account created to access the life chat.

**Output Design:** A quality output is one, which meets the requirements of the end user and information are present clearly. The result of any system processing is communicated to the user and to the other system through. In output design it is determined how the information is to be displaced for immediate need. It is the most important and direct source to the user. Intelligent and efficient design output improves the system's relationship to help user in decision making. Computer output designing should proceed in organized and the right output must be developedensuring that each output element is design so that people will find the system can use easily and effectively [10-11].

**Code Design:** The code is designed to execute using C#.NET as front end to use execute data leakage in CVRDE by using SQL server as back end.A design code is a document that sets rules for the design of a development freshly. It is a programming tool which is used for design and process of planning, however it goes further and more regulatory than other forms of guidance. It should be accompanied by a design rationale that explains objectives, the design code providing instruction to the appropriate degree or precision of the more detailed design work. In this way a design code may be a tool which helps ensure that the aspirations for quality and quantity for housing establishing,for large scale project particularly.

**Architecture Diagram:** Architectural block diagram is a diagram for a system, where principal parts or functions are represented by blocks and connected by lines that show the relationships of the blocks.

The figure shows how the actual working principles take place of Instant Messaging System in Battle Field Management System.

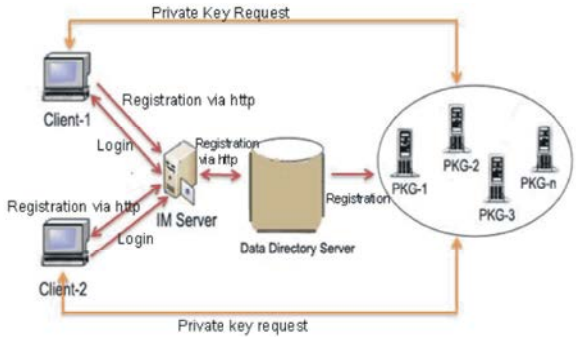


Fig. 4.4.1: ProposeIM System Model

**System Implementation**

**System Description (Work Flow):** The goal the system is to protect data from unauthorized person. It implements the concept Identity-Based Cryptosystem. Private key is generated by the Private Key Generator(PKGs) on request

by the IM client which is more secure than the considered public key. There are three participants in our secure IM model: IM clients, IM Server, PKGs.

IM server is in charge giving authentication to all users of the system and will allow only those users to use its resource. The IM server keeps track of the status for instance online and off-line from computer of each user and stores sufficient information about them to allow another user to set up a peer-to-peer communication channel with them. IM server at the service provider's end know that the user is online and ready to receive messages and the current status of each of their contacts is also downloaded to his client [12-13].

The IM client is a user that can use to send message. Its basic function is to log in the IM server and send message and manage contact list. When a user wishes to send a message to another user, IM client first contacts the IM server to obtain the IP address of the user and the port on which he is listening for incoming messages. The IM client then initiates a TCP connection to that client and sends the secure message by using identity-based cryptosystems. Once the one-to-one communication channel between users has been established, the IM server plays no further part but just to inform the IM clients of updates to the status of their contacts.

The PKGs generate the master key. IM service provider functions as a registration authority, answers for authenticating user information and signing authenticated users' information to PKGs. User can get his private key corresponding to his IM account by performing a blind key issuing protocol with any PKGs. Finally, secure connection between IM client and IM client, IM client and IM Server, which can be proposed using identity-based encryption scheme, identity-based signature scheme, identity-based signcryption or identity-based authenticated key agreement scheme. A user, with an identity ID performs required steps to get his private key according to anonymous key issuing protocol for identity-based cryptosystems. The password is user's chosen password during authentication and the tuple i.eID,password is stored in IM service provider database corresponding to his public key. User can obtain his private key from PKG by type his ID and password at client side.

**Module Description:** In software, a module is a part of programs. Programs are composed of one or more independently developed modules that are not combined until the linked in program. A module can contain one or several routines. In hardware, a module is a self-contained component.

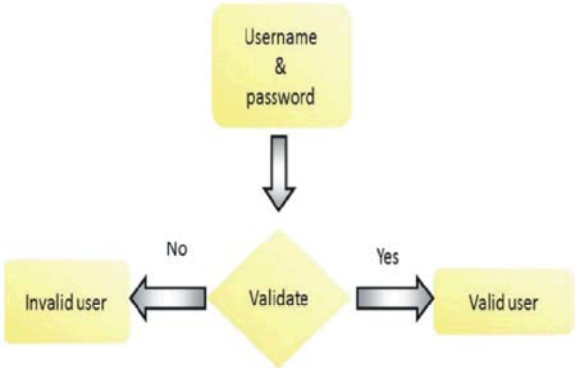


Fig. 5.2.1.1: Authentication Module

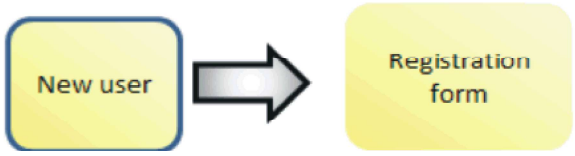


Fig. 5.2.2.1: Registration Module

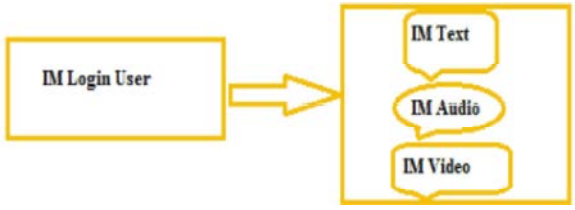


Fig. 5.2.3.1: *Text/video/Audio Module*


Fig. 5.2.4.1: *Talk(Text) Module*


Fig. 5.2.5.1: *Video Module*

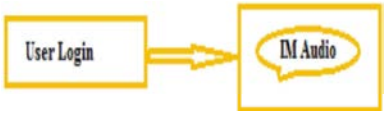


Fig. 5.2.4.1: *Audio Module*

**Authentication Module:** User will be permitted to give the username and password in the login page. If the user name and password is correct means user will allow to accessed the application. If the user name and password is not valid, user will not allow accessing the application.

A user with valid user ID which IM service provider provides will be able to access the service and perform various chat according to his/her preference.

**Registration Module:** User who is new member need to first obtain his private keys by providing his/her public key. By filling various required field in the registration module and after submitting successfully, the new user can use the system.

**IM Text/video/Audio Module:** After successfully login to the chat module, the following (i.e. Text/Audio/Video) are the option that can be selected for communication depending to user ways and mode of communication

**IM Text Module:** After successfully login to the Text module, the use of life Text chat can start. It will display user mood in the chat. Sending text messages and receiving is performed in this module. For instance availability of user can be display.

**IM Video Module:** Once login into the video module, user can have a life video conference on the go. Face to face on the go is communicated at this module.

**IM Audio Module:** Once login into the Audio module, user can communicate one another through talk, it does not involved text or video.

**About(Contact) Module:** This module contain about the details like contacts and other information of the management of Battle field management system. It contains various key personal contacts.

## CONCLUSION

In today's era Internet as a means of communication using Instant Messaging is a very important application. However IM which has very less usage in Battle Field ManagementSystem.Most of these existing instant messaging services were designed giving scalability priority over security. We proposed a secured instant messaging system by using identity-based Cryptosystem, which can further providessecured strong authentication and secured communication for both instant messaging. The proposed instant messaging for usage in Battle Field Management system will help secured the communication to a large extent rather the used of Walky-Talky.

**Future Enhancement:** Future is the stage of the project when the theoretical design is turned out into a system working principal. And also further the application can be integrated with features like the combat vehicles sensors and detectors. The future enhancement of this project can also implement route maps and enemies combat vehicles detectors.

## REFERENCES


1. Mannan, M. and P.C. Oorschot, 2005. Did the study on Instant messaging worms, analysis and countermeasures. ACM workshop.
2. Kikuchi, H., M. Tada and S. Naanishi, 2004. Did the study on secure instant messaging protocol preserving confidentiality against administrator. at 18th International Conference.
3. Raimondo, M.D., R. Gennaro and H. Rawczyk, 2005. Did the study on Secure of-the Record Messaging. ACM 2005 worshop.
4. Eldefrawy, M.H., M.K. Alghathbar, Khan and H. Elkamchouchi did study on Secure Instant Messaging Protocol Centralized Communication Group. 20114th IFIP International Conference.
5. A. Shamir did study on Identity-Based Cryptosystems and Signature Schemes. 1985 at CRYPTO Springer-Verlag.
6. Gennaro, R., *et al.*, 2007. Did study on Secure Distributed key Generation for Discrete-Log Based Cryptosystems. 2007 journal of Cryptology.
7. Wang, C.J., Q. Li, X.Y. Yang, 2006. Did study on Improvement On Sui *et al*'s, that is separable and anonymous key protocol issuing in ID-based Cryptosystem. 2006 IJCS.
8. Boneh, D. and M. Franlin, 2001. Did study on Identity-Based Encryption from the Weil pairing. 2001 Springer-Verlag.
9. Cha, J.C. and J.H. Cheon, 2003. Did study on An Identity-Based Signature from Gap Diffie-Hellman groups. 2003 at PKC, Springer-Verlag.
10. Barreto, *et al*., M., 2005. Did study on Efficient and Provably Secure Identity-Based Signature &Signcryption from Bilinear Maps. at ASIACRYPT, Springer-Verlag.
11. Choie, Y.J., E. Jeong and E. Lee, 2006. Did studyon Efficient identity-based authenticated key agreement protocol from pairings. 2006 at Applied Mathematics and Computation.
12. Shamir, A., 1979. Did study on How to Share a Secret communication at ACM.
13. Pedersen, T.P., 1991. Did study on A Threshold Cryptosystem without a Trusted Party. 1991 at EUROCRYPT, Springer-Verlag.