DESIGN AND IMPLEMENTATION OF INSTANT MESSAGING TOOL FOR BATTLE FIELD MANAGEMENT SYSTEM IN CVRDE

[1]AKHIL NAIR, [2]AMANDEEP SINGH, [3]THEPFUSATUO ALBERT, [4]S.CHAKRAVARTHI

[1,2,3,]Under Graduate Student, [4]Associate Professor Department of computer Science and Engineering
Saveetha School of Engineering Saveetha University Saveetha nagar, Thandalam, Chennai-, India
Email: uma.is95@gmail.com, thepfusatuoalbert@gmail.com, aman27892@gmail.com

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 a public key. The public string could include an email address, domain name, or a physical IP address.

Keywords: Identity-Based Encryption; Identity-Based Signature; Identity-Based Key Issuing; Instant Messaging; Bilinear Pairings;

I. INTRODUCTION

1.1 General Introduction

Instant Messaging enable individual to exchange text messages and track availability of a list of users in real-time. IM worms and secure communication are two safety issues of instant messaging system. Most of the existing systems 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: Confidentiality, Integrity, Authentication and Non-repudiation. 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. In this paper we propose a secure instant messaging system for Battle field Management by using identity-based cryptosystems, 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 from the PKG to the user through a secure channel.

1.2 Identity-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 a public key. The public string could include an email address, domain name, or a physical IP address. The identity-Based system allows any party to generate a public key from a known identity value. Trusted third party, called private key 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 returns to user his private key.

1.2.1 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 Adi shamir in 1984.

1.2.2 Identity-Based decryption

Identity-Based decryption is computed by the PKG based on the ID associated with the receiver and a secret master key. After obtaining the private decryption key from the PKG, the receiver uses it together with the element rp and bilinear map to compute the secret message key, which is then used to decrypt the original message.

1.2.3 Identity-Based signature

Identity-based signature depends on the assumption that secret keys are absolutely secure. Once a secret key is exposed, all signatures associated with this secret key have to be reissued. Therefore limiting the impact of key exposure in Identity-Based Signature is an important task.

II. SYSTEM ANALYSIS

2.1 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.

2.2 Disadvantage of Existing System

There are various disadvantages in the existing. Some of them are as follows:

i) Giving more scalability priority over security.

ii) There is no built in support (like confidentiality, integrity, authentication and non-repudiation).

2.3 Proposed System

We propose a secure IM system by using Identity-Based Cryptosystem, which can provide strong authentication and secure communication (confidentiality, integrity, authentication and non-repudiation) for both IM client to IM client and IM client to IM server. Secure communications include the Properties: confidentiality, integrity, authentication and non-repudiation. For secure and confidentiality proposed a modified Diffie-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.

2.4 Advantage of Proposed System

The Main advantages of using the proposed IM system are as follows:

i). Gives more priority on security than scalability.

ii). IM system support (like confidentiality, integrity, authentication and non-repudiation) by using Identity-Based Cryptosystem.

iii). Generation of private key on request is very secure.

iv). 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.

III. SYSTEM SPECIFICATION

3.1 Technologies Used

Microsoft DOTNET is a set of Microsoft software technologies for rapidly building and integrating XML Theb services, Microsoft Windows-based application, and Theb solution.

3.1.1 Visual Studio Platform

Microsoft Visual Studio is an integrated development environment (IDE) from Microsoft. Microsoft Visual Studio platform includes a code editor supporting IntelliSense as well as code refactoring. The integrated debugger works both as a source-level debugger and a machine-level debugger. Other built-in tools include a forms designer for building GUI applications, web designer, and database schema designer. It accepts plug-ins that enhance the functionality at almost every 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 different programming languages by means of language services, which allow the code editor and debugger to support (to varying degrees) nearly any programming language, provided a language-specific service exists. Support for other languages such as M, Python, and Ruby among others is available via language services installed separately. Individual language-specific versions of Visual Studio also exist which provide more limited language services to the user: Microsoft Visual Basic, Visual J#, Visual C#, and Visual C++.

3.1.2 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 to be simple, modern, general purpose, object-oriented programming language. The language was built for intention to developing software components.

3.1.3 Microsoft SQL Server R2

Microsoft SQL Server is a relational database management system. As a database, it is a software product whose primary function is to store and retrieve data as requested by other software applications, be it those on the same computer or those running on another computer across a network. SQL Server includes better compression features, which also 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 Services, a central management of master data entities and hierarchies.

IV. SYSTEM DESIGN

4.1. 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.

4.2. Output Design

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making. Designing computer output should proceed in an organized, the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively.

4.3 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 new development. It is a tool that can be used in the design and planning process, but goes further and is more regulatory than other forms of guidance. It should be accompanied by a design rationale that explains the objectives, with the design code providing instructions 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 developments, particularly for large-scale projects.

4.4. Architecture Diagram

Block diagram is a diagram of a system, in which the principal parts or functions are represented by blocks connected by lines that show the relationships of the blocks.

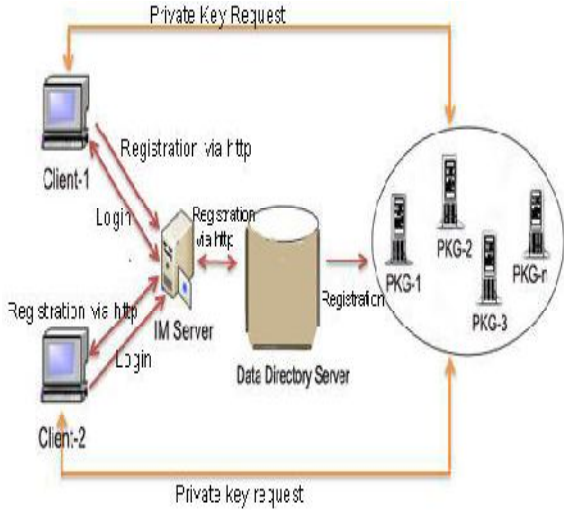

Fig. 4.4.1Propose IM System Model

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

V. SYSTEM IMPLEMENTATION

5.1 System Description (Work flow)

The main goal of this system is to protect the 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. The IM server is in charge to authenticate all users in 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.

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 server, IM client and client, can be implemented by using proposed identity-based encryption scheme, identity-based signature scheme, identity-based signcryption scheme 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.e ID,password is stored in IM service provider database corresponding to his public key. User can type his ID and password at client side for obtaining his private key from PKG.

5.2 Module Description

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

5.2.1 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 to access 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.

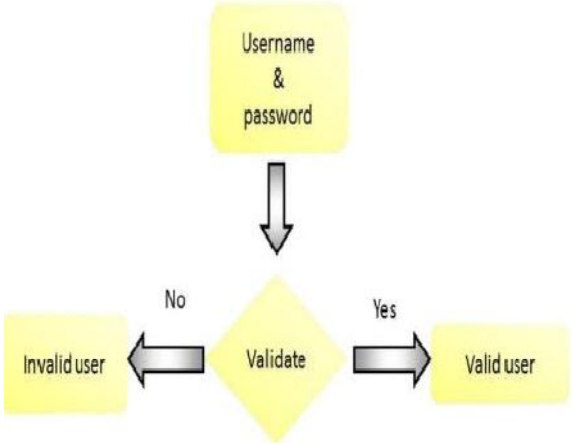

Fig. 5.2.1.1 Authentication Module

5.2.2 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.

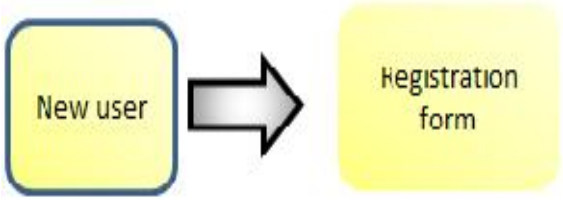

Fig .5.2.2.1 Registration Module

5.2.3 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

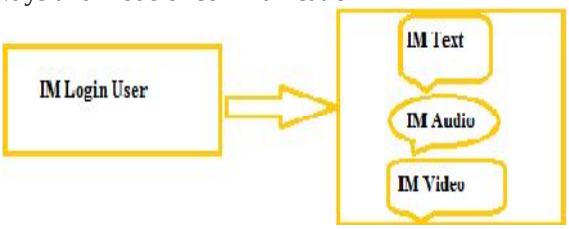

Fig. 5.2.3.1 Text/video/Audio Module

5.2.4 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 thismodule. For instance availability of user can be display.

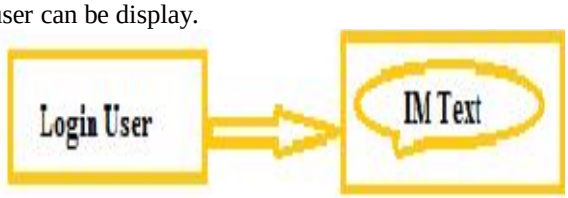

Fig. 5.2.4.1 Talk(Text) Module

5.2.5 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.

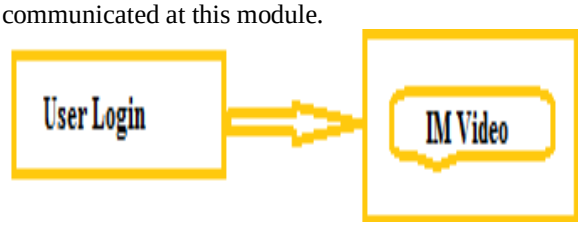

Fig. 5.2.5.1 Video Module

5.2.6 IM Audio Module

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

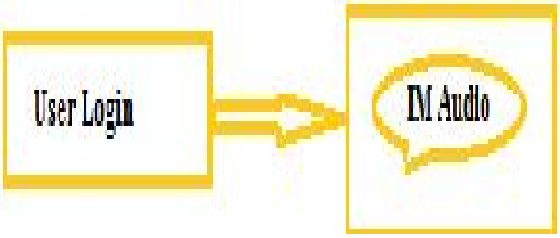

Fig. 5.2.4.1 Audio Module

5.2.7 About (Contact) Module

This module contain about the details like contacts and other information of the management of Battle field management system.

VI. SYSTEM TESTING

6.1 Software Testing

Software testing is an investigation conducted to provide stakeholders with information about the quality of the product or service under test. Software testing can also provide an objective, independent view of the software to allow the business to appreciate and understand the risks of software implementation. Test techniques include, but are not limited to, the process of executing a program or application with the intent of finding software bugs. Software testing can be stated as the process of validating and verifying that a computer program/ application/product:

- meets the requirements that guided its design and development,
- works as expected,
- can be implemented with the same characteristics,
- and satisfies the needs of stakeholders.

Software testing, depending on the testing method employed, can be implemented at any time in the development process. Traditionally most of the test effort occurs after the requirements have been defined and the coding process has been completed, but in the agile approaches most of the test effort is on-going.

6.2 Testing Method

 White-Box testing

White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) tests internal structures or workings of a program, as opposed to the functionality exposed to the end-user. In white-box testing an internal perspective of the system, as well as programming skills, are used to design test cases. The tester chooses inputs to exercise paths through the code and determine the appropriate outputs. Techniques used in white-box testing include:

- API testing testing of the application using public and private APIs.
- Code coverage – creating tests to satisfy some criteria of code coverage (e.g., the test designer can create tests to cause all statements in the program to be executed at least once)
- Fault injection methods – intentionally introducing faults to gauge the efficacy of testing strategies
- Mutation testing methods
- Static testing methods

 Black-box testing

Black-box testing treats the software as a "black box", examining functionality without any knowledge of internal implementation. The tester is only aware of what the software is supposed to do, not how it does it. Black-box testing methods include:

- equivalence partitioning
- boundary value analysis
- all-pairs testing
- state transition tables
- decision table testing
- fuzz testing
- model-based testing
- use case testing
- exploratory testing
- and specification-based testing.

 Visual testing

The aim of visual testing is to provide developers with the ability to examine what was happening at the point of software failure by presenting the data in such a way that the developer can easily find the information he requires, and the information is expressed clearly. Visual testing provides a number of advantages. The quality of communication is increased dramatically because testers can show the problem (and the events leading up to it) to the developer as opposed to just describing it and the need to replicate test failures will cease to exist in many cases. Visual testing is gathering recognition in customer acceptance and usability testing, because the test can be used by many individuals involved in the development process.

 Grey-box testing

Grey-box testing involves having knowledge of internal data structures and algorithms for purposes of designing tests, while executing those tests at the user, or black-box level. The tester is not required to have full access to the software's source code.

CONCLUSION

In today’s era Internet as a means of communication using Instant Messaging is a very important application. It is mostly used as a social communication tool to a large extent and means of business communications tool. However IM which has very less usage in Battle Field Management System. 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 cryptosystems, which can provide 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 working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

REFERENCES

[1] M. Mannan and P. C. Oorschot did the study on Instant messaging worms, analysis and countermeasures. 2005 ACM workshop.

[2] H. Kikuchi, M. Tada & S. Naanishi did the study on Secure instant messaging protocol preserving confidentiality against administrator. 2004 at 18th international conference.

[3] M. D. Raimondo, R. Gennaro and H. rawczyk did the study on Secure of-the record messaging. 2005 ACM workshop.

[4] M. H.Eldefrawy, Alghathbar, M.K. Khan, 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] R. Gennaro, et al did study on Secure Distributed key Generation for Discrete-Log Based Cryptosystems. 2007 journal of Cryptology.

[7] C.J. Wang, Q. Li, X.Y. Yang did study on Improvement on Sui et al.'s Separable and Anonymous Key issuing Protocol in ID-based Cryptosystem. 2006 International Journal of Computer Science.

[8] D. Boneh & M. Franlin did study on Identity-Based Encryption from the Weil pairing. 2001 Springer-Verlag.

[9] J.C. Cha & J.H. Cheon did study on An Identity-Based Signature from Gap Diffie-Hellman groups. 2003 at PKC, Springer-Verlag.

[10] M. Barreto, et al. did study on Efficient and Provably Secure Identity-Based Signature & Signcryption from Bilinear Maps. 2005 at ASIACRYPT, Springer-Verlag.

[11] Y.J. Choie, E. Jeong, & E. Lee did studyon efficient identity-based authenticated key agreement protocol from pairings. 2006 at Applied Mathematics and Computation.

[12] A. Shamir did study on How to Share a Secret Communication of the ACM. 1979.

[13] T. P.Pedersen did study on A Threshold Cryptosystem without a Trusted Party. 1991 at EUROCRYPT, Springer-Verlag.

[14] D. Boneh, Lynn, & H. Shacham did study on Short Signature from the weil Pairing. 2004 Journal of Cryptology.

★★★