P2P Secure Communication System

(For Military Field Environment)

By

Basit Shehbaz

Muhammad Majid Jahangeer

Abdul Rehman

Submitted to Faculty of Department of Computer Software EngineeringNational University of Sciences and Technology, Islamabad in partial fulfilment for the requirements of a B.E Degree in Computer Software Engineering, June 2016

In the name of Allah, the Most Beneficent, the Most Merciful

ABSTRACT

P2P Secure Communication System (For Military Field Environment)

Current age of time is known as “age of communication”. Any institution or department without fluid internal and external communications cannot survive, rather useless, now-a-days. Similarly, there is a strong need for communication in military filed environment. We had many communication devices over past several decades. Most of them works over frequency based communication. Due to significant advancement and revolutions in communication technologies, devices are being converted to digital systems.

P2P Intranet Communication App for Military Filed Environment is also an advancement towards modern age digital systems. All communications are performed over IP based fast and secure network.Operational environment of Army is highly fluid and ad hoc. It is expected that only trivial IT capability will be available to user in operational environment. It is also expected that the user in a military field environment have a very little training of operating digital devices.

This system facilitates field commanders to share information with other command echelons in a secure, encrypted and reliable manner. Application also provides an interface that may be used by operating system or other applications to use application services. Special points are taken into account to fulfill the needs of a military field environment. System is efficient enough to be supported by the minimum hardware technology available to field commanders.

CERTIFICATE FOR CORRECTNESS AND APPROVAL

It is certified that work contained in the thesis – P2P Secure Communication System (for military field environment) carried out by Basit Shehbaz, Muhammad Majid Jahangeer, Abdul Rehman under supervision of Dr. Naima Iltaf for partial fulfilment of Degree of Bachelor of Software Engineering is correct and approved.

Approved By

Dr. Naima Iltaf

Department of CSE, MCS

Dated:

_____

DECLARATION

No portion of the work presented in this dissertation has been submitted in support of another award or qualification either at this institution or elsewhere.

DEDICATION

To great Muslim Scientists and Researchers of the history whose accomplishments have greatly contributed to the progress of this modern world and who are of great inspiration to us to excel in the fields of Science and Technology.

ACKNOWLEDGEMENTS

There is no success without the will of ALLAH Almighty. We are grateful to ALLAH, who has given us guidance, strength and enabled us to accomplish this task. Whatever we have achieved, we owe it to Him, in totality. We are also grateful to our parents and family and well-wishers for their admirable support and their critical reviews. We would like to thank our supervisor. Dr. Naima Iltaf, for her continuous guidance and motivation throughout the course of our project. Without their help we would have not been able to accomplish anything.

Table of Contents

List of Figures

Chapter 1. Introduction

1.1. Overview

This system facilitates field commanders to share information with other command echelons in a secure, encrypted and reliable manner. Application provides an interface that may be used by operating system or other applications to use application services. Special requirement are taken into account to fulfill the needs of a military field environment. System is efficient enough to be supported by the minimum hardware technology available to field commanders.

1.2. Problem Statement

Conventionally, all the communication systems used by military were based on radio communication which wasn't secure because radio signals can be captured more easily. Moreover, radio communication is not much reliable as IP communication. This product will facilitate the field commanders for same function but in much fast, secure, reliable and efficient way. Moreover, all required types of communication would be possible by the software like text message transmission and files of all types and size.

1.3. Approach

The project's research and development comprises of application level protocol designing and implementation based on the reliable underlying channel of network layer. The implementation of communication security features used this project are based on RSA and AES ciphers. SQLite database library is used for modeling the data transmitted over the network. All the components are developed independently and integrated through defined interfaces. Application also provides non GUI version of the project that can be used as API for the further development of this project.

1.4. Scope

This project is intended to provide a reliable application level protocol for smooth flow of information between the peers in military field environment. A complete software application will then be built over the developed protocol. The scope of the project is to transfer text messages and files. API will also be provided to use the protocol and

application services. The communication architecture is entirely peer to peer. All the communication will be in encrypted form. Communication will only be supported on the node's local IP network.

1.5. Objectives

The main objective of this software system is to provide a facility to field commanders of military for easy, secure and reliable communication in the military field environment. All required types of communication are possible by the software system developed i.e. text message and files transmission of all types and size.

During the course of this project, all the aspects of software engineering are covered i.e. survey and feasibility analysis, requirement gathering, architectural and detailed design, implementation and testing along with documentation (SRS, SDS, Test Document, Final Report and User manual). Students are also expected to develop extensive knowledge and technical skills in the following fields:

1.1. Communication Protocols designing
1.2. Socket Programming
1.3. Implementing Public Key Infrastructure
1.4. Implementing AES and RSA

1.6. Deliverables

Sr	Tasks	Deliverables
1	Literature Review	Literature Survey and Feasibility Analysis
2	Requirements Specification	Software Requirements Specification document (SRS)
3	Detailed Design	Software Design Specification document (SDS)
4	Implementation	Project demonstration
5	Testing	Evaluation plan and test document
6	Training	Deployment plan
7	Deployment	Complete application withnecessary documentation

Chapter 2. Literature Review

Military communications or military signals involve all aspects of communications, or conveyance of information, by armed forces. Military communications span from pre-history to the present. The earliest military communications were delivered by humans on foot. Later, communications progressed to visual and audible signals, and then advanced into the electronic age. Examples from Jane's Military Communications include text, audio, facsimile, tactical ground-based communications, terrestrial microwave, tropospheric scatter, naval, satellite communications systems and equipment, surveillance and signal analysis, encryption and security and direction-finding and jamming.

2.1. History of Communication in Military

The first military communications involved the use of runners or the sending and receiving of simple signals (sometimes encoded to be unrecognizable). The first distinctive uses of military communications were called "signals". Modern units specializing in these tactics are usually designated as "signal corps". The Roman system of military communication (cursus publicus or cursus vehicularis) is an early example of this. Later, the terms "signals" and "signaler" became words referring to a highly-distinct military occupation dealing with general communications methods (similar to those in civil use) rather than with weapons.

Present-day military forces of an informational society conduct intense and complicated communicating activities on a daily basis, using modern telecommunications and computing methods. Only a small portion of these activities are directly related to combat actions.Modern concepts of network-centric warfare (NCW) rely on network-oriented methods of communications and control to make existing forces more effective.

2.2. Communication Equipment Used by Armed Forces

Drums, horns, flags, and riders on horseback were some of the early methods the military used to send messages over distances.

Many modern pieces of military communications equipment are built to both encrypt and decode transmissions and survive rough treatment in hostile climates. They use different frequencies to send signals to other radios and to satellites.

Military communications - are activities, equipment, techniques, and tactics used by the military in some of the most hostile areas of the earth and in challenging environments such as battlefields, on land, underwater and also in air. Military communications include command, control and communications and intelligence and were known as the C3I model before computers were fully integrated. The U.S. Army expanded the model to C4I when it recognized the vital role played by automated computer equipment to send and receive large, bulky amounts of data.

2.3. Further Information - C4I

The first military communications tool was the communication automobile designed by the Soviet Union in 1934 to send and receive signals. The signals were encoded to help prevent the enemy from intercepting and interpreting top-secret communications. The advent of distinctive signals led to the formation of the signal corps, a group specialized in the tactics of military communications. The signal corps evolved into a distinctive occupation where the signaler became a highly technical job dealing with all available communications methods including civil ones.

In the modern world, most nations attempt to minimize the risk of war caused by miscommunication or inadequate communication. As a result, military communication is intense and complicated, and often motivates the development of advanced technology for remote systems such as satellites and aircraft, both manned and unmanned, as well as computers. Computers and their varied applications have revolutionized military communications. Although military communication can be used to facilitate warfare, it also supports intelligence-gathering and communication between adversaries, and thus sometimes prevents war.

2.4. Categories of Military Communications

1. Alert measurement systems
2. Cryptography
3. Military radio systems
4. Nuclear command control
5. The signal corps
6. Network-centric warfare

Cryptography is the study of methods of converting messages into disguised, unreadable information, unless one knows of the method of decryption. This military communications method ensures that the messages reach the correct hands. Cryptography is also used to protect digital cash, signatures, digital rights management, and intellectual property rights and secure electronic commerce. It is also used in computing, telecommunications and infrastructure.

2.5. Conclusion

There is a must need to advance in the field of communication for a Military to secure and improve its intelligence. Modern communication systems are IP based systems with strong cryptographic algorithms. Secure IP Communication System, supports encrypted textual data and filetransmission on the same network and fulfills the requirements and standards of Pakistan Army. Secure Server lessCommunication System is a system that can be used in both tactical and strategic systems. Secure Server lessCommunication System supports approved military encryption algorithms.

Chapter 3. Software Req. Specification (SRS)

3.1. Introduction

Purpose

This document includes software requirements for **Intranet P2P Communication Application for Military Field Environment**, release number 1.0. Communication software will provide remote access to systems and exchange files and messages in text. Operational environment of Army is highly fluid and ad hoc. This system will facilitate field commanders to share information with other command echelons in a secure, encrypted and reliable manner. Application will also provide an interface that may be used by operating system or other applications to use application services. Special points will be taken into account to fulfill the needs of a military field environment. System will be efficient enough to be supported by the minimum hardware technology available to field commanders.

This document specifies the detailed requirements of a communication application that is being developed to provide means of information exchange between the field commanders in operational environment. Document also focuses all the stakeholders involved in this project.

Document Conventions

- When writing this document it was inherited that all requirements have the same priority.
- This document mainly addresses the requirements of client (Army). This document also fulfills the requirements for FYP, CSE Dept. MCS, NUST.
- First there is presented an overall view about Intranet P2P Communication App and then all features and functions are analyzed in detail.
- In this document we assume that the user is male for convenience. However the system is intended for both male and female users.
- When writing this document it was inherited that no System/Subsystem Specification documents (SSS) or any other contract document exists.

Intended Audience and Reading Suggestions

This requirements document contains general information about Intranet P2P Communication App, use cases, functions, features and special technologies. It describes in detail all that an intranet communication system needs to do for a military field environment. Functional and non-functional requirements are addressed

separately. System features with use cases and constraints are discussed in detail. System interfaces are also discussed in detail.

For better understanding, the document is divided into sections:

- In section 2 an overall description of Application is provided. First product perspective is presented with product features and main functions. Then follow user classes and characteristics, operating environments that Application supports as well as design and implementation constrains. After all that, user documentation is presented and will provide you with more details about each feature's technology.
- In section 3 most important features are presented with detailed description, use cases and requirements.
- In section 4 user, hardware, software and communication interfaces are described.
- In section 5 requirements about security, safety and performance are presented along with the software quality attributes of the Application.

This document is intended for:

- **Developers:** (Project Group)

  In order to be sure that they are developing the right project that fulfills the requirements provided in this document.
- **Testers:** (Project Group, Supervisor, C4I)

  In order to have an exact list of the features and functions that must respond according to requirements.
- **Users:** (Field Commanders)

  In order to get familiar with the idea of the project and how to use/respond in failure situations and suggest other features that would make it even more functional.
- **Documentation writers:** (Project Group, Field Commanders)

  To know what features and in what way they have to explain. What technologies are required, how the system will respond in each user's action, what possible system failures may happed and what are the solutions to all those failures etc.
- **Project Supervisor:** (Dr. Naima Iltaf)

  This document will be used by the project supervisor to check and guide the group about the understanding and implementation of the requirements properly and completely during the development lifecycle.
- **Project Evaluators:** (CSE Dept. MCS)

  In order to know the scope of the project and evaluate the project throughout the development for grading.

Project Scope

This project is intended to provide a reliable application level protocol for smooth flow of information between the peers in military field environment. A complete software application will then be built over the developed protocol. The scope of the project is to transfer text messages and files. API will also be provided to use the protocol and application services. The communication architecture is entirely peer to peer. All the communication will be in encrypted form. Communication will only be supported on the node's local IP network.

References

More about application can be retrieved from project development team.

Abdul Rehman

BESE 18 MCS NUST

Group Leader – Dev. Team

Email: mail.abdulrehman.pk@gmail.com

3.2. Overall Description

Product Perspective

The product is a new project that will help filed commanders of Pak Army for easy and secure communication in the military field environment. Conventionally all the communication was radio communication which wasn't secure because radio signals can be captured more easily. Moreover, radio communication is not much reliable as IP communication. This product will facilitate the field commanders for same function but in much fast, secure, reliable and efficient way. Moreover, all required types of communication would be possible by the software like text message transmission and files of all types and size.

Product Function:

Main features of the product are given below:

- Broadcasting node's availability
- Node discovery
- Text messaging
- File transfer
- Will use Encrypted Communication
- Can be used as OS/Application service
- Can be invoked by other applications for retrieving and sending messages
- Will maintain encrypted chat logs on remote server
- Admin panel for accessing chat logs

User Classes and Characteristics

Following are user classes and their brief description.

Tester (occasional user)

Tester will use this project to check for bug finding. They will also use the project to check if it's in accordance to the Software Requirements Specification document.

Project Supervisor (occasional user)

Project supervisor will also use the product to evaluate. They will use this product to find the accuracy and error in the output.

Field Commander (Regular user)

Field commander will use the product to communicate the field environment with other field commanders.

Operating environment

Required operating environment for the application is listed below.

Hardware Requirements:

- **Computer/Mobile device:** To install software for communication
- **Network Infrastructure:** To provide the network connection to the software.

Software Requirements:

- **Operating System:** Windows (7, 8, 8.1, 10), Linux
- **Java Virtual Machine:** To run the application

Design and Implementation Constraints

Constraints of the product are given below:

- App will not work without network connection.
- If a node is offline then communication with that node will not be possible.
- Communication and speed will be dependent on network infrastructure's specifications.
- Communication outside the logical (IP network) will not be possible.
- Time required to transfer the file will also be dependent on file size.

User Documentation

A user manual will be provided to the users in which separate instructions will be given according to the particular user i.e. Regular user and the admin, developers and testers. It will include the details of the system's working. Help documents will also be a part of the system.

The project report will also be available for the users which will highlight the system features, working and procedures.

Assumptions and Dependencies

- Overall performance of the product will depend on the hardware infrastructure and network speed.
- User must know the language and User Interface for the better performance of the product.
- Limitations of the product must be kept in mind by the user.

3.3. System Features

System features are organized by use cases and functional hierarchy so that the main functions of the system will be understandable. In the description of system features there are several references in various system interfaces. These interfaces are better explained in section 4.1 of this document.

Node Availability Broadcast

This feature allows a node to broadcast its availability to its local network.

Description

When a node is up on the network it must be able to broadcast its availability to the entire network. So that each node will be able to see all the nodes available on the network for communication.

Stimulus/Response Sequences

Data flow:

Basic Data Flow

1. User opens application and its local network configuration is retrieved.
2. User is displayed its network configuration.
3. User's node availability is broadcasted to entire network automatically.

Alternative Data Flows

Alternative Data Flow 1

1. User opens application and is not connected to any network.
2. Error message is displayed to user.

Alternative Data Flow 2

1. User opens application and application is blocked from firewall.
2. Application prompts user to allow network accessibility to application.

Functional Requirements

1. Application must be installed and system's network is configured properly.
2. Communication channel is available to application.
3. Application is allowed to communicate by the operating system.

Network Nodes' Discovery

This feature provides the ability to discover all nodes broadcasting on local network.

Description

When a node will broadcast its availability then each available node must be able to discover the availability of each availability broadcasting node from the entire local network and display its ID to the user as online node.

Stimulus/Response Sequences

Data flow:

Basic Data Flow

1. User opens Application and its local network configuration is retrieved.
2. Application opens a broadcast listener for the local network on a logical port.
3. Application reads all the broadcasts by the other nodes and discover network.

Alternative Data Flows

Alternative Data Flow 1

1. User opens application and is not connected to any network.
2. Error message is displayed to user.

Alternative Data Flow 2

1. User opens application and is application is blocked from firewall.
2. Application prompts user to allow network accessibility to application.

Functional Requirements

1. Application must be installed and system's network is configured properly.
2. Communication channel is available to application.
3. Application is allowed to communicate by the operating system.

Messaging

This feature will provide text message transfer over the network.

Description

User must be able to transfer text messages on the local network. A friendly user interface must be provided to user to type the message. He must also be able to copy/Paste messages.

Stimulus/Response Sequences

Data flow:

Basic Data Flow

1. User clicks any online node and select text message option.
2. User type text message and press send.
3. Text message is sent.

Alternative Data Flows

Alternative Data Flow 1

1. User clicks any online node and select text message option.
2. User paste text in text filed and press send.
3. Text message is sent.

Alternative Data Flow 2

1. User press send message and message is failed.
2. Error is displayed to the user.

Functional Requirements

1. Application must be installed and running.
2. Remote node is online.

File Transfer

This feature allows user to transfer files.

Description

User must also be able to transfer files on the local network. A friendly user interface will be provided. User must also be able to drag and drop files.

Stimulus/Response Sequences

Data flow:

Basic Data Flow

1. User clicks any online node and select file transfer option.
2. User type selects file from hard drive and press send.
3. File is sent.

Alternative Data Flows

Alternative Data Flow 1

1. User clicks any online node and select file transfer option.

2. User drag and drop file and press send.
3. File is sent.

Alternative Data Flow 2

1. User press send and transfer is failed.
2. Error is displayed to the user.

Functional Requirements

1. Application must be installed and running.
2. Remote node is online.

Encryption

This feature will encrypt all the data.

Description

All the data sent over the network as well as the communication logs must be encrypted before transfer and saving them respectively. Application must provide a highest possible security of data.

Stimulus/Response Sequences

Data flow:

Basic Data Flow

1. User send any message or file over the network or log is created.
2. All the data is encrypted.
3. Data is transferred or log is saved.

Alternative Data Flows

There is not alternative flow available to this system feature.

Functional Requirements

1. Application must be installed and running.

Chat Log

This feature will create communication history.

Description

Application must create chat and file transfer history record and save it on the local device when internet is not available. This log must be synchronized to a remote server when internet is available to a node (see section 3.7).

Stimulus/Response Sequences

Data flow:

Basic Data Flow

1. User send any file or text message to any node.
2. Communication log is created.
3. Log is saved.

Alternative Data Flows

There is no alternative flow available to this system feature.

Functional Requirements

1. Application must be installed and running.

Log Synchronization

This feature will synchronize communication log.

Description

Application must constantly detect availability of internet connection and must synchronize communication log created on a remote server upon the availability of internet.

Stimulus/Response Sequences

Data flow:

Basic Data Flow

1. Application detects internet availability for local node.
2. Communication log created since last sync is synchronized on remote server.

Alternative Data Flows

Alternative Data Flow 1

1. Application detects unavailability of internet for local node.
2. Application keeps on detecting the availability of internet connection.

Functional Requirements

3. Application must be installed and running.
4. Internet connection is available.

Admin Panel

Application also provides an admin panel.

Description

Application must provide an admin panel to the user to access communication logs and history. This feature must be hidden and available on providing password.

Stimulus/Response Sequences

Data flow:

Basic Data Flow

1. User clicks on the admin panel.
2. Login is prompted.
3. User enters correct login ID and password.
4. User is directed to admin panel.

Alternative Data Flows

Alternative Data Flow 1

1. User clicks on the admin panel.
2. Login is prompted.
3. User enters wrong login ID and password.
4. User is redirected to login screen with error message.

Functional Requirements

1. Application must be installed and running.
2. User must provide correct login information.

3.4. External Interface Requirements

User Interfaces

Responsive graphical user interfaces must be provided to user to work with the application. Here are few dummy screenshots of the application:

Text messaging screens:

User can type text messages in the field and press enter to send. Recipient's ID will be shown to user on top of the page.

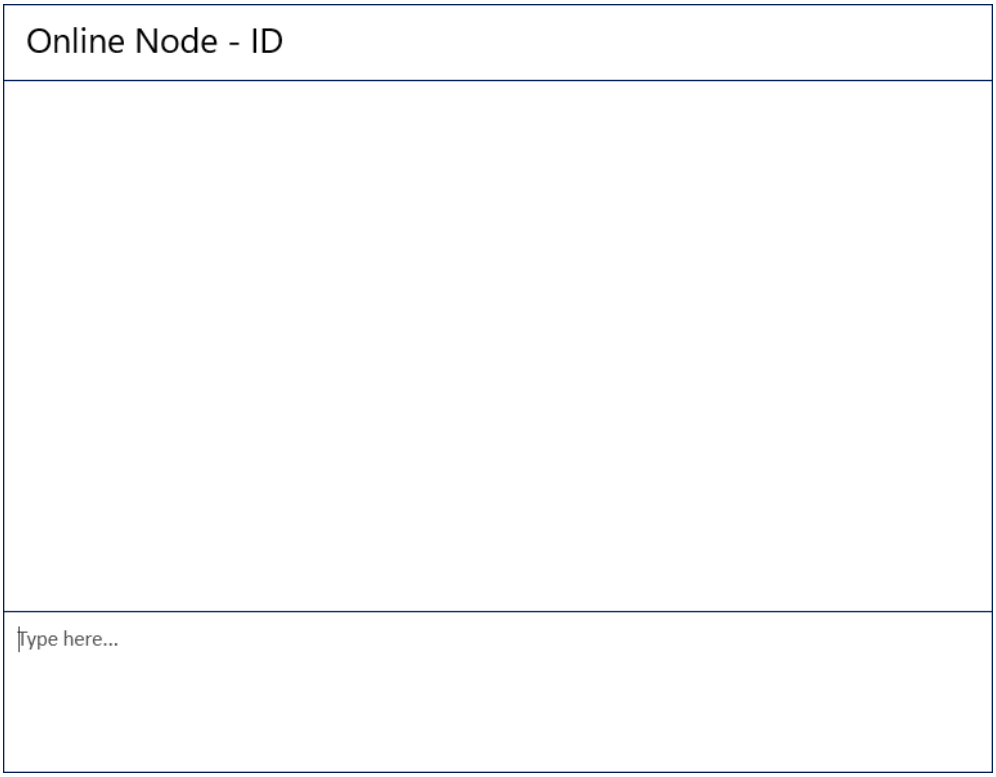

Figure 3.4.1 Text Messaging Screen

File Transfer screens:

User can select files by clicking on the select file button and click send to send files. Recipient's ID will be shown to user on top of the page.

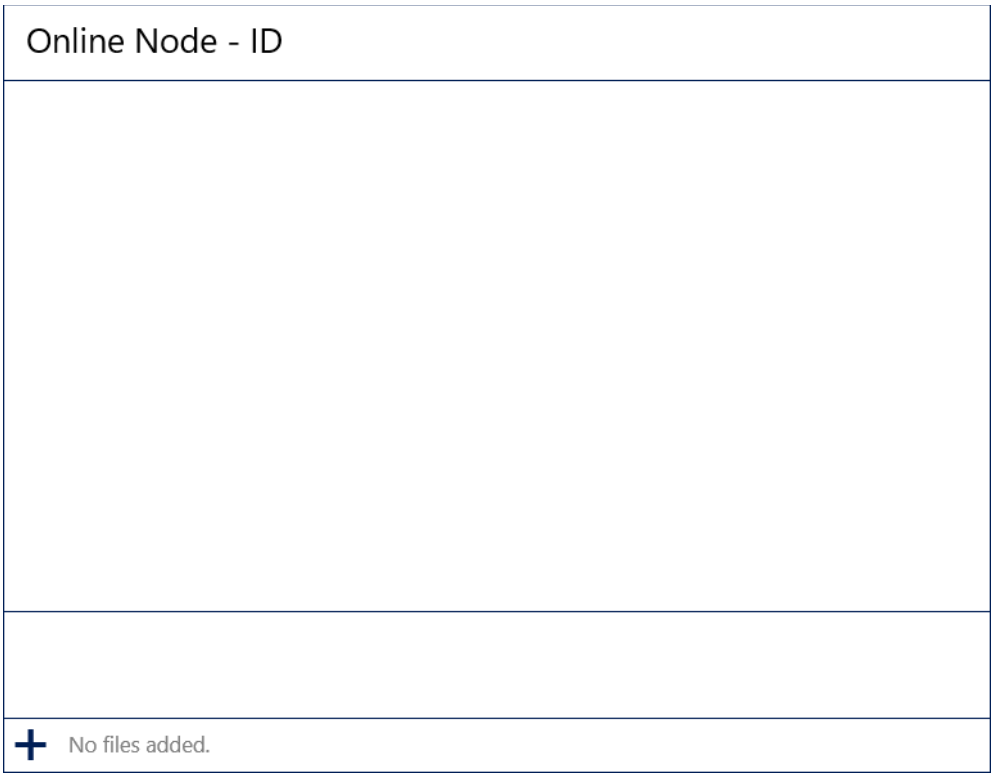

Figure 3.4.2 File Transfer Screen 1

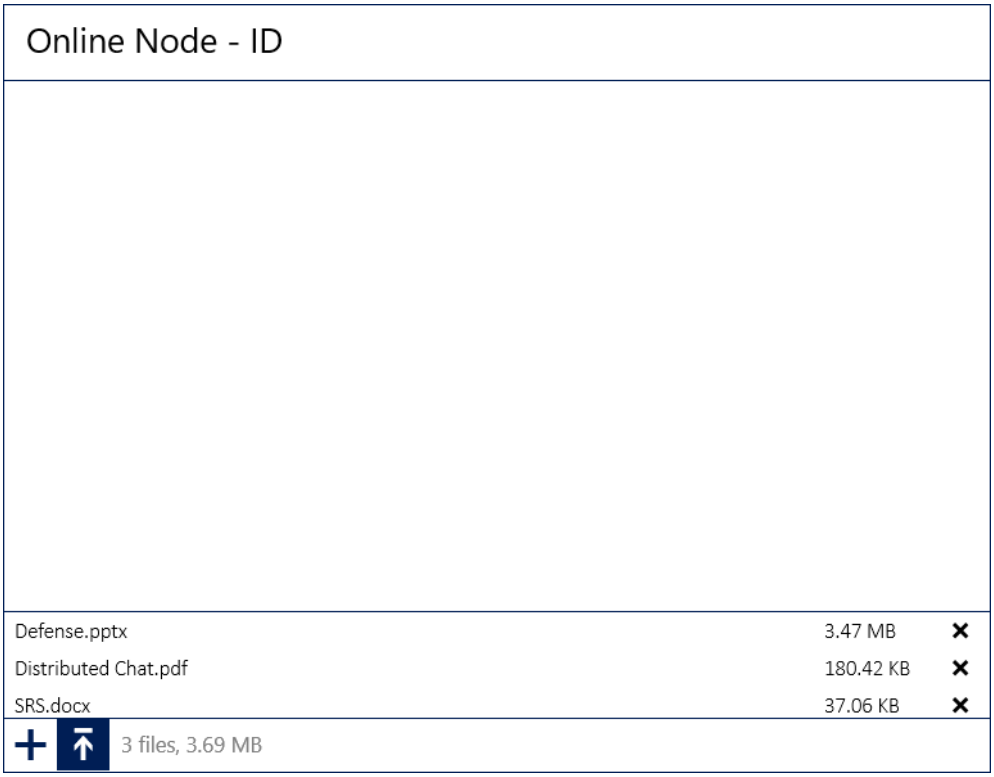

Figure 3.4.3 File Transfer Screen 2

Hardware Interfaces

This product requires a functional PC in order to work properly. Application should be installed on a PC that meets at least the minimum hardware requirements. That means that the PC must work using a Pentium IV or Athlon XP 1.6 GHz processor or newer ones, must have 500 MB RAM and 50 MB free hard drive space. Application supports log synchronization on remote server that require an internet connection. In order for this feature to function the user should also have some kind of Modem or Router connected to his PC and internet, though it does not affect other functions.

Software Interfaces

Application should be able to run on a Windows based platform using Microsoft Windows XP or newer versions. Application should also be able to run on a Linux platform. JVM should also be installed on the platform to run the application. Because application supports copying and pasting messages, therefore it also uses the Clipboard. Applications should also be installed to open the files transferred by other nodes.

Communications Interfaces

Application internally uses TCP to talk with the remote nodes. Application has its own developed protocols for communication and file transfer. The user must also enable firewall to enable communication. System should also be connected to a network for local communication and internet for log synchronization on remote server.

3.5. Other Nonfunctional Requirements

Performance Requirements

Application shall run on a minimal amount of memory and take up a small amount of disk space after install. Depending on the performance of the user's computer, the communication might slow down the Application.

Safety Requirements

This application is a fast and responsive program. However as mentioned in section 5.1 working with large data may lead Application to become unresponsive or even crash. Network crash will also waste a lot of time and user may lose information about message transfer.

Security Requirements

User has direct access in this application. Password or username are not required except for admin panel. To be able to use application user should also allow application on firewall and use system and network resources. The user should also share his IP address only with other trusted users.

Software Quality Attributes

- **Reliability**

  Application should provide reliability to the user. The product will run stably with all the features mentioned above available and executing perfectly. It should be tested and debugged completely. All exceptions should be well handled.

- **User Friendliness/Simplicity**

  Application should have a graphical user interface with user friendly menu and options.

- **Availability**

  Application will be provided to field commander through proper military protocols.

Chapter 4. Design and Development

4.1. Introduction

Current age of time is known as “age of communication”. Any institution or department without fluid internal and external communications cannot survive, rather useless, now-a-days. Similarly, there is a strong need for communication in military filed environment. We had many communication devices over past several decades. Most of them works over frequency based communication. Due to significant advancement and revolutions in communication technologies, devices are being converted to digital systems.

P2P Intranet Communication App for Military Filed Environment is also an advancement towards modern age digital systems. All communications are performed over IP based fast and secure network.

Purpose

This document includes software design for **Intranet P2P Communication Application for Military Field Environment**, release number 1.0. Communication software provides remote access to systems and exchange files and messages in text. Operational environment of Army is highly fluid and ad hoc. This system facilitates field commanders to share information with other command echelons in a secure, encrypted and reliable manner. Application provides an interface that may be used by operating system or other applications to use application services. Special requirement are taken into account to fulfill the needs of a military field environment. System is efficient enough to be supported by the minimum hardware technology available to field commanders.

This document specifies the detailed architectural design of a communication application that is being developed to provide means of information exchange between the field commanders in operational environment. Document includes classes and their inter-relationships, use cases with detailed descriptions, sequence diagrams and various flow charts.

Project Scope

This project is intended to provide a reliable application level protocol for smooth flow of information between the peers in military field environment. A complete software application will then be built over the developed protocol. The scope of the project is to transfer text messages and files. API will also be provided to use the protocol and application services. The communication architecture is entirely peer to peer. All the

communication will be in encrypted form. Communication will only be supported on the node's local IP network.

Definitions

C4I:	Army institution (Project Client)
IP:	Internet Protocol Address
JVM:	JAVA Virtual Machine
P2P:	Peer to Peer (server less) Communication
PC:	Personal Computer
TCP:	Transmission Control Protocol

References

More about application can be retrieved from project development team.

Abdul Rehman

BESE 18 MCS NUST

Group Leader – Dev. Team

Email: mail.abdulrehman.pk@gmail.com

Overview of Document

This document is about the detailed architectural design of P2P Intranet Communication Application for Military Field Environment. For simplicity the document is divided into various sections. Section 1 introduces the document and provides overview for executive purposes. Section 2 includes detailed description of the system with various diagrams and charts. This section includes all the architectural details of system under development. Section 3 describes all the modules and components of the system in detail one by one. Section 4 compares this product to various other similar products available in market. Section 5 throws light on the design decisions and tradeoffs. In the last section pseudo code of all the components in provided.

This design document contains detailed information about Intranet P2P Communication App. All modules, use cases, functions, features and special technologies are their inter relationship is discussed in detailed and also assisted with diagrams where required.

This document is intended for developers, testers, users, documentation writers, project clients, project supervisor and project evaluators. A copy of this document will be made available to all stakeholders.

4.2. System ArchitectureDescription

This section provides detailed system architecture of P2P Intranet Communication App. Overview of system modules, their structure and relationships are described in this section. User interfaces and related issues are also discussed.

Overview of Modules

This P2P Intranet Communication Application has following required modules. Here we give a brief overview of all these modules. Detailed descriptions of these modules are presented in section 3.

1. **Network Discovery Module:**

   This is the module from where the major functioning of application initiates. It discovers the network and index all the network nodes combining their IDs and IPs.

2. **Text Messaging Service:**

   Messaging service is one of the functional requirements of the application. This module handles all incoming and outgoing messages i.e. it communicates with the remote network app for text message transfer. Outgoing messages may be received from application UI or from any other application through OS service.

3. **File Transfer Service:**

   Just like messaging service, file transfer service has the task to handle all incoming and outgoing files. The module divides the outgoing files into chunks and send one by one to destination device. While receiving files, it receives chunks from sending device and save them in a file.

4. **Encryption Module:**

   This module has a task to encrypt all the outgoing and decrypt all incoming communication data. All messages and files transferred over the network pass through this module for encryption/decryption.

5. **Log Manager:**

   Log manager manages all communication log on a remote server in encrypted form. Only admin has rights to access the log manager to see and manage log data.

6. OS Service Provider:

OS service provider provides the services to operating system and all other applications running on the same device to use the application services i.e. see the network and transfer messages and files.

7. User Interface:

User interface is one of the ways to interact with application. It packages all those screens, dialogs and forms that are visible to user. It provides user access to admin panel, messaging and file services.

8. Admin Panel:

This is a hidden module in application and is accessible to user on providing login ID and password. This module has access to application settings and log data.

Structure and Relationships

This section covers the overall technical description of P2P Intranet App. It shows the working of application in perspective of different point-of-views and also shows relationships between different components.

System Block Diagram

This diagram shows the higher level description of the application. It shows all the modules of the system and their associations and flow of data between modules.

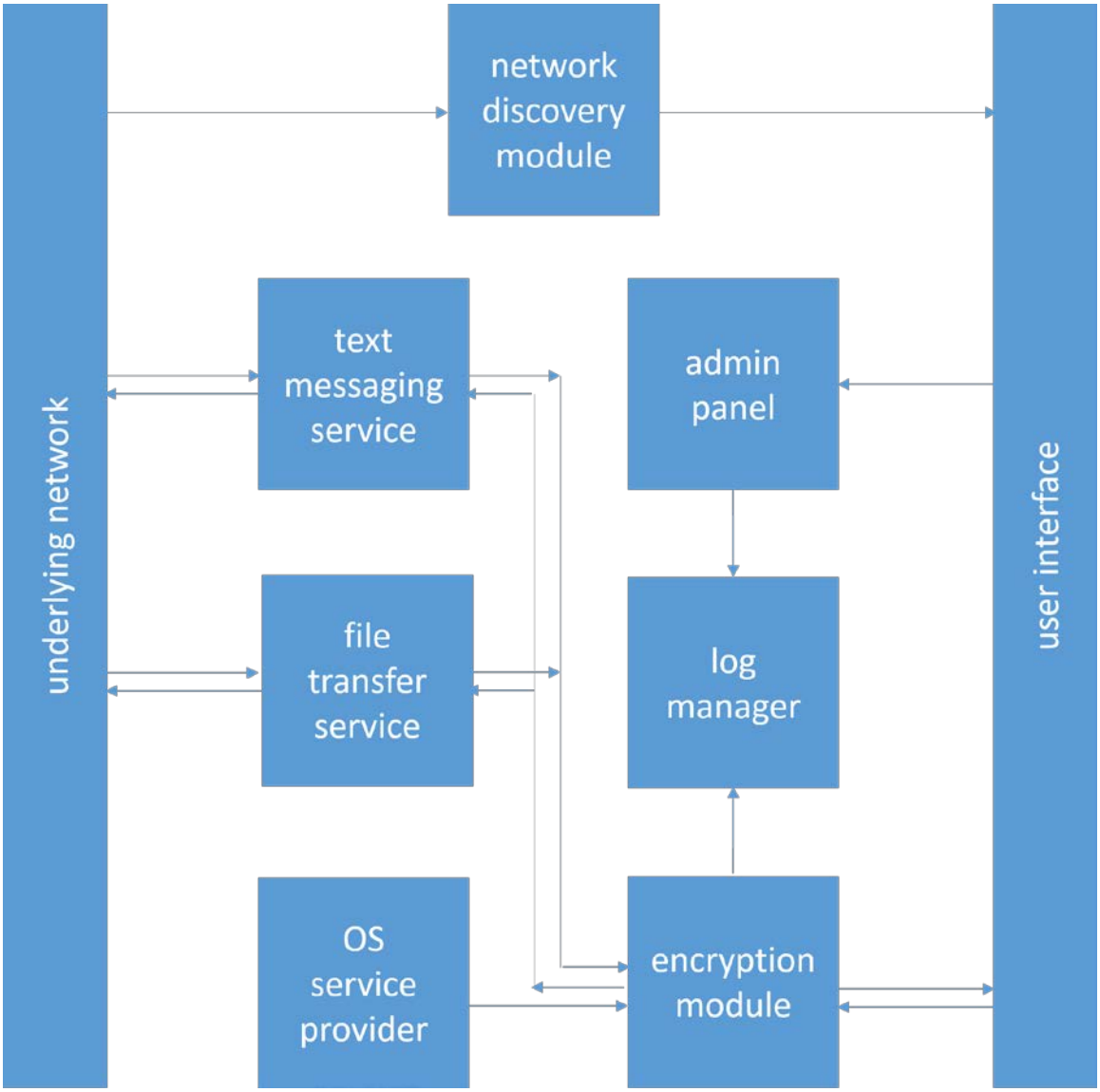

Figure 4.2.1System Block Diagram

Network discovery module discovers the network and pass the information to user interface. Messages and files transferred to remote devices can originate from user interface or OS service. These messages and file have to pass through encryption module. Similarly incoming messages also have to pass through encryption module to be displayed to user. User accesses the log manager through admin panel which have to decrypt the saved encrypted messages.

User View (Use case diagram)

Following diagram shows course of events that take place when an actor (user and other allowed interactions) interacts with system.

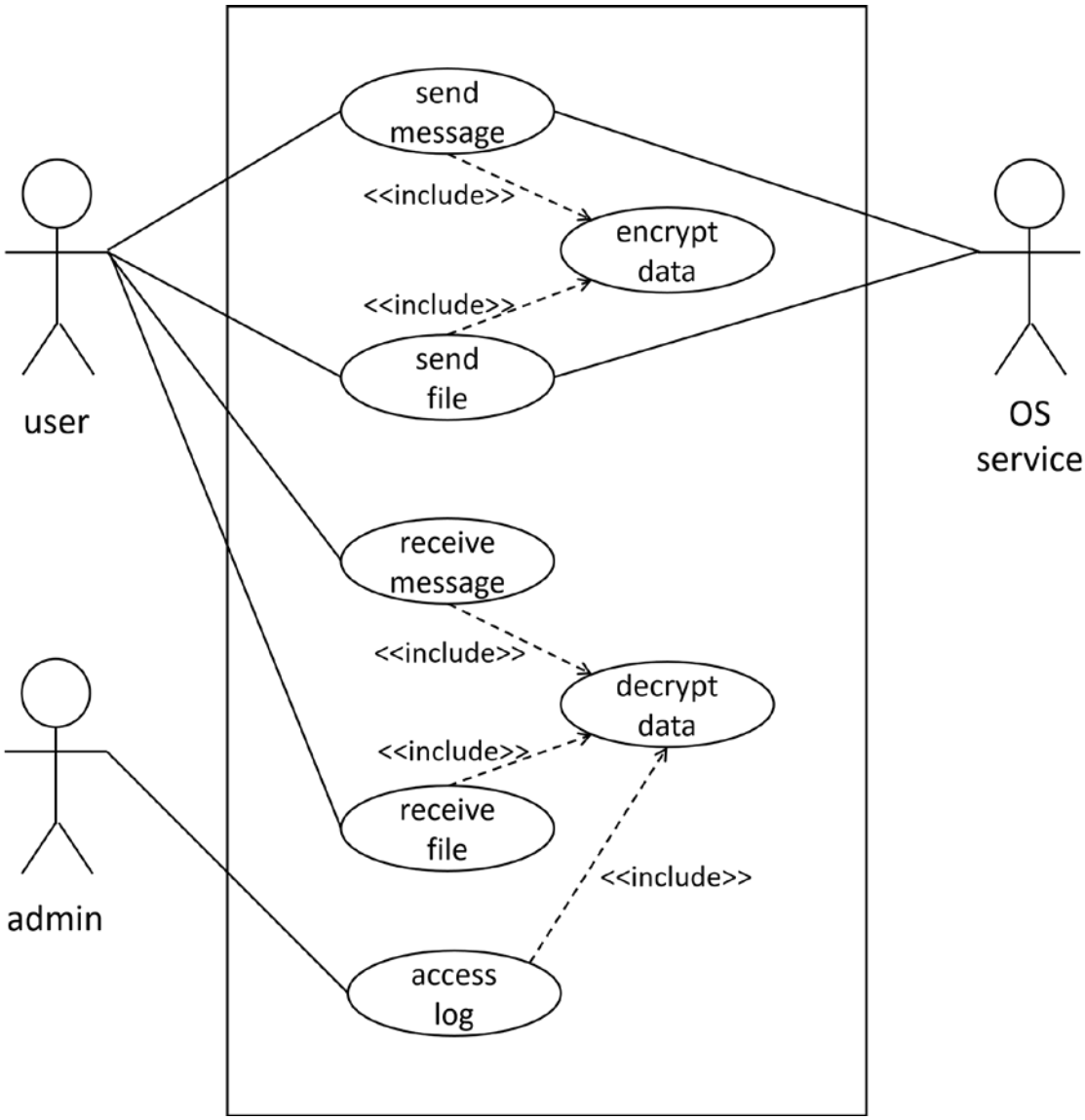

Figure 4.2.2 System Use case Diagram

Uses cases shown in Fig 4.2.2 are described below in detail.

Use Case 1

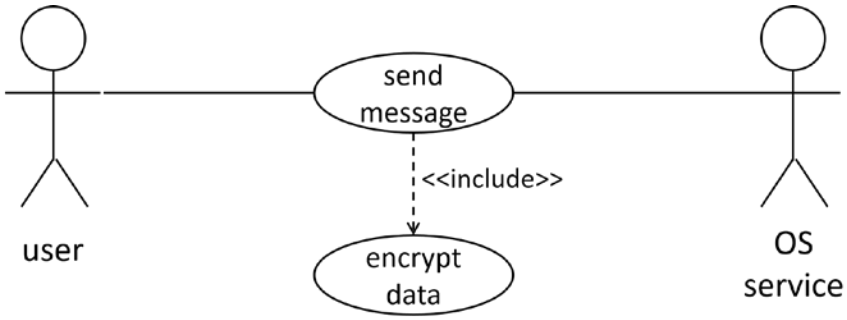

Figure 4.2.3 Use Case - Send Message

Use case name	Send message
Primary actor	User, OS service
Secondary actor	N/A
Normal course	- Send message - Message is encrypted - Message is sent
Alternate course	- Send message - Message is encrypted - Message sending failed
Pre-condition	Network services are initialized and network is discovered
Post-condition	Remote device has received message
Extend	N/A
Include	Encrypt data
Assumptions	Message is not empty

Use Case 2

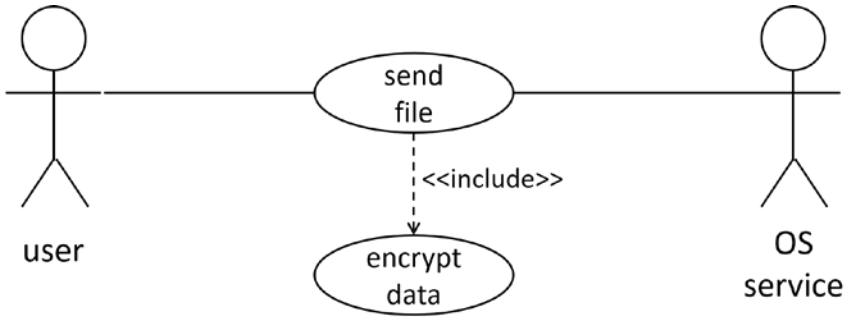

Figure 4.2.4 Use Case - Send File

Use case name	Send file
Primary actor	User, OS service
Secondary actor	N/A
Normal course	- Send file - File is encrypted - File is sent
Alternate course	- Send file - File is encrypted - File sending failed
Pre-condition	Network services are initialized and network is discovered
Post-condition	Remote device has received file
Extend	N/A
Include	Encrypt data
Assumptions	At least one file is selected

Use Case 3

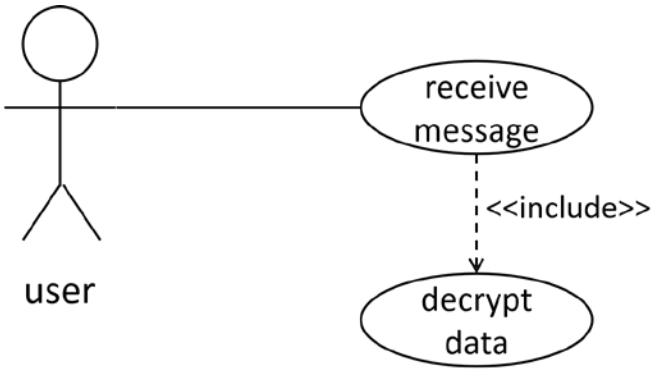

Figure 4.2.5 Use Case - Receive Message

Use case name	Receive message
Primary actor	User
Secondary actor	N/A
Normal course	- Receive message - Decrypt message - Message is received
Alternate course	- Receive message - Decrypt message - Message reception failed
Pre-condition	Network services are initialized and network is discovered
Post-condition	Message has been received by this device
Extend	N/A
Include	Decrypt data
Assumptions	Message is not empty

Use Case 4

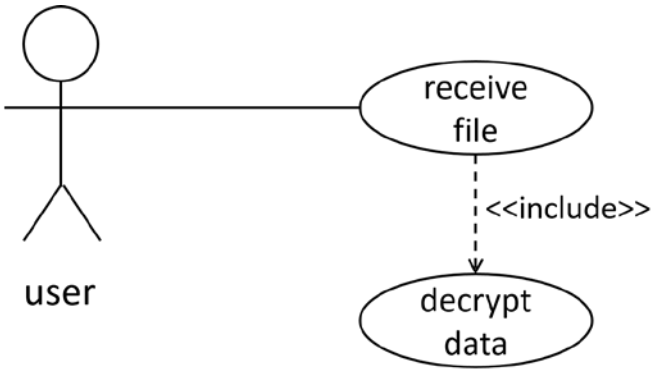

Figure 4.2.6 Use Case - Receive File

Use case name	Receive file
Primary actor	User
Secondary actor	N/A
Normal course	- Receive file - Decrypt file - File is received
Alternate course	- Receive file - Decrypt file - File reception failed
Pre-condition	Network services are initialized and network is discovered
Post-condition	File has been received by this device
Extend	N/A
Include	Decrypt data
Assumptions	At least one file received

Use Case 5

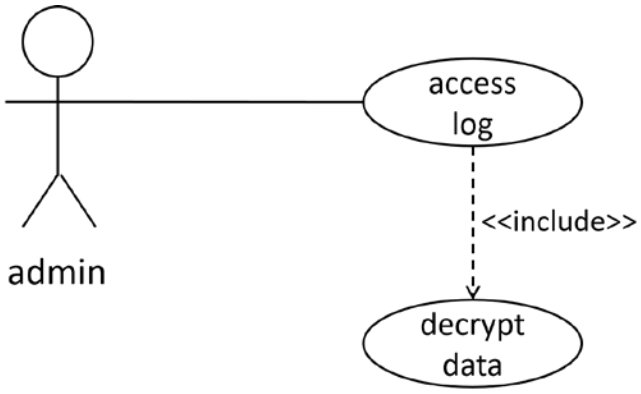

Figure 4.2.7Use Case - Access Log

Use case name	Access log
Primary actor	Admin
Secondary actor	N/A
Normal course	- Access log - Decrypt log - Log is accessed
Alternate course	- Access log - Invalid access - Log is not accessed
Pre-condition	Admin provides security pass to the system
Post-condition	Admin accesses the log
Extend	N/A
Include	Decrypt data
Assumptions	Admin knows how to access log

Sequence Diagrams

Following sequence diagrams show the sequence of activities performed in all use cases described.

Send Message (Use Case 1)

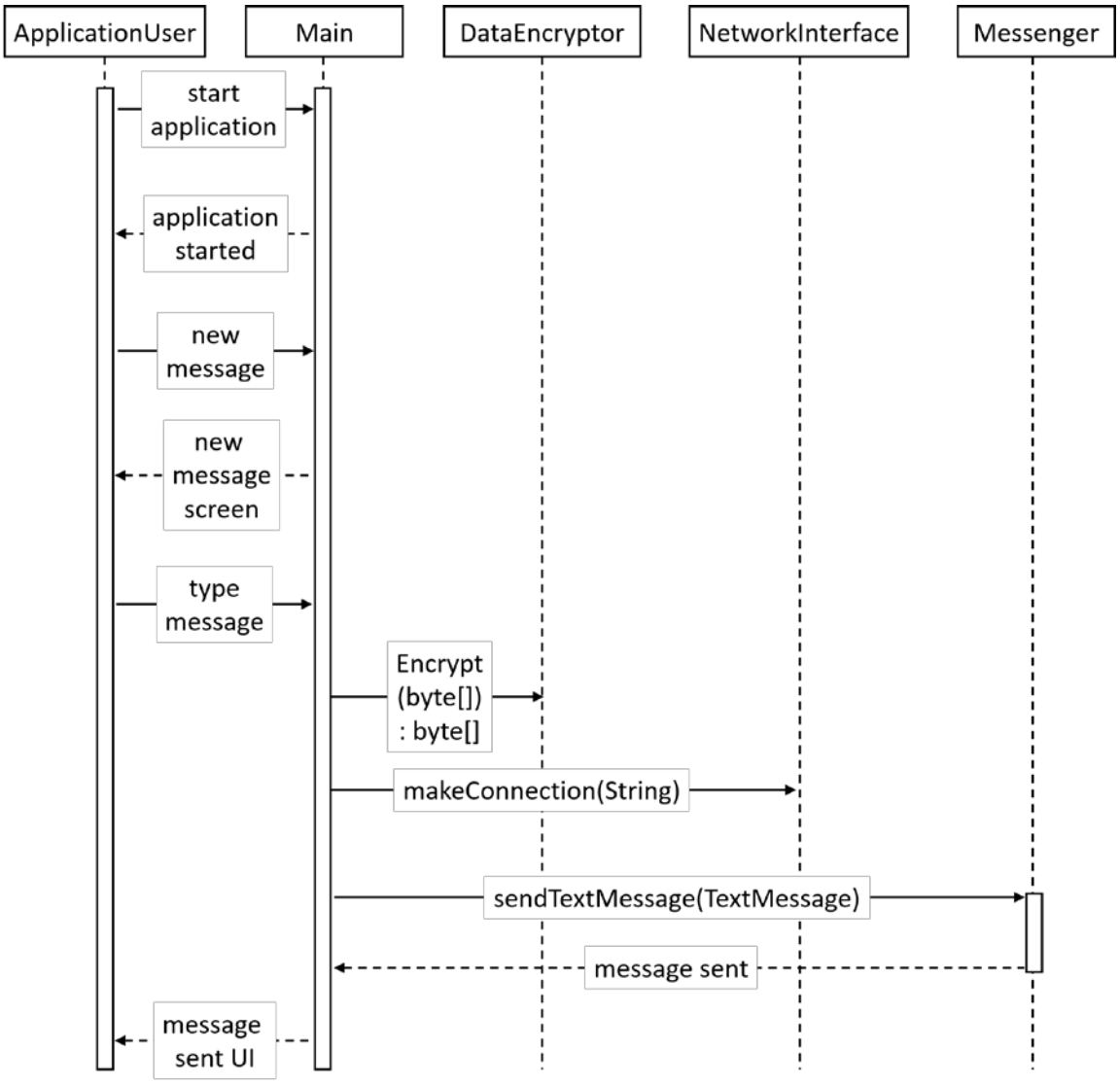

Figure 4.2.8Sequence - Send Message

Send File (Use Case 2)

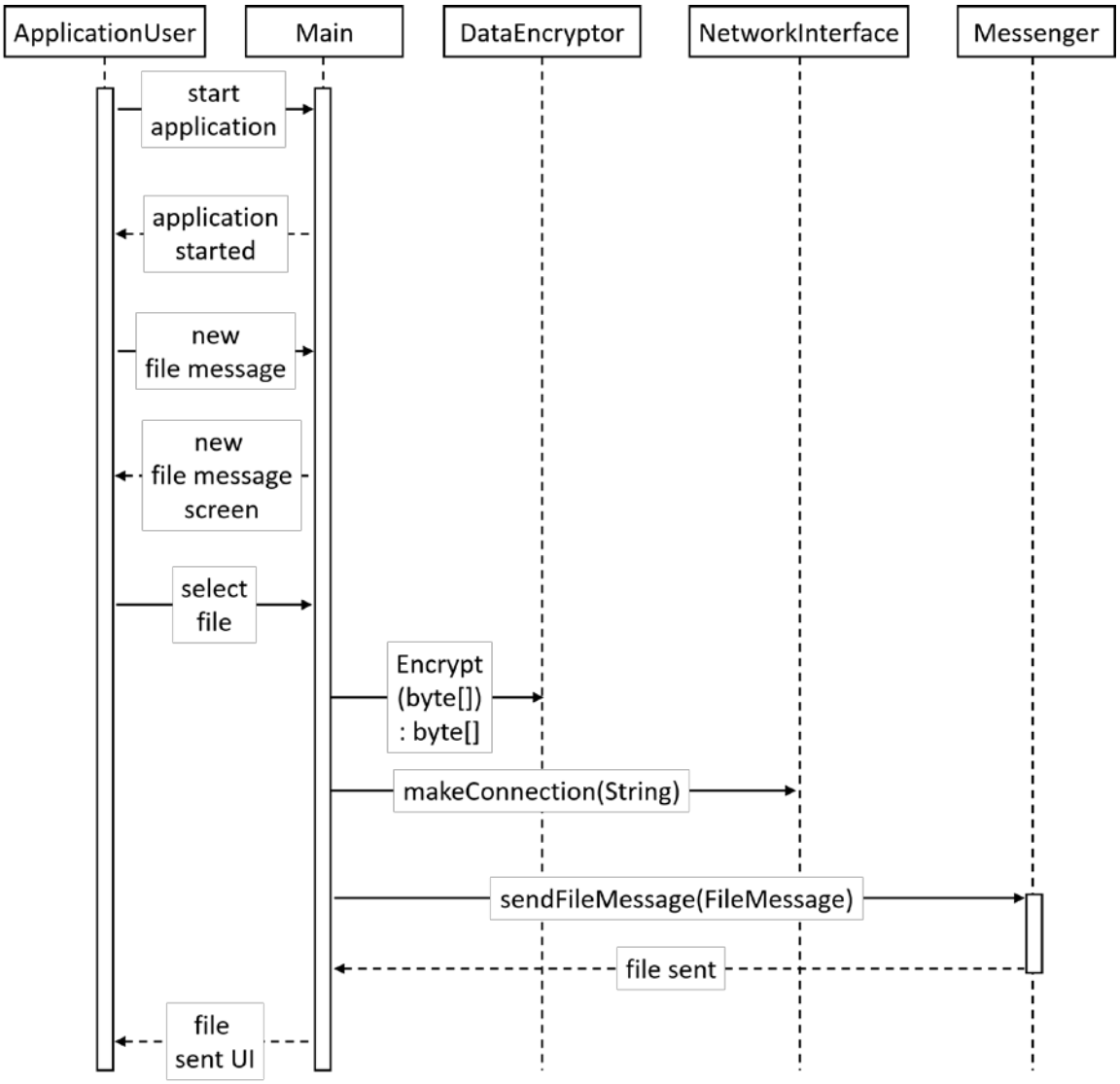

Figure 4.2.9 Sequence - Send File

Receive Text Message (Use Case 3)

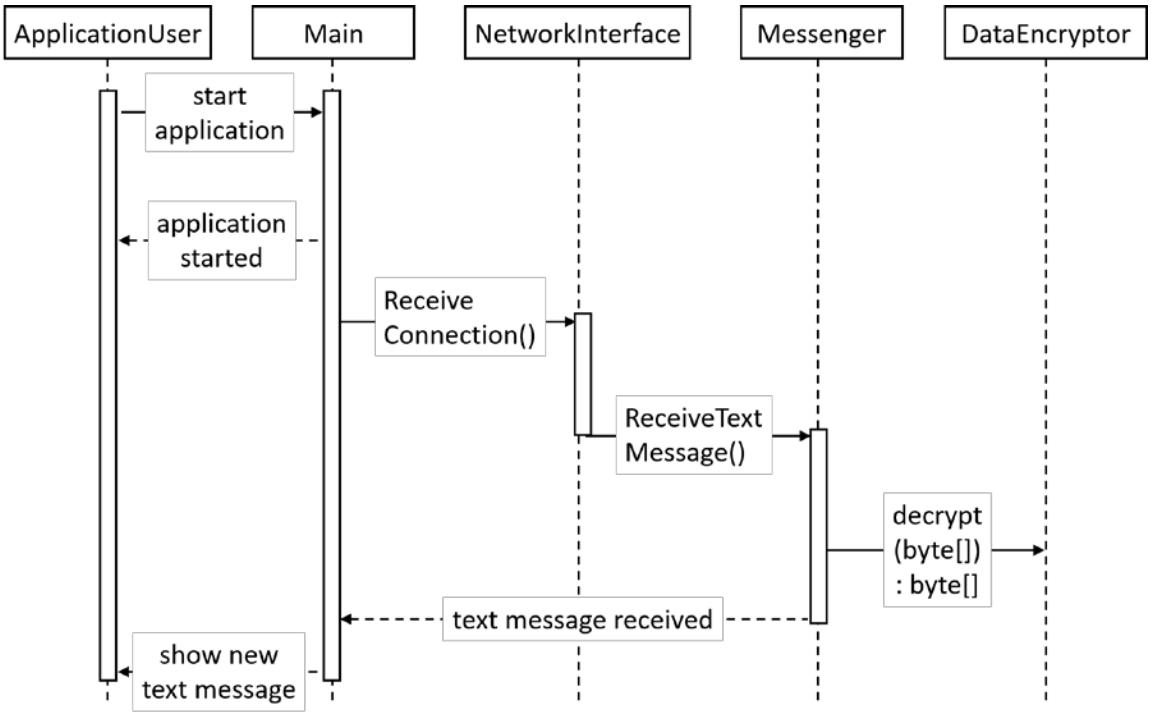

Figure 4.2.10Sequence - Receive Message

Receive File Message (Use Case 4)

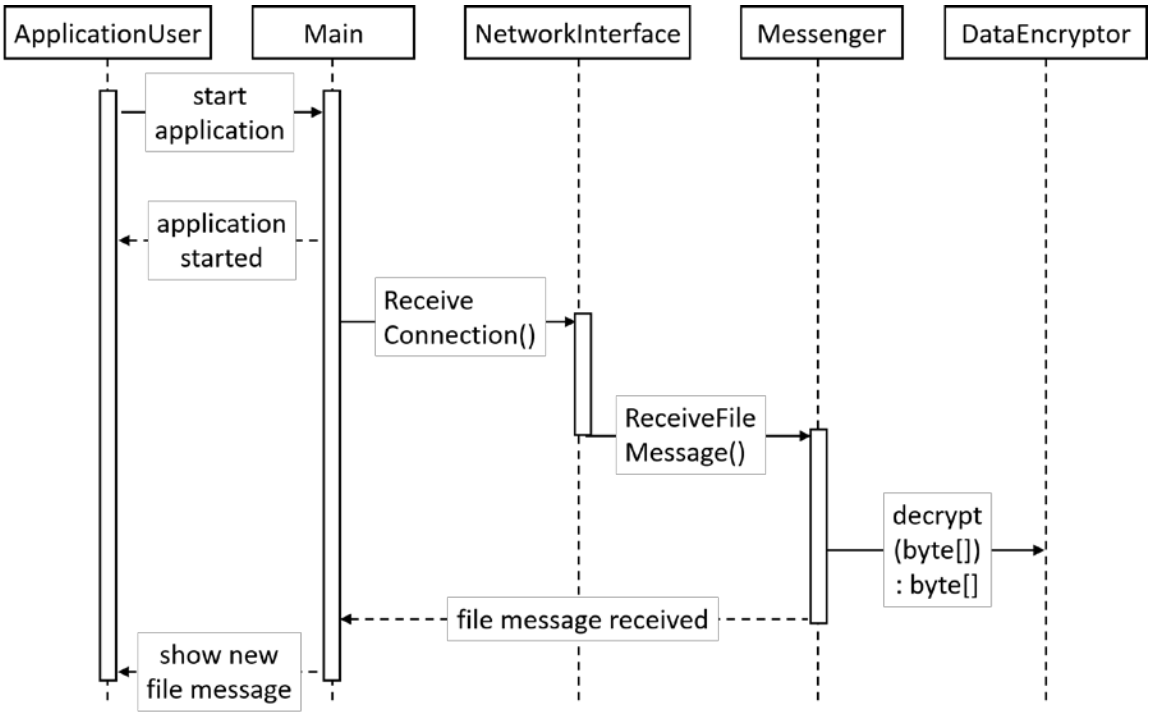

Figure 4.2.11 Sequence - Receive File

Access Log (Use Case 5)

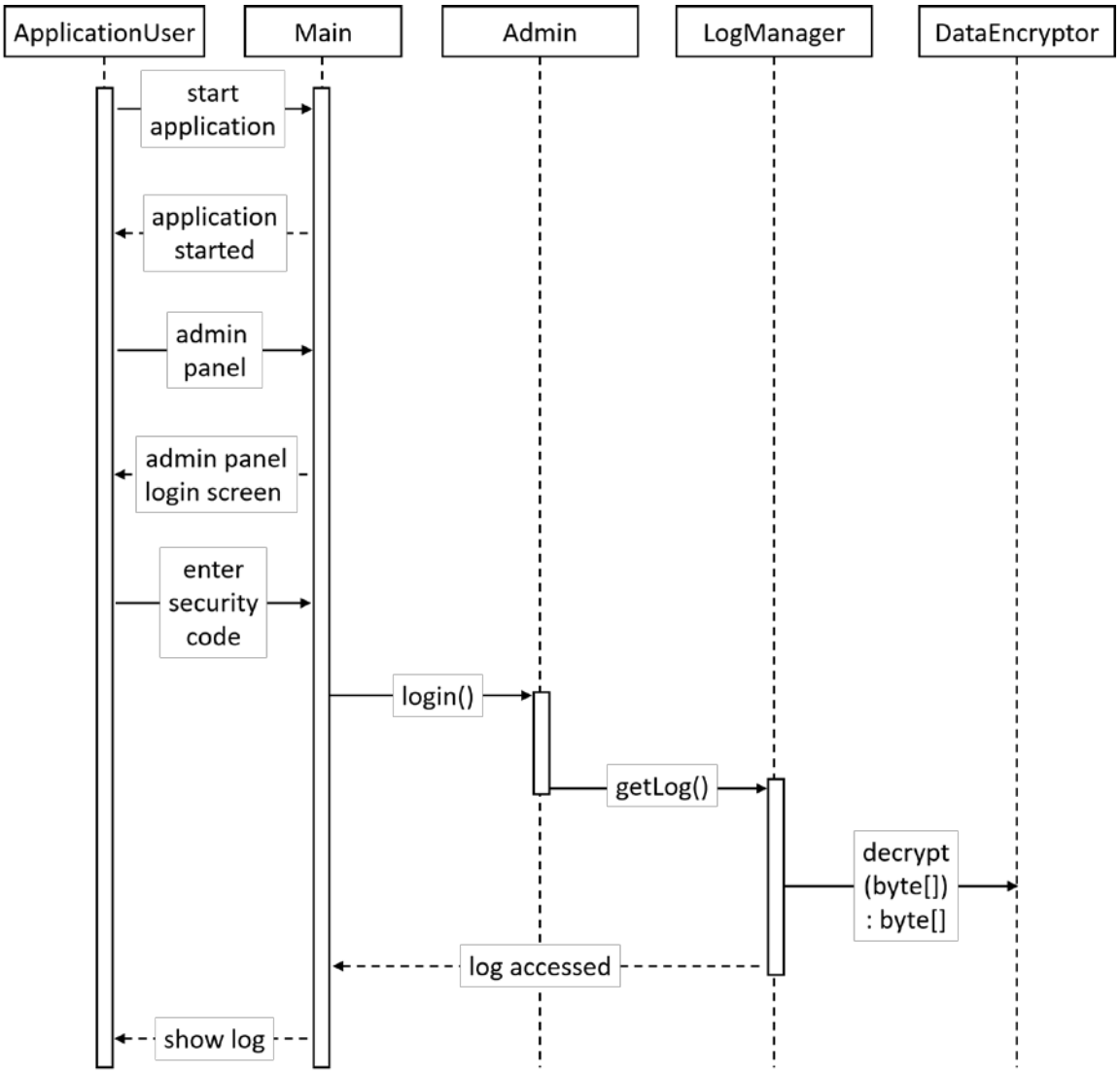

Figure 4.2.12 Sequence - Access Log

Implementation View (Class Diagram)

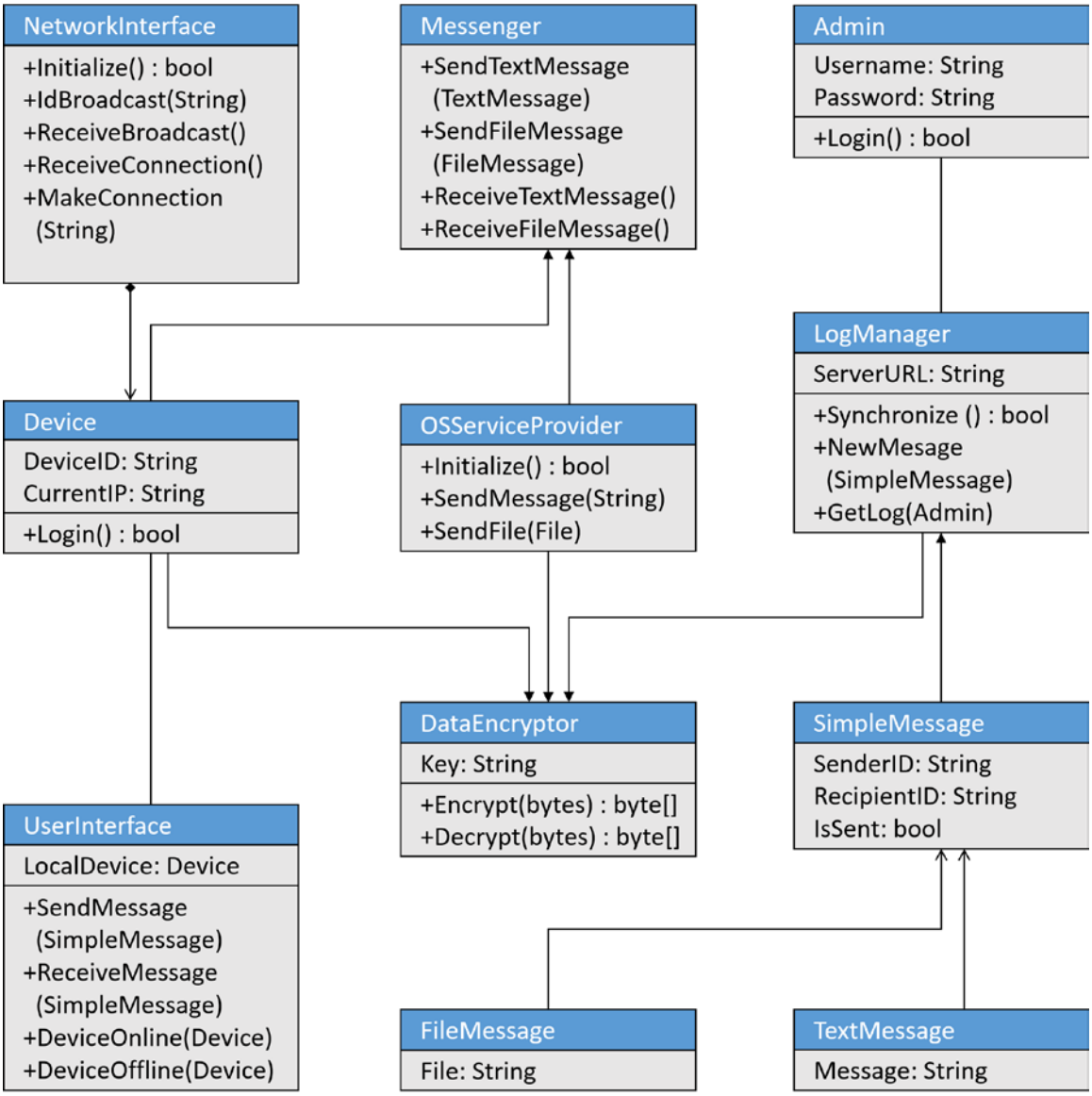

Figure 4.2.13 System Class Diagram

Class	Description
NetworkInterface	This class has all the methods and properties required to interact with underlying network. ID broadcasting to entire network as well as receiving broadcasts from entire network and then notifying the user interface for devices online are the tasks performed by this class. This class also establishes TCP connection to remote devices for sending messages and file and then handover the established connection to messenger to send and receive files and text messages.
Messenger	This class implements all the communication protocols. Receiving / Sending text and file messages are the primary tasks of this class. Messenger receives established connection from NetworkInterface and runs specified protocol over the connection.
LogManager	LogManager manages all the tasks related to managing the message log. All the messages (received / sent) are also sent to log manager. Log manager synchronizes these messages on a remote server in encrypted form. LogManager also helps Admin to view log. LogManager retrieves log from server and pass to DataEncryptor to decrypt log and then present to admin.
OSServiceProvider	This class provides services to underlying operating system and all other applications running on same device to use application services. This service provider actually exposes a public API to the operating system and other applications. This API serves as a gate way to use application services. Services shared by OSServiceProvider are send text and file

	message to specified device.
DataEncryptor	DataEncryption fulfil encryption / decryption functional requirement of the application. All sent / received messages and files call methods of this class to encrypt / decrypt data respectively. Moreover, all the application log that is saved on the remote server is also encrypted by this class. Later when an admin accesses the log, it has to be decrypted by this class as well.
UserInterface	UserInterface presents all the screens, dialogs, notifications and error messages to user. It also includes a panel to show all the devices that are currently online over the network as well as current network information and status.
Admin	Admin holds all the data that is required to access the log manager. This class includes self-authentication method (Login) to verify the security code.
Device	This class holds the information of a network device. The device will be local if ID matches the ID of local device else device will be remote. It also saves the current IP of a network device. Combination of device ID and IP are the necessary information to connect to any of the remote device.
SimpleMessage	This is a generic class of a message. It holds mandatory information of a message such as recipient and send IDs etc.
TextMessage	TextMessage encapsulated information of a text message. This is subclass of SimpleMessage.
FileMessage	FileMessage is also a subclass of SimpleMessage. It extends from SimpleMessage in a way to ensure all the requirements of a file message.

Dynamic View (Activity Diagram)

In activity diagram, the dynamic view of the system is shown. All the activities are shown concurrently with their respective start and end states.

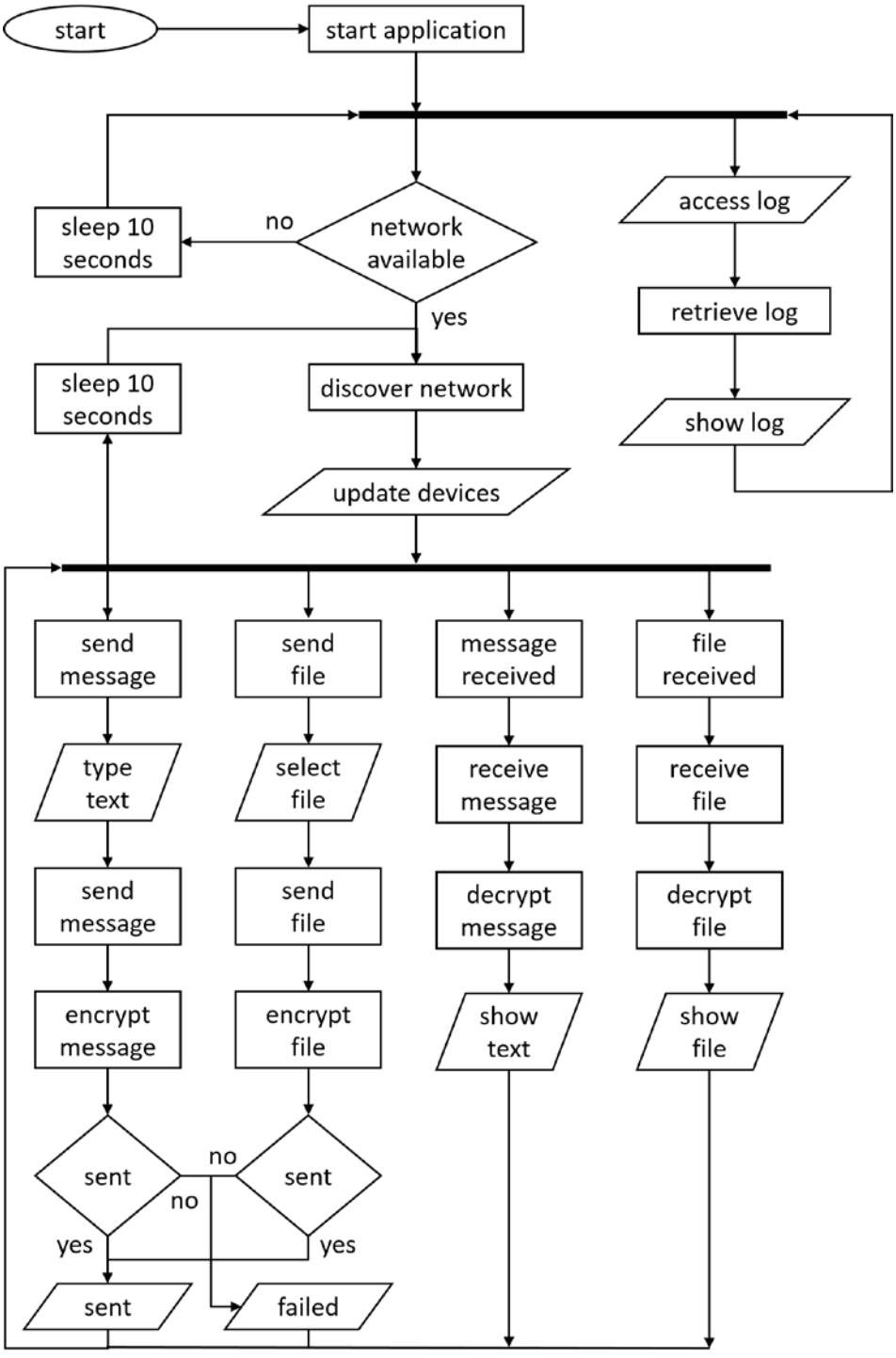

Figure 4.2.14 Activity Diagram

4.3. Detailed Description of Components

This section describes in detail all the modules of P2P Intranet Communication App.

Network Discovery Module

Identification	Name: Network Discovery Module Location: Application Logic Layer
Type	Component
Purpose	This component fulfils following requirement from Software Requirements Specification Document: **3.1 Node Availability Broadcast** This feature allows a node to broadcast its availability to its local network. **Description:** When a node is up on the network it must be able to broadcast its availability to the entire network. So that each node will be able to see all the nodes available on the network for communication. **3.2 Network Nodes' Discovery** This feature provides the ability to discover all nodes broadcasting on local network. **Description:** When a node will broadcast its availability then each available node must be able to discover the availability of each availability broadcasting node from the entire local network and display its ID to the user as online node.
Function	This module broadcasts the local device to entire network as well as discovers the network and index all the network nodes combining their IDs and IPs.
Subordinates	It has two subordinates: 1. Broadcast itself: Requirement 3.1 in SRS 2. Discover Network: Requirement 3.2 in SRS
Dependencies	This component is independent module and runs in parallel to

	entire application.
Interfaces	This component has following interfaces: 1. **Network Interface:** To interact with entire network for incoming and outgoing communications. 2. **Application UI Interface:** To inform user about network status and updates as well as communication notifications.
Resources	**Hardware:** RAM, Processor, Network Adapter **Software:** C# core libraries
Processing	Network Discovery Module processes all the communication on a separate non-UI thread. Each network connection is also handled in a separate thread. Notifications to Application UI are shifted to UI thread before presenting to user.
Data	This component uses following information of the application: 1. Device Info 2. Communication Info

Text Messaging Service

Identification	Name: Text Messaging Service Location: Application Logic Layer
Type	Component
Purpose	This component fulfils following requirement from Software Requirements Specification Document: **3.3 Text Messaging** This feature will provide text message transfer over the network. **Description:** User must be able to transfer text messages on the local network. A friendly user interface must be provided to user to type the message. He must also be able to copy/Paste messages.
Function	This module handles all incoming and outgoing messages i.e. it communicates with the remote network app for text message transfer. Outgoing messages may be received from application UI

	or from any other application through OS service.
Subordinates	This component has following subordinates: 1. Incoming Messages: Requirement 3.3 in SRS 2. Outgoing Messages: Requirement 3.3 in SRS
Dependencies	This component is dependent on Network Discovery Module. Network Discovery Module should be up and running before initialization of this module.
Interfaces	**N/A**
Resources	**Hardware:** RAM, Processor, Network Adapter **Software:** C# core libraries
Processing	Messaging Services component is event driven and runs messaging protocol on a network connection passed by Network Discovery Module. Network Discovery also specifies connection as incoming or outgoing.
Data	This component uses following information of the application: 1. Communication Info

File Transfer Service

Identification	Name: File Transfer Service Location: Application Logic Layer
Type	Component
Purpose	This component fulfils following requirement from Software Requirements Specification Document: **3.4 File Transfer** This feature allows user to transfer files. **Description:** User must also be able to transfer files on the local network. A friendly user interface will be provided. User must also be able to drag and drop files.
Function	This module handles all incoming and outgoing messages i.e. it communicates with the remote network app for text message transfer. Outgoing messages may be received from application UI or from any other application through OS service.

Subordinates	This component has following subordinates: 1. Incoming Files: Requirement 3.4 in SRS 2. Outgoing Files: Requirement 3.4 in SRS
Dependencies	This component is dependent on Network Discovery Module. Network Discovery Module should be up and running before initialization of this module.
Interfaces	**N/A**
Resources	**Hardware:** RAM, Processor, Network Adapter **Software:** C# core libraries
Processing	File Transfer Services component is event driven and runs transfer protocol on a network connection passed by Network Discovery Module. Network Discovery also specifies connection as incoming or outgoing.
Data	This component uses following information of the application: 1. Communication Info

Encryption Module

Identification	Name: Encryption Module Location: Application Logic Layer
Type	Component
Purpose	This component fulfils following requirement from Software Requirements Specification Document: **3.5 Encryption** This feature will encrypt all the data. **Description:** All the data sent over the network as well as the communication logs must be encrypted before transfer and saving them respectively. Application must provide a highest possible security of data.
Function	This module has a task to encrypt all the outgoing and decrypt all incoming communication data. All messages and files transferred over the network pass through this module for encryption/decryption.

Subordinates	This component has following subordinates: 1. Encrypt Log: Requirement 3.5 in SRS 2. Encrypt Messages: Requirement 3.5 in SRS 3. Encrypt Files: Requirement 3.5 in SRS
Dependencies	This component is independent and exposes public static methods to entire application to encrypt / decrypt data.
Interfaces	**N/A**
Resources	**Hardware:** RAM and Processor **Software:** C# core libraries
Processing	This module performs encryption and decryption with non-blocking API.
Data	This component uses following information of the application: 1. Encryption Info 2. Decryption Info

Log Manager

Identification	Name: Log Manager Location: Application Admin Layer
Type	Component
Purpose	This component fulfils following requirement from Software Requirements Specification Document: **3.6 Chat Log** This feature will create communication history. This log will be synchronized to a remote server. **Description:** Application must create chat and file transfer history record and save it on the local device when internet is not available. This log must be synchronized to a remote server when internet is available to a node. **3.7 Log Synchronization** This feature will synchronize communication log. **Description:** Application must constantly detect availability of

	internet connection and must synchronize communication log created on a remote server upon the availability of internet.
Function	Log manager manages all communication log on a remote server in encrypted form. Only admin has rights to access the log manager to see and manage log data.
Subordinates	This component has following subordinates: 1. Log Creation: Requirement 3.6 in SRS 2. Log Synchronization: Requirement 3.7 in SRS
Dependencies	This component is dependent on the availability of internet. Log is saved locally in offline mode and gets synchronized when internet is available.
Interfaces	This component has following interfaces: 1. **Access Log:** To retrieve log from server and present to admin.
Resources	**Hardware:** RAM, Processor, Network Adapter **Software:** C# core libraries **Miscellaneous:** Internet
Processing	This module interacts with internet as well as admin to perform its tasks. It only gets invoked on the availability on internet as well as when admin accesses the log.
Data	This component uses following information of the application: 1. Admin Info 2. Server Info

OS Service Provider

Identification	Name: OS Service Provider Location: Application Interface Layer
Type	Component
Purpose	This component fulfils following requirement from Software Requirements Specification Document: **3.9 OS Service** This feature will provide access to application service.

	Description: Application must provide a method to use application service. I.e. Text Messaging and File transfer. All the application running on the local system must also able to use application services through a single interface.
Function	OS service provider provides the services to operating system and all other application running on the same device to use the application services i.e. see the network and transfer messages and files.
Subordinates	This component has following subordinates: 1. Text Messaging Service API: Requirement 3.9 in SRS 2. File Transfer Service API: Requirement 3.9 in SRS
Dependencies	This component is dependent on the status of Network Discover Module, Text Messaging Service and File Transfer Service. All these components should be integrated before OS Service Provider.
Interfaces	This component has following interfaces: 1. **Text Messaging Service API:** To send text messages. 2. **File Transfer Service API:** To send files.
Resources	**Hardware:** RAM and Processor, Network Adapter **Software:** C# core libraries
Processing	OS Service Provider handles API requests from outside of the application. It only get invoked on request. Translates the request into local application flow and invokes appropriate function call.
Data	This component uses following information of the application: 1. API Info

User Interface

Identification	Name: User Interface Location: Application Interface Layer
Type	Component
Purpose	This component fulfils following requirement from Software Requirements Specification Document: **3.2 Network Nodes Discovery** This feature provides the ability to discover all nodes broadcasting on local network. **Description:** When a node will broadcast its availability then each available node must be able to discover the availability of each availability broadcasting node from the entire local network and display its ID to the user as online node. **3.3 Text Messaging** This feature will provide text message transfer over the network. **Description:** User must be able to transfer text messages on the local network. A friendly user interface must be provided to user to type the message. He must also be able to copy/Paste messages. **3.4 File Transfer** This feature allows user to transfer files. **Description:** User must also be able to transfer files on the local network. A friendly user interface will be provided. User must also be able to drag and drop files. **3.8 Admin Panel** Application also provides an admin panel. **Description:** Application must provide an admin panel to the user to access communication logs and history. This feature must be hidden and available on providing password.
Function	User interface is one of the ways to interact with application. It

	packages all those screens, dialogs and forms that are visible to user. It provides user access to admin panel, messaging and file services. User interface is user friendly and easy to understand.
Subordinates	This component has following subordinates: 1. Home Screen: Requirement 3.2 in SRS 2. Text Messaging Screen: Requirement 3.3 in SRS 3. File Transfer Screen: Requirement 3.4 in SRS
Dependencies	Working of this component is dependent on integration of all other components.
Interfaces	**N/A**
Resources	**Hardware:** RAM, Processor, Display Screen **Software:** C# core libraries
Processing	User Interface display info, notifications and messages to user passed by other components.
Data	This component uses following information of the application: 1. Device Info 2. Network Info 3. Internet Status

Admin Panel

Identification	Name: Admin Panel Location: Application Admin Layer
Type	Component
Purpose	This component fulfils following requirement from Software Requirements Specification Document: **3.8 Admin Panel** Application also provides an admin panel. **Description:** Application must provide an admin panel to the user to access communication logs and history. This feature must be hidden and available on providing password.
Function	This is a hidden module in application and is accessible to user on

	providing login ID and password. This module has access to application settings and log data.
Subordinates	This component has following subordinates: 1. Access Log
Dependencies	Working of this component is dependent on Log Manager and User Interface.
Interfaces	**N/A**
Resources	**Hardware:** RAM, Processor **Software:** C# core libraries
Processing	Admin Panel logs in admin into the Log Manager to access the log and pass it to the user interface.
Data	This component uses following information of the application: 1. Server Info

4.4. Reuse and Relationships to other Products

P2P Intranet Communication System for Military Field Environment is not based on any previous systems neither it's an extension of any other applications at any level. But it can be evolved into a bigger and more complex system with more features and functionality. Developers can also reuse some of the modules of the system. The practical usage of the system can be increased by adding more and more services to system like VoIP, Walkie Talkie, Video Chat, Conference Calls etc.

The application can also be used somewhere else for communication purposes by little changing in some of its modules like Log Manager and Admin Panel.

There are many applications like that in market but almost every application is centralized meaning they also supports communication over internet and the remaining which provide intranet communication are not secure or not trust worthy because client is Pakistan Military so integrity of the source is very important. Adding the source repudiation and source confidentiality along with the data confidentiality and data integrity. This application is being developed by keeping these points in mind.

4.5. Design Decisions and Tradeoffs

The P2P Intranet Communication App is an interactive application which requires multiple types of user interface. Developing such systems require thorough consideration on the design factors as it might result in complexity problem. A poorly-designed communication application results in a system consuming more resources with very little efficiency and a slower response time which directly affects the experience of the target user. Besides this, poor designs make testing and maintenance activities difficult. Resource available to field commander in field environment are kept in mind.

Operational environment of Army is highly fluid and ad hoc. Field commanders require a medium to share information with other command echelons in a secure and efficient manner. It is expected that only trivial IT capability will be available to user in operational environment. The application provides means of information exchange between the field commanders in operational environment.

The application is a context-aware pervasive system. Interface of the system is distinct from the application logic. Layered architecture is used to isolate application logic from the user interface. It can be modeled using Multitier Layered Architecture consisting of three layers i.e.; UI Layer, Application Logic Layer, Admin Layer. Presentation layer corresponds to elements of the user interface such as screens, textboxes, dialog boxes etc. Application Logic Layer controls the communication of data between the

Presentation Layer, Admin Layer and over the network and is the part where the main logic, user actions and working of the system is defined. In general, it controls the complete behavior of the system, while the Admin Layer is responsible for handling access to log saved on remote server.

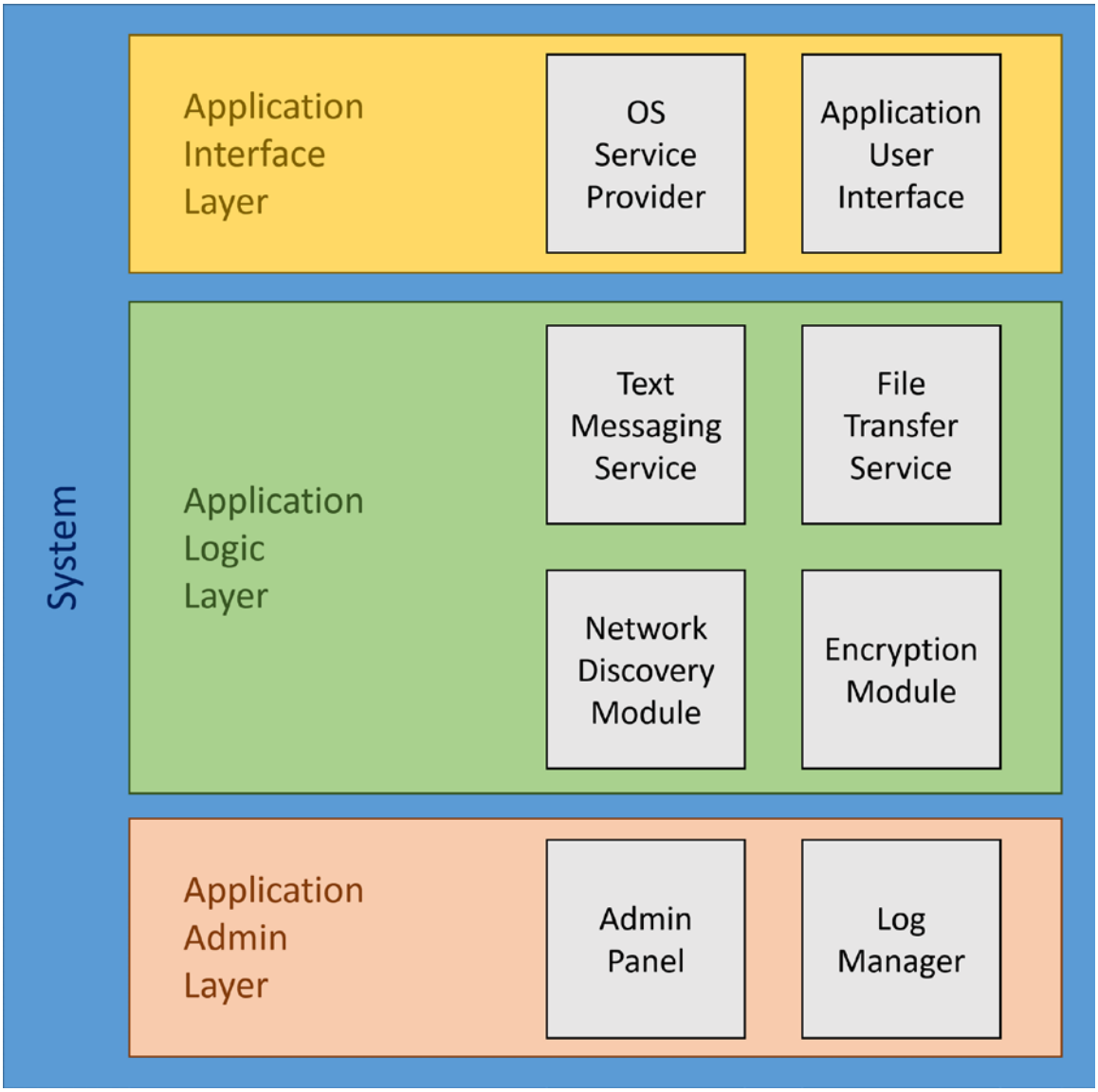

Figure 4.5.1 Architectural Diagram

Chapter 5. Project Test and Evaluation

5.1. Assumptions

This section lists assumptions that are made specific to this project.

1. There is a remote server for log management
2. The is a local network infrastructure
3. Application modules are integrated for integrated testing

5.2. Risks

The following risks have been identified and the appropriate action identified to mitigate their impact on the project. The impact (or severity) of the risk is based on how the project would be affected if the risk was triggered. The trigger is what milestone or event would cause the risk to become an issue to be dealt with.

Scope Creep

Risk: As testers become more familiar with the tool, they will want more functionality.

Impact: High

Trigger: Delays in implementation date

Mitigation Plan: Each iteration, functionality will be closely monitored. Priorities are set and discussed by stakeholders. Since the driver is functionality and not time, it may be necessary to push the date out.

Changes to the functionality

Risk: May negate the tests already written and we may lose test cases already written.

Impact: High – to schedule and quality

Trigger: Loss of all test cases

Mitigation Plan: Export data prior to any upgrade, massage as necessary and re-import after upgrade.

5.3. Test Approach

The project is using waterfall approach, with producing modules and integrating them. All the modules are tested individually and then integrated with system and integration tests are applied.

Unit Testing

Unit testing is that part of testing which requires a thorough check of each module of the project. In our project we have 7 modules which we have to check if they are working fine or not. For this we will start from a unit which is least dependent on other modules for its function and then work our way through to the module which requires all the rest to function ad test.

Integration Testing

Integration testing is process where we will test all the previous tested modules in a way that they are working fine when they are combined together.

System Testing

Finally comes the System Testing which we will require after all the units are working separately and in sync with each other .Then only the finally outcome of the program will decide the correctness of the whole system.

5.4. Test Environment

A network infrastructure, application and a server.

5.5. Milestones and Deliverables

Test Case Name	Broadcast
Test Case Number	1
Description	Connection of Device to the network
Preconditions	1. Application should be installed on PC or on any device 2. The Device should be connected to a network
Input	Public Key and MAC address of the device
Steps	1. Turn on the device and check if it's connected to the internet
Expected output	Application is not throwing any exception
Results	Application will broadcast its MAC and PK to the entire network.

Test Case Name	Listen Broadcast
Test Case Number	2
Description	Connection of the device to the network
Preconditions	1. Application should be installed and open 2. The Device should be connected to a network
Input	Application should be open

Steps	1. Turn on the application 2. Check for the status of the network
Expected output	Application is listening to all the broadcasts
Results	Application will maintain a list of all available nodes.

Test Case Name	Network Availability
Test Case Number	3
Description	Connection of Device to the network
Preconditions	Application should be open
Input	A network must be available to the device on which application is installed.
Steps	Turn on the device and application Check if the internet connection is working properly.
Expected output	Application must be able to broadcast.
Results	Network is available to the application.

Test Case Name	Valid RSA keys
Test Case Number	4
Description	This part deals with the RSA keys which will be used to share the AES shared key for data confidentiality.

Preconditions	1. Application should be open and should generate the RSA key pair.
Input	Application should be open and should be working properly.
Steps	1. Open the application 2. Broadcast the Public key 3. Receive the AES key from some other node. 4. And decrypt the key using your private key
Expected output	Application must be able to decrypt the AES key properly
Results	You will get the AES shared key from other sender.

Test Case Name	Status of device
Test Case Number	5
Description	This part is about the availability of the device how to show its offline.
Preconditions	1. Application should be open and should be broadcasting and listening to broadcasts. 2. Application should maintain a list of all available nodes.
Input	Application must be listening to the Broadcast of other nodes.
Steps	1. Turn on the application and check the internet connection. 2. Check if application is listening to the broadcast. Application will receive the broadcast after every 5 sec from each device 3. If application doesn't receive 3 broadcast means 15 sec and no broadcast is received from a device 4. That device will be shown offline
Expected output	All device will show that device offline
Results	IP, MAC and public key of that device will be removed from the network list of all devices.

Test Case Name	Message Sending
Test Case Number	6
Description	This part deals with the process of sending encrypted

	message over the network.
Preconditions	1. Device and Application should be working fine. 2. Device should be connected to the local network. 3. Sender has shared the AES key for data encryption
Input	Typed text message by the user.
Steps	1. Sharing the AES key with other user. 2. Typing the text message in the message field 3. Encrypting the message 4. Sending the message over the network
Expected output	Encrypted message has been send and will be received as the same size in the non-readable format
Results	Message is decrypted successfully

Test Case Name	File Sending
Test Case Number	7
Description	This part deals with the process of sending encrypted files over the network.
Preconditions	Device and Application should be working fine. Device should be connected to the local network. Sender has shared the AES key for data encryption with the recipient.

Input	File which user want to send
Steps	Sharing the AES key with other user. Choosing the file Encrypting the file Sending the encrypted file over the network
Expected output	Encrypted file has been send and will be received as the same size in the non-readable format
Results	File data is decrypted successfully along with the file name.

Chapter 6. Future Work

The P2P Secure Communication System for Military Field Environment application has been designed as a set of APIs which is dynamic in nature and further enhancements and improvements are possible without affecting the existing system. The development team can cope with changing requirements of military field environment by adding new APIs to the existing system.

Smart phones, tablets, high-speed wireless networks and other sophisticated communications technologies are rapidly changing the way people access, use and exchange information. The military is embracing the communications revolution, turning to a new generation of sophisticated systems to enable faster, richer, less costly and more flexible communications.

However, as communication options multiply, so does the problem of getting disparate technologies to work together efficiently and securely. Communications integration is now one of the top challenges facing military technology leaders to the company that provides communications and security consulting services to the government. “Smart phones and other IP technologies in particular, it’s all really exciting stuff, yet they also pose challenges in terms of interoperability and security.”

After today’s standards and security assurance problems have been resolved, IP is the pathway to interoperability, speedier technology deployment and lower development and maintenance costs. Although past communications development projects often created impressive and reliable systems, the costly and complex projects tended to address only a narrow set needs and frequently fell far behind schedule. “We often see pillars of excellence that were essentially obsolete before they were even fielded.” IP technologies will provide a common technology base to span virtually all communications modes, including phones, tablets, mobile and handheld radios, satellites, sensors and networks.

A command line and a GUI based on JAVA swing library has been provided to use the APIs. One more user interface for Android based smartphone is being developed. More and more interfaces for different environments and hardware can be developed based on existing APIs.

Bibliography

- Instant Messenger for Integrated Messaging System PCS - 172 (2009)
- https://en.wikipedia.org/wiki/List_of_cryptographers
- https://en.wikipedia.org/wiki/Pakistan_Army_Corps_of_Signals
- https://en.wikipedia.org/wiki/Military_communications
- http://searchsecurity.techtarget.com/definition/PKI
- http://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard

Appendix A. System Operational Requirements

Hardware Requirements

- 1.2 GHz Processor or More
- 512 MB of RAM or More
- Network Connection
- Standard Peripheral Devices

Software Requirements

- Supported Operating Systems:
    1. Windows XP or higher versions
    2. Linux
    3. Android 3.0 or higher

- JAVA Virtual Machine