**CHAPTER TWO**

**LITERATURE REVIEW**

**2.1 Introduction**

Android is an operating system for smartphones, tablets and now will be used for Personal Computers also. It includes a touch screen user interface, widgets, camera, network data monitoring and all the other features that enable a cell phone to be called a smartphone. Basically, Multi-Purpose chat application allows users to send asynchronous messages, and enable sharing image files with other peers on the JXTA world using JXME. Instant messaging has become so ubiquitous, an entire generation of internet users is probably unaware there was ever life without it. The use of instant messaging nowadays is more than the calling function itself. The main objective of this paper is to introduce a methodology to provide instant Messaging Service over the intranet which is addressed to android based smartphone and tablet users connected over intranet via Wi-Fi. The proposed method is based on sending/receiving messages in intranet through intranet server via WiFi connection without the need of taking any service from mobile service provider and without the use of internet connection. (Peffers et al., 2014).

Penetration of the smartphones at the global scale is very high. A mobility report from Ericsson company states that by the year 2020 smartphone subscription will be 6.1 billion and 90% of world population over 6 years old will have access to a mobile phone (Peffers et al., 2014). There are many reasons behind this fast growth, but the most important are more powerful hardware and decrease in the cost of manufacturing. These factors make smartphones more affordable in the developing markets, such as China and India, the countries with more than one billion population. Users of smartphones have access to millions of applications in their application stores although there are different smartphone operating systems for smartphones, two are dominant, Androidand iOS.

Each of these operating systems have a big application ecosystem which gives the option to billions of users to choose the desired service and use them right from a device in their pocket. As of July 2014, there is 1,300,000 apps available for Android in Google Play Store and 1,200,000 of apps available for iOS Apple store (Peffers et al., 2014).

**2.2 Overview of Instant Technology**

Instant messaging is a set of communication technologies used for text-based communication between two or more participants over the internet. IM allows effective and efficient communication, allowing immediate receipt of acknowledgment or reply. In the company, colleagues can send and reply instant message in real time without face to face, meanwhile the work report can be shared during the instant chat session; it can make a virtual conference without get all the related people together in a physical meeting room. Using instant messages for interoffice communication is quicker than phone calls or emails. More than one person can chat at the same time.

This is a huge benefit of using an instant messenger. Instead of relying on a conference call or copying others on an email message, everybody can join and have a discussion in real time. Better than email, if you truly want to communicate instantly you need to consider all your options. Sure, an email gets sent instantly but do you really know when if the other person receives it? With an instant message you can send a message and receive a reply within a matter of seconds. Email was the first killer application for the internet but now instant messaging is coming to cellphones. Instant messaging is a form of communication over the internet that offers quick transmission of text-based messages from sender to receiver.

The instant messaging provides a means of sending messages to and from global system for communication, because of its ease of use and cost effectiveness it has become one of the popular service in the communication world. Multi-user applications are commonly implemented using a centralized server. All participants share their views by exchanging the cryptographic digests of the chat room data set. A newly generated message causes a change of the digest at the message originator, which leads to retrieving the new data by all other participants in an efficient way and resynchronization of chat room views.

**2.3 Internet Based Messaging Architecture**

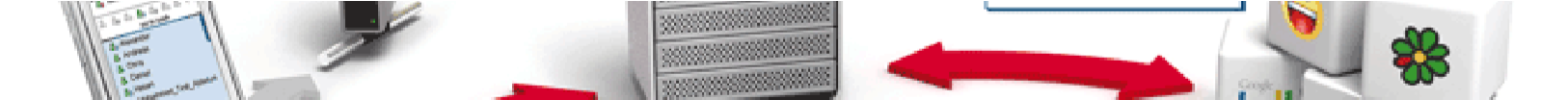
Internet- based instant messaging applications allow users to send/receive messages over the internet. It requires internet connection to transfer messages from one device to another device. There are various applications like BBM (Black Berry Messenger), Ping Chat, Imo etc. are messengers used for communication over the internet. BlackBerry Messenger (BBM) is a proprietary Internet-based instant messenger application included on BlackBerry devices that allows messaging between BlackBerry users. The service communicates over the phone's Internet connection using the mobile phone network. (Gradecki, 2002)

A wireless LAN ("Wi-Fi") network connected to the Internet may also be used to send messages, however, most service providers will not allow sign-in to BlackBerry Messenger without the purchase of a BlackBerry data plan. All above application are based on internet that provides connectivity which includes internet access charges and also need to take the service from mobile service provider as shown in Fig. 2.1. It means intranet based communication may not require the internet connectivity. However, to the best of our knowledge, there is still no instant messaging service that offers intranet based communication in such a way that does not requires internet connectivity as well as any messaging service from the mobile service providers.

Figure. 2.1

:

Internet Based Architecture.



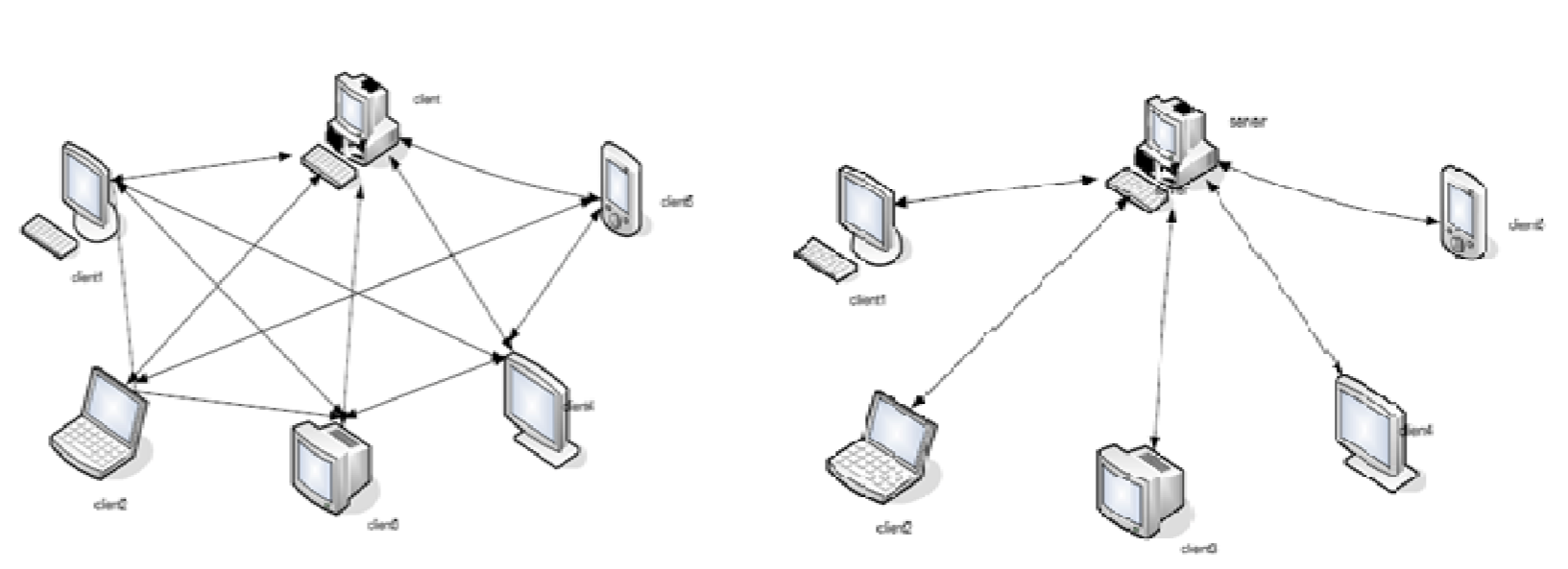


Figure 2.2 Peer to Peer Figure 2.3 Client Server

**2.4 Multipurpose Chat Application**

Multi-purpose chat application is based on JXME proxy-less version ported to Peer-droid. It allows users to send a synchronous messages, and enable sharing image files with other peers on the JXTA world. The application is designed for Android mobile phone users. The application first connects to the JXTA world, and then discovery the peers already connected to the network and the resources available. The peer should also publish advertise the resources it has multipurpose chat application has a edit text field which allow a user to write the message content then press the send button to send message content out the unicast bi-directional pipe. The edit text is designed to handle a certain amount of characters.

When number of characters exceeds the buffer size, an exception occurs. Along with message is the name of the sender. The name is included to show the receiver from whom the message is from and the time of arrival. The Incoming messages will be displayed in scrollable form and can be retrieved later as chat history. When a peer received a message can reply back. First should write the message then click send. A user will be able to download image from the remote web server and share with other users of the system. The downloaded image files could be saved in a local SD card as compressed files and retrieved later for the future uses. As it seems my mobile chat application has many features in common as features available on chat applications above but still all applications already on market use a common communication technology (client-server) to work while my application is based on P2P technology. (Sun Inc, 2007)

The Wifi enabled chat uses Wifi to transfer data /instant messages between devices. The IMS SIP chat uses IMS SIP protocol for communication. In my case peer does not need a central server to discovery and talk to each other, they Just needs a rendezvous peer to enable discovery and make advertisement for resources They have Multi-purpose chat application downloads files directly from remote web Server then share with other peers online. When a peer has a content to share then must retrieve it from the secure digital card (sdard) and send the compressed file to other users.

Multi-purpose chat receives messages with vibration in scrollable format also application is implemented to allow users to log out when they wish to do so, but peer-doid sample doesn’t. Multi-purpose chat allows users to download files from remote web server and save to local SD card. The last thing is different approach in graphical user interface approach in both cases.

**2.4.1 Peer to Peer Architecture**

Peer-to-peer (P2P) networking is a network architecture which allows a group of nodes (peers) to connect with each other and share resources, and any node can operate as either a 12 server or a client. Hence participants in a P2P network do not need a central server to communicate like the traditional client-server architecture which has existed for many years. Unlike client-server architecture, a P2P network is considered alive even if only one peer is active. The network is unavailable only when no peers are active. (Butler, 2011). Nowadays the most popular P2P networks file sharing system such as Napster, Ares, Limewire, and Gnutella use decentralized topology, Instant Messaging (ICQ) and distributed computing. (Butler, 2011). Though peers all have equal status in the network, they do not all necessarily have equal physical capabilities. A P2P network might consist of peers with varying capabilities, from mobile devices to mainframes. A mobile peer might not be able to act as a server due to its intrinsic limitations (Butler, 2011). Peers in P2P network have equal chance in such a way that any peer can act as a server or a client at the same time. (Wilson, 2002).

**2.4.2 Client Server Architecture**

Client-server architecture is the oldest technology where a client machine contacts the server when the services are needed. In other words it is called centralized architecture where the whole network depends on a central point. If the central point fails, the entire system will collapse. With no server the network would make no sense. The procedure is as follows (Gradecki, 2002);

* Client sends a request for a service to a server.
* The server receives the request and processes the request, and then sends back the response to the client.
* The client receives the response.

Some of the servers existing on the Internet are web servers, mail servers, FTP and so on. The communication between the server and the client. (Cherry, 2009).

**2.5 The Smartphone Ecosystem**

The ecosystem of application stores provides a chance for everybody including freelance developers as well as companies to publish their applications to the world via these stores. After the application gets approved by the store, it can be discoverable from anybody who has access to the Internet to surf and search through the app store. Every industry can benefit from such ecosystem. Many industries including insurance, banking, healthcare and even government agencies are getting benefits of smartphones’ penetration and Internet access to better serve their customers and stakeholders. (Fang, 2009).

Among the popular mobile applications, IM applications have hundred millions of users worldwide (Butler, 2011) and there are many companies that provide such a service to their users. All these chat applications compete with each other to get higher penetration rate among the users and to defeat other companies in the market. These IM chat providers try to create better user interfaces and offer more features for their respective users. (Spring et al., 2015).

**2.6 Security Services for Mobile Instant Messaging**

In order to evaluate any chat application from the security point of view, relevant threats to such application should be identified and described. In the following sections a brief description about different security aspects are explained. Security has three key aspects: confidentiality, integrity and availability (NIST, 2014). Confidentiality ensures that certain type of information can be accesses by authorized parties. Integrity means information can be modified only by intended and authorized parties. Availability means that information is accessible to authorized parties at appropriate times (Pfleeger and Pfleeger, 2014).

**2.6.1 Confidentiality**

Confidentiality means messages which are exchanged by two parties through a communication channel should be readable only to the intended parties. In order to achieve such a goal, encryption is the mechanism that provides confidentiality between two parties. A message is encrypted by a cryptographic technique and this encrypted message can only be readable by the intended party. (Pfleeger and Pfleeger, 2014)

**2.6.2 Cryptography**

Cryptography is the practice and study of techniques which are used to secure a communication between two entities while the third party (adversary) exist. Cryptography helps to create an environment or medium channel in which confidentiality, integrity, authentication of the user and non-repudiation are supported.

There are two major types of algorithms in cryptography. One is symmetric key cryptography and the second is public key cryptography. In symmetric key encryption both parties use a shared key to encrypt and decrypt the messages (Delfs and Knebl, 2007). In this method, because the adversary does not have the shared key, even if he intercepts the communication channel, he just receives encrypted messages and is not able to decrypt them.

Public key cryptography, is also known as asymmetric cryptography, uses an algorithm which needs two separate keys: one key is private key and the other key acts as the public key of the user. However there is a link between these two keys which is generated by an algorithm for a user (Delfs and Knebl, 2007). When public key cryptography is used, the application generates two keys. Public key can be shared or broadcast to the whole world, but the knowledge of the private key remains secret. In this method, one party uses the second party’s public key and encrypts the message and sends it over to the second party. The second party receives the encrypted message and opens it with its own private key. If any malicious hacker intercepts the communication channel, he just receives encrypted messages and is not capable to decrypt them, because he does not have the private key of the recipient. (Kaufman et al., 2016)

**2.6.3 Authentication**

Authentication is one of the most important aspects of security, where an entity should identify itself before or during the communication. This avoids any type of attack or malicious activity by which a malicious user impersonates the user and identifies himself as the real user to the server.

There are two types of authentication schemes known as weak authentication and strong authentication. Weak authentication (one factor authentication) means that the entity uses only one type of identity credential such as a PINor password-based authentication. It is considered a weak mechanism because it is prone to many attacks including brute force attacks. A brute force attack is type of attack that the malicious user tries as much as passwords to finally finds out the one which matches the chosen password of the user. (Kaufman et al., 2016).

Strong authentication is usage of typically a challenge-response cryptography. In this scheme the client needs to prove his identity and verify himself to the server with multiple factors. There are different practices to perform such authentication such as one-time passwords (OTP) and certificate-based authentication (CBA). In one-time password, a shared secret key is stored on a device that the entity has, and the system issues one-time passwords based on this shared secret key. CBA is using asymmetric cryptography which provides public-private key cryptography. In this method, each user has a unique digital signature and this digital signature can be used to verify the true identity of the user. (Kaufman et al., 2016)

**2.6.4 Integrity**

Integrity insures that a message has not been edited or changed during the transfer of it between entities. An attacker can eavesdrop the communication channel and modify the message or even replace the message with a new one. Hashing is a mechanism to achieve such a goal in the world of information security. A cryptographic hash function is a function which maps an encrypted message to a fixed size length integer. A hash function is one-way function, meaning that if somebody has an output of a hash, it cannot be reversed. (Kaufman et al., 2016).

**2.6.5 Privacy**

In a digital world privacy of a user means the power to select what type of information to be shared or be accessible by other entities including governments, service providers, and even other applications. Privacy of a user is related to and based on a metadata that an application can collect and send to a second or third party.

Unfortunately privacy is one of the factors that is getting sacrificed in the current mobile application environment. Many applications are free of charge, but the service providers grab metadata of the user and send these information to their servers even sometimes without the knowledge of the users. Metadata means any type of data which includes different information about a user, such as location, name, contact information, creator of data, contact list, type of operating system, etc.( Kaufman et al., 2016).

**2.6.6 Non-Repudiation**

Non-repudiation means that a mechanism in which the entity who has sent the message cannot deny that. A malicious user can sometimes generate a message and send it on behalf of an entity to another party without knowledge of the entity. Non-repudiation solves this problem by introducing a mechanism which proves that the source of a message is a person that claims it. Like the real world where people can have signatures or even seals to seal or sign a contract, in the digital world and in public-private key ecosystem, there are digital signatures which can be related to different entities and individuals can sign their messages with their dedicated digital signature. (Cattiaux, 2013).

**2.7 Mobile Instant Messaging Systems**

Technology trends in both hardware and software have driven the hardware industry towards smaller, faster and more capable mobile hand-held devices that can support a wider-range of functionality and open source operating systems. Mobile hand-held devices are popularly called smart gadgets. Adding text messaging functionality to mobile devices began to gain traction in the mobile communication services community in the early 1980s. (Cattiaux, 2013).

The first action plan of the Group GSM was approved in December 1982, requesting "The services and facilities offered in the public switched telephone networks and public data networks should be available in the mobile system”. This plan included the exchange of text messages either directly between mobile stations, or transmitted via Message Handling Systems widely in use at that time. The first proposal which initiated the development of exchanging information or sent message to the user was made by a contribution of Germany and France into the GSM group meeting in February 1985 in Oslo. Initial growth was slow, with customers in 1995 sending on average only 0.4 messages per GSM customer per month. (Cattiaux, 2013).

In 2013, 6.1 trillion text messages were sent. This translates into 193000 SMS per second. While SMS reached its popularity as a person-to-person messaging, another type of SMS is growing fast: application-to-person (A2P) messaging. A2P is a type of SMS sent from a subscriber to an application or sent from an application to a subscriber. It is commonly used by financial institutions, airlines, hotel booking sites, social networks, and other organizations sending SMS from their systems to their customers. According to research in 2013, A2P traffic is growing faster than P2P messaging traffic. (Cattiaux, 2013).

Over the years several approaches and solutions presented considering the secure exchanging of message thorough client and webserver. The various researches have been done and are going on location based project and in the same ratio various applications have been developed on location-based and message sharing system. As the amount of user deal to exchange the information with other people to store the large amount of data to the centralized database. Sensitive data may also be leaked accidentally due to improper disposal or resale of storage media.

Instant Messenger is a proprietary, simplified version of Internet Relay Chat, which allows two or more people to carry on a conversation, in real-time, using text based messages with context awareness. Instant Messenger is used to avoid boredom, to socialize and to maintain contact with casual acquaintances. There are many chat applications in the mobile market and they have different striking features. Some of the very popular Mobile Messaging Applications and are generally used are Whatsapp, Facebook Messenger and We-chat. (Iqbal et al., 2013).

**2.8 Some Minor Mobile Chat Applications**

As it was mentioned in previous sections, there are many chat applications in the mobile market. Recently some chat applications have started to distinguish themselves in the market by calling themselves as “secure chat application”. Normally in these types of chat applications, they are self-claimed by their providers that they have prioritized security and privacy of their users at the first place. According to number of downloaded applications from the application stores, these so-called security applications have few millions of users each in the market and they are not among the top popular chat applications at all. Although majority of chat applications use various types of encryption, unfortunately in most of the cases, the IM owners’ servers issue the keys or have access to message keys to decrypt them. (Iqbal et al., 2013).

Unfortunately some chat applications have proprietary protocols or architecture and they are not public or open source. These apps cannot be examined by the developer’s community or security experts what makes it harder for evaluation. Therefore the only way is to trust the providers’ wordings regarding their claims.

Another way is to perform extensive reverse engineering or penetration testing routines in order to evaluate security levels of these applications. However they are still black box testing meaning that the security researchers do not have access to the source code to see how the applications works with 100% accuracy. In order to investigate IM apps’ security features, several IM applications have been selected based on their popularity. In the following sections, a range of mobile chat applications will be briefly introduced. Four different chat applications have been selected due to factor of popularity, business orientation, and self-claimed security providing services. (Ozturk, 2010).

**2.8.1 WeChat**

Wechatis the third popular messaging application in the market available in different platforms including iOS and Android. It supports sending voice, video, pictures and text messages. Unfortunately, the architecture of the application is proprietary and it has its own protocol, but it has an official page for developers (WeChat, 2013) regarding WeChat SDK. WeChat does not provide end-to-end encryption meaning that encryption methods that is used is based on public key encryption, but the user needs to trust the WeChat servers.

**2.8.2 Voxer**

While majority of mobile chat applications market themselves for consumers, Voxer is more business oriented and market itself as a mobile messenger for teams. Voxer also has desktop version which can be installed on a normal PC. Voxer has free and paid version. Voxer is a proprietary application and there is not good documentation about the structure of their servers. Based on their official website, they claim that they use military graded encryption for the encryption of the messages and also they use secure communication channel using TLS to send messages between parties. (Saint-Andre, 2004).

**2.8.3 Wickr**

Wickr has some unique features which makes it very appealing for users (Wickr, 2015). For example one of the features that they offer is self-destruct messages meaning that as soon a user reads a message, the message will be wiped from the recipient’s mobile phone. Based on their official website they claim that the application removes all the metadata and they do not upload users’ contact book to their servers. While they claim that they don’t have a backdoor, the software is not open source and there is no way for an external auditor to verify this claim. Wickr uses end-to-end encryption (E2EE). In E2EE, the encryption and decryption of messages happens at the users’ mobile phone. (Saint-Andre et al., 2009).

**2.8.4 Viber**

Viber is one of the most popular free chat applications with hundred millions of users all around the world. A research was conducted (Unhcfreg, 2016) by the UNH Cyber Forensics Research and Education Group in order to investigate security of Viber application. This research revealed explicitly that Viber is not secure at all in many cases. The research has revealed that media files such as pictures or videos which are transferred between the users have no encryption and the data is stored on the Viber server unencrypted which can be accessed without any authentication mechanism! These vulnerabilities gives the ability to a malicious user to simply launch MitM attacks and capture unencrypted data either over the wired or wireless networks. Viber does not support end-to-end encryption.

**2.9 Related Work**

A research (Schrittwieser, 2012) conducted in 2011 has evaluated the security of nine mobile chat applications from authentication point of view. Based on the experiments that they have done, the result of their research shows that there are major security flaws in most of their tested applications and makes the applications prone to different types of attacks. Unfortunately in this research they are not considering other aspects of security and also they have not proposed any design to formulate a secure chat application.

A research was conducted (Cattiaux, 2016) by two researchers to investigate security of iMessage reveals that in spite of the fact that the owner of the application claims that the application has high encryption standards and it is an end-to-end encryption but there is still a possibility for the server owners to read their customer messages in case they want to perform such a task.

A research (Iqbal et al., 2013) was conducted to investigate security of ChatON instant messaging application from forensics point of view which means what a malicious user can retrieve out of a mobile phone if he or she has physical access to the phone. In this research they revealed that by physical access to a mobile phone and proper software, the database of messages for both sent and received messages and their timestamps could be retrieved.

A series of researches (Iqbal et al., 2013) reveals that unfortunately many social media applications, including chat applications, breach privacy of the users and are prone to different type of vulnerabilities for their users. Vulnerabilities include revealing plain-text passwords or storage of private information on the servers which can be revealed to non-authenticated users.

The main shortcoming of all mentioned articles is that neither of them describe the structure of a chat application and also do not have any suggestion for a design of proper security in an IM application. Majority of the reports, articles or researches regarding security of chat applications are addressing solely on evaluation of their security, based on experimentations and lab setups. Even in research cases where researchers have dived more into the structure of a chat application, they have not proposed any solution or a specific design for a secure chat application system. (Krawczyk et al., 2015).