**CHAPTER ONE  
INTRODUCTION**

* 1. **Background to the Study**

Short Message Service (SMS) also known has text message is a communication service standardized in the Global System for Mobile (GSM) system. It supports up to 160 7-bit characters or 140 8-bit characters and the service works on a store-and-forward basis. SMS messages are not sent directly to the recipient; instead they travel through several nodes before reaching the recipient. This leads to serious security and privacy problems. Initially, text messages (SMS) was developed to enable the transmission of short text between mobile phones, especially those that runs on android platform which is most vastly used these days, without considering security issues. Currently, SMS is used for many applications, such as SMS-banking, SMS-voting, and SMS-health (Deglise et al., 2012, Ducos and Castillo, 2008).

Although, mobile SMS has great influence in our daily life, unfortunately, most of the communication is unsafe. The message sent from the android mobile device is stored at the message centre of associated network provider. The message will travel across different base stations in unprotected manner. This means there is an exposure to different attacks (modification, interception, and spoofing) on those confidential messages. Additionally, mobile phones can be stolen or shared between friends, which might lead to leak of confidential information stored on it. Providing the desired privacy and security in communication is not an easy task, since communication channels have always some security holes. There are two mechanisms to communicate using secure SMS (Tiejun et al., 2008). The first one is securing transport layer and the other one is securing application layer. In this thesis work we focused on the application layer techniques which are also considered as the current SMS research issues.

Securing SMS on application layer needs designing and developing an application on the mobile device to secure the transmission of the content of the SMS (Croft et al., 2005). To do this, Cryptography (encryption and decryption) has always been the most important tool to provide some level of security including integrity, confidentiality, authentication, and non-repudiation (Mohiy et al., 2011). Actually this solution needs mobile application that encrypts SMS at the sender side and decrypts at the receiver side to provide end-to-end security.

There are two types of encryption and decryption mechanisms, symmetric (privet) key cryptography and asymmetric (public) key cryptography. Encryption and decryption provide powerful tools for protecting sensitive communications over a public network, but it adds an overhead in terms of additional computation. This additional computation requirement reduces the applicability of cryptography on embedded devices (mobile phone) because mobile phone has limited resources such as computational power, battery life and memory. Therefore, the right choice of the suitable cryptography mechanisms that needs minimal system resource is highly and crucially important (Grillo and Lentini, 2008).

* 1. **Statement of the Problem**

Currently, mobile SMS does not provide any specific security feature. Because of this, one cannot be sure to send and receive confidential and sensitive data such as bank account information and patient information safely. By implementing secure SMS system, many SMS security threats such as Man-in-the-middle attack, SMS-spoofing, interception and other related attacks are greatly reduced. The proposed secure end-to-end encryption will ensure the message to be read only by the right person. The privacy and confidentiality of SMS message content can be protected. As clearly known, mobile phone has limited resources (processer, and memory). Because of this, identifying the technique that needs minimum computational resource with acceptable quality is a major issue in mobile application.

* 1. **Justification for the Study**

The lack of security in current SMS communication for confidential data is a motivation to conduct this final year project work on securing text communication by using encryption and decryption (cryptographic) techniques. These days, mobile phone users need more secure and private SMS messaging for their daily communication. But, because of lack of security infrastructure of conventional SMS communication, the user cannot be sure of transferring of private and sensitive data such as bank account information and patient health information. As an example most financial institutions in Nigeria are providing SMS based services. But the current SMS infrastructure is insecure to be trusted to transmit such sensitive data. This is why they advise users to delete credit alerts and memorize account balance per time.

Technology for Change International is launching a new mobile health initiative in Ethiopia and other Eastern African nations known as SMS Tech for Health (www.healthbound.org). The project is designed for health care professionals and expectant mothers and aims to improve healthy babies by reducing complications during the birth process and improving maternal health. SMS messaging is suitable to transmit patient data and to improve the communication between patient and health care professionals (Deglise et al., 2012). But, using the current SMS service means letting attackers and intruders to access potentially valuable or confidential data which is transmitted without any security measure by intercepting in the meddle.

* 1. **Aim and Objectives**

The aim of this research is to identify the appropriate encryption method for mobile text messaging application and develop SMS security mechanism on android enabled mobile. The objectives are to:

1. Study and identify the appropriate encryption/decryption algorithm for mobile application;
2. Study and identify the appropriate security technique for end-to-end text message security;
3. Design the architecture of secure text message using android studio;
4. Develop a prototype for secure text messaging application which enables the user to send and receive confidential information using any android enabled mobile phone; and
5. Evaluate the performance and quality of service after implementation of the secure system.
   1. **Scope of Study**

The scope of this research is developing a prototype of secure text messaging tool using cryptography techniques for android enabled mobile phone.

**1.6 Research** **Methodology**

* Literature Review: A review of previous literatures that have relevance with the current thesis work will be conducted. From the literature, different concepts and methodologies will be adopted as deemed to be necessary.
* Resource Gathering: Here, the gathering of software tools and other necessary materials that are relevant to bringing the security countermeasure into picture is to be done. The materials are Android Studio IDE, Java 2 Mobile Edition (J2ME), different mobile simulators, etc.
* Developing the Prototype: Java programming language will be used to develop the selected cryptographic technique on text message that can be used by SMS capability of android enabled mobiles.
* Experimenting: Android enabled phones of different capacities will be selected to widen the depth of the application. We will bring the developed application over sample real android enabled mobile phones and configure the application for compatibility with the selected phones.
* Testing the Performance: The degradation of performance would be investigated and Quality of Service due to the added security.
  1. **Limitation of Study**

This application is to be restricted to android platform alone. That means it can only be used on android-enabled phones. Besides, it does not support concatenation of multiple text messages, when the size of the SMS extends 160 7-bit characters. This might be a good area for future researchers to look into.