**Chapter 5**

**SUMMARY OF FINDINGS, CONCLUSIONS AND RECOMMENDATION**

This chapter presents the summary of findings based from the evaluation conducted. Conclusion and recommendations are drawn based on the result of the study.

**Summary of Findings**

The Cryptographic IM (CIM) system is an instant messaging application that allows data exchange and office collaboration such as one-to-one chat, group chat, file transfer, and others. The completion of the three (3) modules/components – Base, Encryption, and File Transfer – allowed the whole system to deliver the desired functionalities as enumerated in the objectives and scope of this study. The CIM was able to provide the basic features found in any typical IM today such as chat and file transfer. Its prowess was seen in the implementation of multi-layered encryption mechanism - the integration of AES 256-bit encryption and HIPS hiding algorithm.

The result of the evaluation revealed that the CIM has little or no advantageous over other typical IM in terms functionalities. It scored low in portability since the application can only be installed in Microsoft Windows platform and not on an android or IOS mobile devices.

However, the system proved advantageous in terms of security as it garnered an average mean of 4.20. The validity of encryption gave the evaluator an assurance of its security.

From the three (3) groups of respondents or evaluators, IT experts gave 3.96 average mean, Cybersecurity experts gave 4.01, and end users gave 4.03. The end users examined the system from a usability perspective and found little or no difference with that of a typical IM, while the cybersecurity experts understand very well the importance of security in an instant messaging application.

**Conclusion**

Based on the result of the study, the following conclusions were drawn:

1. The CIM was successfully designed and developed in accordance with standards and required features. The following are the completed features of CIM:
   1. Multi-layered encryption through the combination of AES 256-bit and HIPS;
   2. Secured One-to-one and room chat;
   3. Secured File transmission;
   4. Secured login authentication;
   5. Able to transmit recorded voice message;
   6. Self-delete or automatic deletion of secret message; and
   7. Use of cipher key exchange methods:

g.1 System Generated Key (SGK); and

g.2 Manual Key Input (MKI).

* 1. Encrypted username and password on the database
  2. The users can decrypt the file at the time of their choosing.

1. The CIM was successfully created using Visual C# .net.
2. The test results proved that the developed application is functional and secure when tested across different Penetration Testing software
3. The test results proved that the CIM will run on any MS Windows operating system except Windows XP.
4. The performance of CIM was evaluated using ISO 25010 software quality criteria with a grand mean of 4.00 and “Very Good” descriptive rating.

**Recommendation**

Based on the foregoing findings and conclusions, the following recommendations are drawn:

1. Further research to develop modules for voice and video communication must be done. Some open-source software libraries, API, and SDK are already available to enable this feature. These libraries can be integrated into the CIM.
2. Improvement of HIPS hiding technique should be considered. Since the programming language that was used to develop the HIPS is already obsolete, there is a need to conduct further study to learn new techniques in steganography. Tools for steganography nowadays can hide data in images, sound clips, videos, and office documents like MS Word, MS Excel, and MS Powerpoint.
3. Further research to develop modules for Short Messaging System or SMS may be conducted. This will allow messaging even if the user is offline and the only available mode of communication is the Global System for Mobile communication (GSM) commonly known as cellphone signal.
4. Development of an android-based and IOS-based CIM client can be initiated. These versions of CIM will provide easier access and mobility to many users.
5. Further research to develop modules for Voice Over Internet Protocol or VOIP may also be considered. This will allow voice communication on any VOIP-enabled phone.
6. Establishment of a standard procedure for the utilization and maintenance of the CIM can be made. This will allow segregation of duties between the administrator and the users.