**Chapter 4**

**RESULTS AND DISCUSSION**

This chapter presents the final output of the system and the result of the evaluation. Project description, project structure, and the capabilities and limitations are briefly discussed to elucidate the finished project. The result of the evaluation and its interpretation was also presented in this chapter.

**Project Description**

The Cryptographic IM (CIM) system is an instant messaging application that allows data communication among peers. It provides essential features for office collaboration such as one-to-one chat, group chat, file transfer, and others. Multi-layered encryption is integrated into the CIM to provide greater security. Advanced Encryption Standard (AES) and the Hidden in Plain Sight (HIPS) algorithm encrypts the data as it traverses across the network. The system was developed in modules or components making it agile in any type of deployment. Meaning, the CIM can be deployed even without the other modules if it is not required for a particular deployment. There are three (3) modules developed, the base, file transfer, and the encryption module. The base component provides the platform for the two (2) components and other future components to be integrated into. These future components can also be a third-party DLL, API, or SDK.

**Project Structure**

The CIM was developed using the Microsoft Visual C# 2017. It runs on both MS Windows 7 and Windows 10 platform and requires dot.Net 4.6 framework. Microsoft Access database engine was included during the installation to allow local storage of user lists and other settings. The figure below shows the final structure of the system.

**Components/Modules/Classes**

**CIM Base Component**

**Forms**

**File Transfer Module**

**Encryption Module**

**Chat Form**

**Login Form**

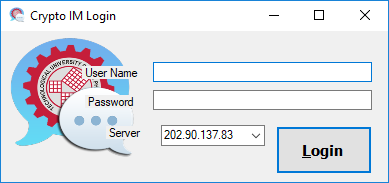
**File Transfer Form**

**Group Chat Form**

*Figure 10.*Final Structure of the CIM

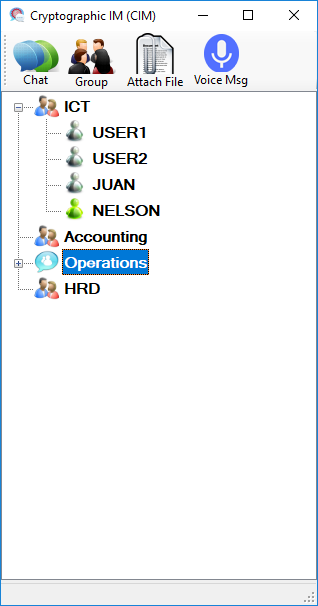
The CIM is composed of Three (3) modules or components, namely:

1. Base Component – This is the most important component of the CIM. It provides the platform in which other components are integrated into. It comprised the forms, references, properties, libraries, and the main program needed to run the system. The following are the forms created for the base component:
2. Login Form – it provides the interface needed to authenticate the user to the CIM server. The password entered by the user is automatically encrypted upon clicking the login button.



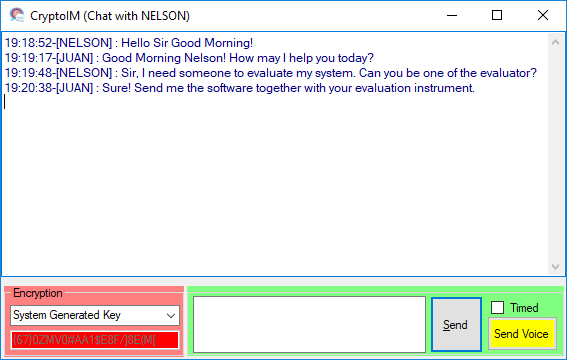
*Figure 11.*Login Form of the CIM

1. Main Window Form – this is the main window that displays after a successful login. Groups and users are populated in the tree view. The green user icon indicates an online user while the gray icon indicates an offline user.



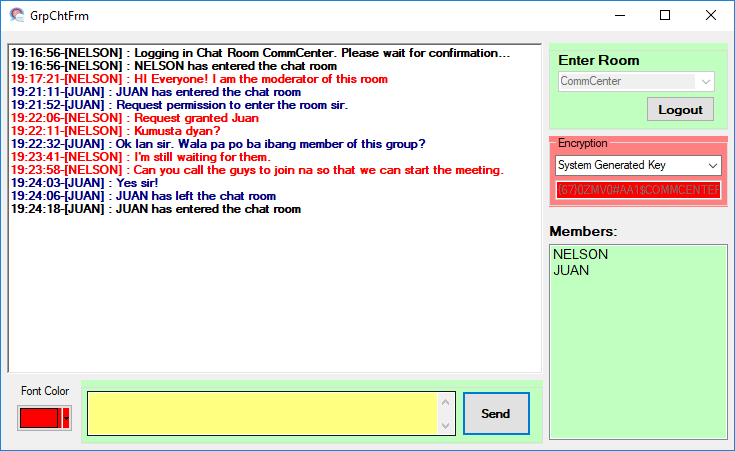
*Figure 12.*Main Window of the CIM after a Successful Login

1. Chat Form – this form allows the user to interact with other peers in the CIM through chat or text-based conversation. The chat communication is encrypted by default using AES 256-bit encryption with passkey generated by the system. The user has the option to manually assign a key for a more private conversation. All system generated keys are changed weekly and stored on the server. This allows the organization to decode the previous conversation during an internal investigation as the need arises. Having keys manually entered denies the possibility of having someone to decode the conversation other than the two (2) communicating peers.



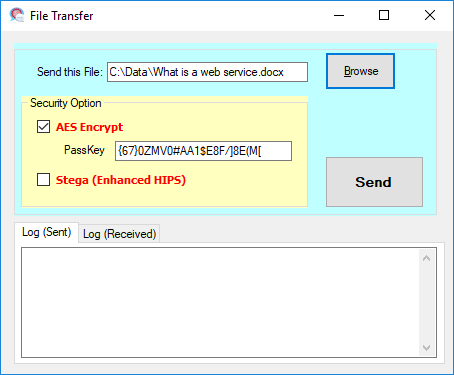
*Figure 13.*One-to-One Chat

1. Group Chat Form – this allows users to broadcast text conversation among members in the room. Like any similar room chat, any users can join the room and the moderator has the privilege to kick any members he or she chooses. Similar encryption is applied in this window.



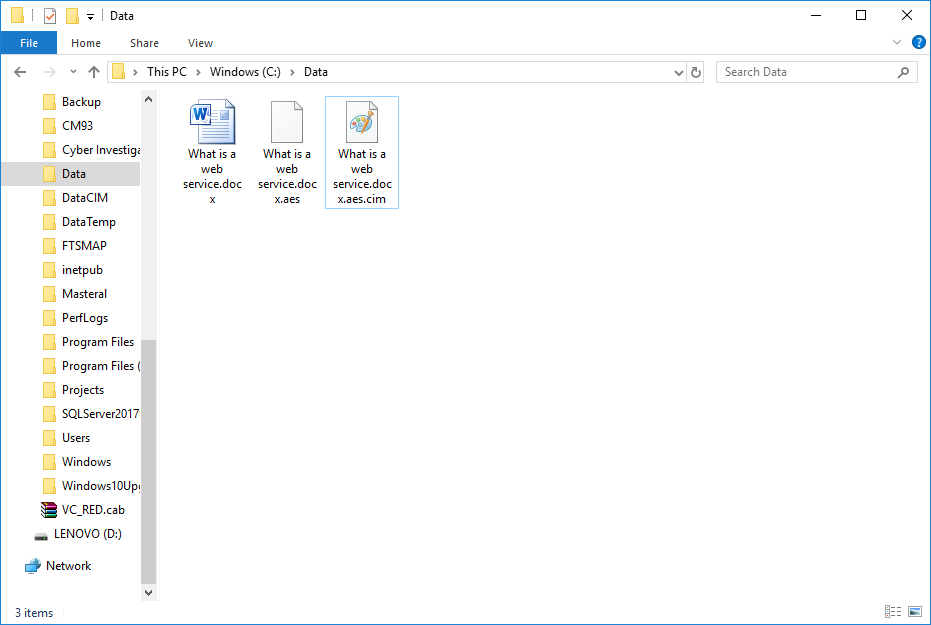
*Figure 14.*Group Chat Form

1. File Transfer Form – this form requires File Transfer module/class to function. It allows transmission of documents, images, audio, video, applications, and other files from one user to another. When applying encryption to the file, encryption module/class is called. The user has the option to use the HIPS for multi-layered encryption of the file.



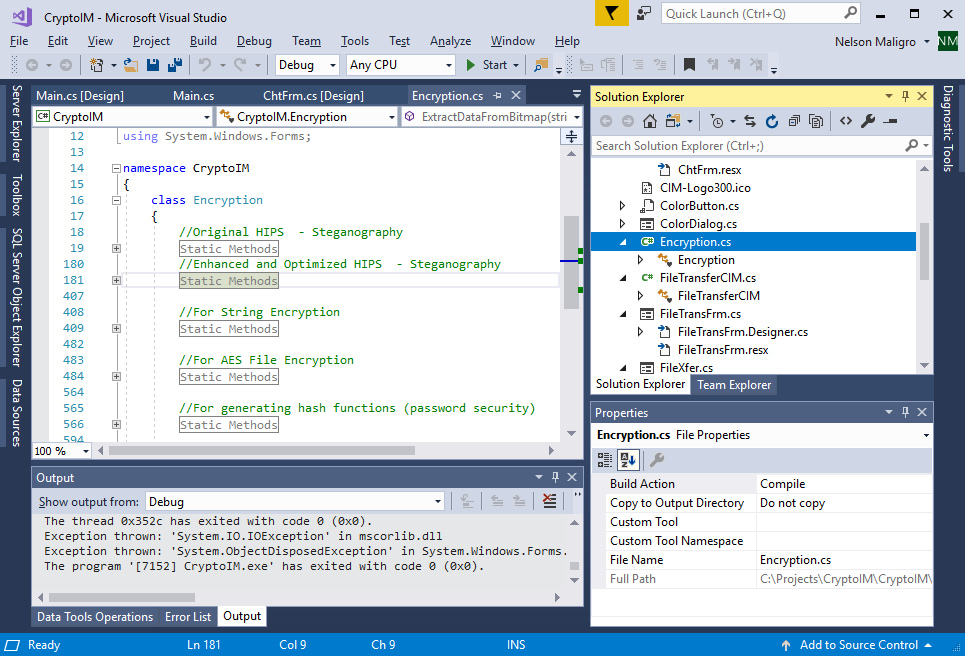
*Figure 15.*File Transfer Form

1. Encryption Component/ Module – this is the component that provides AES encryption and HIPS hiding feature to the CIM. This module can be deployed separately through Dynamic Link Library (DLL) and can be integrated to any applications. The figure below shows the resulting files after encrypted with AES and embedded in an image file (.cim file extension).



*Figure 16.* CIM Automatic Encryption and Decryption

1. AES Encryption – AES as explained in chapter two is an open standard algorithm which can be freely acquired and integrated into an application for strong and robust encryption. The CIM imports the AES library provided in the Microsoft .NET API and wrote specific functions applicable to the system. These four (4) functions are Encrypt String, Decrypt String, Encrypt File, and Decrypt File. The figure on the next page shows the class library for encryption.



*Figure 17.*Encryption Class of the CIM

1. Hidden In Plain Sight (HIPS) Encryption or Hiding Technique- CIM integrates the HIPS source code from Engr. Agustin. Unfortunately, some functions of the code are already obsolete and some controls are no longer supported in the new Visual Studio. Few revisions are necessary to properly integrate the code into the CIM. These modifications improved the HIPS while retaining vital algorithms as formulated in Engr. Agustin’s thesis especially the least significant bit (LSB) replacement and the conversion of the password into a numerical value to be used as a random number (seed value) for picking the pixel positions. The following are some of the enhancement of the HIPS:
   * 1. Auto-resize of the image file – the original HIPS requires the user to import an image file that must be larger than the embedded file or else an error will return. This method was enhanced with a function that auto-resize an image file to a length twice the size of the embedded file.
     2. Direct image file insertion –the original HIPS loads the image file into the Image Control of the Form before hiding the embedded file and then saving the image from the control into another filename. This technique is a slow process; thus, it is replaced with a function that allows direct insertion of the data byte into an object that encapsulates the image file.
     3. Simplified Formula – insertion of the data byte is done by dividing the image file into several bytes and recursively replacing its 4-bits LSB with every 4-bit data byte of the embedded file.
2. File Transfer Component/ Module – this component allows file transmission from one user to another. File transmission is done by establishing TCP socket connection from an online user to the server and then the data byte is transmitted through this socket. The detailed explanation of socket communication is presented in the previous chapters. The Base component calls file transfer module/class when the File Transfer form is opened. Upon clicking the send button, the CIM calls the encryption module and encrypts the file; then the encrypted file is divided into several bytes for transmission. These bytes are sent into streams so that when it reaches the server it is re-assembled back to its original form.

The CIM is further improved to satisfy some of the evaluators’ requirements. These added competitive features are:

1. It allows sending of voice messages;
2. It provides option for self-delete or self-destruct messages;
3. Users are organized into groups or departments;
4. Multi-colored font for room chat;
5. Server logs for auditing;
6. System-generated key is changed weekly;
7. Encrypted username and password on the database; and
8. Users can decrypt the file at the time of their choosing.

**Project Test Results**

A total of ten (10) test cases of the three (3) scenarios were conducted for the operational and functional testing of the CIM. This activity was documented in the Test Incident Log (refer to the appendix). The table below provides the summary of the test results based on the consolidated test cases that was executed during the alpha testing of the system.

Table 11

*Summary of Test Execution*

|  |  |
| --- | --- |
| **Test Execution** | **Results** |
| Total no. of test cases | **10** |
| No. of test cases executed | **10** |
| % executed | **100%** |
| No. of test cases passed | **8** |
| % passed | **80%** |
| No. of test cases failed | **2** |
| % failed | **20%** |
| No. of test cases not executed | **0** |
| % not executed | **0%** |

The result of the functional testing yields eighty percent (80%) or eight (8) test cases successfully run; however, two (2) of the 10 test cases functionally run but generate an error. These failed test cases are minor in severity and are already resolved as of this writing. Documents of these test cases are included in this research for perusal (refer to the appendix).

Portability testing is conducted to check the compatibility of the CIM across different versions of Microsoft Windows operating system. The table below provides the result of this test.

Table 12

*Result of the Portability Testing*

|  |  |  |
| --- | --- | --- |
| Microsoft Windows | Prerequisites | Results |
| Windows 10 |  | * CIM client runs and login window appears * Successfully login to the CIM Server |
| Windows 8.1 | .net 4.0 | * CIM client runs and login window appears * Successfully login to the CIM Server |
| Windows 7 | .net 4.0 | * CIM client runs and login window appears * Successfully login to the CIM Server |
| Windows Vista | .net 4.0 | * CIM client runs and login window appears * Successfully login to the CIM Server |
| Windows XP |  | * CIM Client not running |
|  |  |  |
| Windows 2012 | .net 4.0 | * CIM Server runs and the main window appears |
| Windows 2016 |  | * CIM Server runs and the main window appears |

Among the different versions of the Microsoft Windows operating system, only Windows XP is not supported. This is an obsolete operating system and known to have a number of vulnerabilities; thus, it is not recommended to modify the CIM and pursue installing in this platform.

Vital to the conduct of alpha testing is the security test. It determines the validity of encryption in the CIM. The table below reveals consistent result of a secured data after the system is tested across different Penetration Testing software.

Table 13

*Result of the Security Testing*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Instances | Original Message (Source) | Result Message (Destination) | Penetration Testing Software | | |
| Wireshark | Cain&Abel | Ettercap (Kali) |
| User Login | User: user1  Pass:USER@123 | 24C9E15E52AFC47C225B757E7BEE1F9D  E2B31C4CF92DD40E079B9B8BA414F9BD | Encrypted with MD5 Hash | Encrypted with MD5 Hash | Encrypted with MD5 Hash |
| Send Chat Message | Hello I am user1 | cMYEhI3nugUR4+f97OL1+CjAFe8M7/1vPKrKvBiDvR0= | Encrypted with AES-256 bit | Encrypted with AES-256 bit | Encrypted with AES-256 bit |
| Transmit Document (AES+HIPS) | Smarthouse.docx | Smarthouse.jpg | Image w/ hidden file | Image w/ hidden file | Image w/ hidden file |
| Decrypt Image File | Smarthouse.jpg | Smarthouse.aes  Smarthouse.docx | Encrypted with AES-256 bit | Encrypted with AES-256 bit | Encrypted with AES-256 bit |

There were four (4) instances conducted to test the resulting data or message as it traverses across the network. The penetration testing software sniffed the transmission from clientX (source) to clientY (destination) using ARP Spoofing technique. Sniffing can also be done using a port-mirrored network switches. During login the resulting message appears to be scrambled characters when sniffed. All penetration testing software detected the resulting message as MD5 hash values. Another instance is when clientX sends a chat message to clientY, the message appears to be scrambled characters in the chat window of clientY (the key is changed to prevent decrypting the message). All penetration testing software detected the resulting message as AES-256 bit encryption. During file transmission, clientX sends a plain document to clientY and browsed a JPEG file to hide the document. The jpeg image containing the encrypted file was received by clientY. All penetration testing softwares detected the data as an image file. When clientY manually decrypts the image file, it extracted sequentially the AES file and the plain document (docx) file.

Parallel to the conduct of security testing is the Latency Test. This test is used to determine the time it takes for the data to arrive at the destination when applied with dual-layer encryption. The table on the next page depicts the result of Latency Test using similar instances made with the security testing.

Table 14

*Result of the Security Testing*

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Delay or Timeframe**  (Time it takes for the data to arrive from sender to recipient) | | |
| Instances | Plain  (No Encryption) | Encrypted with  AES | Encrypted with  HIPS |
| Send Chat Message with 50 characters | 0.2 sec | 0.5 sec | Not Applicable |
| Transmit Document with 2mb file size | 8 sec | 14 sec | 17 sec |
| Transmit Document with 10mb file size | 16 sec | 24 sec | 29 sec |

During the chat conversation, the encryption key was removed to test the transfer of text messages when no encryption is applied. The transmitted message appears on the recipient window instantly with a microscopic delay of 0.2 second. This unnoticeable delay was revealed through the use of Desktop Screen Recording software. Similar step is done during the second transmission of text message but with AES encryption applied. This yields with insignificant delay of 0.5 second. However, the delay becomes observable during the file or document transmission. Following similar procedure with chat messaging, yields a truthful result of delayed transmission when AES encryption is applied to the file. The time is increased with 6 seconds when AES is implemented and plus 3 seconds when HIPS is added on a 2mb file. Similarly, on a 10mb file the delay is increased with 8 seconds when AES is implemented and plus 5 seconds when HIPS is added. This shows that the larger the file the longer it takes to encrypt; and this delay consequently adds to the time of transmission.

**Project Capabilities and Limitations**

The CIM provides the essential features of a typical instant messaging application; however, if continually improved, this application can compete with any popular IM today.

**Capabilities**

The following are the capabilities of the CIM:

* + - 1. Secure login through password encryption.
      2. Secure one-to-one text communication or chat.
      3. Secure Group or Room Chat.
      4. File transfer with default AES 256-bit encryption.
      5. File Transfer with reinforced encryption using HIPS hiding algorithm.
      6. Send recorded voice message.
      7. Self-delete of the text message or recorded voice message after several seconds.
      8. Encrypted username and password on the database
      9. Users can decrypt the file at the time of their choosing

**Limitations**

The following are the limitations of the CIM:

1. It only runs on Microsoft Windows 10, 7, 8, and Vista.
2. It requires a Microsoft Net 4.6 framework and Access Database Engine.
3. It does not implement Peer-to-Peer (P2P) technology which means data communication is through the server.
4. Only the CIM can decode the image file that was earlier encoded using the enhanced HIPS. The old HIPS application cannot decode it even if it is the same algorithm that was used. As explained in the above section, there is a need to modify the original codes of HIPS due to obsolescence. For example, the function PSet (*Picture.PSet (r, c), RGB(clrR, clrG, clrB)*) in the legacy HIPS is no longer supported in Visual Studio.Net 2017 thereby replacing it with WriteByte function (*fw.WriteByte((byte)*).

**Project Evaluation**

Five (5) IT professionals, five (5) cybersecurity experts, and five (5) end users evaluated the CIM. The system is evaluated using the eight characteristics/criteria of ISO 25010. These criteria are further broken down into sub-characteristics as discussed in the previous chapter.

The table below shows the average mean score of the CIM in terms of Functional Suitability:

Table 15

*Average Mean Score in terms of Functional Suitability*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Criteria** | **Mean Score** | | | **Average Mean** | **Descriptive Ratings** |
| **Functional Suitability** | **IT Experts** | **Cyber Security Experts** | **End Users** |
| Functional completeness - functions cover all the specific tasks and objectives. | 3.80 | 4.00 | 3.60 | **3.80** | Very Good |
| Functional correctness – the system provides the correct results with a certain degree of precision. | 4.00 | 3.80 | 3.80 | **3.87** | Very Good |
| Functional appropriateness - functions of the system allow the accomplishment of specific tasks and objectives. | 4.00 | 4.20 | 3.60 | **3.93** | Very Good |
| **Average Mean** | **3.93** | **4.00** | **3.67** | **3.87** | Very Good |

As presented in the above table, the CIM got an average mean of 3.87 with “Very Good” descriptive rating. The system definitely provides the needed functionality for data communication and office collaboration.

The table below shows the average Mean score of the CIM in terms of Security:

Table 16

*Average Mean Score in terms of Security*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Criteria** | **Mean Score** | | | **Average Mean** | **Descriptive Ratings** |
| **Security** | **IT Experts** | **Cyber Security Experts** | **End Users** |
| Confidentiality – system ensures that data are accessible only to authorized users. | 4.20 | 4.60 | 4.20 | **4.33** | Very Good |
| Integrity - system prevents unauthorized modification of data. | 4.00 | 4.40 | 4.00 | **4.13** | Very Good |
| Non-repudiation – events and actions can be proven to have taken place. | 4.00 | 4.20 | 4.00 | **4.07** | Very Good |
| Accountability - actions of a user can be traced uniquely to the entity. | 4.00 | 4.60 | 4.20 | **4.27** | Very Good |
| **Average Mean** | **4.05** | **4.45** | **4.10** | **4.20** | Very Good |

As presented in the above table, the CIM got an average mean of 4.20 with “Very Good” descriptive rating. The system is tested and evaluated using the Kali Linux – a popular tool for conducting a vulnerability assessment and penetration testing. The validated encryption of the CIM transcends other IMs in terms of security.

The table on the next page shows the average Mean score of the CIM in terms of Performance Efficiency:

Table 17

*Average Mean Score in terms of Performance Efficiency*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Criteria** | **Mean Score** | | | **Average Mean** | **Descriptive Ratings** |
| **Performance Efficiency** | **IT Experts** | **Cyber Security Experts** | **End Users** |
| Time behavior - running time and rates of the system meet the requirements. | 4.00 | 3.80 | 4.00 | **3.93** | Very Good |
| Resource utilization - amount and types of resources used by the system meet the requirements. | 4.00 | 4.00 | 4.20 | **4.07** | Very Good |
| Capacity – maximum limit of the system meets the requirements. | 4.20 | 3.80 | 4.00 | **4.00** | Very Good |
| **Average Mean** | **4.07** | **3.87** | **4.07** | **4.00** | Very Good |

As presented in the above table, the CIM got an average mean of 4.0 with “Very Good” descriptive rating. The system runs in optimum performance under varying conditions.

The table on the next page shows the average Mean score of the CIM in terms of Usability:

Table 18

*Average Mean Score in terms of Usability*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Criteria** | **Mean Score** | | | **Average Mean** | **Descriptive Ratings** |
| **Usability** | **IT Experts** | **Cyber Security Experts** | **End Users** |
| Appropriateness recognisability – The system is appropriate to the users’ needs. | 4.00 | 4.00 | 3.80 | **3.93** | Very Good |
| Learnability – the system can be used by specific users to achieve certain goals of learning. | 4.20 | 3.60 | 4.00 | **3.93** | Very Good |
| Operability - a system has characteristics that make it easy to control and operate. | 4.20 | 4.20 | 3.80 | **4.07** | Very Good |
| User error protection – the system provides notifications and protects the user during any fault. | 3.80 | 3.80 | 3.80 | **3.80** | Very Good |
| User interface aesthetics - user interface enables satisfying interaction for the user. | 4.00 | 3.80 | 3.80 | **3.87** | Very Good |
| Accessibility - system can be used in a wide range of characteristics to achieve a certain goal in a specific context of use. | 4.00 | 3.80 | 4.00 | **3.93** | Very Good |
| **Average Mean** | **4.03** | **3.87** | **3.87** | **3.92** | Very Good |

As presented in the above table, the CIM got an average mean of 3.92 with “Very Good” descriptive rating. The system is easy to use and analogous with other popular IM in terms of user interface (UI).

The following table is the average Mean score of the CIM in terms of Reliability:

Table 19

*Average Mean Score in terms of Reliability*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Criteria** | **Mean Score** | | | **Average Mean** | **Descriptive Ratings** |
| **Reliability** | **IT Experts** | **Cyber Security Experts** | **End Users** |
| Maturity – the system meets the needs for reliability under normal operation. | 4.20 | 3.80 | 3.80 | **3.93** | Very Good |
| Availability – the system is accessible and fully functional when required for use. | 3.80 | 4.00 | 4.00 | **3.93** | Very Good |
| Fault Tolerance – the system operates despite the presence of software or hardware faults. | 3.60 | 4.60 | 3.80 | **4.00** | Very Good |
| Recoverability – the system can recover and re-establish the desired state after an interruption or failure. | 3.40 | 3.80 | 4.00 | **3.73** | Very Good |
| **Average Mean** | **3.75** | **4.05** | **3.90** | **3.90** | Very Good |

As presented in the above table, the CIM got an average mean of 3.90 with “Very Good” descriptive rating. The system is stable and resilient when tested in an undesirable condition.

The table on the next page shows the average Mean score of the CIM in terms of Maintainability:

Table 20

*Average Mean Score in terms of Maintainability*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Criteria** | **Mean Score** | | | **Average Mean** | **Descriptive Ratings** |
| **Maintainability** | **IT Experts** | **Cyber Security Experts** | **End Users** |
| Modularity – the system is developed into components (so that a change of one component has minimal impact on another). | 4.00 | 4.00 | 4.00 | **4.00** | Very Good |
| Reusability – the system can be used in any mode of application. | 4.00 | 4.00 | 4.20 | **4.07** | Very Good |
| Analysability - the impact of any intended change to a system can be assessed or system deficiencies can be diagnosed. | 4.00 | 3.80 | 4.00 | **3.93** | Very Good |
| Modifiability – the system can be modified without introducing defects to the system. | 3.80 | 3.80 | 3.80 | **3.80** | Very Good |
| Testability – the tests can be performed to determine whether certain criteria have been met. | 4.20 | 4.20 | 3.80 | **4.07** | Very Good |
| **Average Mean** | **4.00** | **3.96** | **3.96** | **3.97** | Very Good |

As presented in the above table, the CIM got an average mean of 3.97 with “Very Good” descriptive rating. The system is developed in modules or components making it agile in any environment.

The table on the next page shows the average Mean score of the CIM in terms of Portability:

Table 21

*Average Mean Score in terms of Portability*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Criteria** | **Mean Score** | | | **Average Mean** | **Descriptive Ratings** |
| **Portability** | **IT Experts** | **Cyber Security Experts** | **End Users** |
| Adaptability - the system can adapt to different or evolving hardware, software or other operating environments. | 4.00 | 4.20 | 4.40 | **4.20** | Very Good |
| Installability – the system can be successfully installed and/or uninstalled in any types of operating environment. | 4.00 | 3.60 | 4.00 | **3.87** | Very Good |
| Replaceability - the system can replace other software for similar purpose and environment. | 3.80 | 4.20 | 4.20 | **4.07** | Very Good |
| **Average Mean** | **3.93** | **4.00** | **4.20** | **4.04** | Very Good |

As presented in the above table, the CIM got an average mean of 4.04 with “Very Good” descriptive rating. The system can only be ported or installed in a MS Windows environment.

The table on the next page shows the average Mean score of the CIM in terms of Compatibility:

Table 22

*Average Mean Score in terms of Compatibility*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Criteria** | **Mean Score** | | | **Average Mean** | **Descriptive Ratings** |
| **Compatibility** | **IT Experts** | **Cyber Security Experts** | **End Users** |
| Co-existence – the system functions efficiently while sharing common resources with other systems and without detrimental impact with each other. | 4.20 | 4.00 | 4.40 | **4.20** | Very Good |
| Interoperability - two or more systems can exchange information and interoperate seamlessly | 3.60 | 3.80 | 4.60 | **4.00** | Very Good |
| **Average Mean** | **3.90** | **3.90** | **4.50** | **4.10** | Very Good |

As presented in the above table, the CIM got an average mean of 4.10 with “Very Good” descriptive rating. The system performs efficiently while sharing a similar .NET library with other applications. It can co-exist with other windows applications.

The table on the next page depicts the overall evaluation rating of the CIM based on ISO 25010 standards for software quality.

Table 23

*Overall Average Mean Score of the CIM*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Criteria** | **Mean Score** | | | **Average Mean** | **Descriptive Ratings** |
| **ISO 25010 Characteristics** | **IT Experts** | **Cyber Security Experts** | **End Users** |
| Functional Suitability | 3.93 | 4.00 | 3.67 | 3.87 | Very Good |
| Security | 4.05 | 4.45 | 4.10 | 4.20 | Very Good |
| Performance Efficiency | 4.07 | 3.87 | 4.07 | 4.00 | Very Good |
| Usability | 4.03 | 3.87 | 3.87 | 3.92 | Very Good |
| Reliability | 3.75 | 4.05 | 3.90 | 3.90 | Very Good |
| Maintainability | 4.00 | 3.96 | 3.96 | 3.97 | Very Good |
| Portability | 3.93 | 4.00 | 4.20 | 4.04 | Very Good |
| Compatibility | 3.90 | 3.90 | 4.50 | 4.10 | Very Good |
| **Total** | **3.96** | **4.01** | **4.03** | **4.00** | **Very Good** |

It was rated high in terms of “security” and garnered an average rating of 4.20. The validity of its encryption gives the evaluator an assurance of its security. The CIM may not have achieved an excellent rating due to its limited features as compared to other popular IM; however, continues improvement of the system and integration of additional modules will enable it to compete in the IM arena.