**Chapter 2**

**CONCEPTUAL FRAMEWORK**

This chapter presents the review of previous literatures and studies related to Instant Messaging applications. It explores the earlier developments, previous research, and existing technologies leading to the development of a prototype cryptographic IM (CIM). It includes the operational definition of terms used, and the conceptual framework to visually synthesize all materials and techniques in achieving the desired objective.

**Review of Related Literature and Studies**

***Historical Development of Instant Messaging (IM)***

The advent of Instant Messenger like Facebook Messenger, Skype, WhatsApp, Telegram, and other popular IM revolutionizes the way people communicate with each other. But its impressive features would not be possible without the earlier breakthrough of their predecessors.

Desjardin (2016), in his article “The Evolution of Instant Messaging”, narrates the written accounts that brought the IM and how it grows prominence in the new era. Instant Messaging became known in the 1990’s but decades ago Massachusetts Institute of Technology (MIT) already demonstrated an information sharing program called Compatible Time-Sharing System (CTSS). In 1988, Jarkko Oikarinen developed the first chat system that allows sending messages to users through their computers (Oikarinen, 1988). His Internet Relay Chat (IRC) paved the way for other IM players like AOL IM, ICQ, and Microsoft IRC to battle for share in the IM market. Yahoo messenger dominates in 1998 with its intuitive designs and feature-rich IM environment. Engel (2014) recounts how IM grow prominence in the 2000s. This was the golden age of instant messenger. MSN Messenger introduced the concept of sharing photos and included the PC-to-PC and PC-to-phone audio capabilities. Skype Messenger peaked in popularity in 2003 as it showcased Audio and Video chat capabilities. Facebook chat was first introduced in 2008 and accelerated its popularity in 2014 when it decouples from the Facebook App.

***Application of IM***

***Military Institution***

The US military has long been using IM for its military operations. In fact, Cummings (2005, p. 654) stated:

*“It was the primary means of communication between navy ships during Operation Iraqi Freedom in 2003”.*

In his journal “The Need for Command and Control Instant Message Adaptive Interfaces: Lessons Learned from Tactical Tomahawk Human-in-the-Loop Simulations” Cummings affirms the obvious advantage in real-time communication embodied in IM. It allows rapid response to inquiries, multiple conversations with various units, and access to previous conversations and orders.

In a thesis presentation entitled “Applicability of Instant Messaging in the Military Command and Control Systems”; Vermaja (n.d.) explains that IM can offer many advantages but security issues in implementing it is a problem. Furthermore, commercial off-the-shelf (COTS) IM does not satisfy wholly the needs of a Command and Control (C2) communication. Customized applications are needed to make the communication easy and practical. Tailor-fit applications with specific platforms are needed in order to build automated systems.

***Businesses***

Various studies were already conducted on the maturity of IM to be used for business communication. Results clarify how businessmen and their clients choose this technology for daily transactions and communication. It was learned that people, generally, uses IM for a variety of substantive business purposes, and their peers include a diversity of co-workers, clients, managers, and other business personalities (Muller, Raven, Kogan, Millen, & Carey, 2003).

Gotrunk (2017), a US company that offers secure and reliable VOIP services, shares their experience in IM. According to them, businesses are now beginning to embrace IM for their office communication. IM is virtually real-time communication like a telephone call. It is a text-based conversation like email but in an instant. It proves advantageous for collaboration among employees from different locations. In fact, some employees even use it for private communication within and outside the office.

***Schools***

People of college age constitute a significant and considerable number or population among IM users. Flanagin (2005), in his study, found out that IM has become a central communication tool within the college population. IM is being used for a variety of personal needs and school requirements and utilized it heavily relative to other forms of communication like email and telephone. Moreover, evidence suggests that college students are satisfied with simultaneously processing multiple conversations and that IM might displace email in many consequential ways.

***Security Issues of IM***

The efficiency and usability of this application come with a major drawback on security. Hackers and cybersecurity professionals found several vulnerabilities with this system. These problems make most organizations to re-think implementing and adapting IM. Moreover, the pervasiveness of this application makes it vulnerable to various attacks especially sniffing and hijacking. Symantec (n.d.), a leader in cyber security applications, exposes some of the threats and vulnerabilities found in popular IM. IMs are designed with usability rather than security in mind. Almost all freeware IM software do not have encryption capabilities.They enumerated some of the threats and vulnerabilities found in many IM. These are eavesdropping, sniffing, man-in-the-middle attack, session hijacking, and malicious software injection such as Worms and Trojans.

Sweigart, C. (n.d.) explains that most IM System configures the server to act as a mediator and relay all message traffic; some, on the other hand, use peer-to-peer communication. The latter offers better security than the former. In peer-to-peer, the client sends the message directly to the recipient allowing data traffic to flow without the IM server’s intervention.

SANS (2003) Institute, a popular training center for information security published a whitepaper to make people understand the risk associated with every IM. According to them, the lack of encryption protocols on free IM means that IM session conducted in a public network is like an open book to the entire Internet community. Classified information and trade secrets if communicated over free IM on a public network can become public knowledge within seconds.

Few news articles can be found as an evidence of this vulnerability, many IM vendors bargain this flaw as leverage for the users to purchase the licensed version. However, major system flaw can cause a commotion among IT professionals and result can be devastating if not fixed. On January 5, 2002, *The Washington Post* reported that a hacking group known as w00w00 found a hole in a software code of a popular IM program. Matthew Conover, the founder of the group, reported the software flaw to AOL. Failing to recognize his effort, the impatient hacker published the flaw to the community and an explosion of national media attention wreaks AOL (Oldenburg, 2002).

A recent news article from ZDNet news, Condon (2017) reported a hacking incident of a popular IM, HipChat. The incident affected a server in the HipChat where messages and content in chat rooms may have been accessed. In response, HipChat posted a security notice to the public about a vulnerability of the third-party library used by their IM.

On an Internet post, Marcel Ackerman explains the need to encrypt the Instant Messenger. Ackerman provides recommendations on existing IM technology that are being used today and posted list of popular IM that is equipped with security protocols. According to his blog, people are fooled by companies that use security as a marketing buzzword. They will show the fancy user interface but do not provide details of the encryption or unwilling to disclose the algorithm for scrutiny (Ackermann, 2018).

***IM Architecture***

***Client-Server Architecture***

The development of this prototype IM software largely depends on previous literary studies on client-server architecture and socket programming techniques. A thesis worth reviewing is the work of Tim Van Lokven (2011) entitled Review and Comparison of Instant Messaging Protocols. Lokven examines the architecture of the three (3) commonly used protocols by popular IM. These are Microsoft Notification (MSN), Open Source for Communication in Real-time (OSCAR), and the Extensible Messaging and Presence Protocol (XMPP) protocol. The efficiency of these protocols is evaluated based on a predefined set of criteria including its security. In his findings, Lokven stated that steps should be taken to encrypt messages sent to the servers.

IM can also be developed using a web-based or browser-based architecture. I3M is an instant messaging and chat system developed by Hans Schmid for web-based reporting and collaboration. The I3M application server stores centrally all user accounts and provides communication to clients in the form of Web service. The server is written in Visual C# and runs on the Windows 2000 platform (Schmid, n.d.).

Yulianto (2015), in his proposed IM architecture model, outlines the use of XMPP protocol and OpenFire web server as a cost-effective means to develop an Android-based IM application. The web server is used to implement a web application and can communicate via XMPP with chat server and MySQL as its database. Yulianto concluded that his proposed architect is running well and ninety-three percent (93%) of the respondents are willing to install his IM to their terminals.

In a presentation during Hackathon – a convention for ethical hackers and cybersecurity professionals, Eugene Letuchy reveals the chat architecture of Facebook Messenger. Facebook uses Erlang Programming Language to develop their chat application. Client browsers send messages using Ajax scripting; web server receives this message and creates a channel for every client. Erlang powers the backend of the web servers aggregating and distributing all messages. Eventually, Facebook rewrites its chat application codes to C++ for stability and scalability (Letuchy, 2007).

Linan Zheng (2005) explains the possibility of developing an integrated communication platform through the combination of “Presence” technology and instant messaging. The “Presence” service allows users to know the status of his peers and can decide what communication channel to use whether SMS, Video Call, or leave a voice message. Zheng also examines the use of the Jabber protocol, a fork from XMPP, and outlines the flow of messages using this protocol.

***Socket Programming***

A socket whether Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) is one of the fundamental and significant protocols in developing a client-server application. TCP or UDP Sockets enable software applications to communicate with each other in a network. Singh (2014) elucidated the process of TCP connections and how it creates sockets. Application X connects to Application Y using the command “tcp.connect” while Application Y waits for any application to connect using the “tcp.accept” command. Once a connection is established a socket is created for that connection. Application X then uses the socket to stream or transmit data through the command “socket.send” while on the other end; application Y receives the packet using “socket.receive”. Sockets act as an endpoint for a two-way communication link between two applications running on a network.

Socket programming is the backbone of almost all client-server applications like web services, email services, telnet services, IM, and other applications who implement similar TCP and UDP protocols. By learning socket programming, programmers can develop network application that allows data transmission from one host to another. Similarly, Microsoft developed MSN or Microsoft Network for its proprietary IM and America Online (AOL) developed Open System for Communication in Realtime (OSCAR) for AIM application. Abba (2013) developed a LAN Chat Messenger (LCM) application using socket programming in JAVA language. His LCM created a solution to the organization’s internal communication problem.

In a journal from sciencedirect.com, Eddie Law and Roy Leung presented a unified layered architecture for any TCP/IP networks. The model, known as Active Network Socket Programming (ANSP), allows an active application to be written once and run on multiple environments. This unified programming interface layer is light-weighted and can be easily deployed (Eddie Law & Leung, 2003).

***Encryption Algorithm***

***Advanced Encryption Standard (AES)***

Data security is of utmost importance in any organization whether private or government sector as stated in previous section of this study. Adoption of an encryption mechanism is an effective, if not the most effective, means to achieve data security. Encryption converts plain messages to a format unreadable by any person. It mathematically scrambles the data as it travels from the sender to the receiver.

Padate (2005), in his journal, emphasized the importance of data security and how Advanced Encryption Standard (AES) improves the security of any data communication application. AES which was originally called Rijndael is an open-standard or open-book specification of an encryption algorithm published by the U.S. National Institute of Standards and Technology (NIST) in 2001. AES was selected among fifteen (15) encryption algorithms that were subjected to rigid test and evaluation. AES was designed to be resistant against all known brute-force attacks. It is a symmetric block cipher that comes in three key lengths: 128, 192, and 256 bit. The basic implementation of AES is simple mathematical and logical table lookup operations. This symmetric key algorithm is fully open to the public for evaluation and scrutiny, and to ensure transparent analysis and validation of the design.

This was further proved by Mahajan (2013) in his journal entitled Study of Encryption Algorithms AES, DES, and RSA for Security. Based on his test result, Mahajan concluded that the AES algorithm is faster than RSA which consumes longest encryption time. Further, decryption of AES is better than other algorithms.

***Steganography or Hiding Technique***

Steganographyis a type of cryptography which conceals or hides valuable information inside a benign object. Previous research on cryptography at Technological University of the Philippines (TUP) offers a viable option for encryption to complement the AES. Agustin (2005), with his Hidden in Plain Sight thesis, discusses the method of hiding plain files into an image file. Contents or bytes of the file fill in the white spaces of the image file using Least Significant Bit (LSB) insertion technique. These blank spaces are almost unnoticeable to the human eye. Such method of encryption is commonly called steganography. While there are several methods in steganography Mardonio provided a unique method in securing the password. The plain password is translated into a numerical value using shift, modulo and XOR bitwise operations.

Steganography technique is further implemented in the thesis of Torres (2012) entitled Development of FileGuard: Steganography Software. Torres simplified steganography technique by creating modules or algorithms for extraction, encryption, and compression. FileGuard software passed the test and evaluation of quality software based on its functionality, Usability, Reliability, Efficiency, Portability, and Maintainability.

***Integration of Cryptography into Software Applications***

***Desktop Applications (Standalone)***

Establishing a secure data transmission requires implementation of cryptographic in the communication channel. Both sender and receiver must agree upon a set of security protocols for them to communicate and understand each other (Del Pozo & Iturralde, 2015).

Remijan (2014) briefly discussed the procedure in integrating encryption to a Visual C# application using the readily available Class component for AES. According to him, the code for AES encryption and decryption is not very long since this is an open standard published by NIST. However, figuring out the right method, variable, and configuration is the tricky part. Remijan uploaded his AES project in the Github.com for anyone to evaluate and use it.

***Email Application (Client-Server)***

Recent developments in email communication introduce the adoption of asynchronous or certificate-based encryption into the email. A study from Jakarta, Indonesia proposes a secure method of e-mail communication using a hybrid encryption. It combines hash function, symmetric encryption and asymmetric encryption (Mantoro & Zakariya, 2012). The study is further enhanced by Criseldo Calinawan in his research “Hybrid Encryption Algorithm Implementation on Electronic Mail Service”. The researcher implemented the Rivest–Shamir–Adleman (RSA), a certificate-based encryption, and his own encryption algorithm written in PHP language into a webmail client. The result shows faster execution time, reliability, and improved security (Calinawan, 2015).

***Communication Application (Client-Server)***

Few studies are conducted to demonstrate the integration of an open standard encryption algorithm like the AES into a communication application (i.e. Instant Messenger). Moh Heng Huong successfully integrates the AES 128-bit encryption into his communication application. According to him, AES 128 encryption provides a more secure communication than other encryption algorithms. The encrypted data is unbreakable until today using this algorithm (Huong, 2014).

***IM Application (Client-Server)***

Integration of the chosen encryption algorithm into the IM presents a huge challenge. By studying and adopting previous development of network application incorporating encryption algorithm significantly reduces the amount of time hard-coding these algorithms. Krishna (2011) published a journal of his method of integrating AES encryption into file transfer application using secure shell protocol. It uses a “Toolkit” to handle the process of encryption and password authentication. Toolkits are a readily available software component that can be integrated into the main application.

Google patented a secure instant messaging called the AOL Instant Messaging. The secure IM adopts a certificate-based encryption. A certificate authority (CA) issues security certificates to users and use its public key to encrypt messages and files for the user. The user then sends his certificate to an IM server which distributes the user's certificate to other users. Users encrypt messages and files using a symmetric encryption algorithm and the recipient’s certificate (US 9,509,681 B2, 2016).

***Software***

***Programming Software***

Visual C sharp (#) dotNET (.NET) is one of the programming languages bundled in Visual Studio.NET. It is designed to develop a wide range of business-driven and enterprise applications. It provides simple but high-performance object-oriented language in a .NET environment. It also enables developers to build applications for an array of needs and requirements including deployable form-based applications, centralized transaction, operational and logistical automation, and network socket communication. (Price & Gunderloy, n.d.).

C++ and C# are the ideal programming languages for socket application development. The C# language aims to leverage the power of C++ with programmer-friendly environment and ease of Visual Basic. The C# language is suitable for a firm and soft real-time applications (Lutz & Laplante, 2003). Samia Tapur introduced online laboratory courses that allow students to learn the basic and advanced functions of network sockets using C language. The students can better understand the behavior, properties, and functions of these sockets during the connection of the client to the server through simulated exercises (Talpur, 2016).

***Operating System Software***

Microsoft Windows Operating Systems (MS Windows OS) is a family of computer operating systems developed by Microsoft since 1985. Almost eighty percent (80%) of computers nowadays runs with Windows OS. Popular versions of MS Windows OS are Window XP, Vista, 7, and 10 (Carpenter, 2012). MS Windows is highly modular. Each function is managed by components of the operating system. The protected subsystems and its applications are structured using the client-server model, which is a common model for distributed computing like the computer networks. A client application requests a service by sending a message. The message is then routed to the appropriate server. The server performs the requested operation and returns the results back to the client through another message (Stallings, 2004).

***Vulnerability Assessment and Penetration Testing (VAPT) Software***

Kali Linux is a variant of Linux Operating System. It is an opensource operating system specifically designed to provide a vulnerability assessment (VA) and penetration testing (Pentest) platform for ethical hackers and cybersecurity professionals in order to test the security of a particular network or information system. (Pérez & Binders, 2003).

Penetration testing is the method of finding vulnerabilities of an application. Global statistics show that more than 70% of the applications have vulnerabilities which can be exploited by any hacker. It needs to be secured and the best way to secure the application is to try hacking into it using a specifically designed tool like the Kali Linux (Sarmah & Hachan, 2018). \_  
 Hackers are categorized as a White hat, Black Hat, or Gray Hat. White Hat hackers are ethical hackers with some certifications. This type of hacker uses tools like Kali Linux for implementing hacking and breaking into systems purposely to identify vulnerabilities and repair them (Gawhale, 2016).

***Database Software***

Microsoft Structured Query Language Server (MS SQL) is an object-oriented and relational database developed by Microsoft. It basically stores and retrieves data required by any connecting applications. It can be accessed through standalone applications or online connectivity using TCP/IP network. SQL is the standard language used to communicate and manipulate the data stored in this database (Sarka, Radevojivec, & Durkin, 2018).

Microsoft Access (MS Access) is a standalone database management system developed by Microsoft to provide the easy, fast, and deployable database. It is the database of choice for programmers and non-programmers to deploy a short-to-medium size application and does not require storage of bulk data. (Hennig, Bradly, Linson, Purvis, & Spaulding, 2010).

***Network Infrastructure***

Computer Network is a series of nodes and terminals interconnected by communication links in order to exchange data, voice and video packets. Popular network devices are routers, hubs, switches, modems, and any terminals equipped with Network Interface Cards (NIC). These devices are joined together by network links like network cables (e.g. UTP, Serial, Fiber Optics) and wireless connectivity (e.g. Wireless Access Points, 3G, LTE). TCP/IP is the commonly used protocol or algorithm for network devices to communicate and interact with each other (Peterson & Davie, 2012). The interconnectivity of vast computer networks across the globe is called the Internet.

The Internet protocol is the networking model and set of communications protocols used for computer networks or the internet. The Transmission Control Protocol (TCP) and the Internet Protocol (IP) are the first networking protocols defined in a public standard. It was originally known as the DoD model because the development was funded by DARPA, an agency of the United States Department of Defense. TCP/IP provides end-to-end connection specifying how data are transmitted, broken (packetized), addressed, and routed at the destination (Nath & Uddin, 2015).

***Evaluation Standards***

The International Organization for Standardization (ISO) 25010 standard is a framework that evaluates the quality characteristic of software. It is divided into eight (8) criteria or characteristic. These are Functional Suitability, Performance Efficiency, Usability, Reliability, Security, Maintainability, Portability, and Compatibility (Galin, 2018).

Functional Suitability defines the completeness, correctness, and appropriateness of various features and functionalities of the software. This test determines whether components of the system meet and satisfy the requirements of the stakeholders.

Performance Efficiency gauges the response time, utilization of resources, and the capacity of the software during runtime under normal and stress condition.

Usability determines the accessibility, operability, user interface friendliness, and appropriateness to the needs of the stakeholder. The degree to which software is easy to operate is evaluated.

Reliability measures the degree of availability, fault tolerance, and recoverability of the software under normal and stress operation.

Security evaluates the ability of software to protect the data processed in terms of confidentiality, integrity, authenticity, accountability, and non-repudiation. Applied encryption and steganography are evaluated for this purpose.

Maintainability determines the effectiveness and efficiency of the software during modification on any of its components.

Portability refers to the degree of effectiveness of the software to adapt various hardware and software environment after installation or during runtime. It is tested on most common Windows platforms such as Windows 7, Vista, and 10

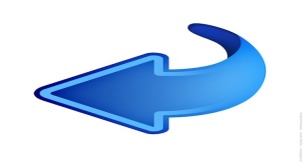
Compatibility measures the interoperability of the software when integrated with various systems, toolkits, Software Development Kits (SDK), Application Programming Interfaces (API), and libraries. Components of the software are evaluated to determine if it performs effectively with no detrimental impact on other identified software while sharing a common environment.

**CONCEPTUAL MODEL OF THE STUDY**

Based on the objectives of this research and the review of previous studies, proven designs, applied theories, and other dependable concepts and literatures, the following model was outlined to conceptualize the development of the CIM

.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **INPUT**  **PLAN**  Software  Requirements:  - Visual C# .net  - Microsoft Windows  7 or 10   * MS SQL and   MS ACCESS   * - KALI Pentest Tool   Hardware  Requirements:  - Two (2) Computer  Set (Client & Server)  - LAN Setup  (Network switch &  Patch cord)  Knowledge  Requirements:  - System Specification  - Socket Programming  - TCP/IP Protocol  - Cryptography |  | **PROCESS (Agile Method)**  **LAUNCH**  **RELEASE**  **RELEASE** |  | **OUTPUT**  CRYPTOGRAPHIC INSTANT MESSAGING SYSTEM (CIM) |



**EVALUATION (ISO 25010)**

***Figure 1.*** Conceptual Model of the CIM System

Figure 1 from the previous page shows the conceptual model that visualizes the processes involved in order to develop the CIM System. Hardware, software, and knowledge requirement, including the system specifications, shall be the input that guides and fuels the entire processes.

Planning should be an interrelated activity between input phase and process phase to identify the necessary requirements needed for the successful completion of every module. This is done to address the issue of needing to acquire additional software or libraries that emerged only during the actual coding.

In the Process phase, Agile methodology shall be adopted for the coding of the software so that one component can be released or launched even without the other unfinished components making it ideal for evolutionary or continuously improved software. **Agile** refers to an effective software development technique that is time-boxed and iterative. It works by breaking the project into components of functionalities, prioritizing them, and then continuously delivering them in cycles called iterations. The entire system shall be divided into three (3) components – the base, data transfer, and encryption. Data transfer component begins its development process upon release of the base component.

Similar with the planning activity, launching or deployment of the entire system shall be an interrelated activity between process phase and output phase. This is to allow immediate debugging on the errors that triggered during the deployment. Evaluation is done after the operational testing of the CIM. Modification of the system can still be done after the evaluation to satisfy the requirements of the end users.

**Operational Definition of Terms**

This section provides the definition of terms which are observable, identifiable and repeatable.

The following terms are defined operationally to better understand the project study:

**API** or Application Programming interface is a set of methods or subroutine definitions that allow communication among various components.

**ARP Spoofing** or Address Resolution Protocol spoofing is a technique used by an attacker to send a spoofed address to the ARP table of every device in a local area network. It reroutes all transmission from the victim computer to the attacker.

**Asymmetric Encryption** isalso known as Public Key Cryptography which uses two (2) keys to encrypt a plain text. A public key is made available to anyone who wants to use it while the private key is kept a secret to the owner.

**Closed Source** refers to proprietary software whose source code is not shared with the public for anyone to look at.

**Command and Control** refer to the exercise of the authority of a designated officer over a group of personnel under his/her command in the accomplishment of task or mission.

**Cryptography** refers to the practice or study of techniques which mathematically scrambles the plain message into a form unreadable to any person except for the intended recipient.

**Internet Protocol (IP)** refers to the dominant communication protocol used by a Local Area Network, Wide Area Network, or the Internet.

**Libraries** or Dynamic Link Libraries (DLL) are Microsoft implementation of modules or subroutines (similar to API) that can be shared or reuse across multiple applications.

**MAC Flooding** or Media Access Control flooding is a technique employed to compromise the security of network switches by flooding the MAC table causing it to broadcast the data out to all ports.

**MD5 Hash Value** or Message Digest Fifth version is a one-way cryptographic hash function with 512 bit block size. It is an encryption algorithm that maps data to a bit string of a fixed size called a hash and is designed to be irreversible.

**Man-in-the-middle attack** is an attack wherein the hacker resides in between two communicating parties in an attempt to sniff, relay, or alter the transmission of data.

**NET Framework** is a Microsoft model or structure of interrelated class libraries which provides interoperability across several programming languages. It allows reuse or sharing of libraries among different windows applications.

**Open Source** refers to a type of software in which the source code is released under a general public license. This license grants other users to study, modify, and redistribute the software to anyone and for any purpose.

**Packet** refers to the chunk or unit of data that is routed over a TCP/IP network or the Internet.

**Session Hijacking** a.k.a. cookie hijacking is a technique used by exploiting a valid network session in order to gain unauthorized access to network services or computer systems.

**Socket** refers to the network stream or channel which allows transmission of packets between hosts in a network.

**Socket Programming** refers to computer programming practices which deal with socket communication between nodes or hosts in a TCP/IP based network.

**Software Developers Kit (SDK)** isa set of software development tools, API, libraries, and documentation to enrich an application with specific functionalities and for a specific platform that is deemed complex to develop. It reduces the amount of time solving programming problems.

**Symmetric Encryption** is the simplest method of encryption which involves only one key to encipher and decipher a message.

**Transmission Control Protocol (TCP)** is one of the main protocols which complement the Internet Protocol (IP) in handling the packets over the internet. It provides reliable, connection-oriented, error-checked, and ordered delivery of data between hosts.

**User Datagram Protocol (UDP)** is one of the core member protocols which complement the Internet Protocol (IP) in handling the packets over the internet. UDP is connectionless and unreliable but transmits faster than TCP.

**VOIP** or Voice over Internet Protocol is a hardware or software technology that allows voice communication over a TCP/IP Network or the Internet.

**Vulnerability Assessment and Penetration Testing (VAPT)** is a systematic way of finding vulnerabilities of an application, computers, or network. It involves the employment of intrusive techniques in order to bring the flaws to the surface with the intent to repair those.