Chapter 3 Research Methodology

The goal of research is to search for knowledge in the particular field of study [86]. Research is done to produce new knowledge and increase one’s knowledge and understanding of the field and topic or matter in the particular area of one’s research. Research can also be defined as a scientific and systematic approach to uncover hidden information on a topic of research. In their book Redman and Mory [87] define research as “systemized effort to acquire knowledge”. Research can be described as an art form for investigating the problem scientifically. Humans as a species are inquisitive about various events and affairs. It is this inquisitiveness that drives humankind to understand their working mechanism and underlying concepts of operation that make events happen. This inquisitiveness causes man to discover knowledge that is previously unknown to mankind. This drive to find unknown knowledge due to its inquisitive nature can be termed as research.

Research in general can comprise of many natural processes [87]. It can include activities such as problem definition, formulation of hypothesis, data aggregation and information organization, deducting facts based on data, reasoning out the facts and examining the conclusion against the earlier formulated hypothesis. Thus, we can say that research is the contribution of an individual with existing knowledge that extends its boundaries. The research is done through a systematic method of generalizing problems and then formulating theory based on the problem. This systematic approach is known as research methodology [88].

A taxonomic approach is required for identifying the problem, formulating the hypothesis, collecting the data through different methods, analyzing the data and finally arriving at a conclusion.

3.1 Need for research methodologies

The research methodology is important to solve any research problem systematically and scientifically. Research methodologies are different scientific techniques employed by researcher to study the research problem [89] [90].

Research methodologies help researchers in understanding various underlying concepts that the researcher will use during the research [90]. These concepts in turn will assist the researcher in
understanding the research problem and enable the researcher to draw it more systematically and scientifically.

There are many programming languages to write code. It is through research methodologies that the researchers can determine which is the most suitable technique to conduct his or her research. It is based on the context of research problem definition and solution.

Research methodologies help researchers in understanding concepts. For example, it helps learning about key exchange protocols, their vulnerabilities and parameters that affect performance of key exchange protocol execution. One of the approaches is to employ empirical study, use simulation and experimental methodology which we followed here. [89].

3.2 Research methodologies applied in research

3.2.1. Qualitative Research Methodology:
Qualitative research methodologies were originally developed in the study of social sciences [89]. They were developed to enable researchers to scientifically study society and culture of civilizations. Some of these methods are action research, case study research and ethnography. Observation and participant observation, interviews and questionnaires, documents and texts, and the researcher's impressions and reactions are some cases of qualitative research methodologies [91]. Design of qualitative methods is such that they help researchers understand various contexts to understand people and cultures [89].

The qualitative aspect deals with detailed description of situations. In the qualitative aspect, description of the problem starts from the generalized description. It ends in a very specific view of the problem [89]. It can be done by using different techniques such as interviews, observations, reviews of existing papers, reports and books. In qualitative methodology a researcher identifies the problem as it is in simple but specific and scientific terms.

Qualitative research is applied to infer the problem from different aspects. It also assists researchers in developing ideas on the solution, or formulating a potential hypothesis. Qualitative technique is one of the most unstructured techniques [89]. The sample size in
qualitative technique is very modest but the sample is chosen such as all it comprises all the parameters equally [89].

In this research, qualitative research method is utilized to understand the process of secret key exchange over insecure network. To study the process of secret key exchange, different key exchange protocols previously proposed by other researchers are examined using the quantitative approach which compares some well-known protocols with the proposed protocol. Different protocols had vulnerabilities that are also covered under the study of the protocols.

The authors used qualitative method such as review of available literature to understand functioning of key exchange protocols. The authors reviewed literature for existing vulnerabilities in protocols. To find out the most suitable protocol for mobile devices from the protocols under study, the authors use qualitative methodology. The authors determine a number of parameters such as execution time, battery power usage, performance of protocols on different bandwidth etc. to quantitatively decide the best suitable protocol for mobile devices. This protocol is then modified to enhance its performance further.

The modified protocol is then checked against vulnerabilities studied under quantitative review of protocol to make sure that the improved protocol does not compromise on security. The authors use an unstructured technique; looking at the literature to find out set of protocols for study based on how old they are, how popular they are, what is their composition and so on, their parameters to be considered, decided about how the notion of security and performance is considered in the system and how they will be measured. The authors have identified this problem and tried to find how other qualitative responses are provided by other researchers.

The authors used detailed descriptions of protocols, study their functioning to the finest detail and provided their own improvements. As for the qualitative research, we have a small sample size of six protocols to look at and compare with our own protocol.
3.2.2 Inferential Research Methodology
Inferential research is about identifying the variables and parameters and their characteristics. In this type of research, the researchers set up a database of variables and parameters [92]. The researcher then infers the behavior of the system under study based on different permutations and combinations of these parameters and variables. This technique can be applied to determine important parameters and variables.

Inferential research methodology in this thesis is applied in conjunction with simulation based research methodologies and experimental research methodology to derive conclusions based on simulation. For this, the authors reviewed several of key exchange protocols and identified different aspects that affect the execution of key exchange protocols. The authors identified variables such as: different vulnerabilities, usage of nonce, time stamps to name a few. The authors have carefully examined their values during their experiments to determine the correctness of their hypothesis.

3.2.3 Experimental Research Methodology
The experimental approach to research is used when it is required to control the environment of the research. In this approach some of the variables are manipulated and effect of manipulation is observed. This observation helps researchers in understanding the relationship between variables and helps in testing hypothesis [93].

We need to experiment as there is no algorithm or established relationship between the variables under consideration. The domain is rather too complex to have a mathematical formulae or relationship. The empirical study is the only alternative. The experimental methodology was used by the authors of this thesis to compare their protocol with industry standard protocols. There were two experiments carried out by authors for different purposes. The first experiment was to demonstrate the efficiency of modified Denning-Sacco protocol proposed by authors against other variations of Denning-Sacco protocol.

The authors employed a combination of quantitative and experiment based methods to devise a solution where the protocol designed by authors is compared with other variations of Denning-Sacco protocols. This comparison is done on the basis of parameters that authors decided after a careful and thorough review of existing literature.
In this experiment the authors prove that their protocol is not only executing faster than the other variations of Denning-Sacco protocol, but also uses less power. All this is achieved without compromising on security of the protocol that the authors are proposing.

The experimental methodology was used by researchers to compare their protocol with industry standard protocols. The experiment was monitored on several parameters that are based on analysis of literature using qualitative methods. The experiment was carried out keeping in mind minute details of the model under consideration. With the results of experiments, the authors were able to gain understanding of internal relationships between different parameters and their effects on performance of the protocol. It also helped the authors of this thesis in obtaining proof of their hypothesis.

### 3.2.4 Simulation Based Research Methodology

Simulation method of research involves the building of an artificial research environment by the researcher to experiment [90]. This environment can be constructed by the researcher based on relevant models. The authors selected simulation based methodology as the mathematical model is not adequate to prove the efficiency of the protocol proposed by the authors. The simulation model is preferred as it models real world application like scenario which will enable authors to highlight features of protocols modified by them.

The authors of this thesis use this methodology with parameters derived using the qualitative methods to compare protocols. The authors use an e-commerce system model to test a secure payment system. In this system the messages are encrypted with modified Denning-Sacco protocol proposed by the authors. The researcher can later analyze the information to prove or disprove the hypothesis. The results are obtained by using a simulation methodology based on parameters that are determined by qualitative methodology. This type of methodology is applied when hypothesis testing is not possible in a real world environment or setting up the environment could present significant financial challenges [90]. This helps in providing proof of hypothesis where the authors claim that their variant is faster than other variations.