# Chapter 3: Methodology

## 3.1 Introduction

This chapter focuses on employing the prototype research methodology to address the detection and prevention of DNS spoofing attacks by leveraging DNSSEC and DNSCrypt. It also shows steps taken to achieve the goal of solving the problem at hand. The system development tools and techniques used in the development of the system are highlighted.

## 3.2 System Development Methodology

The research methodology outlined in this chapter will help us achieve our goal of detecting and preventing DNS spoofing attacks using DNSSEC and DNSCrypt by developing a systematic and structured approach to address the problem of DNS spoofing. It guides us through the essential steps of understanding the requirements, designing a solution, developing a prototype, evaluating its effectiveness, and refining it based on feedback. This iterative process ensures that our solution evolves and becomes more robust, effectively achieving our goal of detecting and preventing DNS spoofing attacks using DNSSEC and DNSCrypt.

![A diagram of a process

Description automatically generated with low confidence]()

Figure 3.1 Prototype Methodology

### 3.2.1 Requirement Analysis

In this step, necessary information about the problem, its techniques, and potential risks are gathered to understand the specific requirements and objectives of the solution, their functionalities, and how they can mitigate the problem. It ensures that there is a clear understanding of the problem and the goals we aim to achieve which aids in developing a prototype. In this case, it seeks to understand the requirements and objectives of the DNS spoofing detection and prevention system. Specific threats such as DNS cache poisoning or man-in-the-middle attacks are addressed. It also gathers information about DNSSEC and DNSCrypt, their functionalities, and how they can mitigate these threats.

### 3.2.2 Design and Conceptualization

In this step, a simple conceptual design of the system from the data gathered will give a brief idea of the system to the user. It considers how DNSSEC and DNSCrypt can be implemented in the system to enhance security and visualizes the overall structure and interaction between different components in the system, such as DNS resolvers, authoritative servers, and clients.

### 3.2.3 Prototype Development

With the design in place, this step proceeds to develop a working prototype that incorporates the solutions. In this case, a prototype that incorporates DNSSEC and DNSCrypt is built which involves configuring DNS servers, implementing DNSSEC features, and integrating DNSCrypt protocols.

### 3.2.4 Evaluation and Testing

In this step, the proposed system undergoes rigorous evaluation and testing it at various stages. In this case, simulation of attack scenarios, such as DNS spoofing attempts, and assessing the effectiveness of DNSSEC and DNSCrypt in detecting and preventing them. Measuring the performance impact on DNS resolution times and evaluating the usability of the solution. This helps to assess its effectiveness, identify areas for improvement, and validate its ability to detect and prevent DNS spoofing attacks. Simulation of attack scenarios, performance measurements, and usability assessments.

### Iterative refinement

Based on the evaluation results, these steps in the methodology seek to refine and iterate the design addressing identified vulnerabilities, performance bottlenecks, or usability issues. This step ensures that the solution continually improves, becoming more effective and efficient in countering DNS spoofing attacks.

### Finalization and Production

After multiple iterations and refinements of the prototype, the design is finalized and prepared for production or further development. Document the implementation details, configuration instructions, and any necessary deployment considerations. The scalability, maintenance, and compatibility aspects of your solution are also taken to account to ensure the practicality and deployment readiness of our solution.

## 3.3 Justification of the Methodology

The research methodology gives a systematic approach to tackling the problem at hand. It provides a structured and systematic approach, guiding the entire research process, and ensuring that each step is followed in a logical sequence. By utilizing the prototype research methodology, we can effectively develop, evaluate, and refine a DNS spoofing detection and prevention system using DNSSEC and DNSCrypt. The methodology provides a solid foundation for conducting research, ensuring the developed solution's practicality, effectiveness, and usability.

## 3.4 Tools and Techniques

### 3.4.1 DNSSEC

DNSSEC will be used as an extension to the DNS protocol that adds security measures to DNS. Its primary goal is to provide data integrity and authenticity to DNS responses, mitigating DNS spoofing attacks.

### 3.4.2 DNSCrypt

DNSCrypt is a protocol that will be used to encrypt DNS traffic between clients and resolvers, preventing eavesdropping, tampering, and DNS hijacking attacks.

### 3.4.3 Ettercap

It is a powerful network and manipulation tool, that will be valuable to demonstrate the vulnerability of the DNS spoofing and security testing of DNSSEC and DNSCrypt to detect and prevent DNS spoofing.

### 3.4.4 Ubuntu Linux

The Ubuntu Linux system will be used to carry out the detection and prevention of DNS spoofing attacks using DNSSEC and DNSCrypt. It will also aid in facilitating a DNS spoofing attack alongside other tools and techniques in the operating system.