Secure DNS over TLS vs DNSSEC

A CAPSTONE PROJECT REPORT

Submitted in the partial fulfilment for the Course of

CSA0735 –COMPUTER NETWORKS FOR COMMUNICATION

to the award of the degree of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE AND ENGINEERING

Submitted by

M.Balaji(192525059)

B.Moksha Sree(192511160)

B.Furthosesamreen(192511164)

Under the Supervision of

Dr.P.Rajaram&Dr.N.Anand

SIMATS ENGINEERING

Saveetha Institute of Medical and Technical Sciences

Chennai-602105

July 2025

SIMATS ENGINEERING

Saveetha Institute of Medical and Technical Sciences

Chennai-602105

Engineer to Excel

DECLARATION

We, **[M.Balaji B.Moksha Sree B.Furthose Samreen]** of the **[COMPUTER SCIENCE AND ENGINEERING],** Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, hereby declare that the Capstone Project Work entitled **'[Secure DNS over TLS vs DNSSEC**]' is the result of our own bonafide efforts. To the best of our knowledge, the work presented herein is original, accurate, and has been carried out in accordance with principles of engineering ethics.

Place: Thandalam

Date:

Signature of the Students with Names

SIMATS ENGINEERING

Saveetha Institute of Medical and Technical Sciences

Chennai-602105

Engineer to Excel

BONAFIDE CERTIFICATE

This is to certify that the Capstone Project entitled **Secure DNS over TLS vs DNSSEC**'" has been carried out by **[M.Balaji B.Moksha Sree B.Furthose Samreen]** under the supervision of [**Dr.P.Rajaram&Dr.N.Anand]** and is submitted in partial fulfilment of the requirements for the current semester of the B.TECH [COMPUTER SCIENCE AND ENGINEERING] program at Saveetha Institute of Medical and Technical Sciences, Chennai.

SIGNATURE

Name of the Program Director

Program Director

Department of computer network
Saveetha School of Engineering
SIMATS

SIGNATURE

Dr. Rajaram

Dr Anand

Department of computer network

Saveetha School of Engineering SIMATS

Submitted for the Project work Viva-Voce held on _____
.

INTERNAL EXAMINER

EXTERNAL EXAMINER

ACKNOWLEDGEMENT

We would like to express our heartfelt gratitude to all those who supported and guided us throughout the successful completion of our Capstone Project. We are deeply thankful to our respected Founder and Chancellor, Dr. N.M. Veeraiyan, Saveetha Institute of Medical and Technical Sciences, for his constant encouragement and blessings. We also express our sincere thanks to our Pro-Chancellor, Dr. Deepak Nallaswamy Veeraiyan, and our Vice-Chancellor, Dr. S. Suresh Kumar, for their visionary leadership and moral support during the course of this project.

We are truly grateful to our Director, Dr. Ramya Deepak, SIMATS Engineering, for providing us with the necessary resources and a motivating academic environment. Our special thanks to our Principal, Dr. B. Ramesh for granting us access to the institute's facilities and encouraging us throughout the process. We sincerely thank our Head of the Department, **Program Director NAME** for his continuous support, valuable guidance, and constant motivation.

We are especially indebted to our guide, **Dr.P.Rajaram&Dr.N.Anand** for his creative suggestions, consistent feedback, and unwavering support during each stage of the project. We also express our gratitude to the Project Coordinators, Review Panel Members (Internal and External), and the entire faculty team for their constructive feedback and valuable inputs that helped improve the quality of our work. Finally, we thank all faculty members, lab technicians, our parents, and friends for their continuous encouragement and support.

M.Balaji(192525059)

B.MokshaSree(192511160)

B.Furthosesamreen(192511164)

S.NO	Content
1.	ABSTRACT
2.	CHAPTER 1 : Introduction
3.	CHAPTER 2 : Literature Review
4.	CHAPTER 3 : System Analysis and Methodology
5.	CHAPTER 4 : Results and Discussions
6.	CHAPTER 5 : Conclusion and Future work

List of Figures

Abstract

This capstone project provides a comparative analysis of two prominent DNS security enhancements: DNS over TLS (DoT) and DNSSEC (Domain Name System Security Extensions). The primary problem addressed is the inherent vulnerabilities within the traditional DNS protocol, which include eavesdropping, data manipulation, and spoofing, leading to significant security and privacy risks for internet users. The purpose of this project is to evaluate the mechanisms, benefits, limitations, and real-world applicability of both DoT and DNSSEC in mitigating these risks. Key outcomes will include a detailed technical comparison, an assessment of their respective strengths and weaknesses in different operational contexts, and recommendations for their strategic implementation to achieve enhanced DNS security and user privacy. This report will synthesize research, practical considerations, and potential deployment challenges to inform more secure DNS infrastructure development.

List of Figures and Tables

(To be populated with actual figures and tables from your report, if applicable)

Acknowledgments

(Acknowledge individuals, mentors, or organizations who contributed to your project)

Chapter 1: Introduction

1.1 Overview

The Domain Name System (DNS) serves as the phonebook of the internet, translating human-readable domain names into IP addresses. However, DNS was not originally designed with security in mind, making it vulnerable to several attacks, including spoofing and man-in-the-middle attacks.

1.2 Background

To address these vulnerabilities, two major security enhancements have been introduced:
•DNSSEC (Domain Name System Security Extensions): Adds authentication to DNS data using cryptographic signatures.
•DoT (DNS over TLS): Encrypts DNS queries and responses to prevent eavesdropping and tampering.

1.3 Problem Statement

Traditional DNS queries are sent in plaintext, making them susceptible to interception, manipulation, and surveillance. This raises significant privacy and security concerns for users.

1.4 Objectives of the Study

•To compare the mechanisms of DNSSEC and DNS over TLS.
•To identify the benefits and limitations of each approach.
•To evaluate their effectiveness in various real-world scenarios.
•To provide recommendations for DNS security improvement.

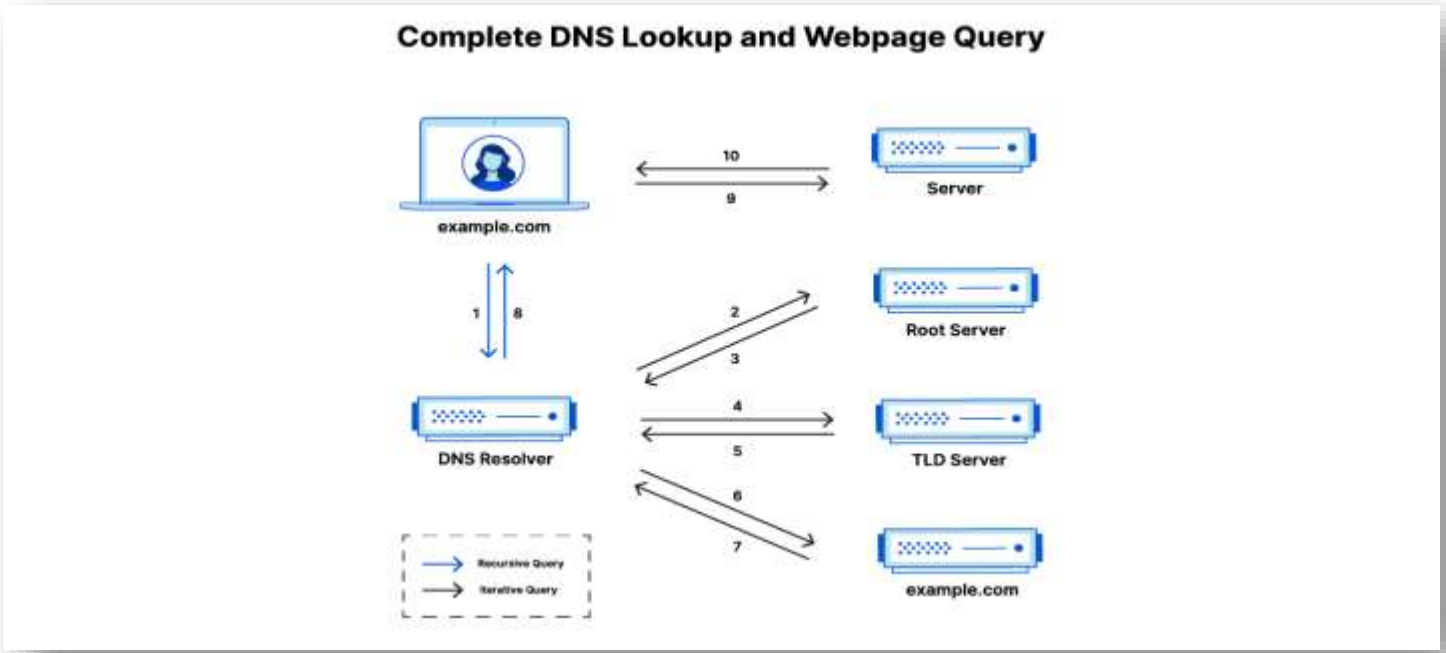
1.5 Scope of the Study

This project will focus on:
•The architecture and working principles of DNSSEC and DoT.
•Their comparative performance and implementation challenges.
•Their roles in improving user privacy and DNS infrastructure security.

1.6 Methodology
•Literature review on existing DNS protocols.
•Comparative technical analysis of DNSSEC and DoT.
•Case studies and evaluation of implementation in different systems.

1.7 Organization of the Report

The report is organized into the following chapters:
•Chapter 1: Introduction
•Chapter 2: Literature Review
•Chapter 3: System Analysis and Methodology
•Chapter 4: Results and Discussion
•Chapter 5: Conclusion and Future Work



Chapter 2: Literature Review

2.1 Introduction

The Domain Name System (DNS) is one of the oldest and most critical components of the internet. However, due to its lack of built-in security mechanisms, several enhancements have been proposed and implemented to improve its trustworthiness and privacy.

2.2 Traditional DNS Vulnerabilities

Traditional DNS suffers from several vulnerabilities:
•DNS Spoofing / Cache Poisoning
•Eavesdropping and Data Interception
•Man-in-the-Middle (MitM) Attacks
•Lack of Authentication and Data Integrity

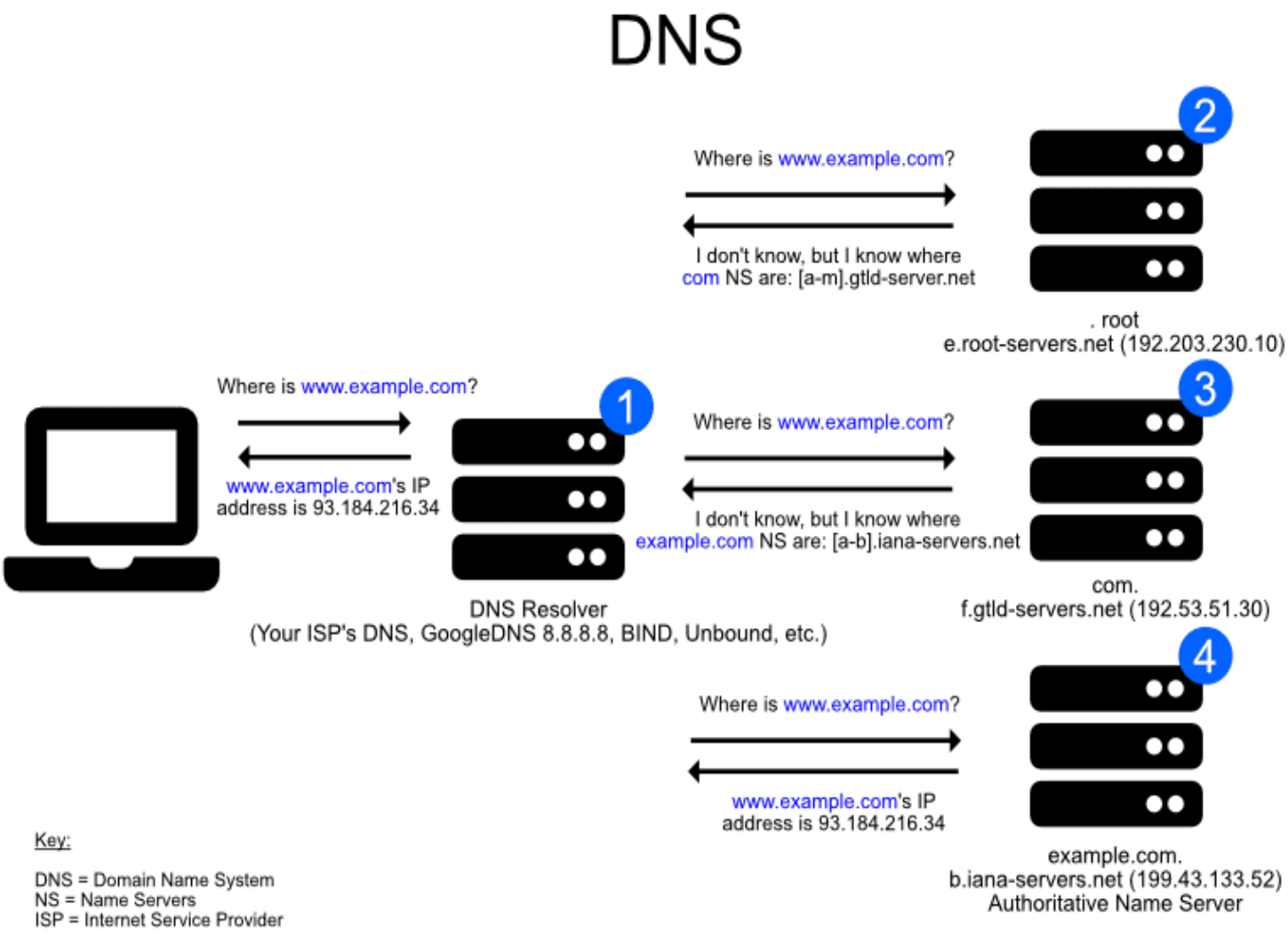
These weaknesses necessitated the development of more secure protocols.

2.3 DNSSEC (Domain Name System Security Extensions)

•Proposed by: IETF in the 1990s.
•Functionality: Provides origin authentication and data integrity using digital signatures and public key cryptography.
•Benefits:
•Protects against spoofing and cache poisoning.
•Validates authenticity of DNS responses.
•Challenges:
•Complex deployment and key management.
•Does not encrypt DNS data — privacy remains a concern.

2.4 DNS over TLS (DoT)

•Introduced by: RFC 7858 (2016).
•Functionality: Encrypts DNS queries and responses between the client and the DNS resolver using Transport Layer Security (TLS).
•Benefits:
•Prevents eavesdropping and tampering.
•Improves user privacy.
•Challenges:
•Does not verify data authenticity (unlike DNSSEC).
•Potential latency due to encryption overhead.



2.5 Comparative Studies

Several research efforts have compared the two protocols:
•Security Focus:
•DNSSEC focuses on data integrity and authenticity.
•DoT focuses on data confidentiality and privacy.
•Adoption:
•DNSSEC adoption is slower due to configuration complexity.
•DoT has seen quicker adoption, especially with browser and OS support (e.g., Android, Firefox).
•Performance:
•DoT may introduce latency due to TLS handshake.
•DNSSEC adds data overhead due to digital signatures.

2.6 Summary

While both protocols aim to enhance DNS security, they address different aspects. A layered or combined approach is often suggested in literature to balance security, privacy, and performance.

Chapter 3: System Analysis and Methodology

3.1 System Study

The study is centered on analyzing and evaluating the two DNS security mechanisms — DNS over TLS (DoT) and DNSSEC — by understanding their working principles, security benefits, implementation processes, and limitations.

3.2 DNSSEC – System Overview

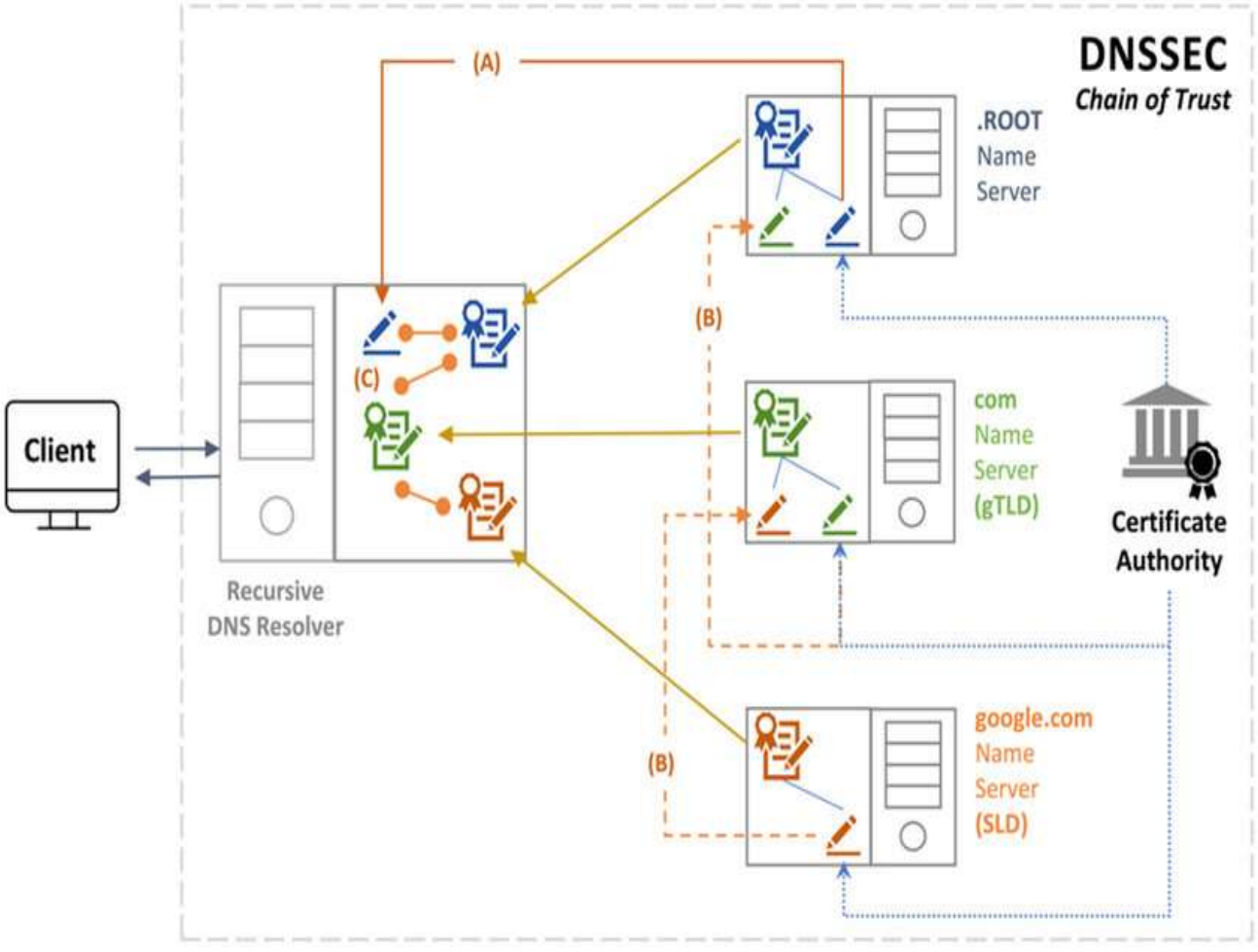
•Working: DNSSEC adds digital signatures to DNS records. When a resolver requests DNS data, it also receives a signature that can be validated against a public key.
•Components:
•Zone signing key (ZSK)
•Key signing key (KSK)
•DS records in parent zones
•Verification Process:
•Resolver checks the digital signature.
•Trust is established through a chain of trust up to the DNS root zone.

3.3 DNS over TLS (DoT) – System Overview

•Working: DNS queries are sent over a TLS-encrypted channel, typically via TCP port 853.
•Components:
•Client-side stub resolver supporting DoT
•Recursive resolver with DoT capability
•Encryption Process:
•TLS handshake establishes a secure channel.
•DNS packets are encrypted before transmission.

3.4 Methodology

The methodology adopted for the study includes:
1.Research and Literature Survey:
2.Collection of academic and industrial publications on DNSSEC and DoT.
3.Review of existing implementations and adoption statistics.
4.Comparative Evaluation:
5.Analysis of technical specifications and architectures.
6.Security comparison: authenticity, integrity, confidentiality.
7.Performance metrics: latency, resource usage.
8.Case Studies:
9.Real-world examples from organizations using DNSSEC and/or DoT.
10.Observation of challenges faced during deployment.
11.Simulation/Testing Setup (if applicable):
12.Simulated environment with DNS resolvers supporting DNSSEC and DoT.
13.Performance and behavior analysis under different network scenarios.



3.5 Tools and Technologies

Some of the tools and platforms considered for analysis and testing include:

- BIND / Unbound – for DNS server configuration
- Wireshark – to inspect DNS query packets and encryption
- Dig / Drill – for testing DNSSEC validation
- Stubby – for testing DoT queries

3.6 Summary

This chapter laid the foundation for the comparative analysis by explaining the technical workings of DNSSEC and DoT. The methodology combines theoretical study and potential simulations to draw meaningful conclusions in the next chapter.

Chapter 4: Results and Discussion

4.1 Introduction

This chapter presents a detailed comparison of DNSSEC and DNS over TLS (DoT) based on performance, security, ease of implementation, and adoption. The goal is to determine the practical strengths and weaknesses of each technology.

4.2 Comparative Analysis Table

Criteria	DNSSEC	DNS over TLS (DoT)
Security Focus	Data integrity and authenticity	Data privacy and encryption
Data Encryption	Not encrypted	Fully encrypted via TLS
Authentication	Authenticates DNS data using signatures	Does not authenticate DNS responses
Confidentiality	DNS data visible in transit	Queries hidden from intermediaries
Performance Impact	Slight overhead due to signature validation	Possible latency due to TLS handshake
Implementation Effort	High (key management, trust chain setup)	Moderate (TLS setup and configuration)
Client-side Support	Requires DNSSEC-aware resolver	Increasing support (e.g., Android, Firefox)
Deployment Complexity	Complex (requires DNS zone signing)	Simpler (only requires encrypted connection)
Resistance to MITM	Strong against tampering and spoofing	Prevents interception, not spoofing
Widely Adopted?	Moderate adoption, mostly by domain registries	Rapidly growing adoption

4.3 Findings

•DNSSEC excels at authenticating DNS records and preventing spoofing and cache poisoning but fails to ensure privacy since DNS traffic remains unencrypted.

•DoT ensures data privacy by encrypting DNS queries/responses but does not verify the authenticity of the DNS data.

•Combined use can offer comprehensive DNS security — privacy from DoT and integrity from DNSSEC.

4.4 Real-World Deployment Scenarios

•DNSSEC is widely implemented in top-level domains like .gov, .org, and many country-code TLDs.

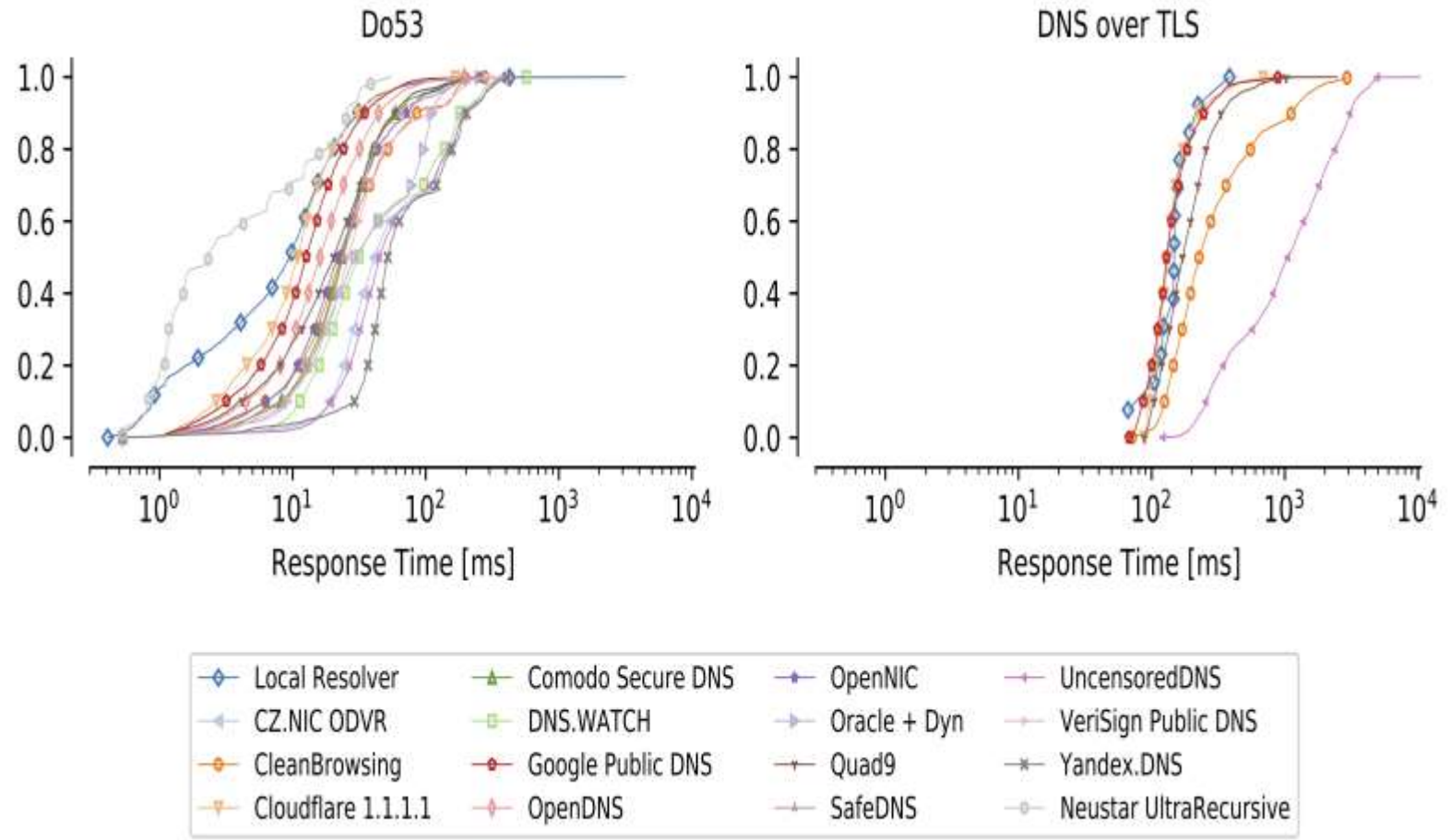
•DoT is used by:

•Google Public DNS

•Cloudflare DNS (1.1.1.1)

•Quad9 DNS (9.9.9.9)

•Operating Systems & Apps: Android (9+), Firefox, and iOS (14+) support DoT natively.



4.5 Limitations Identified

•DNSSEC:

•Complicated configuration, zone signing issues, trust anchor rollover.

•DoT:

•Centralization risk (trusting specific DoT providers).

•Performance drops over mobile or low-bandwidth networks.

4.6 Summary

The comparison reveals that neither DNSSEC nor DoT alone provides complete DNS security. Each addresses a specific aspect — integrity vs. privacy. For full protection, a hybrid approach combining both is recommended, though it requires more robust infrastructure and cooperation from both DNS providers and users.

Chapter 5: Conclusion and Future Work

5.1 Conclusion

This capstone project conducted a comprehensive comparative analysis of DNS over TLS (DoT) and DNSSEC, focusing on their ability to enhance DNS security. The study revealed the following:

- DNSSEC ensures data authenticity and integrity by using cryptographic signatures, thereby protecting users from spoofed or altered DNS responses.
- DoT encrypts DNS queries and responses to protect user privacy and prevent interception by third parties.
- Each technology addresses different security challenges: DNSSEC secures the data itself, while DoT secures the communication channel.
- Both solutions have limitations when implemented individually; however, a combined deployment can provide a holistic approach to DNS security.

In summary, the project emphasizes that a layered security strategy — combining DNSSEC with DoT — is ideal for robust DNS protection in modern internet environments.

5.2 Recommendations

- Adopt Both: Organizations should implement both DNSSEC and DoT to benefit from data authenticity and confidentiality.
- Awareness & Training: Encourage administrators and developers to become familiar with DNS security practices.
- Infrastructure Support: Governments and ISPs should support infrastructure upgrades to accommodate secure DNS protocols.
- Tooling and Automation: Use automated DNSSEC key rollover and DoT configuration tools to reduce operational complexity.

5.3 Future Work

•Performance Benchmarking: Conduct large-scale tests to assess the impact of DNSSEC and DoT on system performance.
•DNS over HTTPS (DoH): Explore and compare DoH with DoT and DNSSEC, particularly in mobile and browser environments.
•Security Analytics: Investigate how secure DNS protocols can be integrated with intrusion detection and prevention systems (IDS/IPS).
•IPv6 Integration: Study the compatibility and performance of DNSSEC and DoT in IPv6-dominant networks.