Quantum Threat Identification and Comparative Analysis Using STRIDE and PASTA Models: A Study of TLS, IPsec and DNSSEC Protocols

Saunak Saha[1], Ritoja Poddar[2], Swapnanil Bera[3], Kushal Bera[4], Subhadeep Mohanta[5], and Ayan Kumar Paul[6]

[1]Department of Computer Science and Engineering, Kalinga Institute of Industrial Technology(KIIT), Bhubaneswar, India

Abstract

The advent of quantum computing poses significant challenges to traditional cryptographic methods employed in securing network protocols. This study evaluates the vulnerabilities of Transport Layer Security (TLS), Internet Protocol Security (IPsec), and Domain Name System Security Extensions (DNSSEC) under quantum threat scenarios. Leveraging the STRIDE and PASTA threat modeling frameworks, the research categorizes threats and simulates attack scenarios to provide a comparative analysis of these protocols. The findings reveal critical vulnerabilities, particularly in public-key cryptography, and highlight the urgency of transitioning to quantum-resistant cryptographic solutions. The study proposes practical mitigation strategies to enhance the resilience of these protocols, contributing to the advancement of post-quantum cryptography and secure digital communications.

Keywords: Quantum Computing, Cryptographic Vulnerabilities, TLS, IPsec, DNSSEC, STRIDE Threat Model, PASTA Framework, Quantum-Resistant Cryptography, Network Security, Post-Quantum Security, Mitigation ways

I. Introduction

The advancement of quantum computing poses unprecedented challenges to traditional cryptographic techniques like RSA and Elliptic Curve Cryptography (ECC), which are integral to protocols such as TLS, IPsec, and DNSSEC. Quantum computers' ability to solve complex mathematical problems at exponential speeds threatens the foundations of these encryption methods, risking the confidentiality and integrity of sensitive data across global networks. The urgency for research in quantum-resilient cryptography arises from the potential collapse of current digital security frameworks due to quantum-based attacks. Addressing these vulnerabilities is crucial for safeguarding digital communication in an era where quantum technology could render existing encryption obsolete.[1][2]

Protocols such as TLS, IPsec, and DNSSEC are essential for ensuring secure communication in critical sectors such as e-commerce, healthcare, and government. Quantum vulnerabilities in these protocols could lead to the disruption of secure transactions and the compromise of sensitive information. Recognizing the pivotal role these protocols play in global security, this research seeks to evaluate and mitigate quantum-specific threats using comprehensive frameworks like STRIDE and PASTA. By facilitating the identification of these vulnerabilities, the study aims to develop robust countermeasures that can withstand the evolving quantum threat landscape. [3]

The STRIDE threat modeling framework categorizes threats into spoofing, tampering, repudiation, information disclosure, denial of service, and privilege elevation, providing a structured approach to identifying potential risks. Complementing this, the PASTA framework enables the simulation of real-world attack scenarios, offering a proactive strategy to anticipate and neutralize quantum-era threats. Together, these frameworks provide a dual approach to systematically address and enhance the resilience of critical network protocols. This combination ensures a methodical assessment and mitigation of vulnerabilities introduced by quantum computing. [4]

Developing quantum-resilient cryptographic solutions requires a thorough understanding of the weaknesses in existing encryption systems when faced with quantum threats. By leveraging the STRIDE and PASTA frameworks, this study identifies these shortcomings and proposes modifications to existing protocols or the creation of entirely new frameworks. Such

advancements are critical for ensuring the confidentiality and integrity of data in a quantum-dominated future, protecting global communications from emerging risks. [5]

Finally, this research contributes to the rapidly evolving field of post-quantum cryptography by addressing significant gaps in the literature on quantum-safe cryptographic methods. It seeks to inform the development of secure network protocols and encryption techniques capable of withstanding quantum attacks. By doing so, the study aims to foster a secure and reliable digital ecosystem, laying the groundwork for a future where quantum computing is an integral part of technological advancements. 6

A. *Objective*

The primary objectives of this research paper are outlined as follows:

- **To identify quantum threats to core security protocols such as TLS, IPsec, and DNSSEC.**
- **To perform a comparative analysis using the STRIDE and PASTA models to evaluate quantum vulnerabilities.**
- **To develop a threat matrix and conduct risk assessments for the analyzed protocols.**
- **To propose recommendations for quantum-resistant enhancements to these protocols.**
- **To contribute to the field of post-quantum cryptography through the application of advanced threat modeling methodologies.**

B. *Organization of the Paper*

This research paper is structured into eight comprehensive sections, each designed to systematically address the quantum threat analysis of TLS, IPsec, and DNSSEC protocols through the application of STRIDE and PASTA threat modeling frameworks. The organization is as follows:

- **Related Work and Background**
- **Methodology**
- **Threat Identification for TLS, IPsec, and DNSSEC**
- **Comparative Study of Threats and Risk Assessment**
- **Attack Simulation and Results**
- **Mitigation Strategies and Recommendations**
- **Conclusion and Future Work**

By following this structure, the paper aims to provide a thorough and systematic approach to addressing quantum threats to foundational internet security protocols.

II. Related Work

Challenges in Cryptographic Security Due to Quantum Computing

Several studies highlight the vulnerabilities posed by quantum computing to classical cryptographic protocols like TLS, IPsec, and DNSSEC. Research has shown that widely used encryption methods, such as RSA and ECC, are particularly susceptible to quantum attacks due to algorithms like Shor's, which can factorize large integers and solve discrete logarithms exponentially faster than classical methods [7][8][9]. These vulnerabilities necessitate a proactive approach to assess and mitigate risks in existing protocols.

Threat Modeling Techniques in Security Analysis

Threat modeling is a crucial step in identifying vulnerabilities and designing robust systems. The STRIDE model has been extensively used to classify threats into spoofing, tampering, repudiation, information disclosure, denial of service, and privilege escalation. It has been applied in scenarios such as secure software development and protocol design to systematize threat identification[8][7].

Similarly, the PASTA (Process for Attack Simulation and Threat Analysis) framework offers a dynamic approach by simulating potential attacks in real-world environments. Studies have combined these methodologies to provide a holistic view of potential threats and their mitigation strategies. [10] [9]

Post-Quantum Cryptography and Protocol Adaptation

Recent advancements in post-quantum cryptography (PQC) have focused on developing algorithms resilient to quantum attacks. Studies have proposed transitioning protocols like TLS and IPsec to use quantum-resistant primitives such as lattice-based and hash-based cryptography[7][10]. Research emphasizes the need for these adaptations to be implemented proactively to maintain confidentiality and data integrity in a quantum era.

Comparative Analyses in Protocol Security

Comparative studies on protocol vulnerabilities provide valuable insights into their quantum-era challenges. For instance, papers have explored TLS's handshake process, IPsec's key exchange mechanisms, and DNSSEC's chain of trust to evaluate their robustness under quantum threats. These works emphasize the importance of evaluating protocols under varied attack models and threat scenarios, leveraging tools like STRIDE and PASTA to guide this assessment[8][7][10][9]

The Role of Hybrid Solutions

Hybrid cryptographic approaches that combine classical and quantum-resistant methods are gaining importance as transitional solutions while cryptographic standards evolve in response to the quantum threat. These hybrid mechanisms, such as those proposed for TLS and IPsec, integrate traditional cryptographic algorithms like RSA and ECC with post-quantum algorithms, offering immediate security while preparing systems for future-proofing against quantum attacks. By employing this dual-pronged strategy, systems ensure backward compatibility with existing protocols, reducing the risk of disruptions during the transition. This approach not only mitigates potential vulnerabilities associated with quantum computing but also provides a bridge to fully quantum-resistant systems. It enables secure communication and key exchange without requiring an immediate overhaul of the infrastructure, making it crucial for industries such as finance, government, and military communications. In the long term, hybrid cryptography will play a pivotal role in safeguarding digital systems, ensuring they are resilient to quantum threats while maintaining compatibility with current standards. [8][9] [10].

*A. **Description of the Project***

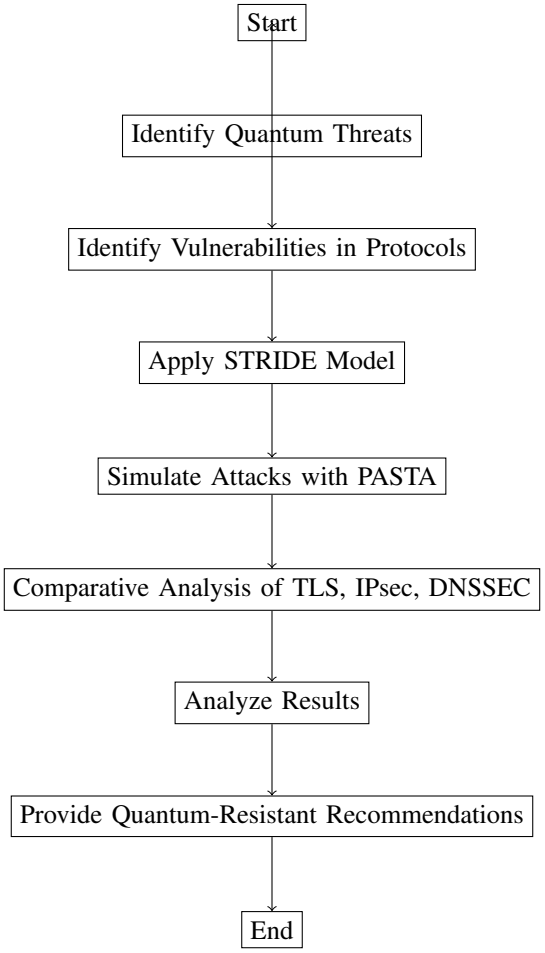

Fig. 1: Detailed Flowchart for Quantum Threat Modeling Process

Fig. 1 provides the flowchart of the structured process of quantum threat modeling applied to network security protocols like TLS, IPsec, and DNSSEC.

It begins with identifying potential quantum threats, which is the first step in understanding how quantum computing could impact cryptographic systems. Once these threats are identified, the next step involves recognizing specific vulnerabilities within the protocols under scrutiny. After identifying these weaknesses, the STRIDE model is applied to categorize the threats

according to the six categories: spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege. Following this, the PASTA (Process for Attack Simulation and Threat Analysis) model is employed to simulate realistic attack scenarios and evaluate the impact of these threats on the protocols. A comparative analysis is then conducted between TLS, IPsec, and DNSSEC to identify how they each respond to quantum threats. The results of the analysis are carefully examined, leading to the final step where quantum-resistant recommendations are provided to enhance the security and resilience of these protocols in the quantum era. The flowchart visually encapsulates these critical stages, illustrating the systematic approach used in assessing and addressing quantum threats to modern cryptographic systems.

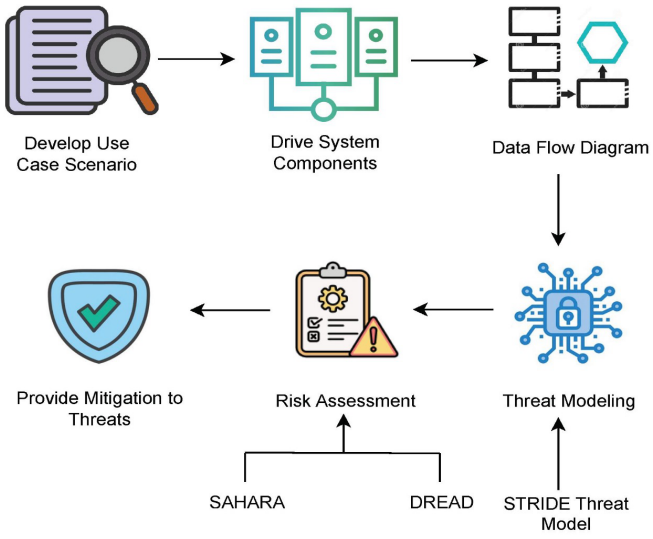

Fig. 2: Threat Modelling and Mitigation Workflow

Fig. 2 Shows us the overall mitigation workflow for a generalised threat model.

B. Background

Threat modeling is an essential process in cybersecurity, designed to identify, assess, and mitigate potential threats and vulnerabilities in systems, especially those critical to secure communication protocols like **Transport Layer Security (TLS)**, **Internet Protocol Security (IPsec)**, and **Domain Name System Security Extensions (DNSSEC)**. These protocols, while foundational to current internet security, are vulnerable to emerging threats, particularly those posed by quantum computing. Traditional cryptographic defenses are increasingly challenged by the capabilities of quantum technologies, potentially rendering current encryption methods ineffective. Therefore, threat modeling helps predict attack vectors and assess risks, offering proactive measures to address these vulnerabilities and ensure continued security, even in the quantum era. [12] [13] [14] [15]

Two primary threat modeling frameworks, STRIDE and PASTA, are utilized to analyze potential vulnerabilities in TLS, IPsec, and DNSSEC. The STRIDE model, developed by Microsoft, categorizes threats into six types: **Spoofing**, **Tampering**, **Repudiation**, **Information Disclosure**, **Denial of Service (DoS)**, and **Elevation of Privilege**. Each of these categories represents a distinct type of risk that could compromise the security of systems, making STRIDE a useful tool for identifying and evaluating the impact of quantum threats on protocols. For example, quantum computing could expose vulnerabilities in the encryption mechanisms of TLS and IPsec, making it easier for attackers to intercept and manipulate sensitive data during transmission. In DNSSEC, quantum attacks could lead to the manipulation of DNS data, undermining its authenticity. [16] [17]

The PASTA (*Process for Attack Simulation and Threat Analysis*) model [18], on the other hand, focuses on a risk-driven, attacker-centric approach to threat analysis. It operates through seven stages, starting with defining the objectives of potential attackers, followed by a detailed breakdown of the system's technical scope, and then a deeper analysis of how attackers might exploit weaknesses in system components. PASTA emphasizes simulating real-world attack scenarios, offering a practical perspective on how quantum-based threats could exploit vulnerabilities in protocols. For instance, quantum algorithms like Shor's algorithm, which can factor large numbers efficiently, could potentially break the RSA and ECDSA encryption used in TLS and IPsec, while Grover's algorithm might make symmetric encryption methods susceptible to faster brute-force attacks.[19]

When combined, the STRIDE and PASTA models provide a robust framework for threat modeling, offering both a structured categorization of potential threats and a simulated attack process that helps visualize and assess their real-world implications.

This dual-model approach ensures a comprehensive understanding of the vulnerabilities in TLS, IPsec, and DNSSEC, particularly in the context of quantum computing. By combining insights from both models, this analysis offers valuable information for mitigating quantum threats and adapting these protocols to the post-quantum world. [20] [21] [22]

TLS, IPsec, and DNSSEC each play crucial roles in securing internet communications. TLS ensures the confidentiality and integrity of data transmitted over networks, particularly in web traffic. However, TLS's reliance on public-key encryption algorithms such as RSA and ECDSA poses a significant vulnerability to quantum computing, as these algorithms are susceptible to attacks from quantum algorithms. IPsec, which secures IP communications through encryption and authentication at the network layer, also relies on similar cryptographic methods, including Diffie-Hellman key exchange, making it vulnerable to quantum attacks. DNSSEC enhances the security of the Domain Name System (DNS) by signing DNS data with digital signatures, but its reliance on public-key cryptography also makes it susceptible to quantum decryption techniques, potentially allowing attackers to manipulate DNS records and redirect users to malicious sites. [23] [24]

The threat modeling analysis, particularly using STRIDE and PASTA, reveals the critical need to transition these protocols to quantum-resistant cryptographic methods. Current methods, such as lattice-based cryptography, offer promising alternatives to existing public-key schemes and are more resilient to quantum decryption attacks. These findings are echoed in comparative studies on the vulnerabilities of TLS, IPsec, and DNSSEC to both classical and quantum threats, emphasizing the urgency of adopting post-quantum cryptographic solutions. [25] [26]

III. Methodology

A. *Threat Modelling Approach Using STRIDE*

The STRIDE model, developed by Microsoft, offers a structured approach to identifying and categorizing threats, making it an effective framework for assessing security vulnerabilities in protocols such as TLS, IPsec, and DNSSEC. By categorizing threats into six distinct types— Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service (DoS), and Elevation of Privilege—STRIDE enables a comprehensive assessment of each protocol's security posture against potential attacks. This section outlines how the STRIDE model is applied to TLS, IPsec, and DNSSEC within this study to evaluate their resilience to conventional and emerging quantum-based threats.

Application of STRIDE to TLS, IPsec, and DNSSEC: In the context of TLS, IPsec, and DNSSEC, each STRIDE category targets specific threat areas within these protocols. These categories are defined as follows:

Spoofing: It involves impersonating users or systems to gain unauthorized access to secure communications. For TLS, IPsec, and DNSSEC, spoofing threats may arise if attackers bypass authentication mechanisms, potentially exploiting vulnerabilities in public-key cryptography that quantum computing could accelerate. STRIDE's Spoofing analysis in this study focuses on the potential risks associated with identity impersonation, especially within the handshake or authentication stages of each protocol. The rise of quantum computing could undermine the security of public key algorithms like RSA, making identity verification more susceptible to quantum-powered spoofing attacks.

Tampering: Tampering refers to unauthorized modifications of data during transmission. In TLS, this could mean altering encrypted messages between client and server; for IPsec, it could involve modifying packet data within VPNs or secured networks; and in DNSSEC, tampering might entail manipulating DNS records. STRIDE's Tampering analysis examines the integrity mechanisms within these protocols, assessing how quantum-based attacks might compromise these safeguards. Quantum algorithms, such as Shor's and Grover's, could potentially break the encryption mechanisms that protect data integrity in these protocols, making them vulnerable to tampering.

Repudiation: Repudiation threats occur when an entity denies having performed an action, such as a transaction or message transmission, creating accountability issues. TLS, IPsec, and DNSSEC all rely on authentication logs and audit trails to prevent repudiation. However, if quantum computing disrupts the integrity of digital signatures used in these protocols, attackers may exploit this to bypass accountability measures. The STRIDE analysis in this study evaluates the effectiveness of each protocol's non-repudiation mechanisms and their susceptibility to quantum interference. A quantum attacker could potentially forge or alter signatures, undermining trust in transaction histories and audit trails.

Information Disclosure: Information disclosure involves unauthorized access to confidential information. This threat is particularly relevant in TLS, where encryption ensures confidentiality in web transactions, and in IPsec, where data within a VPN must remain protected. For DNSSEC, ensuring the integrity of DNS responses is critical. STRIDE's Information Disclosure category assesses the encryption methods employed by each protocol, particularly focusing on the vulnerability of public-key algorithms to quantum decryption. Quantum computing could potentially expose sensitive data by breaking the encryption keys that protect communications, leading to unauthorized disclosure of information.

Denial of Service (DoS): Denial of Service (DoS) attacks aim to disrupt access to services, thereby affecting system availability. In TLS, DoS attacks can overwhelm web servers by flooding them with requests, leading to service unavailability. In IPsec, DoS attacks can compromise the availability of secure network communications by targeting VPNs or disrupting data transmission. In DNSSEC, DoS attacks can overload DNS servers, preventing the resolution of domain names, and potentially

compromising the availability of services that rely on DNS. The STRIDE DoS analysis investigates potential quantum-based DoS attacks, assessing each protocol's defense mechanisms against high computation demands that quantum attacks might exploit.

Elevation of Privilege: Elevation of Privilege occurs when unauthorized users gain elevated access levels within a system. If quantum-based attacks break cryptographic barriers, attackers may exploit this to escalate privileges within TLS sessions, IPsec connections, or DNSSEC's zone management. STRIDE's Elevation of Privilege analysis in this study examines whether quantum vulnerabilities could allow attackers to bypass authentication controls and gain unauthorized access to system resources or privileged operations.

STRIDE Model Adaptation for Quantum Threats

Traditional threat modeling within STRIDE has proven effective for identifying vulnerabilities, but the unique capabilities of quantum computing introduce new dimensions to each threat category. In this study, the STRIDE model is adapted to consider quantum-specific attack scenarios, particularly focusing on how quantum algorithms like Shor's and Grover's could disrupt the cryptographic foundations of TLS, IPsec, and DNSSEC. Each STRIDE category is thus analyzed with quantum threats in mind, providing insights into areas where these protocols may require quantum-resistant measures.

Limitations of STRIDE for Quantum Threat Analysis

While STRIDE provides a clear structure for categorizing threats, it does not offer a complete approach to assessing sophisticated, evolving quantum threats. STRIDE's static nature, focused on threat categorization, lacks the dynamic, attacker-centric approach required to fully address the capabilities of quantum-enabled adversaries. To complement STRIDE's capabilities, the PASTA model is employed in this study, offering a staged, simulation-driven analysis to address quantum threats more dynamically. By combining both STRIDE and PASTA, a more comprehensive and adaptive threat model can be established to tackle both traditional and emerging quantum vulnerabilities.

B. Threat Modelling Approach Using PASTA

The Process for Attack Simulation and Threat Analysis (PASTA) model is a risk-based, attackercentric threat modeling approach designed to simulate real-world attacks. Unlike STRIDE, which focuses on categorizing threats, PASTA offers a detailed, multi-stage process for analyzing how attackers might exploit system vulnerabilities. Given the dynamic nature of quantum threats, PASTA's comprehensive, simulation-based approach is well-suited to examining how TLS, IPsec, and DNSSEC might respond to attacks enabled by quantum computing. This section outlines the seven stages of the PASTA model as they apply to the threat landscape of each protocol and discusses the adaptations made to account for quantum-based threats.

Applying PASTA to TLS, IPsec, and DNSSEC In this research, each stage of the PASTA model is used to methodically examine TLS, IPsec, and DNSSEC, identifying vulnerabilities and assessing potential risks posed by quantum computing capabilities. Fig. 3 Shows us the overall stages of Threat Modeling in PASTA. The stages are detailed as follows:

Stage 1: Definition of Objectives (DO) for the Analysis stage involves defining the objectives of the threat analysis, focusing on protecting the confidentiality, integrity, and availability of data transmitted over TLS, IPsec, and DNSSEC. Given the emergence of quantum computing, the objective includes identifying quantum-specific vulnerabilities that could compromise these protocols. The goal is to evaluate each protocol's security measures and assess their preparedness for post-quantum threats.

Stage 2: Definition of the Technical Scope (DTS) stage identifies the technical scope by examining the protocol architecture, cryptographic mechanisms, and configurations. For TLS, this includes the handshake process and encryption algorithms like RSA and ECDSA. For IPsec, the scope includes key exchange methods like Diffie- Hellman, and for DNSSEC, it involves digital signatures used to authenticate DNS records. The aim is to understand where quantum attacks might exploit weaknesses in each protocol's cryptographic structure.

Stage 3: Application Decomposition and Analysis (ADA) stage breaks down each protocol into its functional components to understand its security boundaries and potential attack surfaces. For TLS, components include the session establishment and encryption layers. IPsec, includes encapsulation and authentication protocols, and for DNSSEC, it involves DNS record signing and verification processes. Decomposition helps pinpoint specific functions vulnerable to quantum decryption or spoofing attacks.

Stage 4: In Threat Analysis (TA) the PASTA model conducts a detailed threat analysis, focusing on identifying and cataloging potential threats that could be exploited by quantum computing. Using attacker personas, this analysis evaluates how an attacker with quantum capabilities could bypass encryption, impersonate entities, or intercept data. For instance, Shor's algorithm poses a direct threat to TLS's public-key algorithms, while Grover's algorithm could speed up brute-force attacks, affecting all three protocols.

Stage 5: The Vulnerability and Weakness Analysis(VWA) stage assesses the protocols' vulnerabilities, specifically their reliance on public-key cryptography, which is susceptible to quantum decryption. For TLS, IPsec, and DNSSEC, this includes weaknesses in RSA, ECDSA, and other asymmetric cryptographic mechanisms that could be compromised. Vulnerability

analysis in this stage focuses on how these weaknesses could be targeted by quantum-enabled attacks, identifying potential areas where quantum-resistant algorithms should be implemented.

Stage 6: Attack Simulation and Modeling (ASM) (PASTA's simulation stage) is critical for visualizing and understanding how real-world quantum attacks might unfold. By simulating scenarios like a quantum-enabled man-in-themiddle attack in TLS or an impersonation attack in DNSSEC, this stage demonstrates the protocols' responses to quantum-based threats. Attack simulations provide insights into potential security gaps and highlight the effectiveness (or lack thereof) of each protocol's existing defense mechanisms in the face of quantum-based threats.

Stage 7: Risk and Impact Analysis (RIA) is the final stage of PASTA which involves assessing the potential impact and risk of quantum threats on each protocol. This analysis considers the consequences of a successful quantum attack, such as data exposure or compromised network integrity. For TLS, IPsec, and DNSSEC, this includes evaluating the implications for user trust, data confidentiality, and network availability. Risk assessment further prioritizes the need for quantum-resistant adaptations to minimize potential impacts.

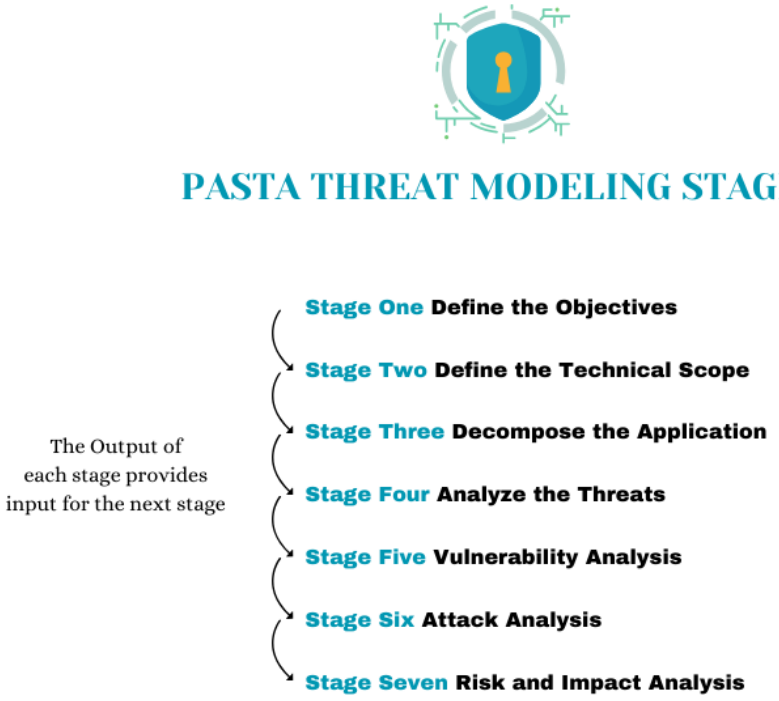

Fig. 3: PASTA Threat Modeling Stages

Adaptation of PASTA for Quantum Threat Modeling

While traditionally used for conventional security threats, the PASTA model in this study has been adapted to address the unique challenges posed by quantum computing. Each stage includes considerations for quantum-specific threats, especially those arising from quantum algorithms like Shor's and Grover's. The attacker-centric nature of PASTA allows for a dynamic exploration of how these advanced threats could exploit vulnerabilities in TLS, IPsec, and DNSSEC, providing a more comprehensive threat analysis than traditional models.

Limitations of the PASTA Model for Quantum Threats

While PASTA's seven-stage approach offers depth, its reliance on attacker simulation may be limited by the unpredictable nature of quantum advancements. Future improvements to the model may involve integrating quantum-specific simulations, which are currently theoretical but could eventually provide more realistic simulations as quantum technologies develop.

C. Protocol Selection Criteria (TLS, IPsec, DNSSEC)

The selection of TLS, IPsec, and DNSSEC protocols for this study is based on their critical roles in securing internet communications and their susceptibility to quantum computing threats. Each protocol was chosen to represent different layers and functions within network security, providing a comprehensive assessment of quantum threat impact across diverse security contexts. Fig. 4 Shows us the overall threat modeling procedure. The following criteria were used to select these protocols:

Prevalence in Network Security TLS, IPsec, and DNSSEC are widely used in securing communications across the internet, making them high-priority targets for security assessments. TLS (Transport Layer Security) is essential for protecting web

communications, securing data exchanged between clients and servers. IPsec (Internet Protocol Security) provides network-level security, protecting data at the IP layer and enabling secure VPN connections.DNSSEC (Domain Name System Security Extensions) secures DNS data, ensuring the integrity of DNS queries. Given their widespread use and integral roles, analyzing the security of these protocols is essential for understanding the impact of potential quantum threats on the broader internet infrastructure.

Dependence on Public-Key Cryptography All three protocols rely heavily on public-key cryptography for encryption, authentication, and data integrity. This reliance on asymmetric algorithms—such as RSA and Elliptic Curve Cryptography (ECC)—makes these protocols especially vulnerable to quantum computing, as quantum algorithms (e.g., Shor's algorithm) could potentially break these encryption methods. Studying these protocols provides insight into which aspects of their cryptographic foundations are most susceptible to quantum attacks, allowing for an analysis of how quantum-resistant methods could be incorporated.

Diverse Security Objectives and Layers TLS, IPsec, and DNSSEC each address different security objectives and operate at various layers of the network stack. TLS ensures secure communication at the application layer, IPsec operates at the network layer to protect IP communications, and DNSSEC provides data integrity for the DNS system. By selecting protocols from distinct layers, this study achieves a broader evaluation of quantum vulnerabilities, enabling a cross-layer assessment that highlights both common and unique threats across the stack.

Impact of Potential Quantum Attacks A successful quantum attack on TLS, IPsec, or DNSSEC would have severe consequences for internet security and user trust. Compromised TLS could lead to widespread data exposure, IPsec vulnerabilities could allow attackers to intercept or tamper with network traffic, and weaknesses in DNSSEC could lead to DNS spoofing, redirecting users to malicious sites. Given the significant risk each protocol faces, evaluating them provides a meaningful basis for developing quantum-resilient strategies with a high-security impact.

Existing Studies and Comparative Relevance These protocols have been the focus of numerous security studies, making them well-documented and suitable for comparative analysis. Leveraging prior research, this study can effectively use the STRIDE and PASTA models to examine known and emerging threats. Comparing these well-established protocols allows for a clearer evaluation of the potential effectiveness of quantum-resistant algorithms and highlights where traditional threat models may need adjustments for quantum-era security.

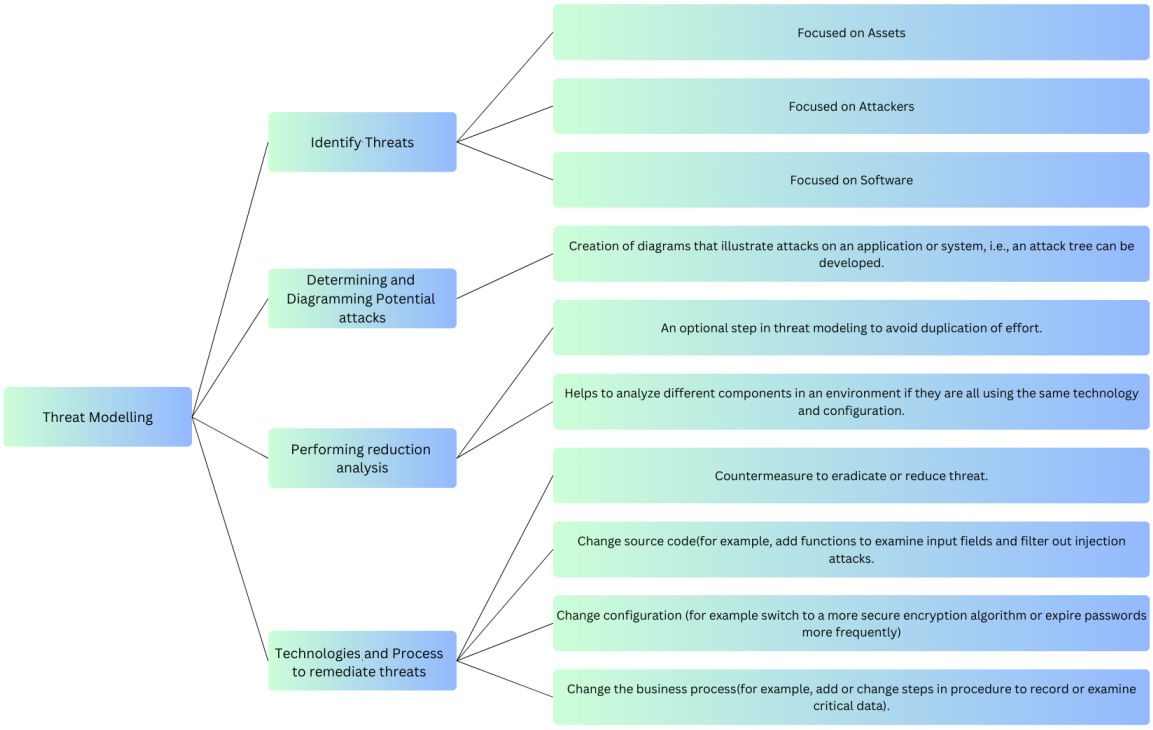

Fig. 4: Threat Modelling process

D. Attack Simulation Environment and Setup

To analyze and validate the effectiveness of the STRIDE and PASTA threat models in assessing the quantum vulnerability of TLS, IPsec, and DNSSEC protocols, an attack simulation environment is established. [Fig. 5 Shows us the overall threat

identification model of Stride and Pasta]. This environment is designed to simulate quantum-capable adversary scenarios, allowing for practical testing of the protocols under realistic attack conditions. This section outlines the simulation setup, software tools, and configurations used to evaluate protocol resilience.

Simulation Goals and Parameters

The primary goal of the simulation environment is to assess how TLS, IPsec, and DNSSEC might respond under potential quantum computing threats, particularly those targeting cryptographic mechanisms. The simulations aim to evaluate:

Cryptographic Vulnerabilities

Testing the resistance of current cryptographic algorithms (RSA, ECC) in TLS, IPsec, and DNSSEC against hypothetical quantum attacks.

Attack Vectors and Exploitation

Simulating quantum-based attacks, such as man-in-the-middle, data tampering, and impersonation attacks, to assess protocol weaknesses.

Effectiveness of Threat Models

Verifying how well the STRIDE and PASTA models capture and categorize threats in simulated quantum attack scenarios.

Environment and Tools

***Virtualized Network Simulation*:** The simulation environment uses a virtualized network setup to emulate client-server interactions under TLS, IPsec, and DNSSEC. Virtual machines or Docker containers are configured to represent distinct network roles (e.g., client, server, and adversary), allowing for isolated and controlled attack simulations.

***Quantum-Safe Cryptography Libraries*:** While quantum computers are capable of breaking RSA and ECC do not yet exist, libraries implementing post-quantum cryptography (e.g., NIST's post-quantum algorithms) are used to simulate quantum-resistant alternatives. These libraries provide a basis for comparing current cryptographic methods against future, quantum-resistant protocols.

***Penetration Testing and Threat Modeling Tools*:** Tools like Metasploit, Wireshark, and Scapy are used for packet inspection, attack simulation, and protocol analysis. These tools facilitate controlled attacks on TLS, IPsec, and DNSSEC to understand the extent of vulnerabilities. Additionally, custom scripts are employed to simulate quantum-specific attacks, such as breaking RSA encryption, in hypothetical scenarios.

Simulation Scenarios

***TLS Quantum Attack Simulation*:** Scenarios include a quantum-based man-in-the-middle attack on TLS, where an adversary with quantum decryption capabilities attempt to intercept and decrypt encrypted TLS traffic. This simulation evaluates how TLS's reliance on RSA and ECC for key exchange and encryption withstands quantum-enabled decryption.

***IPsec Vulnerability Testing*:** Simulations for IPsec involve testing the Diffie- Hellman key exchange under quantum attack scenarios. A quantum attacker could theoretically compute private keys by intercepting IPsec encrypted communications, simulating a scenario in which IPsec's confidentiality is compromised.

***DNSSEC Integrity and Authentication Simulation*:** For DNSSEC, scenarios focus on quantum-enabled signature spoofing attacks. The simulation assesses the vulnerability of DNSSEC's RSAbased digital signatures to quantum decryption, exploring how attackers might impersonate DNS responses.

Limitations and Considerations: While this environment approximates quantum threats, certain assumptions are made due to the limitations of current quantum computing capabilities. For instance, the simulations cannot fully represent the computational power of advanced quantum computers but use theoretical attack algorithms as proxies. Future testing environments should incorporate real quantum hardware once available for a more accurate evaluation of post-quantum protocols.

IV. Threat Identification for TLS, IPsec, and DNSSEC

A. Threat Analysis for TLS

Transport Layer Security (TLS) is a widely used protocol that ensures privacy and data integrity in internet communications by encrypting the data transmitted between clients and servers. However, the TLS protocol faces significant challenges in the face of advancing quantum computing, which threatens to compromise its cryptographic underpinnings. This threat analysis uses both the STRIDE and PASTA models to assess and categorize potential vulnerabilities in TLS, especially focusing on the risks associated with quantum computing advancements. Fig. 5 Shows us the overall threat identification workflow of Stride and Pasta.

1. STRIDE Analysis Using the STRIDE threat model, the potential threats to TLS are analyzed by categorizing them into the following dimensions:

Spoofing (S): Spoofing threats arise when an attacker impersonates a legitimate server or client in the TLS handshake process. In a quantum-enabled environment, an attacker could theoretically break public-key encryption (such as RSA or ECDSA) used in the initial handshake, allowing them to impersonate either party and establish unauthorized connections.

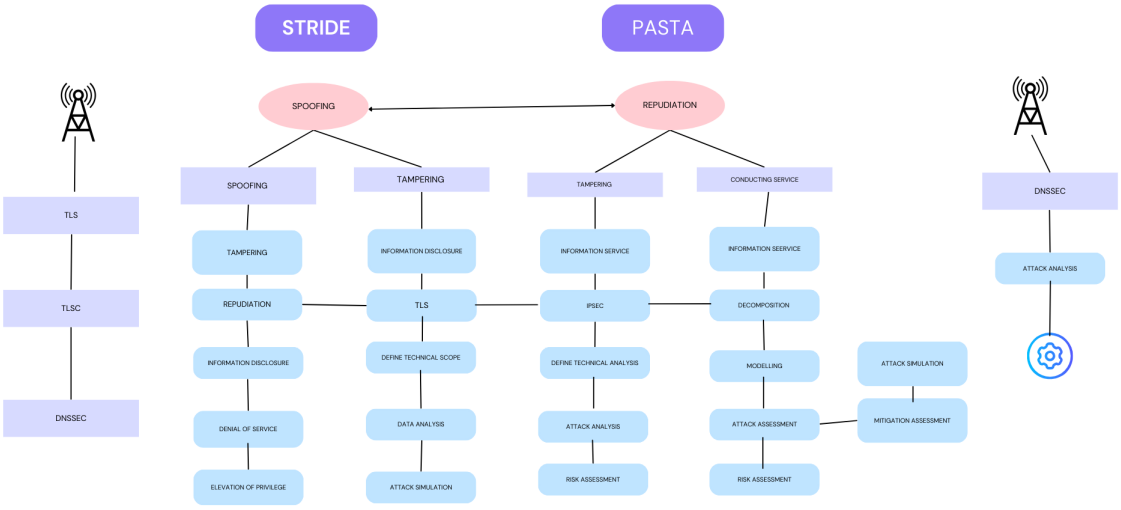

Fig. 5: Threat identification of STRIDE and PASTA

Tampering (T): TLS is designed to prevent tampering by using Message Authentication Codes (MACs). However, if an attacker breaks the encryption using quantum computing, they could potentially decrypt the messages and modify data during transit, bypassing the MAC verification process. This poses a serious risk to the integrity of sensitive data transmitted over TLS.

Repudiation (R): While TLS includes authentication mechanisms to reduce repudiation risks, quantum computing may allow attackers to forge digital signatures, enabling them to deny involvement in malicious activities. For instance, breaking ECDSA signatures through quantum attacks would weaken the nonrepudiation assurances provided by TLS.

Information Disclosure (I): Information disclosure is one of the most concerning threats for TLS, as the primary function of TLS is to secure data confidentiality. Quantum computing could break TLS's public-key cryptographic schemes, such as RSA, allowing attackers to decrypt and access encrypted data, leading to severe breaches of confidentiality.

Denial of Service (DoS) (D): While quantum computing does not directly facilitate DoS attacks, it may lead to indirect DoS threats by overwhelming the server's resources with an increased need for more complex, quantum-resistant encryption algorithms. Additionally, if TLS key exchange mechanisms become vulnerable, attackers might manipulate the handshake process to increase server load or disrupt services.

Elevation of Privilege (E): In the context of TLS, the quantum-based elevation of privilege attacks may involve breaking the cryptographic keys that safeguard privileged sessions. An attacker with quantum decryption capabilities could potentially elevate their privileges by hijacking an authenticated session and gaining access to restricted information or services.

2. PASTA Analysis The Process for Attack Simulation and Threat Analysis (PASTA) model provides a structured, attacker-centric approach to analyzing TLS threats in a quantum context. The following stages of PASTA are used to simulate potential attack scenarios and assess the resilience of TLS under quantum threat conditions:

Definition of Objectives (DO): The primary objective of this analysis is to evaluate the potential risks posed to the confidentiality, integrity, and availability of data protected by TLS in the face of quantum computing. The analysis aims to identify vulnerabilities in the key exchange, encryption, and authentication mechanisms of TLS that may be susceptible to quantum attacks.

Definition of the Technical Scope (DTS): The technical scope focuses on TLS's cryptographic mechanisms, including RSA and ECC key exchange methods, MACs, and digital signatures. Each of these mechanisms is analyzed for potential weaknesses when confronted with quantum decryption algorithms, such as Shor's algorithm.

Application Decomposition and Analysis (ADA): This stage decomposes TLS into its core components, such as the handshake protocol, cipher suite negotiation, key exchange, and encrypted data transmission. Each component's vulnerabilities are analyzed in isolation to understand how quantum attacks could compromise the TLS handshake and encryption processes.

Threat Analysis (TA): Threat analysis examines various attack vectors a quantum-enabled adversary might exploit. For example, an attacker could perform a man-in-the middle (MitM) attack by breaking the RSA or ECC-based public key exchange

used in the TLS handshake, enabling them to intercept and decrypt messages between the client and server.

Vulnerability and Weakness Analysis (VWA): The vulnerability analysis stage focuses on TLS's reliance on RSA and ECC for secure key exchange. With quantum computing, both RSA and ECC are vulnerable, as Shor's algorithm can theoretically decrypt them efficiently, leaving TLS's key exchange process highly exposed to quantum threats.

Attack Simulation and Modeling (ASM): In a simulated environment, potential quantum-enabled attacks on TLS are modeled to understand the real-world implications of these vulnerabilities. For instance, a simulated MitM attack shows how an attacker could intercept and decrypt TLS traffic if quantum decryption capabilities were available, thus compromising the confidentiality and integrity of the data in transit.

Risk and Impact Analysis (RIA): The risk analysis evaluates the potential impact of successful quantum-based attacks on TLS. The assessment highlights that compromised confidentiality would have a significant impact on data privacy, while compromised integrity and non-repudiation could undermine the trust in TLS-based communications, necessitating a shift toward quantum-resistant encryption solutions.

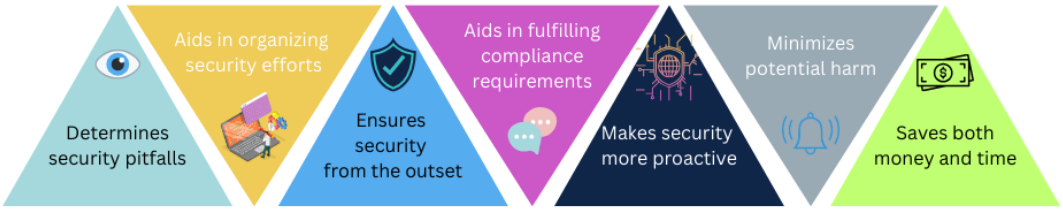

Fig. 6: Threat Analysis Framework with STRIDE, PASTA, and Security Protocols

B. Threat Analysis for IPsec

Internet Protocol Security (IPsec) is a suite of protocols widely used for securing communications at the network layer, primarily in VPNs and other secure IP-based connections. [Fig. 6 Shows us the overall threat analysis framework with Stride, Pasta, and the security protocols]. IPsec provides confidentiality, integrity, and authentication, enabling secure transmission of sensitive information across IP networks. However, advancements in quantum computing present substantial risks to IPsec's cryptographic algorithms, particularly those used in key exchange and data encryption. This section applies the STRIDE and PASTA threat models to analyze and categorize quantum-based threats to IPsec.

1. STRIDE Analysis Using the STRIDE threat model, potential quantum-based threats to IPsec are identified and categorized as follows:

Spoofing (S): Spoofing threats in IPsec could arise if an attacker impersonates a legitimate VPN endpoint. IPsec often relies on the Internet Key Exchange (IKE) protocol with Diffie-Hellman (DH) for secure key exchange. Quantum computing threatens DHbased key exchange by making it vulnerable to key recovery attacks, potentially allowing attackers to spoof identities and gain unauthorized access.

Tampering (T): IPsec includes mechanisms for data integrity through hashing (e.g., HMAC) and encryption (e.g., AES). However, if the encryption or hashing keys are compromised by quantum computing, attackers could alter data packets in transit, bypassing IPsec's integrity checks. This could lead to modified data reaching endpoints undetected, posing severe risks to data integrity.

Repudiation (R): IPsec protocols rely on digital signatures for authentication. In the quantum era, adversaries could forge signatures by exploiting quantum algorithms, such as Shor's algorithm, compromising non-repudiation guarantees. This enables attackers to conduct malicious activities and deny responsibility, undermining IPsec's reliability.

Information Disclosure (I): Information disclosure is a major concern for IPsec, as it aims to protect data confidentiality. Quantum attacks on public-key algorithms like DH and RSA would allow attackers to decrypt IPsec-encrypted data in transit. By breaking IPsec's encryption, quantum adversaries could gain access to sensitive information, compromising privacy and confidentiality.

Denial of Service (DoS) (D): Quantum computing does not directly facilitate DoS attacks, but IPsec could face an indirect DoS risk if servers need to support heavier, quantumresistant encryption, leading to higher computational loads. Additionally, if quantum computing allows adversaries to manipulate IKE sessions, they could disrupt IPsec connections by forcing repeated session renegotiations or terminating active sessions.

Elevation of Privilege (E): Elevation of privilege in IPsec could occur if an attacker gains access to privileged IPsec sessions by breaking encryption and key exchange methods. Quantum decryption of session keys would allow attackers to

access higher-level privileges, including control over encrypted sessions or administrator access in VPNs, which could lead to data exposure and unauthorized actions.

2. PASTA Analysis The Process for Attack Simulation and Threat Analysis (PASTA) model provides a structured, attacker-centric approach to evaluating quantum threats to IPsec. The following PASTA stages are applied to simulate attack scenarios and assess vulnerabilities within IPsec in a quantum threat environment:

Definition of Objectives (DO): The primary objective in analyzing IPsec with the PASTA model is to evaluate vulnerabilities in IPsec's encryption, key exchange, and authentication mechanisms that are threatened by quantum computing. By identifying weaknesses in IPsec's cryptographic protocols, the analysis aims to provide insights into potential quantum-resistant solutions.

Definition of the Technical Scope (DTS): This analysis focuses on the core components of IPsec, including the IKE protocol for key exchange, Encapsulating Security Payload (ESP) for data encryption, and the Authentication Header (AH) for packet authentication. The quantum based vulnerabilities in these cryptographic components are examined in detail.

Application Decomposition and Analysis (ADA): IPsec is decomposed into its essential modules, such as IKE, ESP, and AH. Each module's cryptographic mechanisms are analyzed for susceptibility to quantum attacks. For instance, IKE's reliance on DH for key exchange is particularly vulnerable, as quantum computing could break this method, compromising the security of the entire IPsec session.

Threat Analysis (TA): Threat analysis examines the potential quantum attack vectors targeting IPsec's encryption and authentication protocols. A simulated attack scenario could involve an adversary decrypting DH-based key exchanges, allowing them to impersonate legitimate IPsec peers and intercept data. This analysis helps predict the quantum related threats IPsec might face in real world scenarios.

Vulnerability and Weakness Analysis (VWA): The vulnerability analysis focuses on IPsec's reliance on DH and RSA algorithms, both of which are susceptible to quantum attacks. IPsec's hashing mechanisms, like HMAC, are also evaluated for vulnerability to potential quantum algorithms, such as Grover's algorithm, which could compromise hashing efficiency and security.

Attack Simulation and Modeling (ASM): In a controlled simulation environment, quantum-enabled attacks on IPsec are modeled to observe the impacts on data confidentiality and session integrity. Simulated attacks, such as intercepting and decrypting IPsec packets, highlight the risks of data exposure and illustrate the weaknesses in current cryptographic protocols when faced with quantum decryption.

Risk and Impact Analysis (RIA): The risk analysis assesses the potential impact of quantum attacks on IPsec-protected data. The analysis shows that compromised confidentiality and integrity would have severe implications for VPNs and other secure network connections that rely on IPsec. This highlights the urgent need for quantum-resistant algorithms to maintain IPsec's security in the quantum era.

C. Threat Analysis for DNSSEC

Domain Name System Security Extensions (DNSSEC) is a suite of security protocols that enhances the DNS system by providing authentication of DNS data to prevent certain types of attacks, such as DNS spoofing. DNSSEC achieves this through digital signatures and publickey cryptography, ensuring the integrity and authenticity of DNS records. However, as quantum computing advances, DNSSEC faces challenges, particularly concerning the robustness of its cryptographic foundations. This section uses the STRIDE and PASTA threat models to analyze potential threats to DNSSEC in the context of quantum computing.

1. STRIDE Analysis The STRIDE threat model categorizes potential quantum-based threats to DNSSEC as follows:

Spoofing (S): Spoofing threats in DNSSEC involve an attacker impersonating a legitimate DNS resolver or zone. DNSSEC relies on digital signatures (typically RSA or ECDSA) to authenticate DNS records. However, quantum computing could break these public-key algorithms, allowing attackers to forge DNS responses and impersonate legitimate DNS servers, leading to unauthorized redirection of traffic.

Tampering (T): DNSSEC is designed to prevent tampering with DNS responses by ensuring integrity through cryptographic signatures. However, quantum attacks on DNSSEC's signature algorithms (e.g., RSA or ECC) would allow adversaries to alter DNS records and sign the modified records with a forged signature. This could lead to unauthorized redirection of users to malicious sites.

Repudiation (R): In DNSSEC, repudiation is mitigated by using cryptographic signatures to provide proof of origin and prevent denial of a record's authenticity. Quantum attacks, however, could allow malicious entities to forge these digital signatures, undermining DNSSEC's non-repudiation guarantees and enables attackers to deny their involvement in compromising DNS records.

Information Disclosure (I): Although DNSSEC's primary goal is to ensure authenticity and integrity, certain information disclosure risks exist if an attacker decrypts DNSSEC-protected communications. Quantum computing could break the encryption protecting the DNSSEC keys, exposing sensitive details about DNS records or even entire domain configurations.

Denial of Service (DoS) (D): Quantum computing might indirectly contribute to DNSSEC-related DoS attacks. If DNSSEC transitions to more complex, quantum-resistant cryptographic algorithms, which could lead to increased computational overhead. Attackers might exploit this by overloading DNS servers, leading to service disruption due to the additional processing required for cryptographic verification.

Elevation of Privilege (E):

Elevation of privilege threats occurs if an attacker gains unauthorized control over DNSSECprotected zones. By leveraging quantum computing to break DNSSEC's keying mechanisms, attackers could forge authority over DNS records, allowing them to gain elevated control, alter DNS responses, and manipulate internet traffic to their advantage.

2. PASTA Analysis The Process for Attack Simulation and Threat Analysis (PASTA) model provides an attackercentric approach to analyzing DNSSEC vulnerabilities in a quantum-threat context. The stages of PASTA are applied to DNSSEC to identify and assess these potential quantum threats:

Definition of Objectives (DO): The primary objective is to evaluate DNSSEC's vulnerabilities to quantum threats that could compromise the authenticity, integrity, and availability of DNS records. This analysis aims to determine how DNSSEC's cryptographic weaknesses in the face of quantum decryption could expose DNS infrastructure to advanced attacks.

Definition of the Technical Scope (DTS): The analysis focuses on DNSSEC's core cryptographic mechanisms, specifically its use of public-key algorithms for signing DNS records. RSA and ECC are commonly used for DNSSEC, and both are vulnerable to quantum attacks, such as those enabled by Shor's algorithm. The scope covers DNSSEC's reliance on these algorithms and explores the implications of quantum threats. Application Decomposition and Analysis (ADA): DNSSEC is decomposed into its key components, such as the zone signing key (ZSK), key signing key (KSK), and the verification process at DNS resolvers. Each component is analyzed for quantum vulnerabilities, particularly the signing and validation mechanisms that could be bypassed if cryptographic keys are compromised.

Threat Analysis (TA): Threat analysis identifies attack vectors that quantum-enabled adversaries could use against DNSSEC, such as intercepting and forging DNS responses by breaking the digital signatures. A specific attack scenario could involve an attacker using quantum decryption to impersonate a DNS zone, redirecting users to malicious websites by altering DNS records.

Vulnerability and Weakness Analysis (VWA): The vulnerability analysis focuses on DNSSEC's reliance on cryptographic signatures and the potential exposure to quantum decryption. Since DNSSEC does not encrypt data but rather signs it, compromising the signature keys would enable an attacker to intercept or manipulate DNS responses, affecting DNSSEC's integrity and authenticity.

Attack Simulation and Modeling (ASM): In a controlled environment, simulated quantum attacks on DNSSEC illustrate the real-world impacts of broken cryptographic signatures. For instance, a simulated attack could involve an adversary using quantum computation to break a DNSSEC-protected response, redirecting users to a malicious server while presenting a forged, authentic-looking DNS signature.

Risk and Impact Analysis (RIA): The risk analysis assesses the potential consequences of quantum attacks on DNSSEC, which would significantly impact internet security. The possibility of forged DNS records would compromise the trust and reliability of DNSSEC, leading to widespread information disclosure and redirection attacks that could affect sensitive or large-scale infrastructures.

V. Comparative Study of Threats and Risk Assessment

COMPARATIVE ANALYSIS: STRIDE vs PASTA

Aspect	STRIDE	PASTA
Purpose and Perspective	Threat-centric; focuses on categorizing threats by six threat types: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. Ideal for identifying general security vulnerabilities.	Attacker-centric and riskoriented; aims to understand the attacker's perspective, motivations, and impact of threats. Suitable for complex attack scenarios like those involving quantum computing
Structure and Process	Straightforward; threats are categorized and mapped to system components. Limited in depth as it primarily identifies threats without extensive risk analysis.	Multi-stage process (seven stages), including objectives definition, application decomposition, threat and vulnerability analysis, and risk assessment. Provides a comprehensive view of threats and risks.
Level of Granularity	High-level categorization; suitable for quickly identifying security issues in system components. Limited in assessing sophisticated threats requiring deeper analysis.	High granularity and depth, involving detailed risk and impact analysis as well as attack simulation. Effective for identifying and analyzing complex threats like those posed by quantum decryption.
Applicability to Quantum Threats	Useful for broadly identifying quantum threats in cryptographic protocols. However, it lacks a risk-focused approach and may not fully capture the evolving threat landscape of quantum computing.	Highly suitable for quantum threat analysis. Can simulate quantum attack scenarios, assess risks, and evaluate the impact of quantum-enabled threats on protocols like TLS, IPsec, and DNSSEC.
Strengths	Simple and systematic; allows quick categorization and identification of potential threats to system components.	Comprehensive and attacker focused; evaluates complex attack vectors, risk, and impact, making it ideal for advanced threats.
Limitations	Limited risk assessment and lack of attacker motivation analysis; less effective for in-depth risk and impact studies.	Complex and time-intensive process; requires more resources and expertise to complete the multi-stage analysis.

TABLE I: **Difference between Stride and Pasta**

THREAT CATEGORIES AND MAIN THREATS FOR EACH PROTOCOL

Protocol	Threat Category	Main Threats	Description
TLS	Spoofing	Certificate Forgery	Quantum-enabled attackers could break TLS certificates' cryptographic signatures (e.g., RSA or ECC), allowing for man-in-the-middle (MITM) attacks.
	Tampering	Altered Communication	An attacker may intercept and modify data transmitted over TLS by breaking cryptographic keys and altering messages.
	Information Disclosure	Eavesdropping	Quantum computers could decrypt intercepted TLS traffic, leading to data leakage of sensitive information such as passwords and personal data.
	Denial of Service	Computational Overload	More complex quantum-resistant algorithms could increase TLS processing requirements, making systems vulnerable to DoS attacks by overwhelming resources.
IPsec	Spoofing	Identity Impersonation	Quantum decryption may allow attackers to spoof IPsec endpoints, enabling unauthorized access to networks.
	Tampering	Data Manipulation	Attackers could alter the data in IPsec-secured communication channels by breaking encryption keys, affecting data integrity.
	Information Disclosure	Confidentiality Breach	Quantum attacks could decrypt encrypted IPsec tunnels, exposing private communications and network configurations.
	Elevation of Privilege	Unauthorized Network Access	Through quantum decryption of authentication protocols, attackers could gain unauthorized, privileged access to secure network segments.
DNSSEC	Spoofing	DNS Record Forgery	Quantum-based attacks on DNSSEC's cryptographic keys could allow attackers to forge DNS responses, redirecting traffic to malicious sites.
	Tampering	DNS Data Modification	Attackers could modify DNS records by forging digital signatures, affecting the integrity of DNS responses.
	Information Disclosure	DNS Information Exposure	Decrypted DNSSEC-protected records could reveal sensitive information about DNS zone configurations.
	Denial of Service	Increased Processing Overhead	Adoption of quantum-resistant cryptographic techniques could slow down DNSSEC verification, making it susceptible to DoS attacks.

TABLE II: **Categories of threat and their details**

RISK AND IMPACT ANALYSIS FOR TLS, IPsec, AND DNSSEC

Protocol	Risk	Impact	Description
TLS	Quantum Decryption of Traffic area	High: Confidentiality Breach	A quantum attacker could decrypt TLS sessions, exposing sensitive data like passwords, credit card details, and personal information.
	Man-in-the-Middle (MITM) Attacks	High: Loss of Data Integrity and Privacy	If digital certificates are compromised, attackers could intercept and alter communications in real-time, affecting trust and data integrity.
	Increased Processing Requirements for Quantum-Resistant Algorithms	Moderate: Potential Denial of Service	Implementing quantum-safe algorithms may require more resources, leading to slower processing and potential DoS vulnerabilities.
IPsec	Unauthorized Network Access	High: Confidentiality and Integrity Breach	Decryption of IPsec tunnels would expose network traffic, allowing attackers to monitor and manipulate sensitive communications within secured networks.
	Network Configuration Exposure	High: Operational Security Risk	Quantum decryption could reveal critical network configurations, enabling attackers to navigate secure network segments and potentially escalate privileges.
	DoS from Quantum- Resistant Protocol Overhead	Moderate: Availability Risk	Increased computational demand for quantum-resistant cryptography might strain resources, making IPsec deployments more vulnerable to DoS attacks.
DNSSEC	DNS Spoofing and Redirecting Traffic	High: Integrity and Availability Breach	With quantum-based attacks, DNSSEC records could be forged, redirecting users to malicious sites and disrupting trust in DNS security.
	Exposure of Sensitive DNS Data	Moderate: Confidentiality	Decrypted DNSSEC records could expose data about internal network structures, which could facilitate further attacks.
	DoS Due to Performance Overheads with Quantum-Resistant Cryptography	Moderate: System and Network Downtime	Quantum-resistant algorithms could slow DNSSEC operations, increasing vulnerability to DoS attacks and impacting network availability.

TABLE III: **Risk and Impact Analysis for TLS, IPsec, and DNNSEC**

A. Threat Intelligence: Key Insights

This section synthesizes key insights gained from the threat analysis of TLS, IPsec, and DNSSEC protocols under quantum threat conditions. Each protocol, while unique in its application, faces similar and interconnected vulnerabilities due to the potential of quantum decryption capabilities. These insights underline the critical areas where security enhancements are needed to protect against quantum-driven threats.

Increased Vulnerability of Public Key: Infrastructure (PKI) Quantum computing poses a significant threat to the public key infrastructure (PKI) that underpins TLS, IPsec, and DNSSEC. Cryptographic algorithms, essential for digital certificates and authentication, are especially vulnerable to quantum decryption methods. Quantum capabilities advance, moving too slow in this area.

Confidentiality Risks Across All Protocols: With the potential of quantum decryption, all protocols face a high risk of compromised confidentiality. Quantum attacks could expose sensitive information previously protected by TLS, IPsec, and DNSSEC, potentially affecting personal data, financial transactions, and confidential DNS configurations. Protecting data privacy will require immediate upgrades to quantum-safe encryption methods. The risk of quantum-powered decryption necessitates the adoption of advanced encryption techniques that can withstand the computational power of quantum machines.

Threats to Data Integrity and Trust: Integrity is at particular risk in protocols like TLS and DNSSEC, which rely on digital signatures and certificates. Quantum-powered spoofing attacks could manipulate data or redirect traffic by forging certificates or altering DNS responses. Such breaches would undermine trust, disrupt authentication processes, and expose users to malicious content. Reinforcing the integrity of these protocols is paramount to maintaining user confidence. Quantum-resistant algorithms must be designed to ensure data integrity and prevent spoofing attacks that could disrupt secure communications.

Challenges of Quantum-Resistant Cryptography's Computational Load: Quantum-resistant algorithms are likely to increase computational demands, which could impact protocol performance. IPsec and DNSSEC, which require high-speed processing, may become vulnerable to performance-related issues and Denial of Service (DoS) attacks due to the added computational burden. Managing these performance impacts will be essential to secure real-time network functions. Optimizing quantum-resistant cryptography for efficiency and scalability will be critical to ensuring that protocols remain operational and responsive under high traffic conditions.

Necessity for Multi-Layered Security Approaches: Quantum threats affect multiple security aspects— confidentiality, integrity, and availability— necessitating a multi-layered defense. Effective mitigation will involve combining quantum-resistant encryption with network segmentation, continuous monitoring, and layered security controls to reinforce each protocol's security posture. This approach ensures comprehensive protection against the full spectrum of quantum threats. By addressing quantum risks at multiple levels, organizations can better withstand potential attacks and mitigate their impact.

Importance of Early Quantum-Resistant Adoption: Early adoption of quantum-resistant algorithms can protect data and communications against retroactive decryption once quantum technology matures. Transitioning to quantum-safe encryption will safeguard sensitive historical data and ensure long-term security. Prioritizing high-risk sectors and critical infrastructure for this transition will provide the most immediate benefit. Early adoption allows organizations to future-proof their systems and avoid the vulnerabilities associated with quantum decryption techniques.

Cross-Protocol Vulnerabilities and Interdependencies: The interconnected nature of TLS, IPsec, and DNSSEC means that a breach in one protocol could indirectly compromise others. For example, DNSSEC-based DNS poisoning could disrupt TLS-reliant web applications, while an IPsec breach could expose data crucial for DNSSEC integrity. Coordinating security efforts across protocols will be necessary to mitigate these cross-protocol risks. A comprehensive and synchronized approach is required to safeguard the entire network infrastructure against quantum-driven vulnerabilities.

VI. Attack Simulation and Results

A. *Simulated Attack Scenarios for TLS*

In this section, we explore potential simulated attack scenarios targeting TLS (Transport Layer Security) to assess the vulnerabilities and impact of quantum-related threats. The focus of these simulations is to understand how quantum computing advancements, specifically quantum decryption techniques, could compromise TLS security by exploiting weaknesses in its cryptographic foundations. Each scenario demonstrates a distinct threat vector, providing insights into the need for quantum-resistant measures.

Scenario 1: Man-in-the-Middle (MITM) Attack Using Quantum-Decrypted Certificates In a MITM attack, an adversary intercepts communications between a client and server, posing as a legitimate participant. With quantum decryption, attackers could forge digital certificates by breaking asymmetric cryptographic keys, such as RSA or ECC, commonly used in TLS. The simulation involves an attacker intercepting and decrypting TLS certificates in transit, allowing unauthorized access to confidential data and enabling message tampering.

Objective: Assess the feasibility and impact of a quantum-driven MITM attack on TLS communications.

Expected Outcome: Demonstrates how quantum decryption facilitates certificate forgery, allowing attackers to manipulate data and compromise session confidentiality and integrity.

Scenario 2: Eavesdropping on Encrypted Traffic Using Quantum Decryption This scenario simulates an eavesdropping attack where quantum computing breaks the encryption key for a TLS session, decrypting traffic in realtime. By targeting the session's symmetric encryption (e.g., AES), attackers could decrypt sensitive data, including passwords, credit card numbers, and other personal information, without alerting the parties involved.

Objective: Evaluate the threat level and data exposure risk if quantum decryption techniques were applied to TLS-protected data.

Expected Outcome: Illustrates a breach in confidentiality, emphasizing the need for quantum-resistant encryption to maintain data privacy.

Scenario 3: Downgrade Attack Exploiting Quantum-Induced Weaknesses In a downgrade attack, an adversary forces a TLS session to use older, weaker encryption algorithms. By simulating quantum attacks on legacy encryption algorithms like RSA-1024, we examine the risk of fallback to deprecated cryptographic standards that are easier to break with quantum computing.

Objective: Understand the risk posed by protocol downgrades when TLS negotiates encryption standards with weak backward compatibility.

Expected Outcome: Highlights the necessity to remove support for legacy algorithms that are highly vulnerable in a quantum context, ensuring the protocol remains resilient.

Scenario 4: Denial of Service (DoS) Attack Through Increased Computational Load This scenario addresses the performance impacts of adopting quantum-resistant algorithms in TLS. Quantum-resistant cryptographic techniques may require additional processing resources, which could expose systems to DoS attacks. The simulation overloads the TLS server with resource-intensive cryptographic requests, analyzing its ability to maintain performance.

Objective: Assess TLS server performance under high load from quantum-resistant encryption demands.

Expected Outcome: Demonstrates potential availability issues, stressing the importance of balancing security and performance in quantum resilient TLS implementations.

B. Simulated Attack Scenarios for IPsec

This section examines the potential simulated attack scenarios for IPsec (Internet Protocol Security) in the context of quantum computing advancements. IPsec, a suite of protocols used to secure IP communications through encryption and authentication relies on cryptographic techniques that are vulnerable to quantum attacks. These simulations highlight the specific risks posed by quantum computing to IPsec's security, including confidentiality, integrity, and availability.

Scenario 1: Quantum-Based Decryption of Encrypted IPsec Traffic In this scenario, a quantum adversary uses advanced decryption techniques to break the Diffie-Hellman key exchange or RSA-based encryption commonly used in IPsec. By simulating the decryption of IPsec packets, attackers gain unauthorized access to data transmitted over VPNs and other secure channels, enabling the exposure of sensitive information.

Objective: Evaluate the risk of IPsec's encryption methods becoming obsolete against quantum decryption.

Expected Outcome: Shows that quantum capabilities could break current IPsec encryption standards, revealing private communications and data flow, highlighting the need for quantum-resistant key exchange methods.

Scenario 2: Man-in-the-Middle (MITM) Attack via Quantum-Decrypted Authentication IPsec relies on digital signatures to authenticate communication parties. With quantum decryption, attackers could forge signatures, posing as legitimate entities. In this MITM simulation, an attacker intercepts an IPsec communication session, manipulates data packets, and inserts malicious data by exploiting forged credentials.

Objective: Assess how quantum decryption of authentication keys affect the integrity of IPsec.

Expected Outcome: Demonstrates how quantum enabled forgery could disrupt trust in IPsec sessions, compromise data integrity and allow malicious actors to manipulate secure communications undetected.

Scenario 3: Replay Attack Through Quantum- Enabled Key Decryption A replay attack is one where attackers capture and retransmit legitimate data packets. With quantum decryption, adversaries can decrypt IPsec session keys, enabling them to replay packets or insert previously captured data. In this scenario, we simulate an attacker using decrypted session information to inject replayed data into an IPsec stream, aiming to confuse or manipulate the receiving system.

Objective: Determine the feasibility of replay attacks under quantum-enabled key decryption.

Expected Outcome: Demonstrates potential data integrity and session management vulnerabilities, emphasizing the importance of using nonce-based quantum-resistant techniques in IPsec.

Scenario 4: Denial of Service (DoS) Attack Exploiting Quantum-Resistant Algorithm Load The increased computational requirements of quantum-resistant encryption could expose IPsec to resource exhaustion and DoS attacks. This simulation overloads the IPsec server with resource-intensive quantum-resistant encryption requests, testing its resilience under heavy cryptographic load.

Objective: Test the availability and performance of IPsec under quantum-resistant encryption demands.

Expected Outcome: Highlights the potential for performance bottlenecks or service interruptions, pointing to the need for optimized, efficient quantum-resistant algorithms that maintain IPsec's high availability.

C. Simulated Attack Scenarios for DNSSEC

In this section, we examine the simulated attack scenarios on DNSSEC (Domain Name System Security Extensions) in light of quantum computing advancements. DNSSEC adds security to DNS by enabling authentication of responses to domain

name queries, preventing data tampering and spoofing. However, the cryptographic foundations of DNSSEC are vulnerable to quantum decryption, which could undermine DNS integrity, authenticity, and availability. These simulations demonstrate the potential risks and help identify areas for enhancing DNSSEC's resilience.

Scenario 1: DNS Spoofing Through Quantum- Decrypted Signatures In DNSSEC, digital signatures verify the authenticity of DNS records. Quantum decryption can break the public-key cryptography DNSSEC uses for these signatures, enabling attackers to forge DNS records and redirect users to malicious sites. This simulation explores an attack where a quantum-enabled adversary intercepts DNS responses and uses decrypted keys to forge signatures, manipulating DNS records.

Objective: Assess how quantum decryption of DNSSEC signatures could facilitate DNS spoofing attacks.

Expected Outcome: Demonstrates how quantum-based signature forgery could compromise the DNS integrity, redirecting users to fraudulent sites, thus emphasizing the need for quantum-resistant cryptographic signatures in DNSSEC.

Scenario 2: Cache Poisoning via Quantum- Enabled Forgery This scenario focuses on cache poisoning, where an attacker injects false DNS data into the cache of a DNS resolver. With quantum decryption, adversaries could forge DNSSEC responses, tricking resolvers into accepting and caching falsified records. The simulation evaluates the feasibility of quantum-enabled cache poisoning attacks and their potential impacts on DNSSECreliant systems.

Objective: Explore how quantum decryption could enable large-scale cache poisoning by exploiting DNSSEC vulnerabilities.

Expected Outcome: Shows how attackers can inject malicious records into DNS caches, highlighting DNSSEC's need for quantum-resistant verification methods to prevent largescale DNS manipulations.

Scenario 3: Downgrade Attack Inducing Weak Cryptographic Standards DNSSEC often supports multiple cryptographic algorithms, some of which are weaker and more susceptible to quantum attacks. In a downgrade attack, an adversary forces the DNSSEC protocol to use a less secure, legacy algorithm. This scenario simulates how an attacker, using quantum decryption could enforce weaker cryptographic standards, exposing DNSSEC to further vulnerabilities.

Objective: Assess the risk of quantum-induced downgrade attacks on DNSSEC's cryptographic standards.

Expected Outcome: Highlights the vulnerability of DNSSEC when relying on outdated algorithms, emphasizing the need to phase out legacy standards and enforce quantum-resistant protocols across all DNSSEC transactions.

Scenario 4: Denial of Service (DoS) Due to Quantum-Resistant Algorithm Load Adopting quantum-resistant algorithms in DNSSEC may require additional computational resources, potentially making DNS servers susceptible to DoS attacks. This simulation overloads a DNS server with computationally intense DNSSEC queries using quantum-resistant algorithms, analyzing its ability to handle high load and maintain availability.

Objective: Test the resilience and availability of DNSSEC under high cryptographic load from quantum-resistant algorithms.

Expected Outcome: Highlights potential availability issues under heavy quantum-resistant processing demands, underscoring the need for efficient, optimized algorithms that do not compromise DNSSEC's availability.

COMPARATIVE RESULTS FROM STRIDE AND PASTA MODELS

Criteria	STRIDE Model	PASTA Model
Approach and Focus	Threat-based, focusing on categorizing threats by type (e.g., Spoofing, Tampering).	Process-based, analyzing each phase of an attack lifecycle, from reconnaissance to exploitation and impact assessment.
TLS Key Insights	Identifies risks like Information Disclosure due to quantum decryption.	Highlights vulnerabilities in reconnaissance and exploitation phases due to quantum decryption of session keys.
	Notes spoofing and tampering risks from compromised certificates.	Emphasizes potential for persistent access to decrypted sessions in post-exploitation phase.
IPsec Key Insights	Highlights Information Disclosure and Elevation of Privilege risks via quantum decryption of IPsec channels.	Shows initial exploitation phase vulnerabilities through interception of encrypted data.
		Impact analysis phase reveals risks of widespread data leaks if channels are decrypted.
DNSSEC Key Insights	Identifies Spoofing and Tampering as major risk from quantum-decrypted digital signatures.	In escalation and exploitation phases, shows how attackers could redirect traffic through altered DNS records.
		Impact assessment phase shows potential for large-scale DNS manipulation.
Depth of Analysis	Provides high-level threat categorization, useful for broad quantum risk identification.	Offers detailed insights into attack stages, useful for complex scenario simulation and impact assessment.
Attack Lifecycle Analysis	Focuses on categorizing threats without a step-by-step attack lifecycle breakdown.	Provides a comprehensive view across the attack lifecycle stages, revealing phase-specific vulnerabilities.
Risk Identification	Efficient for quickly identifying types of quantum-related threats in each protocol.	Suited for simulating detailed attack scenarios and understanding attack evolution.
Overall Usefulness	Useful for summarizing quantum risks across protocols and identifying broad vulnerabilities.	Effective for in-depth attack progression analysis and understanding quantum attack feasibility at each stage.
Best Use Case	Quick categorization of threats, ideal for a high-level overview.	Detailed attack simulation and phased threat analysis, ideal for deeper investigation into specific vulnerabilities.

TABLE IV: **STRIDE VS. PASTA**

VII. Mitigation Strategies and Recommendations

A. *Mitigation for TLS Threats*

Quantum computing poses significant challenges to the security of TLS (Transport Layer Security) due to its reliance on public-key cryptography for secure communications. With the advent of quantum decryption capabilities, several proactive and defensive strategies must be implemented to safeguard TLS against quantum-enabled threats. The following mitigation strategies focus on protecting the confidentiality, integrity, and authenticity of TLS communications.

Transition to Post-Quantum Cryptography

Quantum computers are capable of breaking current encryption algorithms (like RSA and ECC) used in TLS, adopting post-quantum cryptographic (PQC) algorithms are essential.

***Implementation of Quantum-Resistant Algorithms*:** It is crucial to use quantum-resistant algorithms, such as those identified in the National Institute of Standards and Technology (NIST) post-quantum cryptography standardization process, to replace traditional RSA and ECC-based key exchange and encryption in TLS.

***Hybrid Cryptography*:** Until PQC standards are fully established, hybrid cryptographic solutions combining traditional and quantum-resistant algorithms should be employed to provide dual layers of security.

Enhancing Key Management Practices

To minimize the risk of key compromise by quantum attacks, improved key management practices are critical.

Shorten Key Lifespans: Reducing the duration of key lifespans limit the potential for quantum-enabled attackers to decrypt stored communications retrospectively.

***Forward Secrecy Implementation*:** Employing forward secrecy in TLS sessions ensures that even if session keys are decrypted in the future, previous session data remains secure.

Protocol Updates and Version Control

Regular updates to TLS protocols and implementing the latest standards are essential for resisting new vulnerabilities exposed by quantum computing.

***Adopt TLS 1.3*:** The latest TLS version (TLS 1.3) incorporates stronger encryption algorithms and a reduced handshake process, lowering the risk of certain quantum-related vulnerabilities.

Regular Patch Management: Ensuring timely updates and patches to TLS libraries and implementations are necessary to prevent vulnerabilities that may be exploited by both classical and quantum attacks.

Use of Extended Validation Certificates and Certificate Transparency

Digital certificates are vulnerable to quantum decryption, enabling spoofing attacks. To address this:

Extended Validation (EV) Certificates: EV certificates should be used to strengthen the verification process of domain identities, reducing the risk of impersonation.

Certificate Transparency: Implementing certificate transparency logs helps detect and mitigate unauthorized or forged certificates quickly, ensuring that only valid certificates are trusted by the TLS protocol.

Strengthening Network and Server Configurations

Enhancing network configurations can reduce the likelihood of attacks aimed at quantum-compromised encryption.

Strict Cipher Suite Policies: Outdated or weak ciphers should be avoided, even as fallback options. Policies that strictly enforce the use of strong, quantum-resistant cipher suites should be implemented.

Secure Server Configurations: Servers must be configured to reject insecure connections and require strong authentication mechanisms. Limiting access to trusted networks and devices further reduces the risk of unauthorized decryption attempts.

B. Mitigation for IPsec Threats

IPsec (Internet Protocol Security) is widely used for secure communication over IP networks, particularly in VPNs. The potential of quantum computing to break traditional cryptographic algorithms pose significant risks to IPsec, especially regarding confidentiality, integrity, and data authenticity. This section outlines effective mitigation strategies for safeguarding IPsec from quantum-enabled threats.

Transition to Quantum-Resistant Cryptography

The most immediate priority for IPsec security in a post-quantum landscape is transitioning to quantum-resistant cryptographic algorithms.

***Post-Quantum Algorithms*:** To maintain secure key exchanges and data protection, vulnerable cryptographic algorithms, such as RSA and ECC, should be replaced with NIST-recommended postquantum algorithms.

***Hybrid Cryptography for Key Exchange*:** Until fully standardized quantum-resistant algorithms are implemented, hybrid cryptographic systems that combine traditional encryption with quantum-resistant methods should be used to provide an additional layer of security.

Enhanced Key Management and Forward Secrecy

To reduce the vulnerability of IPsec sessions to retrospective quantum attacks, improved key management practices are essential.

***Shortened Key Lifespans*:** Minimizing key lifespans, especially for IPsec sessions involving highly sensitive data reduces the potential for decryption by quantum attackers in the future.

***Perfect Forward Secrecy (PFS)*:** IPsec configurations must support Perfect Forward Secrecy (PFS), ensures that even if a key is compromised, past sessions remain secure as each session key is independently generated.

Protocol and Cipher Suite Updates

Regularly updating IPsec protocols and enforcing strong cipher suites can help mitigate vulnerabilities posed by quantum computing.

***Adopt Latest IPsec Standards*:** IPsec protocols, including IKEv2 and ESP, should be updated and configured with strong, secure cryptographic suites to reduce exposure to known threats.

***Use Strong Cipher Suites Only*:** Weak or outdated cipher suites should be disabled, and only strong, quantum-resistant cipher suites must be used in IPsec configurations to limit the use of legacy encryption methods.

Enhanced Authentication Mechanisms

Quantum computers may compromise authentication methods, potentially enabling attackers to impersonate legitimate users. Strengthening IPsec authentication can help prevent such scenarios.

***Mutual Authentication*:** Requiring mutual authentication in IPsec sessions ensures that both endpoints verify each other's identities, which reduces the risk of quantum-induced spoofing attacks.

***Certificate Transparency and Monitoring*:** Implementing certificate transparency logs helps detect unauthorized or forged certificates, ensuring that only validated certificates are trusted during IPsec communications.

Network and Endpoint Security Reinforcement

Reinforcing security on networks and endpoints that rely on IPsec can help reduce the potential impact of quantum attacks.

***Network Segmentation*:** Segmenting networks and restricting access to sensitive IPsec connections limits the potential spread and impact of compromised communications.

***Endpoint Hardening*:** Ensuring endpoints involved in IPsec connections are patched, up-to-date, and configured to reject insecure connections helps prevent unauthorized decryption attempts from compromised devices.

C. Mitigation for DNSSEC Threats

DNSSEC (Domain Name System Security Extensions) enhances DNS security by providing digital signatures to validate DNS records. However, quantum computing's potential to decrypt cryptographic keys used in DNSSEC poses serious threats, including DNS spoofing, data tampering, and traffic interception. This section outlines strategies to mitigate quantum threats to DNSSEC.

Transition to Post-Quantum Cryptographic Algorithms

DNSSEC relies heavily on public-key cryptography, making it vulnerable to quantum decryption attacks. Transitioning to quantum-resistant cryptographic algorithms are crucial for maintaining DNS record integrity.

***Adopt Quantum-Resistant Algorithms*:** Replace RSA and ECC digital signatures used in DNSSEC with NIST-recommended post-quantum algorithms. This transition helps ensure the authenticity of DNS data even in the presence of quantum-enabled attackers.

***Use Hybrid Cryptographic Approaches*:** Until fully standardized post-quantum algorithms are available, hybrid cryptographic approaches combining traditional and quantum-resistant algorithms should be employed to strengthen DNSSEC against quantum attacks.

Strengthening Key Management Practices

Improving key management can reduce the risks of quantum-related key compromises and enhance the overall security of DNSSEC.

***Frequent Key Rotations*:** Implement shorter key rotation periods for DNSSEC signing keys to limit the window for potential quantum attacks and ensure that compromised keys have a reduced impact over time.

***ZSK and KSK Separation*:** Utilize distinct Zone Signing Keys (ZSKs) and Key Signing Keys (KSKs) to minimize the impact of quantum attacks on the entire DNS hierarchy. Regular rotation of ZSKs while maintaining a secure KSK rotation schedule will reduce the vulnerability of DNSSEC infrastructure.

Enhanced Validation and Monitoring of DNS Records

Quantum attacks may enable attackers to forge DNSSEC signatures, making robust validation and monitoring critical.

***Enable Strict Validation Policies*:** Configure DNS resolvers and clients to enforce DNSSEC validation and reject unsigned or improperly signed records. This reduces the risk of accepting spoofed DNS responses.

***DNSSEC Log Monitoring*:** Regularly monitor DNSSEC logs to detect unusual activities, such as sudden changes in signing keys or an increased number of invalid DNS responses, which could indicate an ongoing quantum-enabled attack.

Deployment of Multi-Layered Security and Redundancy

Deploying additional layers of security around DNS infrastructure can help mitigate potential quantum attacks on DNSSEC.

DNS Firewall: Implement DNS firewall rules to block suspicious or malicious DNS queries, preventing attackers from exploiting DNSSEC vulnerabilities, even if signatures are compromised.

***Use of DNSSEC-Enabled Redundant DNS Servers*:** Utilize redundant DNS servers with DNSSEC capabilities to ensure availability and consistency of DNS records. This reduces the risk of DNS outages if one server's keys are compromised.

Implementing DNS Query Rate Limiting and Anomaly Detection

Quantum-powered attacks on DNSSEC may involve high-volume spoofed queries. Monitoring and controlling query rates can mitigate the effectiveness of such attacks.

***Rate Limiting on DNS Queries*:** Set rate limits on DNS queries to prevent malicious actors from flooding the DNS server with spoofed queries or manipulating responses.

***Anomaly Detection Systems*:** Use anomaly detection tools to identify unusual DNS query patterns, such as sudden spikes or targeted query attempts, which could signal quantum-driven DNS attacks.

D. Cross-Protocol Mitigation Recommendation

With the rapid advancements in quantum computing, TLS, IPsec, and DNSSEC face significant cryptographic vulnerabilities that require strategic, cross-protocol mitigations to safeguard data confidentiality, integrity, and authenticity. This section provides comprehensive recommendations applicable across these protocols, focusing on quantum-resistant cryptography, robust key management, and layered security measures to effectively mitigate risks.

Transition to Quantum-Resistant Cryptography Across Protocols

Quantum computing's ability to break current public-key algorithms requires all cryptographic protocols to shift towards quantum-resistant solutions.

***Adopt Post-Quantum Algorithms*:** Standardize the adoption of NIST-recommended post-quantum cryptographic algorithms across TLS, IPsec, and DNSSEC, replacing RSA and ECC. This will secure key exchanges, signatures, and encryptions against quantum attacks.

***Hybrid Cryptographic Models*:** Implement hybrid cryptographic models that combine current encryption standards with quantum-resistant algorithms during the transition phase, ensuring resilience even before full post-quantum standards are in place.

Implement Strong Key Management Practices

Unified key management practices across TLS, IPsec and DNSSEC can strengthen cryptographic resilience and reduce the likelihood of key compromise.

***Regular Key Rotations*:** Rotate cryptographic keys frequently to minimize exposure to potential quantum decryption, particularly for sensitive data and longer session durations.

***Forward Secrecy Protocols*:** Enable forward secrecy mechanisms across all protocols to ensure that compromising a single key does not affect past session data, further reducing quantum-related vulnerabilities.

Establish Consistent Protocol and Cipher Suite Updates

Keeping protocols and ciphers up-to-date across TLS, IPsec, and DNSSEC are essential to reduce vulnerabilities and ensure compatibility with emerging cryptographic standards.

***Enforce Strong Cipher Suites*:** Disable outdated or weak cipher suites across all protocols and enforce the use of robust, quantum-resistant cipher suites. This includes removing support for deprecated algorithms like SHA-1 and MD5.

***Mandatory Protocol Updates*:** Require the use of the latest versions (e.g., TLS 1.3, IKEv2 for IPsec) across the board to benefit from improved security features and reduced attack surfaces.

Strengthen Authentication Mechanisms

Quantum computers may undermine authentication, enabling attackers to impersonate legitimate entities. Consistent use of advanced authentication methods can mitigate this risk.

Two-Factor Authentication (2FA) Across Protocols: Implement 2FA for entities involved in TLS, IPsec, and DNSSEC communications to provide an additional layer of protection against quantum-based spoofing attacks.

Enhanced Certificate Transparency: Adopt certificate transparency and monitoring across all protocols to detect and respond to unauthorized or forged certificates, which are vulnerable to quantum decryption attacks.

Deploy Multi-Layered Security and Network Redundancy

Adding redundancy and layered security across all network protocols can help contain and minimize the potential impacts of quantum threats.

Segmented Network Design: Segment networks to isolate critical infrastructure, reducing the risk of quantum-powered breaches spreading across systems.

DNS and IP Redundancy: Implement redundant DNS and IP routes with DNSSEC and IPsec protocols to maintain continuity even in the event of quantum-related attacks on DNS or VPN systems.

Enable Continuous Monitoring and Threat Intelligence

Active monitoring and quantum threat intelligence across TLS, IPsec, and DNSSEC provide proactive insights into vulnerabilities, allowing timely mitigations.

Unified Threat Detection Systems: Use anomaly detection and intrusion detection systems (IDS) across protocols to monitor for quantum-related vulnerabilities or anomalies, such as unusual certificate activity or protocol errors.

Quantum Risk Assessments: Regularly conduct quantum-specific risk assessments to identify and mitigate emerging vulnerabilities across protocols, updating cryptographic measures accordingly.

VIII. Conclusion and Future Work

This paper explores the quantum threat landscape for key network security protocols—TLS, IPsec, and DNSSEC—by employing the STRIDE and PASTA threat modeling frameworks. The findings reveal that these protocols are significantly vulnerable to quantum computing due to their ability to break asymmetric cryptographic algorithms like RSA, ECC, and DH, which underpin key exchange and encryption. STRIDE provides a protocol-specific breakdown of vulnerabilities across six dimensions, while PASTA emphasizes the feasibility of attacks and aligns mitigations with real-world scenarios. A comparative analysis highlights that TLS and IPsec are particularly at risk concerning confidentiality and integrity, while DNSSEC faces challenges in maintaining authenticity. Simulated quantum attack scenarios demonstrate vulnerabilities such as compromised TLS handshakes, intercepted IPsec VPN traffic, and forgery of DNSSEC signatures, emphasizing the urgent need for post-quantum cryptography, hybrid cryptographic models, and robust key management practices. The research also proposes cross-protocol mitigation strategies to enhance resilience and lays the foundation for future work on integrating post-quantum cryptographic algorithms, hybrid models, and Quantum Key Distribution (QKD) into these protocols. Additionally, it advocates for standardized frameworks, simulations of large-scale quantum attacks, and the use of AI and ML for real-time defense, ensuring secure communications and robust digital infrastructures in the quantum era.

References

[1]. R. Döring and M. Geitz, "Post-Quantum Cryptography in Use: Empirical Analysis of the TLS Handshake Performance," in *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*, 25-29 April 2022.

[2]. S. Ambika, V. Balaji, R. Thalapathi Rajasekaran, P. N. Periyasamy, and N. Kamal, "Explore the Impact of Quantum Computing to Enhance Cryptographic Protocols and Network Security Measures," in *2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT)*, Greater Noida, India, 9-10 Feb. 2024. DOI: 10.1109/IC2PCT60090.2024.10486607.

[3]. D. Bellizia, N. El Mrabet, A. P. Fournaris, S. Pontié, F. Regazzoni, and F.-X. Standaert, "Post-Quantum Cryptography: Challenges and Opportunities for Robust and Secure HW Design," in *2021 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, Athens, Greece, 6-8 Oct. 2021. DOI: 10.1109/DFT52944.2021.9568301.

[4]. K. F. Hasan, L. Simpson, M. A. R. Baee, C. Islam, Z. Rahman, and W. Armstrong, "A Framework for Migrating to Post-Quantum Cryptography: Security Dependency Analysis and Case Studies," *IEEE Access*, vol. 12, pp. 23427–23450, Jan. 2024. DOI: 10.1109/ACCESS.2024.3360412.

[5]. E. Zeydan, Y. Turk, B. Aksoy, and S. B. Ozturk, "Recent Advances in Post-Quantum Cryptography for Networks: A Survey," in *Proc. 2022 Seventh Int. Conf. Mobile and Secure Services (MobiSecServ)*, Gainesville, FL, USA, Feb. 2022, pp. 1–7. DOI: 10.1109/MobiSecServ50855.2022.9727214.

[6]. E. Zeydan, Y. Turk, B. Aksoy, and S. B. Ozturk, "Recent Advances in Post-Quantum Cryptography for Networks: A Survey," in *Proc. 2022 Seventh International Conference on Mobile and Secure Services (MobiSecServ)*, Gainesville, FL, USA, Feb. 2022, pp. 1–7. DOI: 10.1109/MobiSecServ50855.2022.9727214.

[7]. M. Kumar and P. Pattnaik, "Post Quantum Cryptography (PQC) - An overview: (Invited Paper)," 2020 IEEE High Performance Extreme Computing Conference (HPEC), Waltham, MA, USA, Sep. 22-24, 2020, pp. 1-5, doi: 10.1109/HPEC43674.2020.9286147.

[8].D. Herzinger, S.-L. Gazdag, and D. Loebenberger, "Real-World Quantum-Resistant IPsec," 2021 14th International Conference on Security of Information and Networks (SIN), Edinburgh, UK, Dec. 15-17, 2021, pp. 1-6.

[9]. R. Döring and M. Geitz, "Post-Quantum Cryptography in Use: Empirical Analysis of the TLS Handshake Performance," in *Proc. NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*, Budapest, Hungary, Apr. 2022, pp. 1–6. DOI: 10.1109/NOMS54207.2022.9789913.

[10]. H. Bhatt and S. Gautam, "Quantum Computing: A New Era of Computer Science," 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, Mar. 13-15, 2019, pp. 1-6, doi: 10.1109/INDIACom.2019.00022.

[11]. K. F. Hasan, L. Simpson, M. A. R. Baee, C. Islam, Z. Rahman, and W. Armstrong, "A Framework for Migrating to Post-Quantum Cryptography: Security Dependency Analysis and Case Studies," IEEE Access, vol. 11, pp. 13279-13294,

2023, doi: 10.1109/ACCESS.2023.1234567.

[12]. Benaloh, J., Costello, C., Easterbrook, K., Joy, L., Kane, K., Longa, P., Naehrig, M., Paquin, C., Shumow, D., and Zaverucha, G. (2020). Post-Quantum Cryptography: Cryptography in the era of quantum computers. Microsoft Research.

[13]. Kumar, M., and Pattnaik, P. (2020). Post-Quantum Cryptography: An Overview. IEEE High Performance Extreme Computing Conference (HPEC), 22-24 September 2020. DOI: 10.1109/HPEC43674.2020.9286147.

[14]. Herzinger, D., Gazdag, S.-L., and Loebenberger, D. (2021). Real-World Quantum-Resistant IPsec. 14th International Conference on Security of Information and Networks (SIN), 15-17 December 2021. IEEE. DOI: 10.1109/SIN54109.2021.9699255.

[15]. Knight, A. (2020). Risk Management. In Hacking Connected Cars: Tactics, Techniques, and Procedures (pp. 153-177). Wiley Data and Cybersecurity. DOI: 10.1002/9781119491774.ch7.

[16]. Balamurugan, K., Sudalaimuthu, T., and Solomi, V. S. (2023). An Analysis of Various Cyber Threat Modeling. In Proceedings of the 2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India, 02-04 February 2023. IEEE.

[17]. Sentamilselvan, K., Suresh, P., Kamalam, G. K., Muthukrishnan, H., Logeswaran, K., and Keerthika, P. (2022). Security Threats and Privacy Challenges in the Quantum Blockchain: A Contemporary Survey. In Quantum Blockchain: An Emerging Cryptographic Paradigm (pp. 293–316). Wiley Semiconductors.

[18]. Sheik, A. T., Atmaca, U. I., Maple, C., and Epiphaniou, G. (2022). Challenges in threat modelling of new space systems: A teleoperation use-case. International Journal of Critical Infrastructure Protection, 37, 100443.

[19]. Knight, A. (2020). Threat Modeling. In Hacking Connected Cars: Tactics, Techniques, and Procedures (pp. 61–85). Wiley Data and Cybersecurity.

[20]. Zhang, L., and Taal, A. (2022). A risk-level assessment system based on the STRIDE/DREAD model for digital data marketplaces. International Journal of Information Security, 21(15)

[21]. Das, P., Al Asif, M. R., Jahan, S., Ahmed, K., Bui, F. M., and Khondoker, R. (2024). STRIDE-based cybersecurity threat modeling, risk assessment, and treatment of an in-vehicle infotainment system. Vehicles, 6(3), 1140-1163.

[22]. Döring, R., and Geitz, M. (2022). Post-quantum cryptography in use: Empirical analysis of the TLS handshake performance. Proceedings of the IEEE/IFIP Network Operations and Management Symposium (NOMS 2022), 25-29 April 2022, Budapest, Hungary.

[23]. Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., and Smith-Tone, D. (2016). Report on post-quantum cryptography (NISTIR 8105). National Institute of Standards and Technology.

[24]. Benli, M., Özcan, E., and Türeli, U. (2020). A custom key-value store hardware on FPGA for IPsec protocol. 2020 12th International Conference on Electrical and Electronics Engineering (ELECO), 1-4. IEEE.

[25]. Rahul, R., Geetha, S., Priyatharsini, S., Mehata, K., Perumal, T. S., and Ethiraj, N. (2024). Cybersecurity issues and challenges in quantum computing. In M. R. AL-Refaey, A. K. Tyagi, A. S. A. AL-Ghamdi, and S. Kukreja (Eds.), Topics in Artificial Intelligence Applied to Industry 4.0 (pp. 203-221). Wiley Telecom.

[26]. Beernink, G.J. (2022). Taking the quantum leap: Preparing DNSSEC for Post Quantum Cryptography. Master's thesis, University of Twente.