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

Sujata Swain[1], Saunak Saha[1], Ritoja Poddar[1], Swapnanil Bera[1], Kushal Bera[1], Subhadeep Mohanta[1], Ayan Kumar Paul[1], Anjan Bandyopadhyay[1], and Vikas Chouhan[2]

[1]School of Computer Science and Engineering, Kalinga Institute of Industrial Technology(KIIT), Bhubaneswar, India
[2]Cybersecurity canada

**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, STRIDE Threat Model, PASTA Framework, Quantum-Resistant Cryptography and Post-Quantum Security

## I. Introduction

The rapid advancement of quantum computing presents significant challenges to traditional cryptographic techniques like RSA and Elliptic Curve Cryptography (ECC), which are integral to securing protocols such as TLS, IPsec, and DNSSEC. Quantum computers can solve complex mathematical problems exponentially faster than classical computers, making existing encryption methods vulnerable to attacks. Specifically, quantum algorithms like Shor's algorithm threaten to break widely used public-key cryptographic schemes, which could severely impact sensitive data's confidentiality, integrity, and authenticity. As quantum technology continues to evolve, addressing these vulnerabilities becomes increasingly urgent. Quantum-resilient cryptography is paramount to protect digital communication and prevent the collapse of current security frameworks, which could be rendered obsolete by quantum-enabled attacks [1].

Protocols such as TLS, IPsec, and DNSSEC are essential for secure communication in various sectors, including e-commerce, healthcare, and government. They facilitate encrypted exchanges of sensitive data, such as payment information, medical records, and government communications. However, quantum computing could exploit the cryptographic weaknesses of these protocols, potentially disrupting secure transactions and compromising sensitive data. This research focuses on evaluating and mitigating quantum-specific threats to these key protocols by employing established frameworks like STRIDE and PASTA. STRIDE, which categorizes threats into spoofing, tampering, repudiation, information disclosure, denial of service, and privilege elevation, offers a structured method for identifying potential quantum vulnerabilities. Complementing STRIDE, the PASTA framework provides a simulation-driven approach to predict and counteract real-world quantum attack scenarios [2], [3].

By integrating these frameworks, this study aims to systematically analyze the vulnerabilities introduced by quantum computing and propose countermeasures to safeguard these critical protocols. The paper explores quantum-resistant algorithms and hybrid cryptographic solutions, contributing to the development of post-quantum cryptographic standards. By leveraging these methodologies, the study addresses gaps in the current literature and aims to advance the state of quantum-safe encryption. This research is pivotal in ensuring the long-term security of global communications, providing robust solutions that can withstand quantum threats and preserving the integrity of the digital infrastructure in a quantum-enabled future [4]–[6].

### A. Motivation

This research is motivated by the pressing need to develop quantum-resilient strategies to safeguard these foundational protocols. By adapting and integrating advanced threat modeling frameworks such as STRIDE and PASTA, this study aims to identify quantum-specific vulnerabilities, assess risks systematically, and propose robust mitigation techniques. The motivation lies in ensuring that as quantum computing evolves, so too does the resilience of our digital infrastructure, enabling secure communications and data exchanges in a post-quantum era. This work aspires to contribute to the growing field of post-quantum cryptography and provide actionable insights for the development of next-generation cryptographic solutions.

### *B. The primary objectives of this research paper are outlined as follows:*

- We identify quantum threats to core security protocols such as TLS, IPsec, and DNSSEC, and evaluate their quantum vulnerabilities using comparative analyses based on the STRIDE and PASTA models.
- We develop a comprehensive threat matrix and conduct detailed risk assessments for the analyzed protocols, enabling a structured understanding of their security gaps.
- We propose quantum-resistant enhancements to these protocols, contributing to the advancement of post-quantum cryptography through the application of advanced threat modeling methodologies.

### *C. Organization of 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. Section II presents related work and background. Section III provides quantum threat analysis and risk assessment protocol. Section IV contains the threat identification in widely used protocols. Section V provides a comparative study of threats and risk assessment. Section VI contains the attack scenarios for widely used protocols. Section VII contains mainly the mitigation strategies and recommendations. In the final section VIII we have the conclusion and future work.

## II. Related Work

Several studies [7]–[9] 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 [10], [11]. These vulnerabilities necessitate a proactive approach to assess and mitigate risks in existing protocols.

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 [12], [13]

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. [14], [15]

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 [13], [14]. Research emphasizes the need for these adaptations to be implemented proactively to maintain confidentiality and data integrity in a quantum era.

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. [12]–[15]

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 plays a pivotal role in safeguarding digital systems, ensuring they are resilient to quantum threats while maintaining compatibility with current standards. [8]–[10]

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

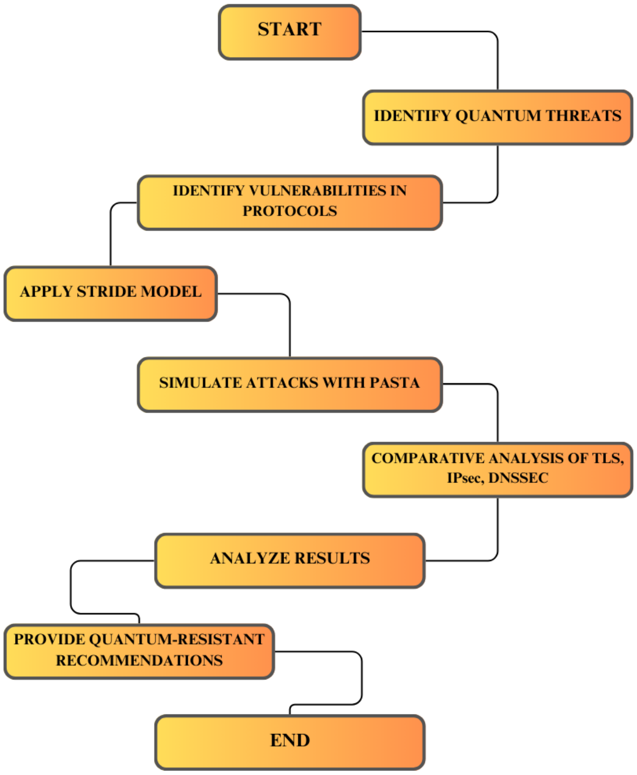
START
IDENTIFY QUANTUM THREATS
IDENTIFY VULNERABILITIES IN PROTOCOLS
APPLY STRIDE MODEL
SIMULATE ATTACKS WITH PASTA
COMPARATIVE ANALYSIS OF TLS, IPsec, DNSSEC
ANALYZE RESULTS
PROVIDE QUANTUM-RESISTANT RECOMMENDATIONS
END

Fig. 1: Detailed flowchart for Quantum Threat Analysis of widely used protocols

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 Shows us the overall mitigation workflow for a generalized threat model.

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]–[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

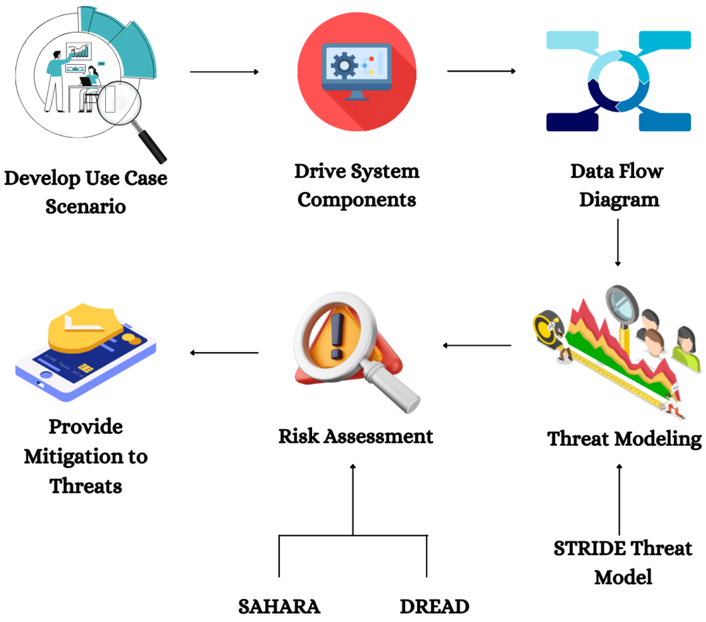

Fig. 2: Threat Modelling and Mitigation Workflow

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]–[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]

## III. Quantum Threat Analysis and Risk Assessment of Protocol

### 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. In the context of TLS, IPsec, and DNSSEC, each STRIDE category targets specific threat areas within these protocols.

Spoofing 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 could accelerate quantum computing. 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 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 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 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) 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 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.

The STRIDE model, traditionally effective in identifying vulnerabilities across various systems, requires adaptation to address the unique challenges posed by quantum computing. Quantum algorithms, such as Shor's and Grover's, have the potential to compromise the cryptographic underpinnings of protocols like TLS, IPsec, and DNSSEC. To account for these emerging risks, this study extends STRIDE to include quantum-specific attack scenarios within each threat category—Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privileges. For example, quantum-enabled attackers could break asymmetric encryption used in authentication (Spoofing) or compromise data integrity by decrypting encrypted data in transit (Tampering). This adaptation of STRIDE highlights areas where these protocols need quantum-resistant solutions, such as post-quantum cryptographic algorithms and enhanced key management practices, to mitigate vulnerabilities effectively.

However, STRIDE's static framework, focused on categorizing threats, has limitations in addressing the dynamic and evolving nature of quantum-enabled attacks. Its lack of an attacker-centric and scenario-driven perspective makes it less suited for assessing the sophistication of quantum threats. To address these shortcomings, this study incorporates the PASTA (Process for Attack Simulation and Threat Analysis) model alongside STRIDE. PASTA's staged, simulation-based approach complements STRIDE by offering a dynamic framework that evaluates the feasibility of quantum attacks and aligns mitigation strategies with real-world scenarios. Together, STRIDE and PASTA provide a more comprehensive and adaptive methodology for identifying and mitigating both traditional and quantum-specific vulnerabilities, ensuring a robust defense against emerging threats.

### *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.

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.

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-the-middle 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.

The PASTA model, typically used for traditional security threats, has been adapted in this study to address quantum-specific challenges. Quantum computing introduces new vulnerabilities, particularly through quantum algorithms like Shor's and Grover's, which could break conventional cryptographic systems such as RSA and ECC. Shor's algorithm can efficiently factor large numbers, threatening RSA encryption, while Grover's algorithm speeds up brute-force attacks on symmetric-key cryptography. This adaptation of the PASTA model revises each stage to consider quantum threats. The model's attacker-centric approach allows for a dynamic examination of how quantum computing could exploit weaknesses in protocols like TLS, IPsec, and DNSSEC. By simulating these quantum-enabled threats, the model offers a more comprehensive analysis than traditional methods, highlighting the evolving risks posed by quantum algorithms and providing insights into how to enhance system resilience in a quantum future.

While the PASTA model provides a detailed, seven-stage framework for simulating and analyzing threats, it has limitations when applied to quantum threats. One of the primary limitations lies in the model's reliance on attacker simulation, which assumes a certain level of predictability about how attackers behave. However, the nature of quantum advancements is highly uncertain, and it is challenging to predict how quantum algorithms, such as Shor's and Grover's, evolve and be implemented in real-world attacks. The current model does not account for the rapid and unpredictable developments in quantum technologies,

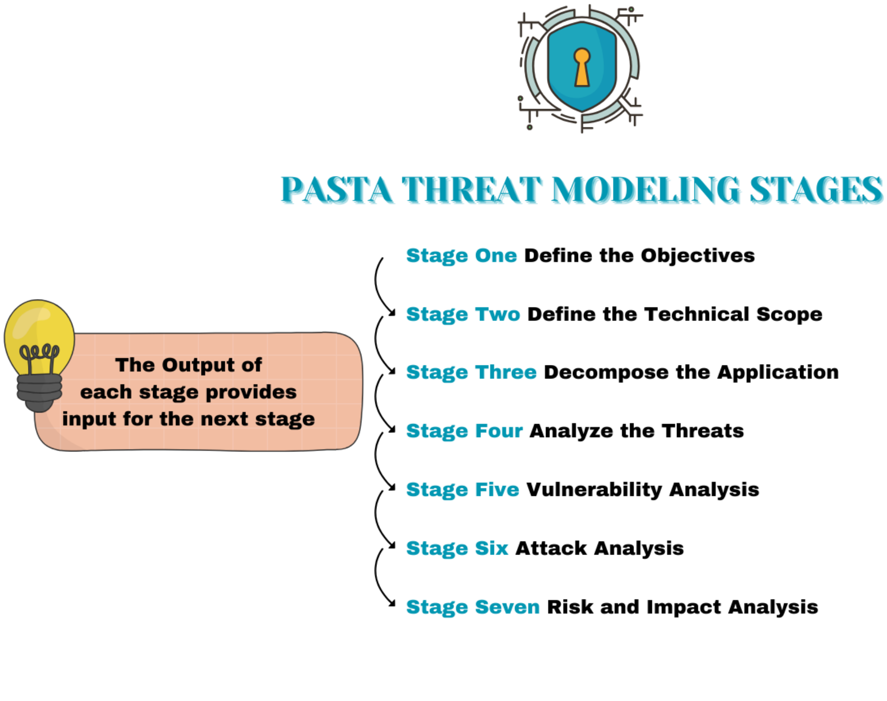
PASTA THREAT MODELING STAGES
The Output of each stage provides input for the next stage
Stage One Define the Objectives
Stage Two Define the Technical Scope
Stage Three Decompose the Application
Stage Four Analyze the Threats
Stage Five Vulnerability Analysis
Stage Six Attack Analysis
Stage Seven Risk and Impact Analysis

Fig. 3: PASTA Threat Modeling Stages

which means that simulations based on existing understanding may not always reflect the most advanced or emerging quantum capabilities. For instance, although quantum computing research has made substantial progress, the practical application of quantum algorithms to real-world systems is still in its infancy. As such, future iterations of the PASTA model may need to incorporate quantum-specific simulations, which are still largely theoretical. These updates could lead to more accurate threat simulations as quantum technologies develop, providing a more robust tool for assessing the impact of quantum-enabled attacks on systems like TLS, IPsec, and DNSSEC.

### *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.

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

All three protocols rely heavily or depend 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.

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.

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.

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.

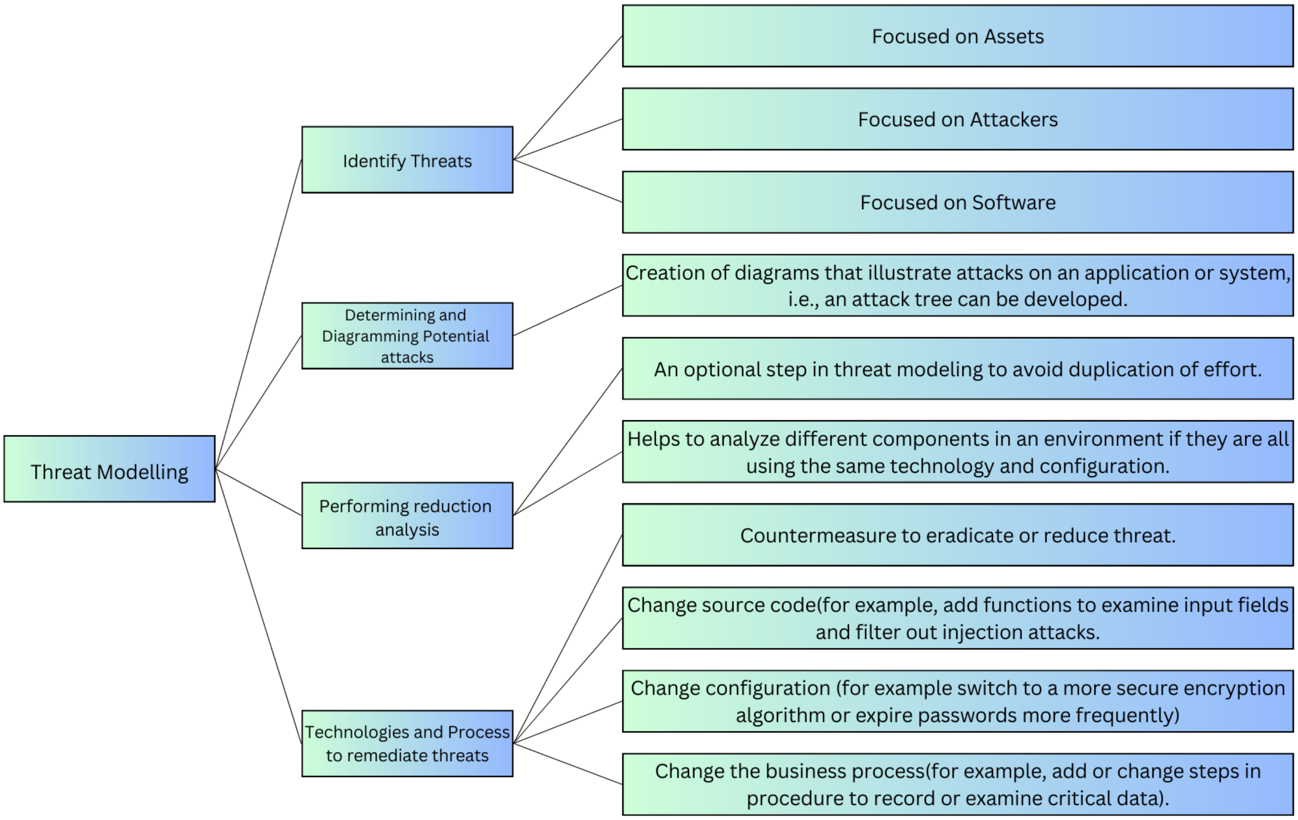
Threat Modelling
Identify Threats
Focused on Assets
Focused on Attackers
Focused on Software
Determining and Diagramming Potential attacks
Creation of diagrams that illustrate attacks on an application or system, i.e., an attack tree can be developed.
Performing reduction analysis
An optional step in threat modeling to avoid duplication of effort.
Helps to analyze different components in an environment if they are all using the same technology and configuration.
Technologies and Process to remediate threats
Countermeasure to eradicate or reduce threat.
Change source code(for example, add functions to examine input fields and filter out injection attacks.
Change configuration (for example switch to a more secure encryption algorithm or expire passwords more frequently)
Change the business process(for example, add or change steps in procedure to record or examine critical data).

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.

The primary objective of the simulation environment is to evaluate the resilience of TLS, IPsec, and DNSSEC protocols against potential quantum computing threats, specifically targeting their cryptographic underpinnings. This involves testing the vulnerabilities of existing algorithms like RSA and ECC, which are foundational to these protocols, under hypothetical quantum attacks leveraging Shor's algorithm. Additionally, the simulations aim to explore attack vectors such as man-in-the-middle exploits, data tampering, and impersonation attacks, which quantum computing could amplify. These scenarios are analyzed using the STRIDE and PASTA threat modeling frameworks to assess their effectiveness in identifying, categorizing, and addressing quantum-induced security challenges, providing insights into protocol weaknesses and the development of quantum-resistant enhancements.

The simulation environment for assessing the impact of quantum threats on cryptographic protocols like TLS, IPsec, and DNSSEC is built on a robust virtualized network infrastructure. This setup uses virtual machines or Docker containers to simulate distinct roles, such as clients, servers, and adversaries, ensuring an isolated and controlled testing environment. The simulations integrate quantum-safe cryptography libraries, particularly those implementing algorithms proposed by NIST for post-quantum cryptography, to model quantum-resistant alternatives. These libraries benchmark the security and performance of existing cryptographic mechanisms like RSA and ECC against prospective quantum-resistant protocols.

Additionally, tools such as Metasploit, Wireshark, and Scapy are employed for detailed packet inspection, protocol analysis, and attack simulation. These are complemented by custom scripts crafted to emulate quantum-specific attacks, like leveraging Shor's algorithm to decrypt RSA-based encryption. Specific scenarios include simulating a quantum-enabled man-in-the-middle attack on TLS to evaluate its reliance on RSA and ECC for key exchange and encryption, testing IPsec's Diffie-Hellman key exchange under quantum attack scenarios to assess the confidentiality of encrypted communications, and examining DNSSEC for potential vulnerabilities to quantum-enabled digital signature spoofing, focusing on RSA-based authentication.

Despite its comprehensive design, this simulation environment has certain limitations due to the current technological constraints of quantum computing. The computational power of advanced quantum systems is approximated through theoretical attack algorithms rather than real quantum hardware. Consequently, while these simulations offer valuable insights into potential quantum threats and protocol vulnerabilities, future research benefits significantly from the inclusion of real quantum computing systems to achieve a more precise evaluation of post-quantum cryptographic solutions. This highlights the need for ongoing refinement of testing methodologies as quantum technologies evolve.

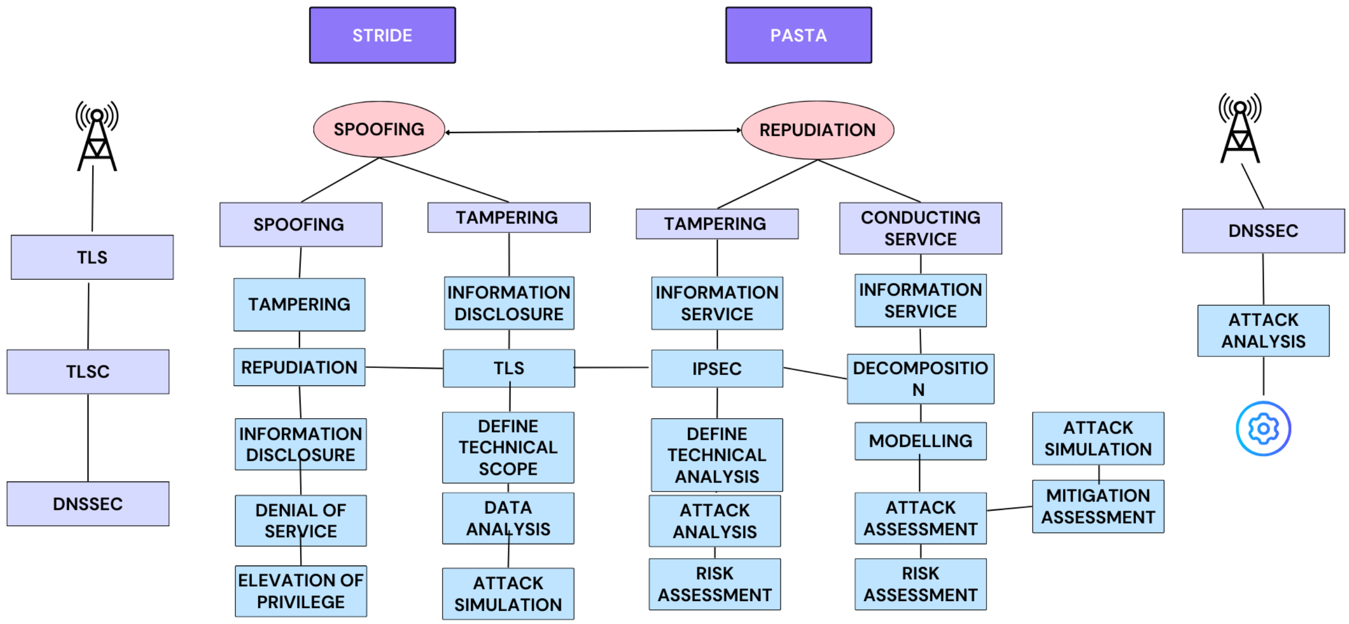

Fig. 5: Threat identification of STRIDE and PASTA

## IV. Threat Identification for widely used protocols

### 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 vulnerabilities of TLS in the face of quantum computing threats are categorized into six key dimensions, offering a detailed perspective on potential risks. Spoofing poses a significant risk as quantum algorithms like Shor's can break public-key cryptographic methods such as RSA and ECDSA. This capability could allow attackers to impersonate legitimate servers or clients during the TLS handshake, enabling unauthorized connections and the compromise of session authenticity. Tampering, another critical threat, could arise if attackers decrypt messages using quantum computing and then modify the data in transit, bypassing TLS's Message Authentication Codes (MACs). This undermines the integrity of sensitive data exchanges.

Repudiation risks escalate as quantum computing could enable the forging of digital signatures, like those based on ECDSA, eroding the non-repudiation assurances provided by TLS and allowing malicious actors to deny involvement in fraudulent activities. Information disclosure represents one of the most alarming vulnerabilities, as quantum computers could decrypt previously secure communications, exposing private data and causing severe confidentiality breaches. While denial-of-service (DoS) attacks are not directly enhanced by quantum computing, the additional computational overhead required for quantum-resistant cryptographic algorithms may strain server resources, making them more susceptible to overload or disruption. Lastly, the elevation of privilege becomes plausible as attackers could use quantum decryption to hijack authenticated sessions, gaining unauthorized access to privileged information and services. These vulnerabilities underscore the pressing need to develop and integrate quantum-resistant mechanisms into TLS to safeguard against emerging threats in the quantum era.

*2) **PASTA Analysis**:* The Process for Attack Simulation and Threat Analysis (PASTA) model provides a systematic, attacker-centric framework for evaluating the resilience of TLS against quantum computing threats. The analysis begins with the Definition of Objectives (DO), which focuses on identifying risks to the confidentiality, integrity, and availability of TLS-protected data due to vulnerabilities in its cryptographic mechanisms, including key exchange, encryption, and authentication. Next, the Definition of the Technical Scope (DTS) narrows the focus to RSA and ECC key exchange methods, digital signatures, and Message Authentication Codes (MACs), all of which are examined for susceptibility to quantum decryption algorithms like Shor's.

In the Application Decomposition and Analysis (ADA) stage, TLS is broken into its core components—handshake protocols, cipher suite negotiations, key exchange, and encrypted communication. Each element is individually scrutinized to determine how quantum threats might exploit these processes. The Threat Analysis (TA) phase identifies potential attack vectors, such as a quantum-enabled man-in-the-middle (MitM) attack, where an adversary compromises RSA or ECC-based key exchanges during the TLS handshake, intercepting and decrypting sensitive data.

The analysis progresses to Vulnerability and Weakness Analysis (VWA), which emphasizes the reliance of TLS on RSA and ECC, both vulnerable to quantum decryption. The Attack Simulation and Modeling (ASM) phase simulates quantum attacks in a controlled environment, demonstrating real-world implications, such as MitM attacks that compromise the confidentiality and integrity of TLS-encrypted data. Finally, Risk and Impact Analysis (RIA) evaluates the consequences of successful quantum-based attacks, highlighting severe risks such as compromised data privacy and weakened trust in TLS-based communication systems. These findings underscore the urgency of transitioning to quantum-resistant cryptographic solutions to safeguard against emerging threats.

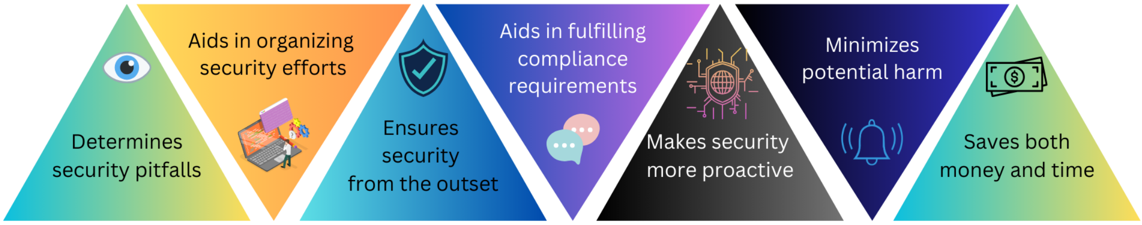
Determines security pitfalls
Aids in organizing security efforts
Ensures security from the outset
Aids in fulfilling compliance requirements
Makes security more proactive
Minimizes potential harm
Saves both money and time

Fig. 6: Importance of Threat Modeling

## *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, the potential vulnerabilities of IPsec in the quantum era are systematically analyzed across six key dimensions. Spoofing poses a significant threat as quantum computing compromises the Diffie-Hellman (DH) key exchange, a cornerstone of the Internet Key Exchange (IKE) protocol. This allows attackers to recover keys, impersonate legitimate VPN endpoints, and gain unauthorized access. Tampering becomes critical when quantum attackers decrypt or derive cryptographic keys, enabling them to modify data packets in transit and bypass IPsec's integrity mechanisms, such as HMAC hashing and AES encryption, leading to undetected alterations of transmitted data.

Repudiation risks emerge as quantum algorithms like Shor's could forge digital signatures used in IPsec authentication, allowing malicious actors to conduct harmful activities while denying responsibility. Information disclosure is perhaps the most severe risk, as quantum attacks on public-key algorithms like DH and RSA would enable adversaries to decrypt IPsec-secured data in transit, compromising privacy and exposing sensitive information. Denial of Service (DoS) attacks may be indirectly facilitated by quantum-resistant encryption demands that increase server computational loads. Additionally, attackers leveraging quantum capabilities could manipulate IKE sessions to disrupt or terminate active IPsec connections. Lastly, the elevation of privilege could occur when quantum attackers decrypt session keys, granting them unauthorized access to privileged IPsec sessions, and potentially allowing full control over VPN connections and administrative privileges. These vulnerabilities highlight the urgent need to develop quantum-resistant cryptographic protocols for IPsec.

*2) **PASTA Analysis:*** The Process for Attack Simulation and Threat Analysis (PASTA) model offers a systematic, attacker-centric framework to evaluate the potential vulnerabilities of IPsec in a quantum environment. The analysis begins with the Definition of Objectives (DO), aiming to identify weaknesses in IPsec's key exchange, encryption, and authentication mechanisms that could be exploited by quantum computing. This step highlights the need to explore quantum-resistant solutions by understanding where current cryptographic protocols fall short. Next, the Definition of the Technical Scope (DTS) focuses on IPsec's core components, such as the Internet Key Exchange (IKE) protocol, Encapsulating Security Payload (ESP) for encryption, and Authentication Header (AH) for packet authentication. Each of these components is scrutinized for quantum vulnerabilities, particularly the susceptibility of Diffie-Hellman (DH) key exchange and RSA encryption methods.

Following this, the Application Decomposition and Analysis (ADA) stage breaks IPsec into its modules for a detailed evaluation of its cryptographic mechanisms. Special attention is given to how quantum attacks might target IKE's DH-based key exchange, which could compromise the security of entire IPsec sessions. The Threat Analysis (TA) simulates potential quantum attack vectors, such as an adversary using quantum decryption capabilities to intercept or impersonate IPsec peers by breaking the DH-based key exchange. The Vulnerability and Weakness Analysis (VWA) evaluates the reliance of IPsec on algorithms like DH and RSA, both of which are vulnerable to quantum algorithms like Shor's, and assesses the impact of quantum attacks on hashing mechanisms such as HMAC. In the Attack Simulation and Modeling (ASM) stage, simulated quantum-enabled attacks on IPsec protocols are carried out in a controlled environment to observe the impact on data confidentiality and session integrity, emphasizing the real-world risks of quantum decryption. Finally, the Risk and Impact Analysis (RIA) evaluates the significant implications of quantum attacks on IPsec, especially regarding compromised confidentiality and integrity. This highlights the critical need for quantum-resistant cryptographic solutions to ensure the continued security of IPsec 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 highlights several quantum-based vulnerabilities that can significantly affect DNSSEC, a protocol designed to ensure DNS integrity through cryptographic digital signatures. Spoofing threats could arise if quantum computers break the RSA or ECDSA signature algorithms used by DNSSEC. Quantum decryption capabilities could allow attackers to forge DNS responses and impersonate legitimate DNS servers, leading to unauthorized traffic redirection. This vulnerability could allow malicious actors to direct users to fraudulent websites, undermining the integrity of the DNS system. Similarly, Tampering risks are amplified in a quantum context. If quantum computers can decrypt or break the cryptographic signatures used in DNSSEC, attackers could alter DNS records and then sign them with forged signatures. This would allow attackers to manipulate DNS responses, potentially redirecting users to harmful websites or disrupting services reliant on DNSSEC's integrity checks.

Repudiation threats would also be exacerbated, as attackers could use quantum computing to forge digital signatures, enabling them to deny responsibility for manipulating DNS records. This could undermine the core non-repudiation guarantees that DNSSEC provides, leaving the authenticity of DNS responses vulnerable to tampering. Furthermore, information disclosure risks are heightened when quantum computers break encryption methods that protect DNSSEC keys. Attackers could potentially decrypt protected communications, exposing sensitive DNS record information and even full domain configurations, compromising privacy and security. As DNSSEC transitions to more complex quantum-resistant cryptographic algorithms, Denial of Service (DoS) attacks might become more prevalent. These algorithms could require significantly more computational power, and malicious actors could exploit this by overloading DNS servers, and disrupting services through resource exhaustion.

Finally, the Elevation of Privilege threats could allow attackers to leverage quantum computing capabilities to break DNSSEC's keying mechanisms, granting them unauthorized control over DNS zones. This would enable attackers to manipulate DNS records at a higher level, directing internet traffic to their desired destinations, and potentially compromising entire networks and services. These vulnerabilities underscore the need for quantum-resistant cryptographic solutions to maintain the security of DNSSEC in the future.

*2) **PASTA Analysis**:* The Process for Attack Simulation and Threat Analysis (PASTA) model offers a structured approach for evaluating DNSSEC vulnerabilities in the context of quantum computing threats. This model is used to understand how quantum-enabled adversaries could exploit weaknesses in DNSSEC's cryptographic mechanisms, especially focusing on its public-key signing system that currently relies on RSA and ECC algorithms, both vulnerable to quantum decryption via Shor's algorithm.

The Definition of Objectives (DO) stage aims to assess DNSSEC's susceptibility to quantum threats, primarily targeting the authenticity, integrity, and availability of DNS records. The goal is to identify potential cryptographic weaknesses in the system, particularly where quantum computing could potentially break current algorithms, leaving DNS infrastructure open to advanced cyberattacks. In the Definition of the Technical Scope (DTS), the analysis specifically targets DNSSEC's cryptographic components, particularly its use of RSA and ECC for signing DNS records. The scope of the analysis covers the vulnerabilities these algorithms have to quantum decryption methods, especially the potential impact of Shor's algorithm on DNSSEC's security.

During the Application Decomposition and Analysis (ADA) stage, DNSSEC is broken down into key components such as the Zone Signing Key (ZSK), Key Signing Key (KSK), and the verification process performed by DNS resolvers. Each element is examined for quantum vulnerabilities, with a particular focus on how the signing and validation processes could be compromised by quantum computing. Threat Analysis (TA) identifies potential attack vectors that a quantum-enabled adversary might exploit. A key scenario involves an attacker using quantum decryption to break digital signatures, allowing them to impersonate DNS zones and redirect users to malicious websites by altering DNS records.

The Vulnerability and Weakness Analysis (VWA) stage highlights DNSSEC's dependence on cryptographic signatures for integrity and authenticity. With quantum computing, the signature keys could be compromised, potentially allowing attackers to intercept or manipulate DNS responses. This breaks the fundamental role of DNSSEC in ensuring the authenticity of DNS records. During the Attack Simulation and Modeling (ASM) phase, simulated quantum attacks provide insight into the real-world implications of broken cryptographic signatures. For instance, a simulated attack might involve a quantum-enabled adversary breaking a DNSSEC-protected response and redirecting users to a malicious server by presenting a forged, yet seemingly authentic, DNS signature.

Finally, Risk and Impact Analysis (RIA) evaluates the consequences of quantum attacks on DNSSEC. The analysis underscores the severe implications for internet security, as forged DNS records could undermine the entire trust model of DNSSEC. Such attacks would facilitate widespread information disclosure, redirection, and potentially devastating security breaches for critical infrastructures relying on DNSSEC for safe communication. The results from this analysis further stress the urgent need for quantum-resistant algorithms to protect DNSSEC from future threats posed by quantum computing.

## V. Comparative Study of Threats and Risk Assessment

This section presents a comparative analysis of two widely recognized threat models—STRIDE and PASTA—focusing on their respective categories and the main threats associated with each protocol. It delves into the strengths and limitations of each model, highlighting their applicability in different security contexts. Additionally, the section includes a risk and impact assessment for several commonly used security protocols, offering a nuanced understanding of their vulnerabilities in the face of both classical and emerging quantum threats. These comprehensive comparisons, I and II below allow for an in-depth evaluation of threat modeling techniques and their relevance in addressing the evolving landscape of cybersecurity risks.

### *A. 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. [26] | Attacker-centric and risk-oriented; aims to understand the attacker's perspective, motivations, and impact of threats. Suitable for complex attack scenarios like those involving quantum computing. [27] |
| **Structure and Process** | Straightforward; threats are categorized and mapped to system components. Limited in depth as it primarily identifies threats without extensive risk analysis. [26] | 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. [28] |
| **Level of Granularity** | High-level categorization; suitable for quickly identifying security issues in the system components. Limited in assessing sophisticated threats requiring deeper analysis. [26] | 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. [29] |
| **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. [30] | 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. [31] |
| **Strengths** | Simple and systematic; allows quick categorization and identification of potential threats to system components. [26] | Comprehensive and attacker-focused; evaluates complex attack vectors, risk, and impact, making it ideal for advanced threats. [29] |
| **Limitations** | Limited risk assessment and lack of attacker motivation analysis; less effective for in-depth risk and impact studies. [26] | Complex and time-intensive process; requires more resources and expertise to complete the multi-stage analysis. [30] |

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

### *B. THREAT CATEGORIES AND MAIN THREATS FOR EACH PROTOCOL*

| Protocol | Threat Category | Main Threats | Description |
|---|---|---|---|
| **TLS** | Spoofing | Certificate Forgery [32] | Quantum-enabled attackers could break TLS certificates' cryptographic signatures (e.g., RSA or ECC), allowing for man-in-the-middle (MITM) attacks. [33] |
| | Tampering | Altered Communication [34] | An attacker may intercept and modify data transmitted over TLS by breaking cryptographic keys and altering messages. [35] |
| | Information Disclosure | Eavesdropping [36] | Quantum computers could decrypt intercepted TLS traffic, leading to data leakage of sensitive information such as passwords and personal data. [37] |
| | Denial of Service | Computational Overload [38] | More complex quantum-resistant algorithms could increase TLS processing requirements, making systems vulnerable to DoS attacks by overwhelming resources. [39] |
| **IPsec** | Spoofing | Identity Impersonation [40] | Quantum decryption may allow attackers to spoof IPsec endpoints, enabling unauthorized network access. [41] |
| | Tampering | Data Manipulation [42] | Attackers could alter the data in IPsec-secured communication channels by breaking encryption keys, affecting data integrity. [43] |
| | Information Disclosure | Confidentiality Breach [44] | Quantum attacks could decrypt encrypted IPsec tunnels, exposing private communications and network configurations. [45] |
| | Elevation of Privilege | Unauthorized Network Access [46] | Through quantum decryption of authentication protocols, attackers could gain unauthorized, privileged access to secure network segments. [47] |
| **DNSSEC** | Spoofing | DNS Record Forgery [48] | Quantum-based attacks on DNSSEC's cryptographic keys could allow attackers to forge DNS responses, redirecting traffic to malicious sites. [49] |
| | Tampering | DNS Data Modification [50] | Attackers could modify DNS records by forging digital signatures, affecting the integrity of DNS responses. [51] |
| | Information Disclosure | DNS Information Exposure [52] | Decrypted DNSSEC-protected records could reveal sensitive information about DNS zone configurations. [53] |
| | Denial of Service | Increased Processing Overhead [54] | Adoption of quantum-resistant cryptographic techniques could slow down DNSSEC verification, making it susceptible to DoS attacks. [55] |

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

### *C. RISK AND IMPACT ANALYSIS FOR TLS, IPsec, AND DNSSEC*

#### *A. Threat Intelligence: Key Insights*

Quantum computing poses significant challenges to the security of protocols like TLS, IPsec, and DNSSEC, which are foundational for the security of Internet communications. One of the most pressing concerns is the increased vulnerability of

| Protocol | Risk | Impact | Description |
|---|---|---|---|
| **TLS** | Quantum Decryption of Traffic [56] | High: Confidentiality Breach [57] | A quantum attacker could decrypt TLS sessions, exposing sensitive data like passwords, credit card details, and personal information. [58] |
| | Man-in-the-Middle (MITM) Attacks [59] | High: Loss of Data Integrity and Privacy [60] | If digital certificates are compromised, attackers could intercept and alter communications in real-time, affecting trust and data integrity. [60] |
| | Increased Processing Requirements for Quantum-Resistant Algorithms [61] | Moderate: Potential Denial of Service [62] | Implementing quantum-safe algorithms may require more resources, leading to slower processing and potential DoS vulnerabilities. [63] |
| **IPsec** | Unauthorized Network Access [64] | High: Confidentiality and Integrity Breach [65] | Decryption of IPsec Tunnels would expose network traffic, allowing attackers to monitor and manipulate sensitive communications within secured networks. [66] |
| | Network Configuration Exposure [67] | High: Operational Security Risk [68] | Quantum decryption could reveal critical network configurations, enabling attackers to navigate secure network segments and potentially escalate privileges. [69] |
| | DoS from Quantum-Resistant Protocol Overhead [70] | Moderate: Availability Risk [71] | Increased computational demand for quantum-resistant cryptography might strain resources, making IPsec deployments more vulnerable to DoS attacks. [72] |
| **DNSSEC** | DNS Spoofing and Redirecting Traffic [73] | High: Integrity and Availability Breach [65] | With quantum-based attacks, DNSSEC records could be forged, redirecting users to malicious sites and disrupting trust in DNS security. [74] |
| | Exposure of Sensitive DNS Data [75] | Moderate: Confidentiality [76] | Decrypted DNSSEC records could expose data about internal network structures, facilitating further attacks. [77] |
| | DoS due to Performance Overheads with Quantum-Resistant Cryptography [78] | Moderate: System and Network Downtime [79] | Quantum-resistant algorithms could slow DNSSEC operations, increasing vulnerability to DoS attacks and impacting network availability. [80] |

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

the public key infrastructure (PKI) that underpins these protocols. Quantum algorithms, especially Shor's algorithm, threaten to break the cryptographic algorithms that rely on public key encryption, such as RSA and ECC. As quantum computing advances, these vulnerabilities become more critical, and there is an urgent need to develop quantum-resistant cryptographic solutions before malicious actors exploit them.

Confidentiality is another major concern across all three protocols. Quantum decryption techniques could potentially expose sensitive data that was previously secured through traditional encryption methods used in TLS, IPsec, and DNSSEC. This includes personal data, financial transactions, and DNS configurations that are crucial for network security. To mitigate these risks, quantum-safe encryption methods need to be adopted to safeguard privacy. The computational power of quantum machines demands the creation of encryption algorithms that are resistant to quantum decryption, requiring significant advancements in cryptography to keep pace with quantum capabilities. Data integrity and trust are at particular risk, especially for TLS and DNSSEC, which rely heavily on digital signatures and certificates to verify the authenticity of communications and data. Quantum-powered attacks could enable spoofing or man-in-the-middle attacks, where attackers could forge certificates or manipulate DNS responses to redirect users to malicious sites. The ability to maintain data integrity and trust is essential in preventing these types of attacks. Quantum-resistant algorithms must be developed to protect against such threats, ensuring that authentication processes remain secure and that users can trust the systems they rely on. The shift to quantum-resistant cryptography, however, is not without its challenges. These algorithms are likely to impose greater computational demands on the systems using them, which could affect the performance of protocols like IPsec and DNSSEC, both of which require high-speed processing. The increased computational burden could lead to vulnerabilities such as Denial of Service (DoS) attacks, where adversaries could overload systems with processing-heavy operations. Ensuring that quantum-resistant algorithms are optimized for efficiency and scalability is crucial in maintaining protocol performance, especially in real-time network functions. As quantum threats affect multiple aspects of security—confidentiality, integrity, and availability—adopting a multi-layered security approach is vital. A comprehensive defense strategy combining quantum-resistant encryption with additional security controls like network segmentation and continuous monitoring is necessary to mitigate quantum-driven vulnerabilities. This layered defense approach provides robust protection against the broad spectrum of quantum threats that could compromise the security of internet communications. Early adoption of quantum-resistant algorithms is critical to safeguarding sensitive data and communications before quantum technologies mature. Transitioning to quantum-safe encryption now can protect not only future data but also historical data that could be vulnerable to retroactive decryption by quantum systems. High-risk sectors and critical infrastructure should prioritize this transition to ensure long-term security and avoid the vulnerabilities associated with quantum decryption techniques. Table III shows us the comparative risk and impact analysis for widely used protocols.

Finally, the interconnected nature of TLS, IPsec, and DNSSEC means that vulnerabilities in one protocol could have cascading effects on others. For example, a DNSSEC breach could undermine the security of TLS-based web applications, while an IPsec breach could expose data crucial for DNSSEC's integrity. To mitigate these cross-protocol risks, a coordinated and synchronized approach to security across these protocols is necessary. This comprehensive strategy helps protect the entire network infrastructure from quantum-driven threats, ensuring that all protocols remain secure in the face of quantum computing advancements.

## VI. Attack Scenarios for widely used protocols

In this section, we analyze the attack scenarios for widely used protocols.

### A. *Attack Scenarios for TLS*

We explore attack scenarios targeting TLS (Transport Layer Security) to assess the vulnerabilities and impact of quantum-related threats. The focus is on understanding how advancements in quantum computing, particularly quantum decryption techniques, could compromise TLS security by exploiting weaknesses in its cryptographic foundations. Each scenario highlights a distinct quantum threat vector, shedding light on the need for quantum-resistant measures to protect against these emerging risks.

One such scenario involves a Man-in-the-Middle (MITM) attack using quantum-decrypted certificates. In this attack, an adversary intercepts communications between a client and a server and impersonates a legitimate participant. Quantum decryption capabilities could enable attackers to break the asymmetric cryptographic keys used in TLS, such as RSA or ECC. These widely used cryptographic algorithms rely on the assumption that breaking their encryption is computationally infeasible with classical computing methods. However, quantum algorithms like Shor's algorithm could efficiently decrypt the private keys, allowing attackers to forge digital certificates. The emulation involves an attacker intercepting and decrypting TLS certificates in transit, thereby gaining unauthorized access to confidential data. Once the certificates are forged, the attacker can manipulate the data being exchanged, potentially altering messages or injecting malicious content into the communication stream. This type of attack undermines both the confidentiality and integrity of the session, as the attacker can access sensitive information without detection and tamper with the communication flow. This scenario aims to assess the feasibility and impact of a quantum-driven MITM attack on TLS communications. The expected outcome demonstrates how quantum decryption could facilitate certificate forgery, which would allow attackers to manipulate data, impersonate legitimate entities, and compromise session confidentiality and integrity. This highlights the urgency of transitioning to quantum-resistant cryptographic algorithms that can withstand the power of quantum computing, ensuring the continued trustworthiness and security of TLS communications in the quantum era.

Another scenario reproduces a sophisticated eavesdropping attack in which quantum computing capabilities break the encryption key used in a TLS session, enabling attackers to decrypt traffic in real time. In traditional TLS encryption, symmetric algorithms like AES (Advanced Encryption Standard) are employed to protect data during transmission. These algorithms rely on the secrecy of the encryption key, which ensures that only authorized parties can decrypt the data. However, with the advent of quantum computing, attackers can leverage quantum decryption techniques to break these encryption methods much more efficiently than classical computers. In this attack, the focus is on how quantum algorithms, particularly Grover's algorithm, could be used to expedite the process of breaking AES encryption. While Grover's algorithm offers a quadratic speedup over classical brute force methods, it could still significantly reduce the time needed to decrypt encrypted traffic. By intercepting a TLS session, an attacker could use quantum computing to decrypt sensitive data, such as passwords, credit card numbers, personal identification details, and other private information, all without alerting the communicating parties. This breach would compromise confidentiality, as sensitive data would be exposed without the knowledge of the users involved in the communication. The objective of this is to evaluate the threat level and the data exposure risk if quantum decryption techniques were applied to TLS-protected data. The expected outcome of this scenario illustrates how quantum attacks could breach the confidentiality of encrypted communications, underscoring the critical need for quantum-resistant encryption methods. These advanced encryption algorithms must be developed to safeguard data privacy in the quantum computing era, ensuring that encryption remains robust even against quantum-powered decryption techniques. This scenario highlights the urgency for transitioning to quantum-safe encryption protocols to protect against future threats to data confidentiality.

In the third scenario, an attack is downgraded where the attacker forces a TLS session to negotiate and use older, weaker encryption algorithms that are no longer considered secure. The focus here is on legacy cryptographic algorithms, such as RSA-1024, which were once widely used but have since been deemed vulnerable to modern attacks. Specifically, quantum computing's potential to break these older algorithms more efficiently than classical methods presents a serious risk. By emulating quantum decryption attacks on outdated encryption methods like RSA-1024, this scenario highlights the possibility that TLS, due to backward compatibility, could fall back to using these weaker algorithms during the negotiation phase. Quantum algorithms, such as Shor's algorithm, can efficiently factorize large numbers, rendering RSA-1024 particularly susceptible to quantum attacks. If an attacker can exploit this weakness, they can intercept or decrypt data, undermining the security of the TLS session. The objective of this simulation is to understand the risk posed by these downgrade attacks, especially when a protocol such as TLS negotiates encryption standards that include weak backward compatibility. In the face of quantum advancements, legacy encryption methods are highly vulnerable and should no longer be supported. The expected outcome is a demonstration of the importance of eliminating deprecated algorithms from TLS configurations. By ensuring that the protocol no longer supports weak encryption methods such as RSA-1024, the overall security of TLS can be reinforced. This scenario emphasizes the need for the adoption of quantum-resistant cryptographic algorithms, which makes TLS more resilient to quantum-based attacks and ensure that backward compatibility does not introduce new vulnerabilities into the system.

The final scenario explores the potential performance degradation of TLS servers when quantum-resistant algorithms are implemented, focusing on the risk of Denial of Service (DoS) attacks. Quantum-resistant cryptographic algorithms, designed to withstand the capabilities of quantum computing, are expected to require significantly more computational resources than current cryptographic techniques. As a result, this increased demand could overwhelm systems not optimized for these new algorithms, leading to a slowdown or even complete service disruption. In this, the attacker targets a TLS server by sending an overwhelming number of requests that are resource-intensive due to the increased cryptographic load of quantum-resistant encryption. The goal is to evaluate how the server manages its computational resources when faced with a flood of these requests. By emulating this scenario, we assess whether the TLS server's performance can withstand the added strain and continue to function effectively. The objective of this simulation is to determine the impact of quantum-resistant encryption on server performance, particularly under high load. As quantum-resistant algorithms are expected to be more computationally demanding, this scenario tests whether TLS servers can continue to operate efficiently without being susceptible to DoS attacks that exploit these increased resource requirements. The expected outcome of this scenario is a demonstration of potential availability issues arising from the adoption of quantum-resistant cryptography. It highlights the need for a careful balance between security and performance when implementing quantum-resistant algorithms in TLS. To avoid performance bottlenecks and ensure system availability, it is crucial for TLS implementations to optimize quantum-safe encryption techniques, ensuring they can handle high traffic volumes without succumbing to DoS attacks.

### *B. Attack Scenarios for IPsec*

This section examines the potential 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 highlight the specific risks posed by quantum computing to IPsec's security, including confidentiality, integrity, and availability.

The first scenario is where the quantum adversary leverages advanced decryption techniques to break the encryption protocols commonly used in IPsec, such as the Diffie-Hellman key exchange and RSA encryption. Quantum computing's potential to solve mathematical problems much faster than classical computers enables attackers to decrypt IPsec packets that were previously secure. The decryption process involves breaking the cryptographic keys used to protect data transmitted over VPNs and other secure communication channels. By bypassing these encryption measures, attackers can gain unauthorized access to sensitive information, compromising the privacy of data in transit. The objective of this analysis is to assess the potential risk of IPsec's current encryption standards becoming obsolete in the face of quantum decryption. Given the power of quantum computing to efficiently solve mathematical problems that underlie traditional encryption algorithms, it's critical to evaluate whether the cryptographic techniques used in IPsec withstands quantum attacks. The expected outcome of this scenario reveals that quantum capabilities could easily break existing encryption methods, allowing attackers to expose private communications and sensitive data flow. This underscores the need for the development and adoption of quantum-resistant encryption techniques, particularly quantum-safe key exchange methods, to ensure the continued confidentiality and integrity of IPsec-secured communications.

In another scenario, the quantum decryption capabilities of an attacker are used to break the digital signatures that IPsec relies on to authenticate communication parties. Digital signatures are a key component of IPsec's security mechanism, assuring that the entities involved in a communication session are legitimate. However, with the advent of quantum decryption, attackers could easily forge these signatures, making it possible to impersonate a trusted entity. The attacker could then intercept an ongoing IPsec session, manipulate the data packets being transmitted, and insert malicious data into the communication stream by exploiting the forged authentication credentials. The objective of this analysis is to evaluate how the decryption of authentication keys using quantum techniques could undermine the integrity of IPsec. By breaking the cryptographic keys that underpin the authentication process, quantum-enabled attackers would have the ability to disrupt the trustworthiness of an IPsec session. This would allow them to covertly manipulate secure communications, undetected by the legitimate participants. The expected outcome of this scenario highlights the potential risks to data integrity in IPsec communications. It demonstrates that quantum decryption could enable attackers to compromise data integrity, disrupt secure connections, and manipulate information without raising any alarms, thus severely undermining the trust and security that IPsec provides in protecting network traffic.

In the third scenario, attackers leverage quantum decryption techniques to break the session keys used in IPsec, enabling them to execute a replay attack. A replay attack occurs when an attacker captures legitimate data packets from a secure communication session and retransmits them to trick the receiving system into acting on outdated or manipulated information. By decrypting the session keys, the attacker can easily access and manipulate the captured data packets, injecting them back into the IPsec stream. This could lead to confusion or manipulation of the receiving system, which would interpret the replayed data as valid, potentially leading to malicious actions or disruptions. The objective of this analysis is to assess the feasibility of replay attacks under the influence of quantum decryption. Quantum computing has the potential to break the encryption mechanisms securing session keys, allowing adversaries to intercept and replay data without detection. The expected outcome of this investigation highlights vulnerabilities in both data integrity and session management within IPsec, underscoring the importance of incorporating quantum-resistant techniques. Specifically, nonce-based methods could be employed to prevent replay attacks, as nonces ensure that data packets are not reused inappropriately, protecting against potential quantum-enabled replays. This reinforces the need for updated, quantum-secure protocols to safeguard the integrity of data and session continuity.

In the final scenario, the increased computational demands of quantum-resistant encryption methods could make IPsec more susceptible to Denial of Service (DoS) attacks. As quantum-resistant algorithms require more processing power and resources to execute, attackers could exploit these increased demands by overloading the IPsec server with resource-intensive cryptographic requests. This overload would exhaust the system's resources, potentially leading to performance degradation or complete service interruptions. The attacker could send a flood of requests that require substantial computational work to be processed, testing the IPsec server's ability to maintain service and performance under high cryptographic loads. The objective of this scenario is to evaluate IPsec's availability and performance when subjected to the increased computational demands of quantum-resistant encryption. The expected outcome highlights the potential for bottlenecks in performance or service disruption, illustrating the need for optimized and efficient quantum-resistant encryption algorithms. These optimized algorithms would need to strike a balance between ensuring quantum security and maintaining IPsec's high availability, thus preventing the system from becoming vulnerable to DoS attacks due to excessive resource consumption. This underscores the importance of designing encryption methods that are both secure against quantum threats and efficient in their computational requirements, ensuring robust network performance even under load.

### C. Attack Scenarios for DNSSEC

In this section, we examine the 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 demonstrate the potential risks and help identify areas for enhancing DNSSEC's resilience.

In the first scenario, DNSSEC's reliance on digital signatures to authenticate DNS records makes it vulnerable to quantum decryption attacks. These signatures are based on public-key cryptography, which quantum computers could potentially break using advanced decryption algorithms. This would allow an attacker to intercept DNS responses, decrypt the digital signatures, and forge valid-looking DNS records. By manipulating these records, the attacker could redirect users to fraudulent websites or otherwise alter DNS information, compromising the integrity of DNSSEC.The objective of this scenario is to assess the risks posed by quantum decryption of DNSSEC signatures, specifically in enabling DNS spoofing attacks. The expected outcome demonstrates how quantum decryption could facilitate the forgery of DNSSEC signatures, leading to the manipulation of DNS records. Such attacks could have serious consequences, including the redirection of users to malicious sites, theft of sensitive information, or the spread of malware. This scenario underscores the critical need for quantum-resistant cryptographic signatures in DNSSEC to protect the integrity and trustworthiness of DNS systems in the future.

In this scenario, cache poisoning is explored as a potential threat to DNSSEC under quantum decryption conditions. Cache poisoning occurs when an attacker injects false DNS data into a DNS resolver's cache, causing the resolver to store and potentially serve incorrect DNS records. With quantum decryption, adversaries would have the ability to forge DNSSEC responses by decrypting the cryptographic signatures used to verify DNS records. This enables attackers to insert malicious records into the cache, tricking DNS resolvers into accepting and storing falsified data. The objective of this scenario is to examine the potential for large-scale cache poisoning attacks facilitated by quantum decryption techniques. If attackers can inject incorrect or malicious DNS records into the resolver's cache, they can redirect users to harmful sites or intercept communications, effectively manipulating the integrity of the DNS system. The expected outcome reveals how quantum decryption could make DNSSEC vulnerable to such attacks, emphasizing the need for stronger, quantum-resistant verification methods to prevent widespread DNS manipulations and maintain trust in DNSSEC systems. The scenario highlights the necessity of preparing DNS systems for quantum threats to ensure continued protection against cache poisoning attacks.

In another scenario, the focus is on a downgrade attack that targets DNSSEC by exploiting its support for multiple cryptographic algorithms, some of which are weaker and more susceptible to quantum attacks. DNSSEC typically supports a variety of algorithms, with some legacy algorithms, such as RSA-1024, being far more vulnerable to the computational power of quantum decryption techniques. An attacker could exploit this weakness by forcing the DNSSEC protocol to fall back to these less secure, outdated algorithms. With quantum decryption capabilities, the attacker could easily break the weaker cryptography, exposing the DNSSEC infrastructure to further vulnerabilities. The objective of this scenario is to assess the risk posed by such quantum-enabled downgrade attacks. If DNSSEC is coerced into using obsolete cryptographic standards, it significantly weakens the overall security of the system. By leveraging quantum decryption to break weaker algorithms, attackers could potentially intercept or manipulate DNS traffic, undermining the trust and integrity that DNSSEC is designed to provide. The expected outcome of this scenario emphasizes the vulnerabilities introduced when outdated cryptographic standards are used, underlining the importance of phasing out legacy algorithms and adopting quantum-resistant protocols across all DNSSEC transactions to prevent such attacks. The scenario highlights the critical need for modernizing cryptographic practices to withstand quantum threats and ensure the continued security of DNSSEC.

In the final scenario, the adoption of quantum-resistant algorithms in DNSSEC introduces a significant challenge related to increased computational requirements. These algorithms, designed to protect against quantum decryption, demand considerably more processing power than current cryptographic methods. This strain on resources can potentially expose DNS servers to Denial of Service (DoS) attacks, where the server is overwhelmed by a high volume of resource-intensive DNSSEC queries. The test here is to understand how well DNS servers can handle such high computational loads while maintaining their availability and performance. The goal of this assessment is to evaluate whether DNS servers can continue to operate effectively under the increased cryptographic demands posed by quantum-resistant algorithms. If DNS servers cannot handle these demands efficiently, it could lead to service disruptions, with performance bottlenecks or even complete service outages. This scenario underscores the need for optimized, efficient quantum-resistant algorithms that can safeguard DNSSEC against quantum attacks without compromising the server's ability to maintain availability. Therefore, ensuring that quantum-resistant protocols are both secure and efficient is essential to the future of DNS security.

### D. *Comparative Results from STRIDE and PASTA Models*

The comparative analysis of STRIDE and PASTA models below ( IV ) highlights their distinct approaches to threat modeling, emphasizing their strengths and limitations in addressing security challenges, including quantum threats.

| Criteria | STRIDE Model | PASTA Model |
|---|---|---|
| **Approach and Focus** | Threat-based, focusing on categorizing threats by type (e.g., Spoofing, Tampering). [81] | Process-based, analyzing each phase of an attack lifecycle, from reconnaissance to exploitation and impact assessment. [82] |
| **TLS Key Insights** | Identifies risks like Information Disclosure due to quantum decryption. [83] | Highlights vulnerabilities in reconnaissance and exploitation phases due to quantum decryption of session keys. [84] |
| | Notes spoofing and tampering risks from compromised certificates. [85] | Emphasizes potential for persistent access to decrypted sessions in the post-exploitation phase. [86] |
| **IPsec Key Insights** | Highlights Information Disclosure and Elevation of Privilege risks via quantum decryption of IPsec channels. [80] | Shows initial exploitation phase vulnerabilities through interception of encrypted data. [87] |
| | | Impact analysis phase reveals risks of widespread data leaks if channels are decrypted. [88] |
| **DNSSEC Key Insights** | Identifies Spoofing and Tampering as a major risk from quantum-decrypted digital signatures. [89] | The escalation and exploitation phases show how attackers could redirect traffic through altered DNS records. [75] |
| | | Impact assessment phase shows potential for large-scale DNS manipulation. [90] |
| **Depth of Analysis** | Provides high-level threat categorization, useful for broad quantum risk identification. [87] | Offers detailed insights into attack stages, useful for complex scenario simulation and impact assessment. [91] |
| **Attack Lifecycle Analysis** | Focuses on categorizing threats without a step-by-step attack lifecycle breakdown. [92] | Provides a comprehensive view across the attack lifecycle stages, revealing phase-specific vulnerabilities. [93] |
| **Risk Identification** | Efficient for quickly identifying types of quantum-related threats in each protocol. [94] | Suited for simulating detailed attack scenarios and understanding attack evolution. [95] |
| **Overall Usefulness** | Useful for summarizing quantum risks across protocols and identifying broad vulnerabilities. [96] | Effective for in-depth attack progression analysis and understanding quantum attack feasibility at each stage. [97] |
| **Best Use Case** | Quick categorization of threats, ideal for a high-level overview. [98] | Detailed attack simulation and phased threat analysis, ideal for deeper investigation into specific vulnerabilities. [99] |

TABLE IV: **STRIDE VS. PASTA**

## VII. Mitigation Strategies and Recommendations

This section provides a detailed discussion of the various solutions and strategies to solve the threats followed by recommendations for them, respectively.

### 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 table V below contains the mitigation strategies focusing on protecting the confidentiality, integrity, and authenticity of TLS communications.

| Mitigation Area | Strategy | Details |
|---|---|---|
| [100]<br>**Transition to Post-Quantum Cryptography** | Implementation of Quantum-Resistant Algorithms. [101] | Replace RSA and ECC with NIST-recommended post-quantum cryptographic algorithms to secure key exchange and encryption in TLS. [102] |
| | Hybrid Cryptography [103] | Use hybrid cryptographic solutions that combine traditional and quantum-resistant algorithms to provide dual layers of security during the transition phase. [104] |
| [105]<br>**Enhancing Key Management Practices** | Shorten Key Lifespans [106] | Reduce key lifespans to limit the potential for retrospective decryption by quantum attackers. [107] |
| | Forward Secrecy Implementation [108] | Ensure TLS sessions use forward secrecy so that past session data remains secure even if session keys are compromised in the future. [108] |
| [109]<br>**Protocol Updates and Version Control** | Adopt TLS 1.3 [110] | Implement TLS 1.3, which features stronger encryption algorithms and a simplified handshake process to reduce quantum-related vulnerabilities. [110] |
| | Regular Patch Management [111] | Ensure timely updates and patches for TLS libraries to address vulnerabilities that may be exploited by classical or quantum attacks. [111] |
| [112]<br>**Use of Extended Validation Certificates and Certificate Transparency** | Extended Validation (EV) Certificates [113] | Use EV certificates to enhance domain identity verification and reduce the risk of impersonation. [113] |
| | Certificate Transparency [114] | Utilize certificate transparency logs to detect and respond to unauthorized or forged certificates, ensuring only valid certificates are trusted. [114] |
| [115]<br>**Strengthening Network and Server Configurations** | Strict Cipher Suite Policies [116] | Enforce strict policies to avoid outdated or weak cipher suites and mandate the use of strong, quantum-resistant options. [117] |
| | Secure Server Configurations [118] | Configure servers to reject insecure connections, require strong authentication and restrict access to trusted networks and devices to prevent unauthorized decryption. [118] |

TABLE V: **Mitigation Strategies for TLS against Quantum Threats**

### B. Mitigation Recommendations 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. The table VI below outlines the effective mitigation strategies for safeguarding IPsec from quantum-enabled threats.

| Mitigation Area | Strategy | Details |
|---|---|---|
| [119]<br>**Quantum-Resistant Cryptography** | Post-Quantum Algorithms [120] | Replace RSA and ECC with NIST-recommended post-quantum algorithms to secure key exchanges and data protection. [121] |
| | Hybrid Cryptography for Key Exchange [122] | Utilize hybrid systems combining traditional and quantum-resistant encryption until fully standardized quantum algorithms are implemented. [123] |
| [124]<br>**Enhanced Key Management and Forward Secrecy** | Shortened Key Lifespans [106] | Minimize key lifespans for sessions involving sensitive data to reduce the risk of future quantum decryption. [107] |
| | Perfect Forward Secrecy (PFS) [108] | Configure IPsec to support PFS, ensuring session keys are independently generated so past sessions remain secure even if a key is compromised. [125] |
| [116]<br>**Protocol and Cipher Suite Updates** | Adopt the Latest IPsec Standards [126] | Update protocols like IKEv2 and ESP with strong, secure cryptographic suites to mitigate known vulnerabilities. [127] |
| | Use Strong Cipher Suites Only [117] | Disable weak or outdated cipher suites and implement quantum-resistant options to limit legacy encryption use. [117] |
| [128]<br>**Enhanced Authentication Mechanisms** | Mutual Authentication [129] | Require mutual authentication to ensure both endpoints verify each other's identities, reducing quantum-induced spoofing risks. [129] |
| | Certificate Transparency and Monitoring [114] | Utilize certificate transparency logs to detect unauthorized or forged certificates, ensuring only validated ones are trusted during communications. [114] |
| [130]<br>**Network and Endpoint Security** | Network Segmentation [131] | Segment networks and restrict access to sensitive IPsec connections to limit the spread and impact of compromised communications. [131] |
| | Endpoint Hardening [132] | Patch and update endpoints involved in IPsec communications to reject insecure connections and prevent unauthorized decryption attempts. [132] |

TABLE VI: **Mitigation Strategies for IPSec against Quantum Threats**

### C. Mitigation Recommendations 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. The following table VII outlines strategies to mitigate quantum threats to DNSSEC.

| Mitigation Area | Strategy | Details |
|---|---|---|
| [133]<br>**Transition to Post-Quantum Cryptographic Algorithms** | Adopt Quantum-Resistant Algorithms [134] | Replace RSA and ECC digital signatures used in DNSSEC with NIST-recommended post-quantum algorithms to ensure DNS data authenticity against quantum-enabled attacks. [134] |
| | Use Hybrid Cryptographic Approaches [135] | Until fully standardized post-quantum algorithms are available, implement hybrid cryptographic solutions combining traditional and quantum-resistant algorithms to protect DNSSEC. [135] |
| [136]<br>**Strengthening Key Management Practices** | Frequent Key Rotations [137] | Implement shorter key rotation periods for DNSSEC signing keys to limit the window of quantum attack exposure and reduce the impact of any compromised keys over time. [137] |
| | ZSK and KSK Separation [138] | Use separate Zone Signing Keys (ZSKs) and Key Signing Keys (KSKs) for added security. Rotate ZSKs regularly while maintaining secure KSK rotation schedules to minimize quantum risk. [138] |
| [139]<br>**Enhanced Validation and Monitoring** | Enable Strict Validation Policies [140] | Configure DNS resolvers to enforce DNSSEC validation, rejecting unsigned or improperly signed records to protect against spoofed responses. [140] |
| | DNSSEC Log Monitoring [139] | Monitor DNSSEC logs regularly to identify unusual activities such as unauthorized key changes or invalid DNS responses, which may indicate quantum-enabled attacks. [139] |
| **Deployment of Multi-Layered Security and Redundancy** | Implement DNS firewall rules [141] | Implement DNS firewall rules to block malicious or suspicious DNS queries, preventing exploitation of DNSSEC vulnerabilities even if signatures are compromised. [141] |
| | Use DNSSEC-Enabled Redundant DNS Servers [142] | Deploy redundant DNS servers with DNSSEC capabilities to ensure availability and consistency of DNS records, reducing risks if one server's keys are compromised. [142] |
| **Implementing DNS Query Rate Limiting and Anomaly Detection** | Rate Limiting on DNS Queries [143] | Set rate limits on DNS queries to prevent attackers from flooding DNS servers with spoofed queries or manipulating responses. [143] |
| | Anomaly Detection Systems [144] | Use anomaly detection tools to identify irregular DNS query patterns (e.g., sudden spikes), which could signal quantum-driven DNS attacks or other malicious activities. [144] |

TABLE VII: **Mitigation Strategies for DNSSEC against Quantum Threats**

### 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 comparative study VIII below provides comprehensive recommendations applicable across these protocols, focusing on quantum-resistant cryptography, robust key management, and layered security measures to effectively mitigate risks.

| Mitigation Area | Recommendations | Details |
|---|---|---|
| [133]<br>**Quantum-Resistant Cryptography** | Adopt Post-Quantum Algorithms. [134] | Standardize NIST-recommended post-quantum cryptographic algorithms to replace RSA and ECC, ensuring secure key exchanges, signatures, and encryption. [134] |
| | Hybrid Cryptographic Models [135] | Implement hybrid models combining current encryption with quantum-resistant algorithms during the transition to post-quantum standards. [135] |
| **Key Management Practices** | Regular Key Rotations [137] | Rotate cryptographic keys frequently to minimize exposure to quantum decryption, especially for sensitive data and long sessions. [137] |
| | Forward Secrecy Protocols [108] | Enable forward secrecy mechanisms to ensure past session data remains secure even if a key is compromised. [145] |
| **Protocol and Cipher Suite Updates** | Enforce Strong Cipher Suites [116] | Disable outdated or weak cipher suites (e.g., SHA-1, MD5) and adopt robust quantum-resistant cipher suites. [146] |
| | Mandatory Protocol Updates [126] | Use the latest protocol versions (e.g., TLS 1.3, IKEv2 for IPsec) to benefit from enhanced security and reduced attack surfaces. [127] |
| **Authentication Mechanisms** | Two-Factor Authentication (2FA) [147] | Implement 2FA across TLS, IPsec, and DNSSEC to mitigate quantum-based spoofing attacks. [147] |
| | Enhanced Certificate Transparency [148] | Adopt certificate transparency to detect unauthorized or forged certificates vulnerable to quantum decryption attacks. [148] |
| **Multi-Layered Security and Redundancy** | Segmented Network Design [149] | Segment networks to isolate critical infrastructure, reducing risks of quantum-powered breaches spreading across systems. [149] |
| | DNS and IP Redundancy [150] | Use redundant DNS and IP routes with DNSSEC and IPsec protocols to maintain continuity during quantum-related attacks. [150] |
| **Continuous Monitoring and Threat Intelligence** | Unified Threat Detection Systems [151] | Employ anomaly detection and intrusion detection systems (IDS) to monitor quantum-related vulnerabilities or anomalies (e.g., unusual certificate activity). [151] |

TABLE VIII: **Mitigation Strategies for Cross-Protocol against Quantum Threats**

## VIII. Conclusion and Future Work

This paper examines the evolving quantum threat landscape for critical network security protocols—TLS, IPsec, and DNSSEC—using the STRIDE and PASTA threat modeling frameworks. The analysis highlights the significant vulnerabilities of these protocols to quantum computing, primarily due to their capability to break asymmetric cryptographic algorithms such as RSA, ECC, and DH, which are foundational to key exchange and encryption mechanisms. Through STRIDE, the research provides a protocol-specific assessment of vulnerabilities across six dimensions, while PASTA emphasizes the practical feasibility of attacks and aligns mitigation strategies with real-world scenarios. A comparative analysis reveals that TLS and IPsec are particularly susceptible to breaches in confidentiality and integrity, whereas DNSSEC faces critical challenges in maintaining authenticity. Simulated quantum attack scenarios further underscore vulnerabilities such as compromised TLS handshakes, intercepted IPsec VPN traffic, and forged DNSSEC signatures, illustrating the urgency of adopting post-quantum cryptography, hybrid cryptographic models, and robust key management practices. The paper proposes cross-protocol mitigation strategies to enhance resilience and offers a roadmap for future research. Key recommendations include integrating post-quantum cryptographic algorithms, deploying hybrid models, and exploring Quantum Key Distribution (QKD) for enhanced security. Furthermore, the study advocates for the development of standardized frameworks, large-scale quantum attack simulations, and leveraging AI and ML for real-time threat detection and response. These measures are critical to ensuring secure communication and robust digital infrastructure in the quantum computing 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*. IEEE, 2022, pp. 1–5.

[2] D. Bellizia, N. El Mrabet, A. P. Fournaris, S. Pontié, F. Regazzoni, F.-X. Standaert, É. Tasso, and E. Valea, "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)*. IEEE, 2021, pp. 1–6.

[3] K. F. Hasan, L. Simpson, M. A. R. Baee, C. Islam, Z. Rahman, W. Armstrong, P. Gauravaram, and M. McKague, "A framework for migrating to post-quantum cryptography: Security dependency analysis and case studies," *IEEE Access*, 2024.

[4] E. Zeydan, Y. Turk, B. Aksoy, and S. B. Ozturk, "Recent advances in post-quantum cryptography for networks: A survey," in *2022 Seventh International Conference On Mobile And Secure Services (MobiSecServ)*. IEEE, 2022, pp. 1–8.

[5] S. Ambika, V. Balaji, R. T. Rajasekaran, P. 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)*, vol. 5. IEEE, 2024, pp. 1603–1607.

[6] M. Kumar and P. Pattnaik, "Post quantum cryptography (pqc)-an overview," in *2020 IEEE High Performance Extreme Computing Conference (HPEC)*. IEEE, 2020, pp. 1–9.

[7] D. Herzinger, S.-L. Gazdag, and D. Loebenberger, "Real-world quantum-resistant ipsec," in *2021 14th International Conference on Security of Information and Networks (SIN)*, vol. 1. IEEE, 2021, pp. 1–8.

[8] 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*. IEEE, 2022, pp. 1–5.

[9] H. Bhatt and S. Gautam, "Quantum computing: A new era of computer science," in *2019 6th International Conference on Computing for Sustainable Global Development (INDIACom)*. IEEE, 2019, pp. 558–561.

[10] K. F. Hasan, L. Simpson, M. A. R. Baee, C. Islam, Z. Rahman, W. Armstrong, P. Gauravaram, and M. McKague, "A framework for migrating to post-quantum cryptography: Security dependency analysis and case studies," *IEEE Access*, 2024.

[11] L. Chen, L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. A. Perlner, and D. Smith-Tone, *Report on post-quantum cryptography*. US Department of Commerce, National Institute of Standards and Technology . . . , 2016, vol. 12.

[12] M. Kumar and P. Pattnaik, "Post quantum cryptography (pqc)-an overview," in *2020 IEEE High Performance Extreme Computing Conference (HPEC)*. IEEE, 2020, pp. 1–9.

[13] D. Herzinger, S.-L. Gazdag, and D. Loebenberger, "Real-world quantum-resistant ipsec," in *2021 14th International Conference on Security of Information and Networks (SIN)*, vol. 1. IEEE, 2021, pp. 1–8.

[14] A. Knight, *Hacking connected cars: Tactics, techniques, and procedures*. John Wiley & Sons, 2020.

[15] K. Balamurugan *et al.*, "An analysis of various cyber threat modeling," in *2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS)*. IEEE, 2023, pp. 426–429.

[16] K. Sentamilselvan, P. Suresh, G. Kamalam, H. Muthukrishnan, K. Logeswaran, and P. Keerthika, "Security threats and privacy challenges in the quantum blockchain: A contemporary survey," *Quantum Blockchain: An Emerging Cryptographic Paradigm*, pp. 293–316, 2022.

[17] U. I. Atmaca, C. Maple, G. Epiphaniou *et al.*, "Challenges in threat modelling of new space systems: A teleoperation use-case," *Advances in Space Research*, vol. 70, no. 8, pp. 2208–2226, 2022.

[18] S. K. Khan, N. Shiwakoti, P. Stasinopoulos, and Y. Chen, "Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions," *Accident Analysis & Prevention*, vol. 148, p. 105837, 2020.

[19] L. Zhang, A. Taal, R. Cushing, C. de Laat, and P. Grosso, "A risk-level assessment system based on the stride/dread model for digital data marketplaces," *International Journal of Information Security*, pp. 1–17, 2022.

[20] P. Das, M. R. A. Asif, S. Jahan, K. Ahmed, F. M. Bui, and R. Khondoker, "Stride-based cybersecurity threat modeling, risk assessment and treatment of an in-vehicle infotainment system," *Vehicles*, vol. 6, no. 3, pp. 1140–1163, 2024.

[21] 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*. IEEE, 2022, pp. 1–5.

[22] L. Chen, L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. A. Perlner, and D. Smith-Tone, *Report on post-quantum cryptography*. US Department of Commerce, National Institute of Standards and Technology . . . , 2016, vol. 12.

[23] M. Benli, E. Özcan, and U. Türeli, "A custom key-value store hardware on fpga for ipsec protocol," in *2020 12th International Conference on Electrical and Electronics Engineering (ELECO)*. IEEE, 2020, pp. 150–154.

[24] R. Rahul, S. Geetha, S. Priyatharsini, K. Mehata, T. Sundaresan Perumal, N. Ethiraj, and S. Sendilvelan, "Cybersecurity issues and challenges in quantum computing," *Topics in Artificial Intelligence Applied to Industry 4.0*, pp. 203–221, 2024.

[25] G. Beernink, "Taking the quantum leap: Preparing dnssec for post quantum cryptography," Master's thesis, University of Twente, 2022.

[26] A. Shostack, *Threat modeling: Designing for security*. John Wiley & Sons, 2014.

[27] S. Myagmar, A. J. Lee, and W. Yurcik, "Threat modeling as a basis for security requirements," 2005.

[28] T. UcedaVelez and M. M. Morana, "Intro to pasta," 2015.

[29] ——, *Risk Centric Threat Modeling: process for attack simulation and threat analysis*. John Wiley & Sons, 2015.

[30] D. Bellizia, N. El Mrabet, A. P. Fournaris, S. Pontié, F. Regazzoni, F.-X. Standaert, É. Tasso, and E. Valea, "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)*. IEEE, 2021, pp. 1–6.

[31] P. Bhatia and R. Sumbaly, “Framework for wireless network security using quantum cryptography,” *arXiv preprint arXiv:1412.2495*, 2014.

[32] U. Maurer, “Modelling a public-key infrastructure,” in *Computer Security—ESORICS 96: 4th European Symposium on Research in Computer Security Rome, Italy, September 25–27, 1996 Proceedings 4*. Springer, 1996, pp. 325–350.

[33] L. Chen, L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. A. Perlner, and D. Smith-Tone, *Report on post-quantum cryptography*. US Department of Commerce, National Institute of Standards and Technology . . . , 2016, vol. 12.

[34] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM review*, vol. 41, no. 2, pp. 303–332, 1999.

[35] D. Boneh and V. Shoup, “A graduate course in applied cryptography,” *Draft 0.5*, 2020.

[36] V. Mavroeidis, K. Vishi, M. D. Zych, and A. Jøsang, “The impact of quantum computing on present cryptography,” *arXiv preprint arXiv:1804.00200*, 2018.

[37] P. N. Kokare, D. Vora, S. Patil, K. Kotecha, V. Khairnar, and T. Choudhury, “Post quantum cryptography: A survey of past and future.”

[38] O. S. Althobaiti and M. Dohler, “Cybersecurity challenges associated with the internet of things in a post-quantum world,” *Ieee Access*, vol. 8, pp. 157 356–157 381, 2020.

[39] Y. Baseri, V. Chouhan, and A. Hafid, “Navigating quantum security risks in networked environments: A comprehensive study of quantum-safe network protocols,” *Computers & Security*, p. 103883, 2024.

[40] V. Mavroeidis, K. Vishi, M. D. Zych, and A. Jøsang, “The impact of quantum computing on present cryptography,” *arXiv preprint arXiv:1804.00200*, 2018.

[41] P. S. Emmanni, “The impact of quantum computing on cybersecurity,” *Journal of Mathematical & Computer Applications*, vol. 2, no. 2, pp. 1–4, 2023.

[42] F. Cavaliere, J. Mattsson, and B. Smeets, “The security implications of quantum cryptography and quantum computing,” *Network Security*, vol. 2020, no. 9, pp. 9–15, 2020.

[43] Y. Baseri, V. Chouhan, and A. Hafid, “Navigating quantum security risks in networked environments: A comprehensive study of quantum-safe network protocols,” *Computers & Security*, p. 103883, 2024.

[44] M. S. Akter, J. Rodriguez-Cardenas, H. Shahriar, A. Cuzzocrea, and F. Wu, “Quantum cryptography for enhanced network security: A comprehensive survey of research, developments, and future directions,” in *2023 IEEE International Conference on Big Data (BigData)*. IEEE, 2023, pp. 5408–5417.

[45] P. W. Shor, “Algorithms for quantum computation: discrete logarithms and factoring,” in *Proceedings 35th annual symposium on foundations of computer science*. Ieee, 1994, pp. 124–134.

[46] O. S. Althobaiti and M. Dohler, “Cybersecurity challenges associated with the internet of things in a post-quantum world,” *Ieee Access*, vol. 8, pp. 157 356–157 381, 2020.

[47] G. Alagic, G. Alagic, D. Apon, D. Cooper, Q. Dang, T. Dang, J. Kelsey, J. Lichtinger, Y.-K. Liu, C. Miller *et al.*, “Status report on the third round of the nist post-quantum cryptography standardization process,” 2022.

[48] S. W. S. Pan, D. D. N. Nguyen, R. Doss, W. Armstrong, P. Gauravaram *et al.*, “Double-signed fragmented dnssec for countering quantum threat,” *arXiv preprint arXiv:2411.07535*, 2024.

[49] M. Müller, J. de Jong, M. van Heesch, B. Overeinder, and R. van Rijswijk-Deij, “Retrofitting post-quantum cryptography in internet protocols: a case study of dnssec,” *ACM SIGCOMM Computer Communication Review*, vol. 50, no. 4, pp. 49–57, 2020.

[50] Y. Baseri, V. Chouhan, and A. Ghorbani, “Cybersecurity in the quantum era: Assessing the impact of quantum computing on infrastructure,” *arXiv preprint arXiv:2404.10659*, 2024.

[51] R. A. Jowarder and S. Jahan, “Quantum computing in cyber security: Emerging threats, mitigation strategies, and future implications for data protection,” *World Journal of Advanced Engineering Technology and Sciences*, vol. 13, no. 1, pp. 330–339, 2024.

[52] G. Schmid, “Thirty years of dns insecurity: Current issues and perspectives,” *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2429–2459, 2021.

[53] P. Rodriguez, *Perceptions of IT Decision-Makers on the Use of Domain Name System Security Extension (DNSSEC): Qualitative Exploratory Case Study*. University of Phoenix, 2020.

[54] J. P. Mattsson, B. Smeets, and E. Thormarker, “Quantum-resistant cryptography,” *arXiv preprint arXiv:2112.00399*, 2021.

[55] L. Malina, P. Dobias, J. Hajny, and K.-K. R. Choo, “On deploying quantum-resistant cybersecurity in intelligent infrastructures,” in *Proceedings of the 18th International Conference on Availability, Reliability and Security*, 2023, pp. 1–10.

[56] A. AlMudaweb and W. Elmedany, “Securing smart cities in the quantum era: challenges, solutions, and regulatory considerations,” 2023.

[57] K. Blightman, S. Griffiths, and C. Danbury, “Patient confidentiality: when can a breach be justified?” *Continuing Education in Anaesthesia, Critical Care & Pain*, vol. 14, no. 2, pp. 52–56, 2014.

[58] S. Wang, C. Adams, and A. Broadbent, “Password authentication schemes on a quantum computer,” in *2021 IEEE International Conference on Quantum Computing and Engineering (QCE)*. IEEE, 2021, pp. 346–350.

[59] B. Bhushan, G. Sahoo, and A. K. Rai, “Man-in-the-middle attack in wireless and computer networking—a review,” in *2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)(Fall)*. IEEE, 2017, pp. 1–6.

[60] E. Pina, J. Ramos, H. Jorge, P. Váz, J. Silva, C. Wanzeller, M. Abbasi, and P. Martins, “Data privacy and ethical considerations in database management,” *Journal of Cybersecurity and Privacy*, vol. 4, no. 3, pp. 494–517, 2024.

[61] G. Alagic, G. Alagic, J. Alperin-Sheriff, D. Apon, D. Cooper, Q. Dang, Y.-K. Liu, C. Miller, D. Moody, R. Peralta *et al.*, “Status report on the first round of the nist post-quantum cryptography standardization process,” 2019.

[62] V. D. M. Rios, P. R. Inácio, D. Magoni, and M. M. Freire, “Detection and mitigation of low-rate denial-of-service attacks: A survey,” *IEEE Access*, vol. 10, pp. 76 648–76 668, 2022.

[63] N. Vishnu, R. S. Batth, and G. Singh, “Denial of service: types, techniques, defence mechanisms and safe guards,” in *2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*. IEEE, 2019, pp. 695–700.

[64] E. G. AbdAllah, M. Zulkernine, and H. S. Hassanein, “Preventing unauthorized access in information centric networking,” *Security and Privacy*, vol. 1, no. 4, p. e33, 2018.

[65] M. Rijah, “Security analysis, threats, & challenges in database,” 2021.

[66] J. Luo and Q. Ji, “Password acquisition and traffic decryption based on l2tp/ipsec,” in *2020 IEEE 20th International Conference on Communication Technology (ICCT)*. IEEE, 2020, pp. 1567–1571.

[67] Y.-P. Lai and P.-L. Hsia, “Using the vulnerability information of computer systems to improve the network security,” *Computer Communications*, vol. 30, no. 9, pp. 2032–2047, 2007.

[68] G. C. Wilshusen, M. Gilmore, A. Lawrence, K. C. Dorsey, L. A. McCracken, and G. A. O. W. DC, “Cybersecurity: Threats impacting the nation,” *United States Government Accountability Office*, p. 3, 2012.

[69] M. S. Akter, J. Rodriguez-Cardenas, H. Shahriar, A. Cuzzocrea, and F. Wu, “Quantum cryptography for enhanced network security: A comprehensive survey of research, developments, and future directions,” in *2023 IEEE International Conference on Big Data (BigData)*. IEEE, 2023, pp. 5408–5417.

[70] D. Sikeridis, P. Kampanakis, and M. Devetsikiotis, “Assessing the overhead of post-quantum cryptography in tls 1.3 and ssh,” in *Proceedings of the 16th International Conference on emerging Networking EXperiments and Technologies*, 2020, pp. 149–156.

[71] B. Kumar, V. Sridhar, and K. Sudhindra, “A case study: risk rating methodology for e-governance application security risks,” *i-Manager’s Journal on Software Engineering*, vol. 13, no. 3, p. 39, 2019.

[72] B. Halak, T. Gibson, M. Henley, C.-B. Botea, B. Heath, and S. Khan, “Evaluation of performance, energy, and computation costs of quantum-attack resilient encryption algorithms for embedded devices,” *IEEE Access*, 2024.

[73] I. Dissanayake, “Dns cache poisoning: A review on its technique and countermeasures,” in *2018 National Information Technology Conference (NITC)*. IEEE, 2018, pp. 1–6.

[74] M. Southam, “Dnssec: What it is and why it matters,” *Network Security*, vol. 2014, no. 5, pp. 12–15, 2014.

[75] G. Schmid, “Thirty years of dns insecurity: Current issues and perspectives,” *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2429–2459, 2021.

[76] M. Chapple, “Confidentiality, integrity and availability–the cia triad,” 2020.

[77] E. Heftrig, H. Schulmann, N. Vogel, and M. Waidner, “The harder you try, the harder you fail: The keytrap denial-of-service algorithmic complexity attacks on dnssec,” in *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*, 2024, pp. 497–510.

[78] F. Opiłka, M. Niemiec, M. Gagliardi, and M. A. Kourtis, “Performance analysis of post-quantum cryptography algorithms for digital signature,” *Applied Sciences*, vol. 14, no. 12, p. 4994, 2024.

[79] M. Jammal, H. Hawilo, A. Kanso, and A. Shami, “Mitigating the risk of cloud services downtime using live migration and high availability-aware placement,” in *2016 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*. IEEE, 2016, pp. 578–583.

[80] Y. Baseri, V. Chouhan, and A. Hafid, “Navigating quantum security risks in networked environments: A comprehensive study of quantum-safe network protocols,” *Computers & Security*, p. 103883, 2024.

[81] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, “Stride-based threat modeling for cyber-physical systems,” in *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*. IEEE, 2017, pp. 1–6.

[82] G. Karantzas and C. Patsakis, “An empirical assessment of endpoint detection and response systems against advanced persistent threats attack vectors,” *Journal of Cybersecurity and Privacy*, vol. 1, no. 3, pp. 387–421, 2021.

[83] E. Parker, “When a quantum computer is able to break our encryption, it won’t be a secret,” 2023.

[84] J. R. Lindsay, “Surviving the quantum cryptocalypse,” *Strategic Studies Quarterly*, vol. 14, no. 2, pp. 49–73, 2020.

[85] A. A. Ahmed, “Lightweight digital certificate management and efficacious symmetric cryptographic mechanism over industrial internet of things,” *Sensors*, vol. 21, no. 8, p. 2810, 2021.

[86] H. Singh, “Managing the quantum cybersecurity threat: Harvest now, decrypt later,” in *Quantum Computing*. CRC Press, pp. 142–158.

[87] M. J. H. Faruk, S. Tahora, M. Tasnim, H. Shahriar, and N. Sakib, “A review of quantum cybersecurity: threats, risks and opportunities,” in *2022 1st International Conference on AI in Cybersecurity (ICAIC)*. IEEE, 2022, pp. 1–8.

[88] A. Mehmood, A. Shafique, M. Alawida, and A. N. Khan, “Advances and vulnerabilities in modern cryptographic techniques: A comprehensive survey on cybersecurity in the domain of machine/deep learning and quantum techniques,” *IEEE Access*, vol. 12, pp. 27 530–27 555, 2024.

[89] A. Kuznetsov, A. Kiian, V. Babenko, I. Perevozova, I. Chepurko, and O. Smirnov, “New approach to the implementation of post-quantum digital signature scheme,” in *2020 IEEE 11th international conference on dependable systems, services and technologies (DESSERT)*. IEEE, 2020, pp. 166–171.

[90] A. S. George, S. Sagayarajan, T. Baskar, and A. H. George, “Extending detection and response: how mxdr evolves cybersecurity,” *Partners Universal International Innovation Journal*, vol. 1, no. 4, pp. 268–285, 2023.

[91] Y. Baseri, V. Chouhan, A. Ghorbani, and A. Chow, “Evaluation framework for quantum security risk assessment: A comprehensive study for quantum-safe migration,” *arXiv preprint arXiv:2404.08231*, 2024.

[92] T. UcedaVelez and M. M. Morana, *Risk Centric Threat Modeling: process for attack simulation and threat analysis*. John Wiley & Sons, 2015.

[93] A. S. Mohammed, S. Jha, A. Tabbassum, and V. Malik, “Assessing the vulnerability of machine learning models to cyber attacks and developing mitigation strategies,” in *2024 International Conference on Intelligent Systems and Advanced Applications (ICISAA)*. IEEE, 2024, pp. 1–5.

[94] Y. Baseri, V. Chouhan, and A. Ghorbani, “Cybersecurity in the quantum era: Assessing the impact of quantum computing on infrastructure,” *arXiv preprint arXiv:2404.10659*, 2024.

[95] M. M. Yamin, “Modelling and analyzing attack-defense scenarios for cyber-ranges,” 2022.

[96] A. Huang, S. Barz, E. Andersson, and V. Makarov, “Implementation vulnerabilities in general quantum cryptography,” *New Journal of Physics*, vol. 20, no. 10, p. 103016, 2018.

[97] Y. Shamoo, “Adversarial attacks and defense mechanisms in the age of quantum computing,” in *Leveraging Large Language Models for Quantum-Aware Cybersecurity*. IGI Global Scientific Publishing, 2025, pp. 301–344.

[98] N. Shevchenko, T. A. Chick, P. O’Riordan, T. P. Scanlon, and C. Woody, “Threat modeling: a summary of available methods,” *Software Engineering Institute— Carnegie Mellon University*, pp. 1–24, 2018.

[99] T. UcedaVelez and M. M. Morana, *Risk Centric Threat Modeling: process for attack simulation and threat analysis*. John Wiley & Sons, 2015.

[100] D. Joseph, R. Misoczki, M. Manzano, J. Tricot, F. D. Pinuaga, O. Lacombe, S. Leichenauer, J. Hidary, P. Venables, and R. Hansen, “Transitioning organizations to post-quantum cryptography,” *Nature*, vol. 605, no. 7909, pp. 237–243, 2022.

[101] S. A. Käppler and B. Schneider, “Post-quantum cryptography: An introductory overview and implementation challenges of quantum-resistant algorithms,” *Proceedings of the Society*, vol. 84, pp. 61–71, 2022.

[102] S. Sadeghi, V. Chouhan, M. Aldarwbi, A. Ghorbani, A. Chow, and R. Burko, “Securing financial sector applications in the quantum era: A comprehensive evaluation of nist’s recommended algorithms through use-case analysis,” *Available at SSRN 4836780*.

[103] M. Jain and A. Agrawal, “Implementation of hybrid cryptography algorithm,” *International Journal Of Core Engineering & Management (IJCEM)*, vol. 1, no. 3, pp. 126–142, 2014.

[104] A. K. Bishwas and M. Sen, “Strategic roadmap for quantum-resistant security: A framework for preparing industries for the quantum threat,” *arXiv preprint arXiv:2411.09995*, 2024.

[105] D. S. K. M. Devulapally Swetha, “Quantum-enhanced security advances for cloud computing environments,” *Quantum*, vol. 15, no. 6, 2024.

[106] B. Hale, N. Bindel, and D. L. Van Bossuyt, “Quantum computers: The need for a new cryptographic strategy,” in *Handbook for Management of Threats: Security and Defense, Resilience and Optimal Strategies*. Springer, 2023, pp. 125–158.

[107] A. Rodríguez-Pérez, N. Costa, and T. Finogina, “An electoral exception? quantum computing-readiness and internet voting,” *JeDEM-eJournal of eDemocracy and Open Government*, vol. 16, no. 3, 2024.

[108] N. Aviram, K. Gellert, and T. Jager, “Session resumption protocols and efficient forward security for tls 1.3 0-rtt,” *Journal of Cryptology*, vol. 34, no. 3, p. 20, 2021.

[109] M. Fingerhuth, T. Babej, and P. Wittek, “Open source software in quantum computing,” *PloS one*, vol. 13, no. 12, p. e0208561, 2018.

[110] H. Lee, D. Kim, and Y. Kwon, “Tls 1.3 in practice: How tls 1.3 contributes to the internet,” in *Proceedings of the Web Conference 2021*, 2021, pp. 70–79.

[111] J. Ahn, R. Hussain, K. Kang, and J. Son, “Exploring encryption algorithms and network protocols: A comprehensive survey of threats and vulnerabilities,” *IEEE Communications Surveys & Tutorials*, 2025.

[112] Z. Wang, J. Lin, Q. Cai, Q. Wang, D. Zha, and J. Jing, “Blockchain-based certificate transparency and revocation transparency,” *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 1, pp. 681–697, 2020.

[113] K. Borgolte, T. Fiebig, S. Hao, C. Kruegel, and G. Vigna, “Cloud strife: mitigating the security risks of domain-validated certificates,” 2018.

[114] B. Laurie, “Certificate transparency: Public, verifiable, append-only logs,” *Queue*, vol. 12, no. 8, pp. 10–19, 2014.

[115] W. Bul’ajoul, A. James, and M. Pannu, “Improving network intrusion detection system performance through quality of service configuration and parallel technology,” *Journal of Computer and System Sciences*, vol. 81, no. 6, pp. 981–999, 2015.

[116] D. E. Simos, K. Kleine, A. G. Voyiatzis, R. Kuhn, and R. Kacker, “Tls cipher suites recommendations: A combinatorial coverage measurement approach,” in *2016 IEEE International Conference on Software Quality, Reliability and Security (QRS)*. IEEE, 2016, pp. 69–73.

[117] K. F. Hasan, L. Simpson, M. A. R. Baee, C. Islam, Z. Rahman, W. Armstrong, P. Gauravaram, and M. McKague, "A framework for migrating to post-quantum cryptography: Security dependency analysis and case studies," *IEEE Access*, 2024.

[118] T. Karygiannis and L. Owens, *Wireless Network Security:*. US Department of Commerce, Technology Administration, National Institute of …, 2002.

[119] J. P. Mattsson, B. Smeets, and E. Thormarker, "Quantum-resistant cryptography," *arXiv preprint arXiv:2112.00399*, 2021.

[120] I. Gorbenko and V. Ponomar, "Examining a possibility to use and the benefits of post-quantum algorithms dependent on the conditions of their application," *Eastern-European Journal of Enterprise Technologies*, no. 2 (9), pp. 21–32, 2017.

[121] S. Darzi, K. Ahmadi, S. Aghapour, A. A. Yavuz, and M. M. Kermani, "Envisioning the future of cyber security in post-quantum era: A survey on pq standardization, applications, challenges and opportunities," *arXiv preprint arXiv:2310.12037*, 2023.

[122] M. Jain and A. Agrawal, "Implementation of hybrid cryptography algorithm," *International Journal Of Core Engineering & Management (IJCEM)*, vol. 1, no. 3, pp. 126–142, 2014.

[123] G. Surla and R. Lakshmi, "Retracted article: Design and evaluation of novel hybrid quantum resistant cryptographic system for enhancing security in wireless body sensor networks," *Optical and Quantum Electronics*, vol. 55, no. 14, p. 1252, 2023.

[124] E. A. Alrashed, F. Bagci, and E. Alquraishi, "A key management approach for forward and backward secrecy in unattended wsns," *Journal of Engineering Research*, vol. 4, no. 4, 2016.

[125] C. Cremers, "Key exchange in ipsec revisited: Formal analysis of ikev1 and ikev2," in *Computer Security–ESORICS 2011: 16th European Symposium on Research in Computer Security, Leuven, Belgium, September 12-14, 2011. Proceedings 16*. Springer, 2011, pp. 315–334.

[126] N. Dunbar, "Ipsec networking standards—an overview," *Information Security Technical Report*, vol. 6, no. 1, pp. 35–48, 2001.

[127] C. Cremers, "Key exchange in ipsec revisited: Formal analysis of ikev1 and ikev2," in *Computer Security–ESORICS 2011: 16th European Symposium on Research in Computer Security, Leuven, Belgium, September 12-14, 2011. Proceedings 16*. Springer, 2011, pp. 315–334.

[128] A. Hussain, "Enhanced authentication mechanism using multilevel security model." *Int. Arab. J. e Technol.*, vol. 1, no. 2, pp. 49–57, 2009.

[129] Y. Zheng and C.-H. Chang, "Secure mutual authentication and key-exchange protocol between puf-embedded iot endpoints," in *2021 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 2021, pp. 1–5.

[130] J. Heino, C. Jalio, A. Hakkala, and S. Virtanen, "A method for endpoint aware inspection in a network security solution," *IEEE Access*, vol. 10, pp. 44 517–44 530, 2022.

[131] K. Sundholm, "Hardening industrial network using isolated segments," 2019.

[132] S. Frankel, K. Kent, R. Lewkowski, A. D. Orebaugh, R. W. Ritchey, and S. R. Sharma, "Guide to ipsec vpns:." 2005.

[133] D. Joseph, R. Misoczki, M. Manzano, J. Tricot, F. D. Pinuaga, O. Lacombe, S. Leichenauer, J. Hidary, P. Venables, and R. Hansen, "Transitioning organizations to post-quantum cryptography," *Nature*, vol. 605, no. 7909, pp. 237–243, 2022.

[134] K. Hageman, "The performance of ecc algorithms in dnssec: A model-based approach," Master's thesis, University of Twente, 2015.

[135] G. Beernink, "Taking the quantum leap: Preparing dnssec for post quantum cryptography," Master's thesis, University of Twente, 2022.

[136] J. O. Ogala, S. Ahmad, I. Shakeel, J. Ahmad, and S. Mehfuz, "Strengthening kms security with advanced cryptography, machine learning, deep learning, and iot technologies," *SN Computer Science*, vol. 4, no. 5, p. 530, 2023.

[137] T. Chung, R. van Rijswijk-Deij, B. Chandrasekaran, D. Choffnes, D. Levin, B. M. Maggs, A. Mislove, and C. Wilson, "A longitudinal,{End-to-End} view of the {DNSSEC} ecosystem," in *26th USENIX Security Symposium (USENIX Security 17)*, 2017, pp. 1307–1322.

[138] S. Huque, P. Aras, J. Dickinson, J. Vcelak, and D. Blacka, "Rfc 8901: Multi-signer dnssec models," 2020.

[139] S. Ariyapperuma and C. J. Mitchell, "Security vulnerabilities in dns and dnssec," in *The Second International Conference on Availability, Reliability and Security (ARES'07)*. IEEE, 2007, pp. 335–342.

[140] R. M. van Rijswijk-Deij, *Improving DNS security: a measurement-based approach*. University of Twente, 2017.

[141] F. Hock and P. Kortiš, "Design, implementation and monitoring of the firewall system for a dns server protection," in *2016 International Conference on Emerging eLearning Technologies and Applications (ICETA)*. IEEE, 2016, pp. 91–96.

[142] A. S. Jahromi, A. Abdou, and P. C. van Oorschot, "Dnssec+: An enhanced dns scheme motivated by benefits and pitfalls of dnssec," *arXiv preprint arXiv:2408.00968*, 2024.

[143] C. Deccio, D. Argueta, and J. Demke, "A quantitative study of the deployment of dns rate limiting," in *2019 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2019, pp. 442–447.

[144] G. Shan, Y. Wang, M. Xie, H. Lv, and X. Chi, "Visual detection of anomalies in dns query log data," in *2014 IEEE Pacific Visualization Symposium*. IEEE, 2014, pp. 258–261.

[145] R. Canetti, S. Halevi, and J. Katz, "A forward-secure public-key encryption scheme," in *Advances in Cryptology—EUROCRYPT 2003: International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4–8, 2003 Proceedings 22*. Springer, 2003, pp. 255–271.

[146] J. P. Mattsson, B. Smeets, and E. Thormarker, "Quantum-resistant cryptography," *arXiv preprint arXiv:2112.00399*, 2021.

[147] A. S. Chauhan, *Practical Network Scanning: Capture network vulnerabilities using standard tools such as Nmap and Nessus*. Packt Publishing Ltd, 2018.

[148] M. J. Vermeer, C. Heitzenrater, E. Parker, A. Moon, D. Lumpkin, and J. Awan, "Evaluating cryptographic vulnerabilities created by quantum computing in industrial control systems," *Journal of Critical Infrastructure Policy*, vol. 5, no. 2, pp. 88–110, 2024.

[149] C. Daniel, "Building a more secure network: A comprehensive guide to network segmentation strategies and best practices," *Revista de Inteligencia Artificial en Medicina*, vol. 15, no. 1, pp. 959–968, 2024.

[150] S. Bates, J. Bowers, S. Greenstein, J. Weinstock, Y. Xu, and J. Zittrain, "Evidence of decreasing internet entropy: the lack of redundancy in dns resolution by major websites and services," National Bureau of Economic Research, Tech. Rep., 2018.

[151] J. Jabez and B. Muthukumar, "Intrusion detection system (ids): Anomaly detection using outlier detection approach," *Procedia Computer Science*, vol. 48, pp. 338–346, 2015.