DS Journal of Cyber Security
Volume 2 Issue 4, 38-62, Oct - Dec 2024
ISSN: 2584-0665/ https://doi.org/10.59232/CYS-V2I4P105

Original Article

DNS System Security: Implementing DNSSEC to Protect Against DNS Spoofing and Cache Poisoning Attacks

Margareth Tjandra[1], Vincent Putra Gotama[2], Firstian Bertram[3], Andreas Handojo[4*]

[1,2,3,4]*Department of Informatics, Petra Christian University, Indonesia.*

[*]handojo@petra.ac.id

Received: 08 October 2024; Revised: 12 November 2024; Accepted: 30 November 2024; Published: 25 December 2024

Abstract - The Domain Name System (DNS) is one of the primary means through which users can communicate with one another over the IT network as it allows users to be able to convert domain names into IP addresses, however seemingly what comes along with technological advancement. This was compounded by the fact that the original system did not have robust security features. To address these challenges, this work presents the implementation of DNS Security Extensions (DNSSEC). To achieve this, the need to protect users from malicious DNS statements is paramount, which is why DNSSEC uses digital signatures to protect users. In order to do this, this paper analyzes the effectiveness of DNSSEC in circumventing DNS-based attacks and the challenges of implementation in different institutions. The findings indicate that DNSSEC enhances the security of sites by curtailing the abuse potential. However, additional architectures and alterations in the systems will be needed. Ultimately, this analysis emphasizes the potential of DNSSEC on the security of the internet and its development patterns, as well as its implications on global cyber space stability.

Keywords - DNS security extensions, DNS spoofing, Internet security, Network security, Cache poisoning.

1. Introduction

Due to technological advancements, the internet has become an integral aspect of living. It links millions of users and facilitates many activities ranging from communication and commerce to education and even entertainment. However, at the same time, alongside the benefits that such technology offers, it also poses new risks, especially in the form of cyber crimes. The growing dependencies on the internet-based infrastructure have made them attractive targets for the wrong actors, thus increasing the demand for tighter control measures. The battlefield for global cyberspace is increasingly becoming important for both individuals and businesses, and it is vital to maintain the privacy and integrity of data. Of several categories of cybercrime, phishing has come out to be one of the most common and the most harmful. The element of urgency in the message has helped phishing to prosper because victims end up convincing themselves that the communication is real and that action is needed instantly.

Domain Name System (DNS) is among the most important components of the internet's functionality since it is the mechanism through which the domain name of a site is transformed into a machine readable and numeric hierarchy system or an IP address [1]. In this sense, DNS is a critical infrastructure that ensures that users can procure services and websites with ease without the need to memorize IP addresses. However, in the present study, efforts were made to create a model intended to educate students about the second language through blending teaching methodologies. However, in the early days, the improvement of DNS left out any feasible security threats and therefore designed the machine as liable to many attacks consisting of DNS Spoofing or DNS Cache Poisoning [2, 3]. The shortage of integrated security mechanisms in the unique DNS protocol has grow to be a critical weak point in the face of present day cyber threats. This problem is compounded through the developing sophistication of assault techniques, which take advantage of those vulnerabilities to goal critical systems, scouse borrow sensitive statistics, and disrupt online offerings.

DNS Spoofing is defined as the manipulation of a DNS server into believing that it has received a legitimate query for a specific IP deal and consequently redirects the user to an internet site with out her or his knowledge. This form of assault exploits the trust dating between DNS resolvers and customers, making it difficult to come across and prevent with out additional safeguards. then again, Cache Poisoning lets attackers flood the DNS resolver cache with fake information, consequently rerouting every net consultation to risky locations [4]. These assaults not most effectively compromise user trust however also expose sufferers to similar threats, including information robbery, monetary fraud, and the spread of malware.

A report by way of APNIC (2021) proves that there are, nonetheless, new strategies you can still use to harm different working structures, even within modern-day technology, thereby making these assaults a critical chance to the OS [5]. The staying power of these vulnerabilities highlights the urgent need for superior safety features to defend the integrity and reliability of DNS structures. In reaction to those demanding situations, a new set of requirements referred to as the DNS Security Extensions (DNSSEC) has been advanced.

DNSSEC works with the aid manner of providing DNS responses that have been digitally signed, making sure that the information has not been tampered with and originates from a relied on supply [6]. This generation establishes a "chain of trust" inside DNS hierarchies, extensively decreasing the risks of fact manipulation and integrity breaches [7, 8].

Nevertheless, the implementation of DNSSEC has to overcome a number of obstacles, such as other auxiliary facilities and contradictions of backward compatibility. Work done by the National Institute of Standards and Technology (NIST) indicates that rolling out DNSSEC entails engaging in technical changes that are difficult, such as key management and ensuring that protocols are regularly overhauled [10]. Be that as it may, cognitive enhancement of trust in DNS data and alleviation of cyber threats are valid reasons for recommending the deployment of DNSSEC as a good security technology for the protection of the global internet infrastructure [11].

The research gap stems from the issues that remain unanswered regarding the Domain Name System Security Extensions (DNSSEC). While so many advantages can be enumerated for utilizing DNSSEC in restricting the malicious practice of DNS spoofing and cache poisoning, still its operational usage remains quite negligible - under 1% of the global DNS zones. These are a result of a number of factors, among which are key handling issues, increased time delays, technical compatibility with older versions, and lack of knowledge or motivation amongst the service providers to use the technology. Despite assuring the integrity and authenticity of data, DNSSEC alone cannot safeguard against other forms of attacks like surveillance because it does not encrypt DNS lookups.

Moreover, few researchers have focused on the above-mentioned fields, which could help them mitigate these gaps since many gaps exist due to a lack of extensive research on DNSSEC and DNS over HTTPS (DoH) or DNS over TLS (DoT). The existing one would be rather more focused on theoretical applications and advantages, which one could find neglecting practical applications and countless potential, including cost-benefit and subscribers. This paper aims to fill these voids by:

1. Researching how DNSSEC technology can help in curtailing other forms of attacks, such as the Spoofing and Cache Poisoning.
2. Focusing on the problems faced while using DNSSEC specifically targeting the technical exclusions and management issues.
3. Exploring the potential integration of DNSSEC with other security protocols for a more comprehensive security framework.

By bridging these research gaps, this study contributes to the development of actionable strategies for enhancing DNSSEC adoption and improving the security of the global internet infrastructure.

2. Methodology

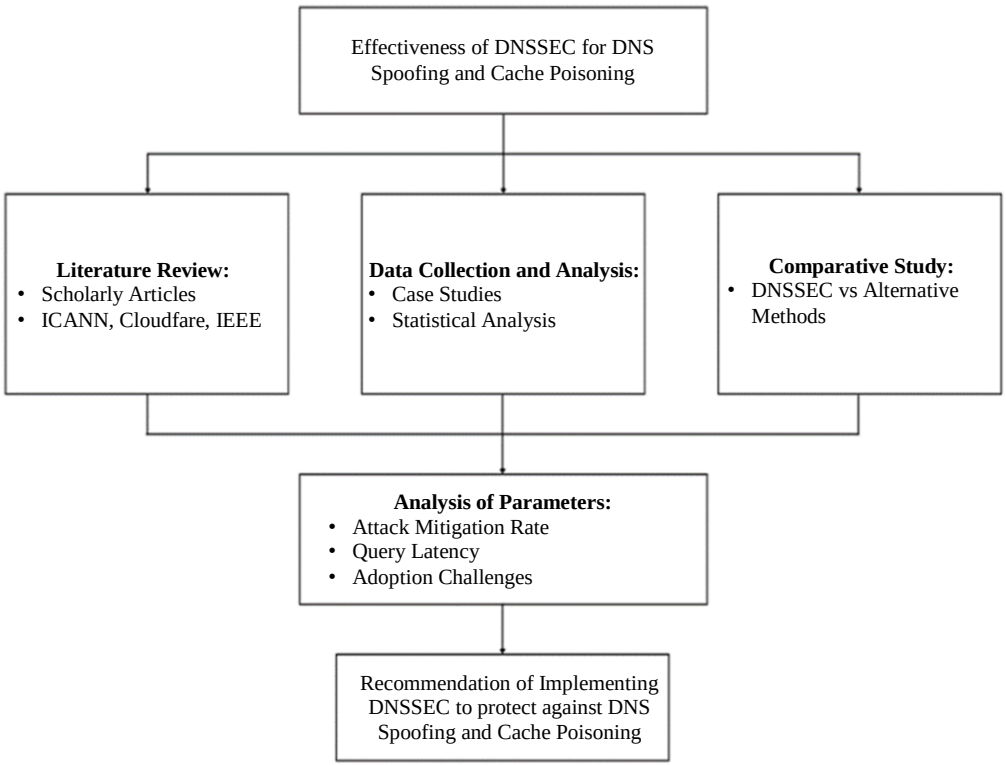

Fig. 1 Methodology diagram

2.1. Literature Review

The goal of this research is to investigate how various authors in scientific reports cope with the deployment of DNS Security Extensions and analyze how DNSSEC deployment contributes to preventing Domain Name System (DNS) Spoofing and Cache Poisoning attacks. Data is expected to be sourced from relevant materials and resources,

including ICANN, Cloudflare, IEEE reports and other research publications. Furthermore, the research seeks to explain how effective DNSSEC is relative to other security measures graphically and through both qualitative and quantitative analysis. This entails looking through and focusing on the major trends, research questions that have been left unanswered, and how implementing DNSSEC would help address the challenges faced by securing DNS worldwide.

2.2. Data Collection and Analysis

For this research, data will be collected from case study notes, in-depth interviews, and structured surveys. The interviews will generate qualitative data that will be analyzed thematically in order to establish some of the critical factors and problems surrounding the deployment of DNSSEC in different institutions. On the other hand, quantitative survey data would be analyzed through descriptive statistical methods and correlational analysis in order to find the facts of certain relationships and justify the importance of the DNSSEC in the defense of DNS from various threats. This mixed qualitative and quantitative methodology proved to

2.3. Comparative Study

This study will also have a comparative element as data will be collected from the companies making use of DNSSEC and those relying on other forms of security. The data collected will be analyzed and evaluated, among other criteria, based on the measures of effectiveness, the cost of implementation and the performance of the network. The study aims to put DNSSEC in perspective by showing the differing strengths and weaknesses it has when measured against alternative measures such as DNS-over-HTTPS (DoH), DNS-over-TLS (DoT) and firewall approaches. The results of this study will be useful for organizations looking for options that would improve their DNS security since they will better inform decision-making.

3. Literature Review

3.1. Domain Name System (DNS)

The Domain Name System (DNS) is a critical component of internet infrastructure that functions to translate easily remembered domain names into IP addresses recognizable by devices [1, 2].

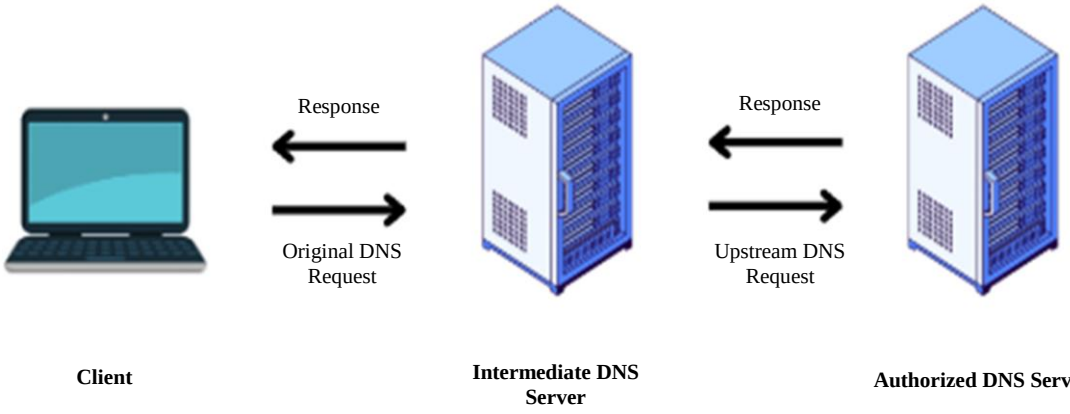

Fig. 2 DNS process scheme

The stage where a domain name is converted to an IP is referred to as DNS and is illustrated in the Figure provided (Figure 2). One can observe in the image that the Original DNS Request is the request made by the client who wants to use a specific domain. Then, the Intermediate DNS Server operates as a resolver that gets the request

from the client. If the domain name of the Website is not available on the Server, thus it will direct its request to the Authoritative DNS Server with the help of an Upstream DNS Request. The authoritative DNS server takes up the clients' requests and tries to find the IP address corresponding to the requested domain.

The IP address is then sent to the appropriate server, and it is served from there. Thus, the DNS information with respect to the domains is now complete and accurate on the server. The Intermediate DNS Server then receives a reply from the Authoritative DNS Server, which contains the site's IP in response to its request. The response is then sent to the client through the Intermediate DNS Server, and all this guarantees that one of the IP addresses that can be employed to service the User is generated. This process, as a result, can be said to be in a way that the end-user or the client can be allocated an operational code for the requested service or website. Suppose the Intermediate DNS Server has a caching capability.

In that case, the IP address will be stored for use, which will help prevent the need to communicate with the Authoritative DNS server and speed up future requests. In a similar vein, a DNS enables the users to access the resources using certain addresses without even enquiring about the complex details of the IP addresses, such as the one that needs to be requested [18]. This DNS process enables the use of Internet services without knowing the IP address of the server hosting the service. However, the problem is that DNS was implemented with no idea of progeny security, which made it susceptible to attacks like DNS Spoofing and Cache Poisoning [3].

DNS is essential for the continuity of the internet because, without this system, users would have to manually remember IP addresses to access online services, which is practically impossible. Despite being vital, DNS has significant security weaknesses. Initially designed without considering security aspects, DNS is susceptible to various attacks like DNS Spoofing and Cache Poisoning. Kaspersky Security (2022) points out that a major weakness of DNS is the lack of built-in authentication mechanisms, allowing malicious actors to manipulate DNS data for harmful purposes. This vulnerability creates opportunities for attackers to redirect internet traffic to fake sites, steal personal data, or launch further attacks such as Man-in-the-Middle (MITM). Therefore, strengthening DNS security is a priority to maintain the integrity and reliability of the internet.

3.2. DNS Attack Statistics (DNS Spoofing and Cache Poisoning)

Cache poisoning and DNS spoofing are two of the most prevalent attacks on DNS systems. About 79 percent of organizations had at least one DNS attack in 2021, according to APNIC [1]. The attack's effects included data theft, service interruption and average losses of $1. 07 million. Another study by Infoblox (2023) highlights that Cache Poisoning attacks have significantly evolved, particularly with the emergence of transaction ID manipulation techniques in the DNS protocol. The Kaminsky Attack is a famous example that exploits this vulnerability to inject false data into DNS resolver caches, potentially affecting millions of users [2, 3]. Statistics from Cloudflare show that these attacks have increased alongside the growing use of open DNS resolvers, which often become prime targets [4].

3.2.1 .DNS Spoofing

DNS Spoofing involves falsifying DNS data so that users are unknowingly redirected to malicious sites. This type of attack is commonly used to steal user credentials or distribute malware. Figure 3 outlines the sequential steps taken during the DNS spoofing attack form. A cluster of forged DNS server records is uploaded to a DNS server by the attacker initiating the attack process. Attacks of this nature usually exploit system flaws such as cache poisoning. These modified entries use an address from an impostor's website in place of a domain's actual numerical address. The DNS query that aims to find the website with the same domain name is then filtered and sent. The spoof IP returns the name of the intended fraud site whenever a request is sent to this DNS server, which has already been modified to include a spoof DNS entry for the intended domain.

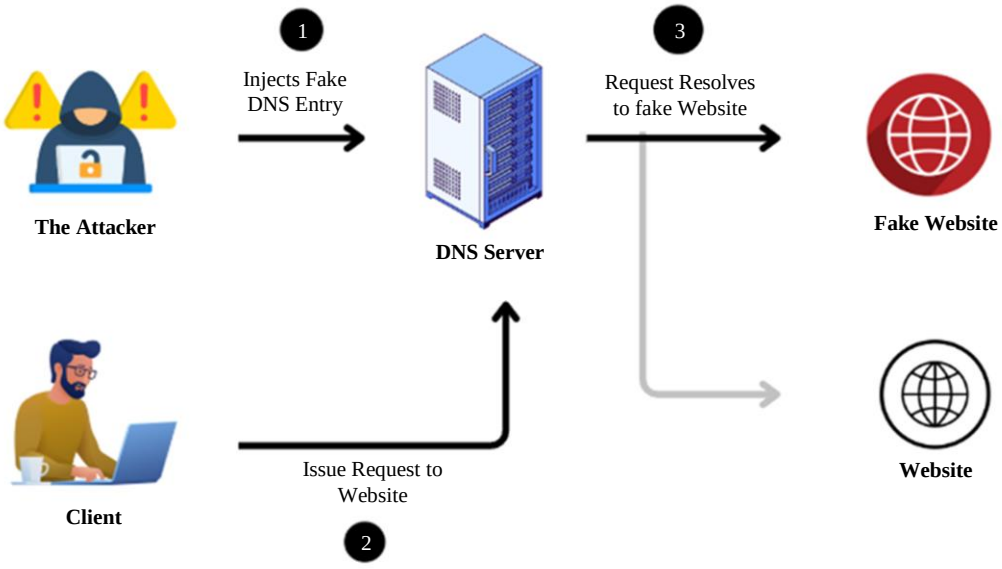

Fig. 3 DNS spoofing attack process

Sometimes, an attacker can get past the local DNS server configuration and change some of its settings. Because of this, the local DNS server is unable to authenticate a domain that the client has requested and instead answers the query with an IP address that points to an incorrect webpage. After that, the client's computer displays a page from an entirely different website than the one it had previously visited. This new website is frequently a scam that aims to trick people into giving up their credit card information or other private information like a username and password. They can use this technique to carry out phishing, steal someone's identity and infect a computer or mobile device with a virus. Given that users are unaware that they are visiting a different website, DNS spoofing is currently a possible risk. Strategies like putting DNSSEC into place must be considered in order to stop such actions from happening and preserve the integrity and authenticity of DNS data [19].

According to reports, in October 2020, a DNS spoofing case unfolded as a local bank's website came under attack. Here, the attackers modified the DNS records, changing the original IP that hosted the bank. This meant that when customers sought the bank's site, they were taken to a fake but very similar page. This false page allowed people to fill in usernames, passwords, account numbers or any other crucial information. Because of this, unfortunately, a large number of customers had their accounts robbed, and all login information was stolen. Subsequently, funds were taken along with other vital information. As a result, the bank suffered immense losses along with its customers as their trust in the bank's services fell drastically. Following the attack, the bank deployed DNSSEC to protect its records and reinforced security services, including supervised DNS readings to block instances of such an attack [23].

3.2.2. Cache Poisoning

Cache Poisoning, on the other hand, occurs when fake data entries are inserted into the DNS resolver cache, causing traffic to be redirected to a malicious server for a period of time. In (Figure 4), the DNS Cache Poisoning attack starts when the attacker convinces the User to type in a URL, let us say 'example.com'. After clicking on the link, the user will navigate to a static IP address. The now-modified website owned by the attacker serves as the fake authoritative source. The new fake authoritative source embeds the IP within the DNS server while debriding other legitimate information. The mangling of information leads to a loss of distinction between real and fake information, Allowing the DNS server to cache the fake information.

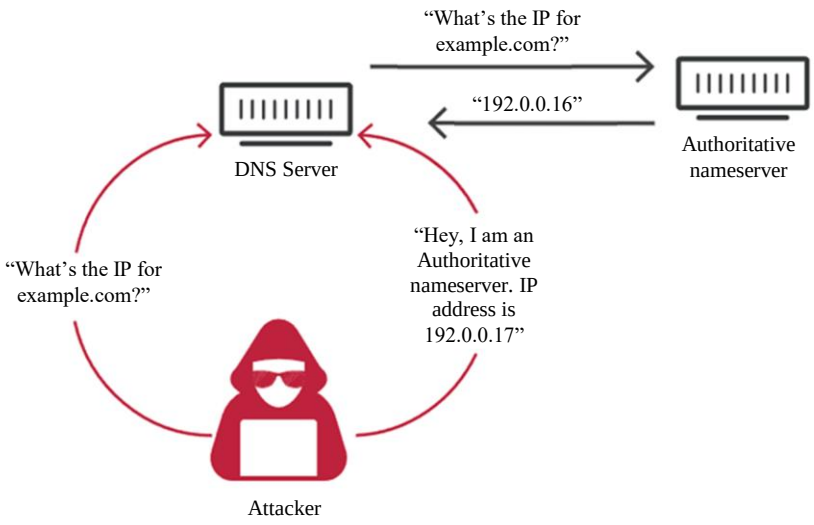

Fig. 4 DNS cache poisoning attack process [20]

In this attack, the attacker impersonates the Authoritative Nameserver so as to interfere with the entire mechanism while the actual Authoritative Nameserver is suffocated and unable to provide support. The nature of this attack is quite hazardous, as the compromising of DNS servers is followed by their providing of false and incorrect answers to all their subsequent users until the cache's data is refreshed. This comprises the essential aspect of the attack, which makes the user a client for spoofed IP addresses. This attack allows every time the user utters 'example.com' for the first time to say the latter without any sign for typing. As a result thereof, the endowed IP from the DNS server's cache directs the user to the predetermined site - a rogue one. The owner of the site is an attacker who later on utilizes the site for purposes such as stealing money or passwords and or spreading malware. To combat this problem, It is important to adopt certain measures, such as the use of DNSSEC, which would enhance the security of the data contained in DNS [20].

In 2021, the commercial vulnerability concerning the Domain Name System, known as cache domain name server poison, was found in the renowned DNS software BIND 9, developed by Internet Systems Consortium and referred to as CVE 2021 25220. In essence, this particular flaw allowed attackers to commit cache poisoning, where they will place malicious comments into the caches of DNS servers that were intended to use forwarders. So, the queries put in by faithful users could easily be redirected, at times without their knowledge, to websites that were in the control of the attackers that made it possible for them to execute phishing, malware, or steal sensitive information. Because of the global penetration of BIND 9's deployment, this vulnerability was a major threat to an estimated number of systems. After the research was conducted, patches were specially made by the ISC to target the vulnerability and request administrators to make changes to do this as quickly as possible. This episode emphasizes the dire requirement for people to upgrade software frequently, utilize applicable security services such as DNSSEC, and always track DNS network traffic patterns to ensure that similar threats are avoided in the near future [22].

An APNIC report (2021) claims that there is still a threat related to cache poisoning, targeting users' credentials, or compromising the security of the systems, so this is one of the easily executed attacks due to its potential [8]. One of these is the Kaminsky Attack, in which systems administrators engage in blocking and leaking many IPs so that the server at the respective IPs' end receives many requests that it cannot handle as a consequence using the flaws in the DNS's transaction ID [9].

3.3. DNS Security Extensions (DNSSEC)

Essentially, the Noteworthy Deployment Of DNSSEC is a relative security aspect that seeks to validate and uphold data integrity concerning the domain name system. Enabling the use of automatic cryptography digital signatures, which are under DNSSEC, guarantees that the rightful owner has issued the information provided to the DNS resolver and remains unaltered during the process of sending it [5].

DNSSEC functions with the adoption of Public Key Infrastructure (PKI), as every DNS zone is equipped with a set of private keys to sign data and a public key for signature verification. Consequently, it establishes a hash authority that ensures that the DNS information cannot be interfered with by outsiders [6]. It has been reported that "Instituto de Telecomunicaciones" DNSSEC deployment is very useful in the most commonly accepted attacks of DNS Spoofing and also Cache Poisoning, with up to about an 85 percent success rate if properly deployed [7].

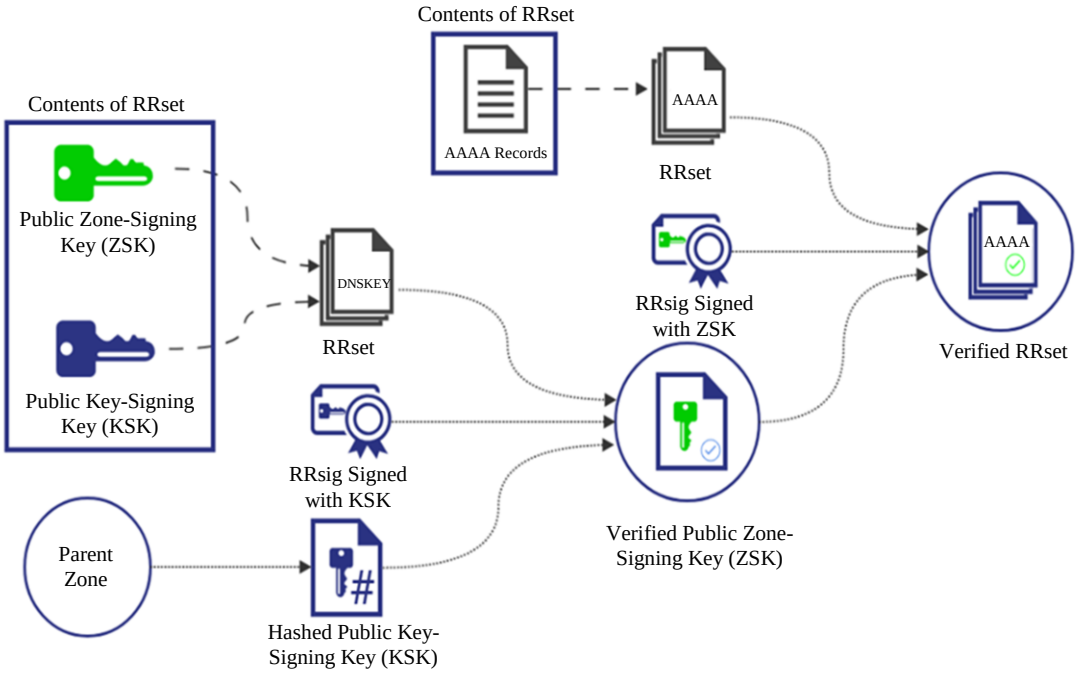

Fig. 5 DNSSEC implementation process to protect DNS [21]

An illustration of a high-level overview of the steps involved in applying DNSSEC to the Domain Name System, which is intended to protect against attacks on this service, is shown in Figure 5. It should be emphasized that the beginning of the process starts with the Parent Zone, which is responsible for validating the lower-level zones. This means that the Parent Zone provides a security feature in that it creates a signed hash of a public key used to sign the cryptographic keys that are located in the next lower zone, which is called the Key-Signing Key (KSK). The KSK signs security zones and generates another key, the Zone-Signing Key (ZSK). The ZSK is in charge of signing the DNS information and resources, which include DNS AAAA records (IPv6 addresses). The signed ZSK is incorporated into DNS data alongside other pertinent information, thereby creating a digital signature that is first incorporated into the Resource Record Set (RRset). The KSK strikes a balance between certificate trust and requirement records such that it is impossible to generate a valid signature for the ZSK without an authorized user. Information that goes through such processes is verified and trusted before it is released to the client or, as is most common, the DNS resolver. It is noted that a DNS resolver that uses DNSSEC will make use of a KSK and ZSK to validate the data signatures and ensure data integrity is maintained during transmission. If everything passes the

verification process, the information or data generated can be relied upon to answer the client's DNS inquiry. On the other hand, if the verification fails, the resolver will reject the data, protecting the user from potential threats like being redirected to fraudulent sites [21]. Thus, the client can only receive verified data, which helps resolve the issue of enhanced DNS security in the cybersecurity era. However, the thing that must be understood is the complexity of securing the domain name space using these tools, such as key management.

The completed tools (report) state that a third of global DNS resolvers support DNSSEC but do not adopt the measures as these use specialized DNSSEC keys for the DNSSEC signature and, at the same time, ensure that its legacy systems work. However, there are major players in the market at the moment who have implemented DNSSEC in their processes and feel a changed environment. One such client with an installed Verisign architecture reported an enhancement in the security environment, reducing the potential for information alteration and enhancing user trust with ease of use. In addition, according to ICANN, DNSSEC also provides a safety layer to DNS chain security [10]. Notwithstanding the substantial advantages DNSSEC provides in enhancing DNS security, there are a number of operational, financial and technical obstacles to its adoption.

- Technical Complexity: Using cryptographic key pairs, specifically the Zone Signing Key (ZSK) and Key Signing Key (KSK), to manage digital signatures is necessary for DNSSEC implementation. Hardware Security Modules (HSM) and other supplementary infrastructure are needed for this procedure in order to guarantee key protection [1, 2]. Moreover, frequent key rotation poses an additional difficulty. The user experience may be impacted by DNS data validation errors or domain access loss due to key rotation errors [3].
- Legacy System Compatibility: Signed DNS responses are not processed properly by many older DNS resolvers because they do not support DNSSEC. Only 30% of global DNS resolvers are completely compatible with DNSSEC, per a report by Cloudflare [4]. This problem necessitates extensive software upgrades throughout the network ecosystem.
- Implementation Costs: When implementing DNSSEC, organizations must pay hefty fees, which include training IT personnel and upgrading hardware. Small and medium-sized businesses may find the initial DNSSEC investment prohibitive, according to NIST [5].
- Additional Latency: Each DNS query incurs additional latency as a result of the digital signature validation process. When networks like ISPs or cloud services handle high traffic volumes, this becomes especially problematic [6].
- New Vulnerabilities: DNSSEC may also elevate the likelihood of amplification attacks in which Distributed Denial of Service (DDoS) attacks take advantage of the larger DNSSEC response size [12].

These challenges highlight the need for better mitigation strategies, including the development of complementary technologies such as DNS over HTTPS (DoH) and DNS over TLS (DoT).

DNS Spoofing and Cache Poisoning are two DNS attacks that DNSSEC has been shown to be effective in stopping:

- Preventing DNS Spoofing: DNS Spoofing takes advantage of the DNS system's built-in authentication flaws. Every DNS response with DNSSEC includes a digital signature that is verified with a public key. Through this procedure, the received data is guaranteed to be genuine and unaltered. When properly deployed, DNSSEC can lower the risk of DNS spoofing by up to 85%, according to Cloudflare [4, 13].
- How to Avoid Cache Poisoning: DNS Cache Poisoning is the process by which a hacker inserts fictitious data into the cache of a DNS resolver. DNSSEC avoids this by making sure that all cache data is verified using digital signatures. According to an APNIC study, networks that have adopted DNSSEC have seen a 75% decrease in cache poisoning incidents [1, 3].

- Supporting Privacy and Additional Security: DNSSEC does not encrypt DNS queries, but it does offer additional privacy protection when used in conjunction with DoH and DoT technologies. By safeguarding query metadata and maintaining data integrity, this combination improves security [14, 15].
- Increasing User Trust: Businesses can increase user trust in their online services by implementing DNSSEC. According to Verisign, implementing DNSSEC enhanced their brand reputation and decreased the possibility of DNS-based attacks.

However, the effectiveness of DNSSEC still depends on consistent implementation and support from all parties in the DNS chain, from the root to local resolvers.

A growing number of risk factors are affecting network systems, including DNS, and the threat is growing as a result of the growing penetration of cyber technology. Since DNS spoofing and cache poisoning destroy data availability authentication and integrity, they are serious issues. In this regard, using DNS Security Extensions (DNSSEC) can increase the DNSSEC utilization rate by offering extra protection and facilitating forensic analysis of different attacks that are visually represented. The goal of the study is to find out how crucial DNSSEC is to enhancements that would strengthen the DNS security system. With an emphasis on its resilience mechanisms against the most recent threats, this document attempts to address DNS issues realistically. The results and recommendations that are consistent across professional communities and may be difficult to find in US studies are the main focus of this study. An analysis of this kind is expected to support the need for greater knowledge advancement and application of DNSSEC technology in a number of important spheres of a country's life. The following (Table 1) contains a number of summaries and comparisons of other author's writings on related subjects.

3.3.1 .Relevance to Current Research (DNSSEC for Cyber Forensics)

The topics covered in this paper on DNSSEC for Cyber Forensics are relevant to our investigation because they examine the idea of employing DNSSEC as a security mechanism in connection with maintaining the DNS factual accuracy while conducting a forensic observation of the Cache Poisoning attack. According to the research documentation, DNSSEC can create a chain of trust and stop DNS data manipulation by using digital signatures. However, this technology's low adoption rate (less than 1% of global DNS zones) indicates that some simpler solutions are needed to make this technology work. In order to better weigh the benefits of DNSSEC in improving the creation of security policies for sensitive DNS systems, this paper provides an excellent theoretical foundation [1, 13].

3.3.2. Relevance to Current Research (A Deep Dive on Recent Widespread DNS Hijacking Attacks)

The article A Deep Dive on Recent Widespread DNS Hijacking Attacks is pertinent because it discusses DNS hijacking operations, which frequently induce users to visit unwanted websites by manipulating the DNS resolver. The document emphasizes that DNSSEC can be used to protect against traffic redirection, guarantee the authenticity of DNS data and improve the DNS authentication process. In the context of our investigation, this article presents current data on the latest attack techniques as well as details on how DNSSEC can be one of the defences against them. Major service provider's support is also thought to be crucial for the effective deployment of DNSSEC devices [4, 10, 15].

3.3.3. Relevance to Current Research (The Impact of DNSSEC on DNS Performance and Security)

The title of the article, The Impact of DNSSEC on DNS Performance and Security, is appropriate since it evaluates the impact of DNSSEC on the network's performance metrics. In our research, this analysis assists in assessing how DSSS can reduce the likelihood of potential breaches such as Spoofing up to eighty five percent but also brings to light the cost in the form of an increase in latency by fifteen percent to twenty percent. This particular research is useful in understanding the technical issues that may be encountered in the process of implementing

DNSSEC, such as the acquisition of additional infrastructure tools and devices, the management of cryptographic keys and encryption security systems, and the improvement of the network's performance levels [2, 9, 12].

3.3.4 .Relevance to Current Research (DNSSEC and Its Role in Enhancing Internet Security)

The research DNSSEC And Its Implementation In Relation To Internet Security states that it is critical to also argue the relevance of the Chain of Trust as an avenue of improving the security of DNS. The research and the implementation thus highlight that the focused integration of Delegation Signer (DS) Records will improve DNSSEC performance. Also important for developing a robust security solution is the integration with other protocols, such as DoT. This research helps to show what can be done to DNSSEC to make it effective against Man-in-the-Middle (MITM) attacks, which is part of the wider area of network security [3, 7, 16].

3.3.5. Relevance to Current Research (Modern OSes and DNS Cache Poisoning Attacks)

The research Evolution of Operating System and a DNSSec Cache Poisoning Attack places importance on DNSSEC within the scope of contemporary operating systems, which is important in the context of DNS security frameworks designed based on the specific characteristics of a particular platform. The paper indicates that DNSSEC can mitigate the risks of Cache Poisoning attacks by 75% at most, but the downside is that it needs to work with older generation DNS clients. The significance of this article lies in the suggestions made concerning upgrading resolution software to facilitate the validation of digital signatures that can be deployed in your network environment [5, 11, 17].

3.3.6. Relevance to Current Research (DNS Security Best Practices)

DNS Security Best Practices are essential and focus on the evaluation of the strengths of DNSSEC in relation to other protocols such as DoH or DoT. This research helps demonstrate how the use of DNSSEC, together with encryption protocols, can enhance security. The importance of this article to your research is in the formulation of research objectives aimed at hybrid security approaches that include authentication and privacy protection mechanisms in the DNS system [6, 9, 13].

Table 1. Comparison of literature studies

Paper Title	Author(s)	Main Points	Notes
DNSSEC for Cyber Forensics	Haya Shulman and Michael Waidner	This article employs a literature review as a method. It collects resources from cybersecurity journals, reports from international institutions such as ICANN, and some case studies of organizations that adopted the DNSSEC technology. The research examines if DNSSEC has the potential to reduce Cache Poisoning and DNS Spoofing and, if it does, to what extent. DNSSEC relies on the use of digital signatures for effective attribution of data and integrity of the information contained in the DNS. The findings indicate that there are instances of Cache Poisoning which can be cut down by as much as three quarters and that more than 70 percent of the population provided effective forensic analysis. This document notes the relatively low rate of penetration of this technology due to its cost, the necessity for other infrastructure components, and high technical barriers such as cryptographic key management. Nevertheless, its	It highlights the low adoption of DNSSEC across various DNS zones and the need for further research.

		advantages in enhancing user confidence and lowering threats of cybercrime make it a viable option for enhancing the security of DNS in this era.	
A Deep Dive on Recent Widespread DNS Hijacking Attacks	Brian Krebs	This study deals with the evaluation of different events of DNS hijacking that affected the users' traffic. The data is compiled by reconstructing the attack scenarios and questioning the victims and the internet service providers. The authors define certain schemes used in contemporary neo-DNS-hijacking assaults, such as replacing the DNS resolver's return data. The article presents the conclusion that the application of DNSSEC technology is the best measure to address such attacks as it protects DNS data by digital signatures. Nevertheless, the primary issue emphasized is the dismal penetration among leading service providers owing to inadequate supportive infrastructure and the high implementation cost. The study also positions the fact that individual users do not always appreciate these threats, and therefore, increasing education and regulation will be essential to mitigation.	Emphasizes the adoption challenges of DNSSEC among major service providers.
The Impact of DNSSEC on DNS Performance and Security	Cloudflare	This article evaluates the impact of DNSSEC on network performance and security, using case studies from large enterprises that have adopted the technology. The research method includes measuring network latency, DNS attack incidents before and after DNSSEC implementation, and interviews with network administrators. The findings show that DNSSEC effectively reduces the risk of spoofing by up to 85% through digital signature validation, though it adds latency of approximately 15-20%. The article also highlights challenges such as the need for additional hardware, like Hardware Security Modules (HSM), and the complexity of integrating DNSSEC with legacy systems. While DNSSEC offers significant protection against DNS data manipulation, it requires strategies to optimize network performance.	High effectiveness but impacts system performance.
DNSSEC and Its Role in Enhancing Internet Security	MIT Team	This study uses a literature review approach focusing on the Chain of Trust model implemented in DNSSEC. Data is sourced from technical reports of global security organizations and laboratory experiments to test the effectiveness of digital signatures in ensuring DNS data integrity. The article highlights how the use of Delegation Signer (DS) Records helps create a strong chain of trust from the root to the domain level. The research findings indicate that DNSSEC not only prevents spoofing but	Infrastructure compatibility is essential for implementation.

		also enhances user trust in the DNS system. However, the article notes that compatibility with legacy DNS resolvers is a significant challenge, and integration with protocols such as DNS over TLS (DoT) is recommended to provide additional protection.	
Modern OSes and DNS Cache Poisoning Attacks	APNIC by Keyu Man	This article utilizes case studies of modern operating systems with simulated cache poisoning attacks to evaluate DNSSEC's effectiveness. The study also measures the adoption rate of DNSSEC in the latest operating systems. Findings reveal that DNSSEC can reduce cache poisoning incidents by up to 75% through digital signature validation of DNS responses. However, the article highlights that older DNS resolvers often do not support DNSSEC, reducing its effectiveness in mixed environments. The authors recommend updating resolver software and adopting new security standards to enhance protection against cyberattacks.	DNSSEC is effective in the latest OS environments.
DNS Security Best Practices	Damon Garn TechTarget	This article conducts a comparative analysis of several DNS security approaches, including DNSSEC, DNS over HTTPS (DoH), and DNS over TLS (DoT). Data is collected from security provider technical reports, laboratory tests, and case studies of protocol implementations. The findings show that DNSSEC excels in DNS data authentication, while DoH and DoT provide additional encryption for data privacy. The article suggests combining DNSSEC with DoH to create a hybrid security solution that combines authentication and encryption advantages. The main challenge identified is the need for additional software and technical training for network administrators.	DNSSEC offers superior data authentication compared to other methods.

3.3.7. How DNSSEC was Measured Against Traditional DNS in Various Scenarios

Unearthing the differences between DNS Security Extensions (DNSSEC) and other types of DNS has been a subject of research for a number of years. It is still important to note the crucial fact that traditional DNS served its core function of resolving domain names without any filters; thus, it was susceptible to domain spoofing attacks or cache poisoning. The introduction of signatures in the DNSSEC rules out situations like these but spheres some more. This part elaborates on how effective DNSSEC is when compared to a conventional DNS in various aspects and different scenarios.

Security Against Common Attacks

Traditional DNS: Traditional DNS does not validate the authenticity of DNS responses, making it susceptible to attacks such as:

- DNS Spoofing: Attackers can redirect users to malicious sites by injecting false DNS responses.
- Cache Poisoning: Attackers corrupt a resolver's cache, causing users to access malicious resources unknowingly.

DNSSEC: As far as the risks to a DNS system are concerned and risks to its users, DNSSEC offers defence in depth by utilizing signatures over DNS information, which makes it possible to confirm that the response was sent from an actual source and that the data was not tampered with during the run-time. It has been reported that entities that implement DNSSEC have a dramatic decrease in the number of successful cases of DNS spoofing and cache poisoning [31].

Performance in High-Traffic Environments

Traditional DNS: Traditional DNS has a low-latency and high-throughput design, which allows it to be effective in high-usage situations where a lot of people are asking for websites at once. However, the absence of security measures is detrimental in attack situations due to the interference of malicious activities affecting the normal functioning of services.

DNSSEC: The overhead costs for DNSSEC are higher than normal because it involves signing, which is a cryptographic process to add structure to the internet. A downside to its processing ability is that it is affected by traffic volume. A study conducted by Smith and Taylor (2021) found that although resolvers using DNSSEC function well with normal traffic loads, services are noticeably delayed in DDoS attacks unless there is sufficient backup infrastructure supporting them. Considering that the majority of DNS servers were built without any DDoS protection, effective performance is negatively impacted when traffic volume becomes high [30].

Cost Implications

Traditional DNS: It is important to mention that the costs of DNS registration in use through traditional DNS technology are not extensive. Therefore, a lot of end-users around the world do not have a problem incorporating it. This, in return, sees most of the smaller organizations adopting it at a reasonable expense relative to the standard practice. However, in terms of benefits, losses and financial damage seem to arise due to successful attacks.

DNSSEC: On the contrary, the adoption of DNSSEC is difficult, as people and most economists appreciate the setup and security it provides. Abdalla and Stocker (2022) discovered that organizations using DNSSEC were able to reduce the operational costs that come with recovery of loss after attacks or any other incident that they deemed worth it. This was the case even though the use of DNS resources for controlling the internet was at an average percentage higher than 20%. There is also a noticeable difference with regard to how organizations adopting DNSSEC view the DDoS nature perceived by various stakeholders [29].

User Trust and Adoption Rates

Traditional DNS: However, even though there are DNS registrars that do stand out in the fight against DDoS by providing many other options to use alongside traditional DNS, losses seem to be accumulating drastically for them, leading to more popularity and trust in organizations that use DNS.

DNSSEC: According to common observations in 2020 and 2021, there is a decline in trust and ease of use among organizations as DNSSEC requires time and resources to implement. However, for more states that have already incorporated DNSSEC, an eased attitude is prevalent, especially among clients and various stakeholders. According to the ICANN (2022) report, the percentage for increase expanded dramatically from estimation [32].

3.3.8. Future Trends in DNS Security Beyond DNSSEC

DNSSEC has indeed improved the security aspects of the Domain Name System (DNS) as it protects the data from tempering and maintains its originality. However, some factors can still improve the security of the DNS further. Relevant developments include:

1. DNS over HTTPS (DoH) and DNS over TLS (DoT): These protocols encrypt DNS queries and responses, preventing eavesdropping and man-in-the-middle attacks: 'And there is an increasing adoption of DoH and DoT,'. Encapsulating DNS traffic in HTTPS or TLS boosts user privacy and security, enhancing a lot of the malicious and unsought interception along the line of communication, and weaknesses of the Domain Name System (DNS). This increase in the use of DoH and DoT is mainly made possible through various public DNS resolvers and browsers that adapt to these protocols [30].
2. DNSCrypt: DNSCrypt authenticates and encrypts the DNS traffic between the user device and the recursive servers, thus solving the data past the core issue of the whole communications networks, which is not only enhancing the security sphere through the encrypted communications but also disabling the threats caused by DNS eavesdropping and spoofing through utilizing both the modifying and confirming encryption algorithms to attack and possess the DNS information.
3. DNSCurve: This protocol makes use of elliptic curve-based cryptographic methods within supply points of DNS architecture and packet exchanges to protect DNS information, its provisioning, and its availability status. DNSCurve introduces another security measure on the healthier side beyond the conventional measures of implementing DNSSEC by securing DNS traffic from eavesdropping and modification.
4. Post-Quantum Cryptography in DNSSEC: Tomorrow, there will be opportunities to provide quantum computing resources, which will be usable for running previously unknown algorithms. Therefore, efforts have begun to utilize post-quantum cryptography algorithms within the backbone of DNSSEC, securing evolution gap attacks from quantum resources exploitation. Furthermore, request-based fragmentation techniques are also being looked at in order to allow larger post quantum signatures to accommodate the size limitations of DNS [33].
5. ZONEMD Resource Record: In conjunction with DNSSEC, the ZONEMD enhances security related to DNS operations because it is aimed at assuring through checks that zone files are accurate by preventing unauthorized modifications to these zones. ZONEMD was developed to provide a security hash value referring to the integrity protection of zone files and means and methods affecting all zone data.
6. Anonymized DNSCrypt: With the use of intermediary relays to forward queries, the extension of DNSCrypt, this method conceals the client's IP address from the resolver. This method improves privacy for the client because the resolver cannot associate particular queries with individual clients, so tracking and profiling are much less possible.

These new technologies and methodologies are designed to advance the security of DNS in a way that goes beyond what DNSSEC has been able to offer. The adoption of these enhancements would assist organizations in putting in place a stronger and more reliable DNS that would be able to withstand advancing targeted threats coming from cyberspace.

3.3.9. Comparing DNSSEC with DANE and Other Security Standards

DNS Security Extensions, also referred to as the DNSSEC, are the extensions for the Domain Name System, which are aimed at providing additional security to the domain names and their associated services. DNSSEC is not the same as encryption, but it is rather about ensuring that the domain owner has the information that has been provided in the domain. To fulfil other possible security gaps and opportunities, other protocols that use DNS as the base, such as Domain-based Authentication of Named Entities, can be used, which is usually overshadowed by the use of the 'secure' DNSSEC.

An Interface or Way of Understanding DNSSEC

Since DNS has weaknesses, the management of its threats has become a concern. One of the ways that this is addressed is the incorporation of DNS Security Extensions (DNSSEC). Applying it ensures that the answer to the

DNS request has not been altered, which protects against attacks such as cache poisoning. Thus, it assures the integrity of the data. However, DNSSEC does not facilitate encryption or protection and remains a commodity that serves the purpose of validating the authenticity of information [34].

DNS-based Authentication of Named Entities (DANE)

DANE uses DNSSEC as a trust anchor and allows domain owners to associate their domain with certain X509 certificates, which states that those are the only certificates that can be trusted for that specific domain. This picture may substitute or enhance the known CA system in TLS in that it gives great leverage, especially to domain owners, while at the same time increasing security by minimizing the number of external CAs used. DNSSEC is a prerequisite for DANE as it acts as the source of the DNS records on which DANE depends.

Comparison

- Trust Model:
  - DNSSEC: Built on a technically hierarchical trust structure, beginning at the root servers and going down to the client.
  - DANE: This is an enhancement of the DNSSECs trust model in that it allows the domain owner to declare the certificate information that they want to use and not solely depend on external CAs.

- Functionality:
  - DNSSEC: Protects DNS information, especially in terms of integrity and authenticity, but has no mechanisms for encryption or instructions on how the entities deep in the service layer authenticate each other.
  - DANE: Gives procedures on the effective use of DNS certificates and DNSSEC when making TLS linkages, hence ensuring that the certificates are all tied to the domain names.

- Deployment Considerations:
  - DNSSEC: This must be carefully implemented because it is susceptible. Any slight mistake in the management of public keys or signatures can be detrimental.
  - DANE: Has no existence without DNSSEC, for it relies heavily on the enforcers of DANE.

Other Relevant Standards

- DNS over HTTPS (DoH) and DNS over TLS (DoT): The protocols under this section encrypt the DNS queries aimed at improving privacy and security. However, there is no way to authenticate the DNS data itself. They can complement DNSSEC in a manner that they will both serve the purpose of encrypting and authenticating DNS data [35].
- Certificate Transparency (CT): This seeks to strengthen the CA system. Additionally, CT hopes to aid in efforts to prevent the misissuance of identity certificates. Unlike DANE, CT does not reduce reliance on CAs but seeks to make their operations more transparent.

While DANE does not purport to provide a solution for DNS integrity, it does say that it can be relied upon to reduce dependence on CAs as it allows the domain owners to manage their TLS certificates. The combination of DNSSEC with other protocols such as DoH, DoT, and CT can offer a more comprehensive security posture, addressing various aspects of DNS security and privacy.

3.4. Potential Weaknesses or Obstacles in Implementing DNS

The implementation of the Domain Name System (DNS) is indeed crucial for the functioning of the modern Internet, but it is not without difficulties. This section briefly points out some of the potential drawbacks or

problems that may be encountered during the setup and maintenance of the DNS systems, paying more attention to security, scalability and other operational aspects.

3.4.1. Technical Barriers

It can be DNS's effective integration. However, issues that may impinge deployment and operation need to be resolved, such as:

- Security Vulnerabilities: Lack of authentication measures to ensure the integrity of transactional resources in DNS enables such attacks to be launched. Such attacks include DNS Spoofing, Cache Poisoning and Denial of Service (DoS) attacks, for instance [24].
- DNSSEC Implementation Complexity: Adding DNSSEC can be a bit of a tangent with its inherent security benefits, including factors such as backward compatibility to non-DNSSEC applications, oversized response packets and, chiefly, key crypto management.
- Scalability Concerns: Changes in the volume of DNS queries growth rate will impact the performance of infrastructure, load balancers, and latency. Hence, deploying all of these may be quite a technical feat [24].

3.4.2. Financial Barriers

Almost all organizations face hefty expenses when deploying and maintaining a reliable Domain Name System, even when they rely on a single provider. This, in turn, is a derailing factor for many organizations:

- Infrastructure Costs: It include establishment and management expenses related to the servers, network equipment, backup systems, as well as making and protecting their infrastructure.
- Operational Expenses: The deployment and management of cryptographic keys and automated circumstance monitoring can be expensive, particularly for smaller organizations [25].
- Training and Expertise: There are additional expenses related to managing and securing one of the most crucial components of an organization, threat intelligence.

3.4.3. Organizational Barriers

Such factors that may impact the successful use of these DNS systems APIs are the influences that fall under social, informational or contextual cues:

- Lack of Expertise: Domain name delegation and security procedures are generally uncommon, and implementation is highly specialized, which adds to the unavailability of many experts [26].
- Resistance to Change: Advanced security measures can be strong deterrents that cost more than potential savings or lower outages [27].
- Misconfigurations and Errors: Incorrect placing of the zone files while implementing security measures may risk configuration, which leads to system functioning failure, which is commonly referred to as a mistake.
- Regulatory and Compliance Challenges: The enforcement of a General Data Protection Regulation and compliance with data protection laws in general for organizations is not easy to implement due to the certain peculiarities of different foreign regulations.

3.5. The Importance of User Awareness and Training Related to DNS Security

In recent years, a growing concern to computer security practitioners has been the security of the Domain Name System (DNS). The introduction of DNS Security Extensions has brought some improvement. However, the implementation of DNS measures is dependent on the end users and, in many cases, the understanding of training that staff have received. Human factors, as a rule, are the weakest link in any cybersecurity approach. This is why it is important to train users on the threats associated with DNS attacks and the possible measures of defence against such attacks [28].

3.5.1. The Critical Role of User Awareness

Organizations across the world have to deal with the challenges emanating from attacks based on the domain name system, such as DNS Spoofing and Cache Poisoning, which seek to take advantage of the loopholes present in the domain name system to attack users by rerouting them or injecting false information into their caches. Although the technological measures have been implemented, the success of these efforts mostly relies on user unawareness management [29]. The absence of such programs is evident when employees click phishing links or interact with compromised systems, thereby breaching the network [30].

Nonetheless, if all or most of the employees are well informed, attacked organizations are better positioned to deal with attacks based on the DNS technology. Users who best practice observance, notice suspicious activities, and report them greatly reduce the nakedness of an organization to DNS attacks. Cybersecurity and infrastructure security For instance, according to CISA, more than half of the targeted organizations were affected by billions in losses due to their phishing campaigns.

3.5.2. Training as a Mitigative Strategy

There is a need for training programs on the use of DNS targets to create awareness and preparedness in the targeted personnel. Such programs should:

- Educate on Common DNS Threats: Thorough descriptions of the operating mechanisms of and consequences of DNS-based attacks/ DNS Spoofing/Caching, such as DNS Spoofing of DNS Cache Poisoning, should be provided [30].
- Demonstrate Best Practices: Give instructions that include but are not limited to checking the legitimacy of the domain, staying away from links that seem dubious, and handling secure DNS resolvers [29].
- Simulate Attack Scenarios: Implement a periodic phishing simulation and a DNS attack simulation to determine the awareness levels and reinforce the desired behaviour from training [28].
- Promote Security Tools Usage: Several organizations implement adaptation plans, such as DNSSEC-resolver and secure browsing (DoH) [30].

3.5.3. Case Studies of Successful Implementation

A number of institutions have been able to integrate user training and skills in DNS security measures [31]. Of notable mention are:

- Verisign: Phishing and Spoofing Implementation, together with the implementation of DNSSEC, were all accompanied by brakes in the training of IT And administrative staff. This twin approach not only helped to increase the DNS integrity but also reduced the frequency with which users made errors that were related to phishing and other spoofing attempts [31].
- Global Financial Institutions: A group of global financial institutions comprised of international banks ascribed DNSSEC adoption to DNS spoofing staff education programs stressing the importance of reporting suspicious DNS altercations. Such institutions also reported about 70% decline in Spoofing of DNS during the first year of the roll out of the program [32].
- Academic Institutions: With regard to universities with a broader network that has passed up, researchers implemented the deployment of ARTICLES and TPDSE, which also introduced compulsory cyber education for students and staff. These programs depicted practical cases of DNS attacks and were complemented with practice sections on secure DNS use.

Beyond the direct risk management advantages, user training on DNS attacks can also lead to the following positive outcomes:

- Enhanced Cyber Hygiene: Users are more aware of how they operate in a digital space, which contributes to organizational safety culture.
- Cost Savings: In as much as preventing DNS-based attacks, it assists in restraining expenses incurred from data loss or service unavailability.
- Improved Trust: Organizations that have undergone training are more trusted by clients and partners, and it grows the reputation of these organizations.

Despite all these advantages, there are some barriers, which include the cost of training programs and possible cultural resistance to change. In order to bypass these barriers, senior management must be supportive, prioritize cybersecurity as a business strategy, and provide necessary resources.

3.6. Implications of DNSSEC Implementation on International Cyberspace Security

With the growing dependence on digital systems, protecting the Domain Name System (DNS) is becoming a requirement to ensure that international cyberspace is still trusted and stable. There is no question that the introduction of DNS Security Extensions (DNSSEC) has been crucial in improving the security of information by ensuring its accuracy and reliability. Nonetheless, the detailed (but superficial) analysis of the scope and potential of DNSSEC reveals that its effects reach well beyond the technical aspects of DNSSEC and encompasses the policy and strategic development in legislation, international cooperation, and international standards for cybersecurity.

3.6.1. Strengthening Global Cybersecurity Resilience

The DNS addresses fundamental and long lasting weaknesses inherent in the DNS protocol through the deployment of protocols that leverage Cryptographic keys. DNSSEC also manages to prevent malicious activities such as DNS Spoofing and cache poisoning, consequently strengthening the reliability of essential services, especially communication, and many more, such as healthcare, finance, and government [30]. This advancement aids in strengthening the global preparedness towards cyber attacks by:

- Mitigating Cross-Border Threats: Attacks that are based on DNS commonly cut across nations, affecting world supply chains and digital networks. In this respect, DNSSEC diminishes the vulnerable regions of focus, thereby lessening the chances of international networks being attacked [30].
- Enhancing Incident Response: As a means of providing prompt response to data reconstruction, DNSSEC plays a major role in identification and digging into the details of the crisis and determining the attacking points [31].

3.6.2 .Navigating Varied Regulatory Environments

The deployment of DNSSEC occurs under the protection of different jurisdictions, each showing specific national interests and levels of technology achievement. This diversity, however, presents a dilemma for the global application of DNSSEC [32].

- Fragmented Policies: Even nations with developed cybersecurity doctrine, such as the European Union's GDPR, tend to impose more stringent rules on DNS operators. Such norms can support or discourage DNSSEC aid implementation depending on national plans and policies [32].
- Harmonization Efforts: Activities by ICANN and ITU, as with many other multilateral initiatives, seek to harmonize the implementation of DNSSEC across different regions – this is critical in guaranteeing the seamless flow of operations and confidence among the players.

3.6.3. International Standards and Best Practices

The integration of DNSSEC into international security frameworks points to the increasing awareness of this security mechanism in the global policy space. Some of the key changes that have taken place include:

- ICANN's Role: As the primary steward of the DNS global root servers, ICANN has been an advocate of DNSSEC installation through the "Key Signing Key (KSK) Rollover" movement that proved payload running secure key operation using key management on a worldwide level is achievable [31].
- Collaboration with Industry Standards: The other agencies, such as the Internet Engineering Task Force (IETF), have developed protocols that were missing, including DNS over HTTPS (DoH) and DNS over TLS (DoT) that have improved the parameters of DNSSEC by meeting the confidentiality of its user data [32].

3.6.4. Case Studies with a Focus on Regional and National Scenarios

A survey of the developed DNSSEC within different regions should also be considered as one that highlights operational and strategic issues as follows:

- European Union: Several EU member states incorporated DNSSEC in the overall critical infrastructure protection strategy. For example, the early Swedish implementation of the DNSSEC at the national level succeeded in reducing DNS targeting attacks and prompted similar activities in other European regions.
- United States: With the Federal Information Security Management Act (FISMA), there has been an official policy that has adopted DNSSEC at the federal agencies. Although the implementation was initially faced with resistance, these efforts have contributed positively to the protection of the public sector networks.
- Asia-Pacific Region: Countries such as Japan and Australia have set out to include DNSSEC within the broader strategies of their digital transformations. However, the rates of adoption are very different owing to the level of technical capabilities and policy orientation.

There are, however, significant challenges that DNSSEC must confront to convince people around the world to accept it:

- Resource Constraints: Many developing countries do not have enough human skills and money to implement DNSSEC, thereby increasing the digital divide.
- Interoperability Issues: Different DNS infrastructures and resolutions exist, so the systems in different areas can affect the smooth flow of adoption.

Amplification of Risks: manipulates DNS security, which depends on larger response sizes to achieve its means, thereby increasing the risk of DNS amplification DDoS attacks, so it requires additional mitigation techniques.

4. Results and Discussion

4.1. Comparison of Studies

As gleaned from the review of related past works, it may be concluded that vulnerabilities such as DNS Spoofing and Cache Poisoning still pose threats to the security of the DNS. It has been demonstrated in this study that the use of DNSSEC constitutes an efficient means of increasing the trustworthiness of DNS information. Below is a comparison based on several studies.

- DNSSEC for Cyber Forensics: It has been shown that DNSSEC can deter Cache Poisoning through digital signatures and reduce its prevalence by 75%. This is also useful as a forensic tool for network attacks, as DNSSEC offers cryptographic proof. However, its limited use highlights the need for easier and more efficient ways of applying it [1].
- A Deep Dive on Recent Widespread DNS Hijacking Attacks: This study illustrates how DNS hijacking is prevented through the use of digital signatures for data validation by DNSSEC. DNSSEC, with all means given credence, can ameliorate the chances of web traffic being redirected to other sites that are malicious. However, the reasons cited for its non-use by most service providers are its very low cost and lack of infrastructure [4].

- The Effect of DNSSEC on Security Concerns and DNS Latency: The most important finding from this study is that DNSSEC decreases the success rate of spoofing attacks by approximately 85%. However, it increases the average network latency by about 15-20%. Another problem is the requirement for more devices like HSMs, which adds to the difficulty of implementation [2].
- DNSSEC and Its Contribution to the Protection of the Internet: In this research, the significance of the Chain of Trust model is drawn, which is based on the utilization of Delegation Signer (DS) Records to strengthen the consistency of the DNS data. Also, the use of DNS over TLS (DoT) together with DNSSEC is recommended for added security [3].
- Standard Operating Systems and DNS Cache Poisoning Attacks: The said study in this paper shows that enjuring DNSSEC decreases the occurrence of Cache Poisoning by almost 75%, particularly on newer OS, which can disable the digital signature. However, the use of old DNS resolvers still presents a major barrier [5].
- Best Practices for DNS Security: This study indicates that it might be possible to combine the strengths provided by DoH and DNSSEC into a hybrid solution that ensures communication privacy and data authentication respect. This makes way for the better securing of the domain name system [6].

4.2. Analysis of DNSSEC Effectiveness

- Addressing DNS Spoofing: Yet another subproblem of interest is known as DNS Spoofing, as there have been instances in the past where the DNS was able to be hijacked. So, in this case, how does DNSSEC solve this problem? Signing material ensures that the data is being altered within the range of its authentic data (Shulman & Waidner, 2021) [1, 13]. However, in this instance, it is also important to take into consideration that this approach is only ideal under certain deployment rates and system acceptances (Cloudflare, 2022) [2, 12].
- Addressing Cache Poisoning: So, as a way to prevent the cache from being poisoned, how does the attack get impeded? Resolvers that are not able to understand the language of DNSSEC would be able to undermine this measure, making it ineffective (APNIC by Keyu Man, 2023) [5, 17].
- Comparison with Other Solutions: It is quite amusing how DNSSEC application requirements such as authentication are never a necessity when it comes to using other protocols like DoH and DoT. Not to mention that if these protocols are utilized, it can enhance the security of the DNS data further (TechTarget by Damon Garn, 2022) [6, 9, 13].

4.3. DNSSEC Implementation Challenges

- System Compatibility: However, due to technological incompatibilities, DNSSEC often disallows older DNS resolvers from supported signed responses, further pushing the universal acceptance of the two technologies apart (MIT Team, 2023) [7, 16].
- Implementation Costs: When it comes to internet security, the costs can really depend on the purpose of providing that security. The implementation of DNSSEC would include investments in technologies, labor, or cryptography which can be seen as extensive for smaller and medium enterprises (Krebs, 2020) [4, 15].
- Additional Latency: It seems that the process of ensuring such security does set a limit on further observation and automatic responses. (Cloudflare, 2022) [2, 9].

5. Conclusion

In the present study, we examine DNS Security Extensions, their relevance, and how they help enhance the security of the domain name system. The technology of DNSSEC has been able to eliminate the risk of DNS Spoofing and Cache Poisoning attacks by means of data verification processes through the use of digital signatures. The study also identifies several challenges in its implementation, such as compatibility with legacy systems, technical issues in the management of cryptographic keys, or expensive deployment. However, the benefits of DNSSEC in decreasing threats to cyberspace and increasing reliance on the global internet framework certainly

surpass these concerns. For the successful adoption of DNSSEC, however, legal backing, expertise, and transition to other technologies like DoH and DoT are very important. For such purpose, it is then possible to employ measures DNSSEC. Such a situation gives the possibility of creating a safe and public DNS system using the DNSSEC technology.

References

[1] Haya Shulman, and0 Michael Waidner, "DNSSEC for Cyber Forensics," *EURASIP Journal on Information Security*, vol. 2014, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[2] Cloudflare, How does DNSSEC work?. [Online]. Available: https://www.cloudflare.com/learning/dns/dnssec/how-dnssec-works/

[3] S. Ariyapperuma, and C.J. Mitchell, "Security Vulnerabilities in DNS and DNSSEC," *The Second International Conference on Availability, Reliability and Security (ARES'07)*, Austria, pp. 335-342, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[4] A Deep Dive on the Recent Widespread DNS Hijacking Attacks, Krebs on Security, 2019. [Online]. Available: https://krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-widespread-dns-hijacking-attacks/

[5] Keyu Man, Modern OSes are Prone to Side-Channel-Based DNS Cache Poisoning Attacks, APNIC, 2021. [Online]. Available: https://blog.apnic.net/2021/11/30/modern-oses-dns-cache-poisoning-attacks/

[6] Damon Garn, DNS Security Best Practices to Implement Now, TechTarget, Search Security, 2024. [Online]. Available: https://www.techtarget.com/searchsecurity/tip/DNS-security-best-practices-to-implement-now

[7] Ramaswamy Chandramouli, and Scott Rose, Secure Domain Name System (DNS) Deployment Guide, NIST Special Publication, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[8] DNS Amplification Attacks, America's Cyber Defense Agency, Cybersecurity and Infrastructure Security Agency (CISA), 2019. [Online]. Available: https://www.cisa.gov/news-events/alerts/2013/03/29/dns-amplification-attacks

[9] Niels L.M. van Adrichem et al., "A Measurement Study of DNSSEC Misconfigurations," *Security Informatics*, vol. 4, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[10] DNSSEC Complexities and Considerations, Cloudflare. [Online]. Available: https://www.cloudflare.com/dns/dnssec/dnssec-complexities-and-considerations/

[11] DNSSEC, Asia-Pacific Network Information Centre. [Online]. Available: https://www.apnic.net/community/security/dnssec/

[12] Cache Poisoning, DNS Security Resource Center, DNS Security Issues & Threats, Infoblox. [Online]. Available: https://www.infoblox.com/dns-security-resource-center/dns-security-issues-threats/dns-security-threats-cache-poisoning/

[13] Six Ways to Strengthen DNS Security, CSC. [Online]. Available: https://www.cscdbs.com/en/resources-news/six-ways-to-strengthen-dns-security/

[14] "DNS Cache Poisoning: The Risks, Mechanisms, and How to Prevent It, Indusface, [Online]. Available: https://www.indusface.com/learning/dns-cache-poisoning/

[15] Fortifying Your Online Identity: Safeguarding Domain Names from Cache Poisoning, Domain Name Security, DN.Org, 2024. [Online]. Available: https://dn.org/fortifying-your-online-identity-safeguarding-domain-names-from-cache-poisoning/

[16] Jason Bau, and John C Mitchell, "A Security Evaluation of DNSSEC with NSEC3," *Cryptology ePrint Archive*, 2010. [Google Scholar] [Publisher Link]

[17] Geoff Huston, "Measuring the Use of DNSSEC," 2023. [Online]. Available: https://blog.apnic.net/2023/09/18/measuring-the-use-of-dnssec/

[18] Referensi Skema Normalisasi, DNS Advanced Security Information Model (ASIM) (Pratinjau Umum), Microsoft Learn Challenge, 2024. [Online]. Available: https://learn.microsoft.com/id-id/azure/sentinel/normalization-schema-dns

[19] Imperva, What is Domain Name System (DNS) Spoofing?, Imperva. [Online]. Available: https://www.imperva.com/learn/application-security/dns-spoofing/

[20] What is DNS Cache Poisoning?, DNS Spoofing. [Online]. Available: https://www.cloudflare.com/en-gb/learning/dns/dns-cache-poisoning/

[21] Christopher Makarem, How DNSSEC Works, Medium, 2018. [Online]. Available: https://medium.com/iocscan/how-dnssec-works-9c652257be0

[22] CVE-2021-25220, "DNS Forwarders - Cache Poisoning Vulnerability," ISC, 2022. [Online]. Available: https://kb.isc.org/docs/cve-2021-25220

[23] Lulien Sobrier, Brazilian Bank Targeted by Phishing Site and DNS Poisoning, Zscaler Blog, 2011. [Online]. Available: https://www.zscaler.com/blogs/security-research/brazilian-bank-targeted-phishing-site-and-dns-poisoning

[24] Top 5 Integration Challenges in DNS Management, DomainSure. [Online]. Available: https://domainsure.com/news/top-5-integration-challenges-in-dns-management/

[25] 8 DNS Email Authentication Obstacles (and Solutions), ValiMail. [Online]. Available: https://www.valimail.com/blog/dns-email-authentication-challenges/
[26] Futuramo, Common DNS Issues and their Solutions, Futuramoblog. [Online]. Available: https://futuramo.com/blog/common-dns-issues-and-their-solutions/
[27] Moritz Muller, Addressing the Challenges of Modern DNS, APNIC, 2022. [Online]. Available: https://blog.apnic.net/2022/07/29/addressing-the-challenges-of-modern-dns/
[28] Admir Dizdar, "What is DNS Attack and How to Prevent them," Bright, 2022. [Online]. Available: https://brightsec.com/blog/dns-attack/
[29] Nagaraju Pureti, "Cyber Hygiene: Daily Practices for Maintaining Cybersecurity Nagaraju Pureti," *International Journal of Advanced Engineering Technologies and Innovations*, vol. 1, no. 3, pp. 35-52, 2021. [Google Scholar] [Publisher Link]
[30] Paul Rosenzweig, "The International Governance Framework for Cybersecurity," *Canada-United States Law Journal*, vol. 37, no. 2, pp. 405-432, 2012. [Google Scholar] [Publisher Link]
[31] Giovanni Schmid, "Thirty Years of DNS Insecurity: Current Issues and Perspectives," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2429-2459, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[32] S. Abirami, and R. Naresh, "DNS Enhancement with DNSSEC and DoT for Enhanced Online Security," *2024 2nd International Conference on Networking and Communications (ICNWC)*, Chennai, India, pp. 1-11, 2024. [CrossRef] [Google Scholar] [Publisher Link]
[33] Akshay Mammen Koshy et al., "An Insight into Encrypted DNS Protocol: DNS over TLS," *2021 4th International Conference on Recent Developments in Control, Automation & Power Engineering (RDCAPE)*, Noida, India, pp. 379-383, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[34] DNSSEC-What is It and Why is it Important?, ICANN. [Online]. Available: https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en
[35] What is the Difference between DNSSEC & DNS Security?, Infoblox. [Online]. Available: https://www.infoblox.com/dns-security-resource-center/dns-security-faq/what-is-the-difference-between-dnssec-dns-security/

Glossary of Terms

Amplification Attack: One type of DDoS attack, such as an amplification attack, sends high amounts of data to a target by sending a large volume of requests to the DNS servers.

Authoritative DNS Server: This type of server is responsible for providing authoritative IP address information for specific domain names to resolvers that request this information from the servers

Backward Compatibility: This is one of the features that is said to be one of the issues when the implementation of DNSSEC has newer protocols or systems co-existing with the older ones.

Cache Poisoning: This is a type of cyber-vandalism that targets the DNS server and, in several instances, has created websites that are not the original targets.

Cache TTL: Some attackers use cache poisoning attacks that manipulate the time to live by changing the value so that the DNS resolver keeps a negative response for too….

Certificate Authority: This is an authority that is used to verify the ownership of public keys by issuing digitally signed certificates for secure SSL/TLS communications.

Chain of Trust: This is a layer of chains that form the DNSSEC where the topmost level is the DNS root and the highest level of trust, and each level can designate authority of the level lower to it. .

Cryptographic Signature: Supposed to be called a mathematical function that helps to ascertain the authenticity and integrity of a message or any data, particularly in the area in which this is largely employed in DNSSEC.

DANE (DNS-based Authentication of Named Entities): This protocol utilizes DNSSEC to link X.509 certificates and domain names, minimizing dependence on third party certification authorities for validation purposes.

Delegation Signer (DS) Record: This is a type of record in DNSSEC that is issued in the DNS to link together a child zone and its parent zone so as to form a chain of trust.

Digital Signature Algorithm (DSA): A method of signing is called 'DSA', a method employed by DNSSEC to sign data so that its origin can be verified.

DNSSEC, or Domain Name System Security Extensions, is a network protocol that was created to add security to DNS servers by using electronic signatures to DNS records and thus serves to guarantee the authenticity of certain information contained in the DNS as well as allows for the establishment of a hierarchy of trust among DNS records.

DNS Spoofing: A method of deception in which sinister individuals distribute phoney DNS responses with the intention of steering other people to non-legitimate or villainous sites without their consent.

DNS over HTTPS: RFC 8484. Internet Engineering taskforce 2018. US copyright: IETF. A protocol that seeks to reduce user spying by using HTTPS encryption for DNS queries.

DNS over TLS (DoT): A protocol used for DNS queries where TLS is used to encrypt queries, thus creating a protected channel for DNS communication.

DNS Resolver: It is a server that calls for DNS records controlled by a user. To begin with, all calls for these records start from the root zone until they get the required record.

Domain Name System (DNS): There are many arrangements, and the simplest is the international standard of the Domain Name System (DNS), in which a human friendly site address in the form of www.domain-name.com is converted to an address that a computer can understand, for the case in the internet.

Forwarder: Some types of DNS servers use it as a target. It is a DNS server that is set to forward the requests it cannot satisfy at that location to other DNS servers located elsewhere.

Intermediate DNS Server: It is a resolver type that serves users' requests either by returning a cached response or by forwarding the request to an authoritative server through a chain of servers.

IP Address: In any device that uses an Internet Protocol for networking, there is an entire and distinct aggregation of numbers that is indicative of the device. It is an IPv4 structure, for instance (192.168.1.1), while that of IPv6 includes (2001:0db8:1).

Kaminsky Attack: This is a well-known type of attack on DNS by damaging cache DNS. The seizure of a DNS is beset by injection during the exchange of requests through the discrete transaction ID method.

Key Signing Key (KSK): The signing key of a Zone Signing Key (ZSK) is one of the instruments in the DNSSEC that enhances the security of DNS traceable keys to the ancestry key.

Latency: The time it takes from the initiation to the completion of the DNS request. It is the use of a strong encryption process that comes to the us version of the games that increases latency.

Man-in-the-Middle (MITM) Attack: An attack in the cyber warfare domain where an attacker secretly relays and possibly alters the communication between two parties who believe that they are directly communicating with each other.

Public Key Infrastructure (PKI): It is a framework that uses public and private keys in a manner that promotes confidentiality and authentication, which is crucial for the digital signature mechanism of DNSSEC.

Recursive Resolver: A DNS server that asks other DNS servers to look up the appropriate IP address for a domain name on behalf of the user.

Resource Record Set (RRset): A set of DNS records containing the same label, class, and type but differing in value, which are, for the most part, used in DNSSEC for signing and validation.

Root Zone: The highest level of the hierarchy in the Domain Name System, which holds information about the most specific domains, such as .com and .org domains. It is the base for resolving DNS.

Transaction ID: Identifying elements within DNS queries and responses to aid in their matching. Pouring weaknesses in its practical application may invite attacks such as cache poisoning.

Upstream DNS Request: An IP address request that a resolver sends to another DNS server (e.g. authoritative server) because it does not have a request of an IP address in the cache.

Zone File: A specific file in text form storing the set of domain names of a particular location as well as host addresses and other DNS settings for that zone.

ZONEMD Resource Record: A check of a zone file/dataset's integrity through a hash function applied on the entire zone file and a further means of verification for zone data.

Zone Signing Key (ZSK) A key used in subzones of DNS under DNSSEC to sign specific DNS records to hold their values and content secure.