

Cybersecurity Challenges in Managing Domain Names. From DNS to ENS in the Web3 Era

Adrian-Victor VEVERA¹, Andreea Cătălina CRĂCIUN¹, Mihail DUMITRACHE^{1,3}, Ionut SANDU¹,
Carmen-Ionela ROTUNĂ^{1,2}, Radu Alexandru BOSTAN¹

¹National Institute for Research & Development in Informatics - ICI Bucharest

²Politehnica University of Bucharest

³University of Bucharest, Faculty of Letters

victor.vevera@ici.ro, andreea.craciun@ici.ro, mihail.dumitrache@ici.ro, ionut.sandu@ici.ro, carmen.rotuna@ici.ro, alexandru.bostan@ici.ro

Abstract: The Domain Name System (DNS) remains a foundational component of the Internet infrastructure, which is frequently exploited by cybercriminals through increasingly diverse and sophisticated attack vectors. This paper explores the evolving cybersecurity challenges faced by domain name systems (DNSs) and their decentralized counterparts in the Web3 ecosystem, particularly the Ethereum Name Service (ENS), as such, it surveys both the established and novel attack patterns. Furthermore, it explores the implications of decentralized naming systems like the ENS, which introduced novel cybersecurity challenges within the Web3 environments and it highlights the future risks and possible research directions related to the transition to decentralized web services. This study provides a comparative analysis of the cyberattacks targeting the DNS and the ENS, highlighting the evolving threat landscape for each of the two ecosystems. By examining the architectural differences between the DNS and ENS, their common attack vectors, and their security mechanisms, it underscores both the distinct vulnerabilities inherent to each ecosystem and the overlapping risks they share.

Keywords: DNS, ENS, cybersecurity, threats, cyberattacks.

INTRODUCTION

Internet infrastructure relies on the domain name system (DNS) which enables navigation by mapping human-readable names to IP addresses. However, the very openness and accessibility that underpin DNS have made it a main target for a wide array of cyberattacks. Traditional DNS protocols were not designed

with strong security in mind, leaving gaps that attackers have long exploited through tactics such as hijacking, cache poisoning, and domain impersonation.

Simultaneously, the rise of Web3 and decentralized platforms like Ethereum has introduced a new architecture, that is ENS. While promising greater domain ownership, censorship resistance, and cryptographic

security, these systems are not immune to attacks and inherit a part of the vulnerabilities of the DNS system while introducing others unique to their decentralized, smart-contract-based nature.

This paper provides a structured examination of technical risks in domain name systems, both the classical and decentralized ones. By assessing the existing protective measures and outlining the emerging attack models, it aims to provide a clear technical understanding of how a domain name infrastructure can be hardened against the evolving threats (Vevera, 2018).

The remainder of this paper is as follows. The second section highlights the state of the art in domain names cybersecurity, while the third section describes the role of DNS Security Extensions (DNSSEC) and their limitations. The fourth section provides a comprehensive overview of domain name system attacks, and the fifth section describes the future developments in domain name systems, that is Web3 and ENS, and the emerging risks. Further on, the sixth section highlights the Domain Names Cybersecurity Mitigation Methods. Finally, the seventh section presents the conclusion of this study.

STATE OF THE ART IN DOMAIN NAME CYBERSECURITY

The Domain Name System (DNS) remains one of the most important yet vulnerable components of the Internet infrastructure. Designed in an era with minimal security considerations, DNS has become a primary target for a wide spectrum of cyber threats. In response, researchers and engineers have developed numerous defensive mechanisms aimed at improving resilience, ranging from cryptographic protocols to intelligent anomaly detection systems. Simultaneously, the advent of decentralized naming systems like the Ethereum Name Service (ENS) has introduced both novel opportunities and new attack surfaces.

The most prominent standard for securing DNS is the Domain Name System Security Extensions (DNSSEC), which authenticates

DNS responses using digital signatures. By establishing a chain of trust from the DNS root to individual domain zones, DNSSEC helps prevent cache poisoning and data spoofing. However, DNSSEC suffers from several operational challenges, including complicated key rollover procedures, a limited support for automated debugging, and performance overheads due to large cryptographic payloads (Ariyapperuma & Mitchell, 2007; Rishith et al., 2024).

Alternatives and supplements to DNSSEC have been proposed to address these limitations. DNSCurve employs elliptic-curve cryptography to encrypt DNS queries and responses, offering a better protection against eavesdropping and man-in-the-middle attacks while maintaining performance efficiency (Anagnostopoulos et al., 2012). More recently, DNSSEC+, a hybrid scheme combining resolver authentication and lightweight trust models, has demonstrated an improved scalability and a reduced latency during DNS resolution (Sadeghi Jahromi et al., 2024).

With the increasing sophistication of DNS-based attacks, machine learning has emerged as a promising tool for threat detection. Supervised and unsupervised models are employed to analyze DNS traffic patterns, detect domain fluxing behavior, and identify features indicative of malicious activity. Techniques such as random forests, clustering algorithms, and neural networks have been applied to detect botnets, DNS tunneling, and domain impersonation (Sadegh-Zadeh & Tajdini, 2025; Kusumi et al., 2025).

These methods typically rely on domain metadata, lexical analysis of domain names, temporal query behavior, and DNS record consistency to flag anomalies. While effective in controlled environments, their accuracy in real-world applications depends heavily on dataset quality, feature engineering, and resistance to adversarial evasion.

Beyond cryptographic and behavioral detection approaches, DNS infrastructure itself is being rearchitected to mitigate threats. Filtering systems are deployed at recursive resolvers to reduce the risk of amplification attacks and domain abuse. Hasegawa et al.

(2023) proposed a FQDN-based whitelist filter that dynamically allows only domains with verified positive DNS responses, thus limiting the exposure to DNS water torture DDOS attacks.

In addition, authoritative DNS services now frequently incorporate rate limiting, query minimization, and aggressive caching strategies to reduce information leakage and service exhaustion. The integration of DNS logging with SIEM (Security Information and Event Management) platforms further supports real-time alerting and forensic analysis.

Decentralized naming systems, particularly the Ethereum Name Service (ENS), represent a shift toward blockchain-based domain ownership. ENS maps human-readable names to Ethereum addresses and resources via smart contracts, offering several benefits such as censorship resistance and user-controlled identity. However, this paradigm introduces new vulnerabilities.

ENS is susceptible to front-running attacks, where adversaries preemptively register the desired domain names by monitoring the pending transactions and offering higher gas fees. Vulnerabilities in smart contracts can lead to domain loss or hijacking, and malicious resolver contracts may redirect users to unauthorized destinations. The absence of traditional recovery mechanisms, such as registrar intervention, further exacerbates these issues (Sinha, 2025; Dixon, 2024).

Hybrid vulnerabilities are also emerging where DNS names are bridged to ENS records. If the DNS layer is compromised, for example via hijacking or spoofing, it can lead to fraudulent associations at the ENS level. Additionally, expired domain name sniping, phishing through visually similar names (homoglyph attacks), and reverse record manipulation represent ongoing concerns for decentralized domain systems.

The state of the art reflects an increasingly layered approach to domain name cybersecurity. No single solution suffices across the varied landscape of threats. Instead, a combination of cryptographic validation, behavioral analytics, architecture hardening, and decentralized governance is needed to protect the naming systems.

Recent work suggests that bridging the best features of both DNS and ENS could pave the way toward a more secure and user-centric domain naming future. Further research is essential to develop interoperable protocols, lightweight trust models, and efficient systems that can withstand both technical and social engineering attacks.

THE ROLE OF DNS SECURITY EXTENSIONS (DNSSEC) AND LIMITATIONS

The Domain Name System Security Extensions (DNSSEC) specifications represent a step forward in preventing attacks on the Domain Name System (DNS). The DNS is a key component of the critical infrastructure of the Internet, and its proper functioning is essential for Internet users. However, DNS was designed with a view to availability rather than security. It has no authentication mechanism and is currently the primary Internet attack vector for cyber-criminals. As such, due to its widespread use, flexibility and its vital role in the Internet, DNS presents an extremely high-value target for online data theft and other online attacks (Southam, 2014).

DNSSEC (Domain Name System Security Extensions) enhances the security of the DNS by incorporating asymmetric cryptographic algorithms. It ensures the authenticity and integrity of DNS data by digitally signing all records within a domain's DNS zone. These digital signatures, along with the corresponding public cryptographic keys, are published through the DNS system itself.

To validate DNSSEC data, a DNS resolver starts with a trusted public key from the DNS root zone and systematically verifies each level in the DNS hierarchy, forming a complete chain of trust. For a domain to be fully validated, its parent zone must publish a Delegation Signer (DS) record. This DS record links the parent zone to the child zone's DNSSEC information, allowing resolvers to authenticate the entire trust chain from the root to a specific domain.

While researching how DNSSEC works, Ariyapperuma & Mitchell (2007) found a range

of vulnerabilities and operational challenges. It does not protect against poor configuration in the authoritative name server and does not protect against buffer overruns or Distributed Denial-of-Service (DDoS) attacks. DNSSEC works based on a hierarchical trust model, meaning that a key injection attack can undermine the integrity of the entire trust path. Furthermore, the key size, algorithm and validity period should be taken into account as they determine the key functionality. Being more complex than DNS, DNSSEC does not benefit from plenty of management tools, therefore, the debugging is mainly performed manually. Other challenges include key rollovers, timing issues, an increased computational load and the lack of consistency control (Ariyapperuma & Mitchell, 2007).

There are several DNSSEC alternative solutions, most of them aiming to solve the issues within DNSSEC. Anagnostopoulos et al. (2012) provided a comprehensive side-by-side comparison between DNSSEC and DNSCurve, a new secure protocol for the DNS, providing confidentiality, integrity and availability. While DNSSEC has most of its features standardized, DNSCurve offers a stronger security against man-in-the-middle attacks, while keeping the computational load of the nameserver low. In spite of its enhanced security, DNSCurve obscured some of DNS protocol characteristics. DNSSEC complies better with DNS protocol, but increases the workload of the nameserver and increases the overall response time. Taking into account all the advantages from both protocols, they concluded that a new tool combining these features could be useful in providing secure and reliable DNS services (Anagnostopoulos et al., 2012).

Ali Sadeghi Jahromi et al. (2024) introduced a new scheme, DNSSEC+, built for the second stage of a DNS resolution process which consists in the interaction between resolvers and nameservers. The new scheme, built on the original DNS scheme and using a DNSSEC-like trust model, aims to mitigate name resolution privacy and security with a minimal impact on system performance. The proof of concept has shown promising results in comparison with

other DNS schemes, both time-wise as regards the DNS resolution and server-side processing and performance-wise as regards the CPU utilization.

A COMPREHENSIVE OVERVIEW OF DOMAIN NAME SYSTEM ATTACKS

The Domain Name System (DNS) remains a critical component of Internet infrastructure, but its vulnerabilities have increasingly become targets for a wide range of cyberattacks. Understanding the typology and mechanisms of these attacks is essential for strengthening the cybersecurity defenses and maintaining the integrity of digital ecosystems.

One significant attack is the NXDOMAIN Flood, wherein excessive DNS queries are intentionally directed toward non-existent domains, overwhelming the recursive servers and degrading their performance. DNS Hijacking exploits system misconfigurations or server breaches to redirect legitimate traffic to malicious destinations. Similarly, Fast Flux techniques rotate IP addresses linked to a single domain name rapidly, obfuscating the actual location of malicious servers.

Another pervasive threat is Domain Bulk Registration Abuse, involving the automated mass acquisition of domains used for phishing, spam, and evasion tactics. Complementary to this, Domain Impersonation seeks to deceive users by registering lookalike domains to harvest sensitive information. DNS Botnet Attacks deploy compromised devices for coordinated assaults on DNS infrastructures, often leading to service disruptions.

Further on, visual deception plays a role in Homoglyph Attacks, where similar Unicode characters are exploited to create domains that visually mimic legitimate ones. Meanwhile, Social Engineering attacks manipulate human behavior rather than technical vulnerabilities to gain unauthorized access or information.

Intercepting communications without the knowledge of the involved parties defines Man-in-the-Middle (MitM) attacks, which compromise both confidentiality and data integrity. DNS

Cache Poisoning and DNS Spoofing share the objective of corrupting DNS responses to misdirect users to fraudulent or malicious sites.

Data exfiltration tactics such as DNS Tunneling leverage legitimate DNS queries to covertly transfer information from compromised networks. User input errors are exploited in Typosquatting, where attackers register mistyped domain names to deceive inattentive users. Subdomain Takeover exploits improperly decommissioned subdomains to gain control over the associated resources.

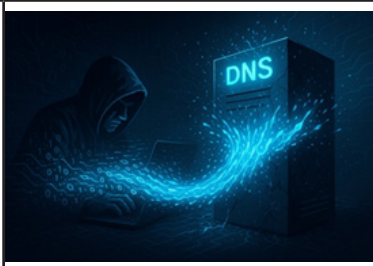


Operational abuses such as Domain Kiting, involving repeated domain registration and cancellation without payment, and Registrar Hijacking, the unauthorized manipulation of domain registration accounts, further threaten domain ownership security.






Performance degradation is targeted by Phantom Domain Attacks, which flood DNS resolvers with requests to slow or non-responsive domains. In this context, integrity assurance mechanisms are also at risk. Broken Trust Chains in DNSSEC arise when cryptographic links between DNS zones fail, undermining secure validation processes.





Finally, DNS Amplification Attacks exploit open DNS resolvers to flood targets with large volumes of unsolicited traffic, intensifying the Distributed Denial of Service (DDoS) assaults.

Altogether, these nineteen attack vectors highlight the multifaceted vulnerabilities inherent to the DNS infrastructure. Addressing them demands a combination of technical reinforcement, organizational vigilance, and continual research into the emerging threats.



Table 1. *DNS Threat Landscape*

NXDOMAIN Flood (Apostu et al., 2025)	The NXDOMAIN Flood attack involves the intentional generation of an excessive volume of DNS queries towards non-existent domains, aiming to exhaust the resources of recursive servers and degrade their performance.	
DNS Hijacking (Houser et al., 2021)	DNS Hijacking involves the unauthorized manipulation of domain name resolution by compromising DNS servers or system configurations, resulting in the redirection of traffic to malicious destinations.	
Fast Flux (Logaprakash et al., 2025)	Fast Flux is an evasion technique used by malicious infrastructures to conceal the real location of servers through frequent rotation of the IP addresses associated with a single domain name.	

Domain Bulk Registration Abuse (Lim et al., 2025)	Domain Bulk Registration Abuse refers to the automated acquisition of a large number of domains, often used for illicit purposes such as phishing, spam, or evading detection.	
Domain Impersonation (Simpson et al., 2020)	Domain Impersonation involves registering domain names that imitate legitimate names with the intention of deceiving users in order to extract sensitive information or compromise systems.	
DNS Botnet Attacks (Mathew et al., 2025; Sheheryar & Sharma, 2025; Rawat et al., 2025)	DNS Botnet Attacks utilize distributed networks of compromised devices to launch coordinated campaigns aimed at overwhelming or manipulating DNS infrastructure.	
Homoglyph Attacks (Almuhaideb et al., 2022)	Homoglyph Attacks exploit visual similarities between Unicode characters to create fraudulent domains that are difficult to distinguish from legitimate ones, thereby deceiving users.	
Social Engineering (Birthriya et al., 2025; Rathod et al., 2025)	Social Engineering represents a non-technical threat vector that targets the behavioral manipulation of individuals to facilitate the disclosure of information or unauthorized access to secured systems.	

<p>Man-in-the-Middle (MitM) (Faqrunnisa et al., 2025 ; Fereidouni et al., 2025 ; Basri et al., 2025)</p>	<p>A Man-in-the-Middle attack involves intercepting and potentially altering communications between two entities without their knowledge, thereby compromising data confidentiality and integrity.</p>	 <p>MAN-IN-THE-MIDDLE</p>
<p>DNS Cache Poisoning (Afek et al., 2025)</p>	<p>DNS Cache Poisoning is an attack where falsified information is introduced into a DNS resolver's cache, leading to the delivery of altered responses to user queries.</p>	 <p>CACHE POISONING</p>
<p>DNS Spoofing (Panda et al., 2025; Jadoaa et al., 2025)</p>	<p>DNS Spoofing consists in generating counterfeit DNS responses to redirect legitimate user requests to unauthorized or malicious entities.</p>	 <p>Falsified Response</p> <p>Falsified Response</p>
<p>DNS Tunneling (Bykov & Chernyshov, 2024)</p>	<p>DNS Tunneling involves using DNS protocols to covertly transmit data between a client and a server, being often employed for information exfiltration from compromised networks.</p>	 <p>DNS</p>

Typosquatting (Moubayed et al., 2018)	Typosquatting refers to the registration of domain names containing common typing errors for well-known addresses, which are exploited to deceive inattentive users.	
Subdomain Takeover (Biswas et al., 2023)	Subdomain Takeover becomes possible when a subdomain points to a non-existent resource, allowing an attacker to register that resource and gain control over it.	
Domain Kiting (Rodenbaugh, 2009)	Domain Kiting refers to the abusive practice of repeatedly registering and canceling domain names within the grace period to avoid payment, thus exploiting the registration system.	
Registrar Hijacking (Chung et al., 2017)	Registrar Hijacking involves the unauthorized access to a domain registrar account, allowing the attackers to modify or transfer DNS records illegitimately.	
Phantom Domain Attack (Ramdas & Muthukrishnan, 2019)	Phantom Domain Attacks target the performance of DNS resolvers by initiating requests to slow or non-functional domains, causing systematic delays in traffic processing.	

Broken Trust Chains in DNSSEC (Rishith et al., 2024)	Broken Trust Chains in DNSSEC occur when cryptographic links between DNS zones are absent or invalid, undermining the secure validation of DNS data.	
DNS Amplification Attack (Kambourakis et al., 2007)	A DNS Amplification Attack is a form of Distributed Denial of Service (DDoS) attack where open DNS servers are exploited to amplify the traffic volume directed at a target, by sending forged requests that generate large response packets.	

FUTURE DEVELOPMENTS IN DOMAIN NAME SYSTEMS SUCH AS WEB3, ENS, AND EMERGING RISKS

The domain name ecosystem is transitioning into a new paradigm with the emergence of blockchain-based solutions such as the Ethereum Name Service (ENS) and platforms like Unstoppable Domains. These decentralized alternatives promise an enhanced ownership, censorship resistance, and interoperability within the Web3 infrastructures. However, while decentralization mitigates certain vulnerabilities inherent to the traditional DNS, it also introduces novel attack vectors that echo the existing risks.

Domain Squatting persists in both the DNS and ENS environments. In ENS, attackers their practices resembling classic cybersquatting practices classic cybersquatting practices found in DNS. Similarly, Phishing with Fake Domains is prevalent, where fake .eth domains trick users into transferring cryptocurrencies to malicious addresses, mirroring phishing attacks based on typosquatting and homoglyph manipulation in DNS.

Front-Running represents another critical challenge. In ENS, adversaries monitor the pending transactions to preemptively register high-value domain names by paying higher gas

fees, which is similar to domain front-running observed among opportunistic DNS registrars. Meanwhile, Smart Contract Exploitation threatens ENS integrity, as the vulnerabilities inherent to smart contracts are abused for unauthorized control which parallels the exploitation of the configuration weaknesses in DNS management protocols.

A hybrid vulnerability arises with DNS-ENS Bridging Attacks, where traditional DNS hijacking compromises the linkage between DNS names and ENS records. Likewise, Reverse Record Manipulation enables the impersonation of trusted Ethereum addresses in ENS, in order to manipulate PTR records in DNS for spoofing attacks.






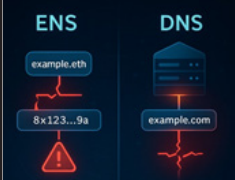
The phenomenon of Expired Domain Sniping also extends into ENS, where attackers swiftly register valuable expired domain names to hijack their identity or reputation, making it equivalent of traditional domain sniping in DNS registries. Additionally, Social Engineering remains a potent tactic, deceiving users to disclose private keys in ENS or targeting DNS administrators.


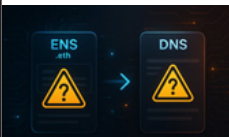
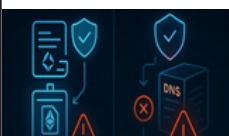
Finally, Malicious Resolver Contracts in ENS, deploying altered smart contracts to steal funds, reflect malicious DNS resolver behaviors seen in cache poisoning and DNS spoofing.

In conclusion, while Web3 naming services unlock a tremendous potential for sovereignty and innovation, they inherit familiar threats and introduce complex new risks. Therefore,

coordinated advances in decentralized security standards and cross-layer threat mitigation will be essential for safeguarding the future of digital identity.

Table 2. *ENS Threat Landscape*

Type of Attack	ENS Attack Description	Similar DNS Attack	
Domain Squatting	Registering popular .eth names to resell them or deceive users.	Domain Squatting (classic cybersquatting on brand names).	
Phishing with Fake Domains	Creating fake .eth names to trick users into sending cryptocurrencies to wrong addresses.	Phishing websites with fake domain names (typosquatting, homoglyph attacks).	
Front-Running	Monitoring the pending transactions to preemptively register ENS names with higher gas fees.	Domain registration front-running (less common but it exists) via registrars.	
Smart Contract Exploitation	Exploiting the vulnerabilities in ENS smart contracts to gain unauthorized control.	Exploiting the vulnerabilities in DNS management software or protocols.	
DNS-ENS Bridging Attack	Attack via compromised DNS names linked to ENS records.	DNS hijacking leading to wrong ENS associations.	
Reverse Record Manipulation	Manipulating reverse records to impersonate trusted Ethereum addresses.	Manipulating PTR records (reverse DNS lookups) to fake IP addresses.	

Expired Domain Sniping	Quickly registering valuable expired ENS names to steal their identity or reputation.	Manipulating PTR records (reverse DNS lookups) to fake IP addresses.	
Social Engineering	Deceiving users to give up private keys or approve malicious transactions.	Social engineering targeting domain owners or DNS admins.	
Malicious Resolver Contracts	Deceiving users to give up private keys or approve malicious transactions.	Sniping expired valuable domains.	

The advent of Web3 technologies, particularly the decentralized naming systems like the Ethereum Name Service (ENS), represents a fundamental evolution in the architecture of the Internet. Traditional Domain Name System (DNS) infrastructures rely on centralized authorities for domain registration and management, which, although effective, expose their critical vulnerabilities. DNS hijacking, cache poisoning, registrar compromising and centralized censorship are persistent threats within the classic DNS model.

ENS and other blockchain-based domain systems attempt to resolve these weaknesses by decentralizing domain ownership through smart contracts recorded immutably on the Ethereum blockchain. In theory, this ensures that no central authority can unilaterally revoke, modify, or censor a domain name. However, this shift also introduces novel forms of security risks specific to decentralized environments.

Certain attack patterns, such as domain squatting and phishing with fake domains, persist in both DNS and ENS ecosystems. In ENS, the attackers register popular .eth domains either to deceive users or to resell them at inflated prices. Similarly, phishing attacks using slight variations of legitimate ENS domains parallel DNS-based typosquatting and homoglyph attacks, aiming to trick users into disclosing sensitive information or sending cryptocurrency to fraudulent addresses.

Other attacks, however, are more related to the decentralized nature of ENS. Smart contract

exploitation where the vulnerabilities in the ENS registry or resolver contracts are manipulated has no direct counterpart in DNS but represents a significant threat to domain ownership integrity. Front-running, in which the attackers monitor the pending blockchain transactions to preemptively register the desired ENS names by paying higher gas fees, can also be encountered in domain registration but is far more pervasive in blockchain systems.

The bridging between DNS and ENS also features critical hybrid vulnerabilities. DNS-ENS bridging attacks, where a compromised DNS domain can mislead users about the legitimacy of an associated ENS name, exemplify the need for robust cross-system authentication. Additionally, attacks like reverse record manipulation in ENS (analogous to PTR record manipulation in DNS) and expired domain sniping remain potent threats, targeting the mechanisms that the users rely on for trust.

In conclusion, while ENS addresses many of the structural weaknesses of the traditional DNS such as centralization and censorship, it simultaneously introduces a broader and more sophisticated threat landscape. The decentralization of domain ownership demands a heightened user awareness, rigorous smart contract auditing, and a reassessment of the best practices in identity verification and domain security. As Web3 continues to mature, a comprehensive understanding of both DNS and ENS attack models will be crucial for safeguarding the integrity of the next-generation Internet.

COMPARATIVE ANALYSIS OF DNS AND ENS ATTACKS. MITIGATION METHODS

As it was highlighted in the previous sections both the Domain Name System (DNS) and the Ethereum Name Service (ENS) represent critical infrastructures for navigating digital environments. DNS, as a foundational component of Web2, is centralized and has been widely adopted, yet it remains highly susceptible to a broad range of cyberattacks due to its original design, which prioritized availability over security. In contrast, ENS represents the emerging class of decentralized naming systems within the Web3 paradigm, offering an enhanced user control and censorship resistance through the blockchain technology. However, it introduces a parallel set of vulnerabilities, particularly those arising from smart contract logic, front-running, and bridging with traditional DNS layers. To support a comprehensive understanding of these contrasting yet increasingly interconnected systems, Table 3 presents a comparative analysis that outlines their respective attack surfaces, technical characteristics, and defensive considerations.

This comparative analysis is based on a series of criteria which were chosen for their value in assessing the cybersecurity posture and operational context of both DNS and ENS. These criteria reflect a balance between technological depth, user impact, and system governance, providing a multi-dimensional perspective on the similarities and divergences regarding their characteristics:

System Type and Technological Base provide the distinction between the centralized structure of DNS and the decentralized architecture of ENS. This distinction is pivotal, as it shapes not only system governance but also the type of vulnerabilities they are exposed to and the nature of the incident response process.

Common Attack Vectors refer to the most prevalent forms of exploitation ranging from cache poisoning and DNS hijacking in DNS to smart contract exploitation and malicious resolver contracts in ENS underscoring how the attackers adapt their strategies to the underlying infrastructure.

The Domain Ownership Control is another relevant criterion. While DNS relies on registrars and intermediary authorities, ENS shifts control directly to users via private keys. This has significant implications for both cybersecurity and user responsibility.

Security Mechanisms, including DNSSEC and blockchain immutability, are reviewed in terms of their effectiveness and deployment challenges. *Attack Consequences*, such as traffic redirection, identity theft, or asset loss, represent a criterion which meant to evaluate the impact of cyberattacks on end-users and services.

Other essential dimensions include *User Protection Tools*, which assess the availability of the mechanisms of defense against exploitation. *Adoption Scope* contextualizes how broadly each system is used, and the resulting variation in security maturity. Finally, *Similitude* captures the overlapping risks such as domain squatting, phishing, and social engineering, which persist across both ecosystems despite their architectural differences.

Table 3. *Comparative analysis of DNS and ENS Attacks*

Aspect	DNS Attacks	ENS Attacks
System Type	Traditional Domain Name System	Ethereum Name Service (Web3, blockchain-based)
Technological Base	Centralized Internet infrastructure	Decentralized blockchain infrastructure (Ethereum)
Security Mechanisms	Cache poisoning, DDoS, domain hijacking, spoofing	Smart contract exploitations, wallet impersonation, phishing via deceptive names
Common Attack Vectors	Controlled by registrars and DNS servers	Controlled by the holder of the private key owning the ENS domain
Domain Ownership Control	DNSSEC (Domain Name System Security Extensions), HTTPS, firewalling	Smart contract logic, blockchain immutability, private keys
Attack Consequences	Redirecting users to malicious websites, disrupting services	Loss of crypto assets, redirection to malicious dApps or wallet impersonation
User Protection Tools	Antivirus, browser security, DNSSEC validation	Wallet warnings, ENS verification, trusted dApps
Adoption Scope	Global, highly established in Web2	Growing in Web3 and decentralized applications
Similitude	Translating human-readable names into machine-usable addresses	Can be targeted by attackers to deceive users or reroute data traffic

CONCLUSION

As domain naming systems underpin the essential aspects of digital identity, communication, and service delivery, their security remains a high-stakes priority. While DNS continues to face sophisticated and evolving threats, the emerging systems like ENS are introducing new challenges under the guise of decentralization. The innovative aspect typical of this research is the comparative analysis of the attack types related to DNS and ENS.

The evolving landscape of domain name cybersecurity reflects the tension between its growing complexity and its persistent vulnerability. Despite the deployment of protocols such as DNSSEC or innovations like FQDN-based filtering and DNSCurve, DNS infrastructures remain attractive targets for

adversaries due to misconfigurations, their fragmented adoption, and the emerging multi-vector attacks.

Therefore, securing domain name systems in the modern web era requires a layered defense strategy. This includes the widespread deployment of cryptographic DNS extensions, a rigorous smart contract auditing, a dynamic anomaly detection, and a proactive domain management. While no single solution can eliminate the existing risks entirely, a coordinated innovation and continuous adaptation can significantly enhance the resilience of both traditional and decentralized domain ecosystems.

A limitation lies in the rapidly evolving nature of both threat landscapes. In particular, ENS and other decentralized naming systems are emerging technologies that are

undergoing frequent protocol updates and security paradigm shifts. New smart contract vulnerabilities, governance models, and cross-chain interactions can introduce attack vectors that were not previously considered. Consequently, any static comparison could quickly become outdated, which highlights the need for dynamic and regularly maintained threat landscapes.

Future work should focus on expanding this analysis into a more dynamic and empirical framework. This could involve developing a

real-time risk assessment model that would integrate the current attack trends and threat mitigation efficacy. Additionally, cross-disciplinary research incorporating behavioral cybersecurity could enrich the understanding of how end-users interact with domain systems and contribute to security gaps. A further exploration of cross-protocol defenses particularly at the intersection of DNS and ENS would also be valuable in building robust naming systems that are secure across both the Web2 and Web3 environments.

ACKNOWLEDGEMENTS

This research work was supported by a grant of the Romanian Ministry of Innovation and Research, the Nucleu Programme, project code: PN 2338 02 01, project name: „Architecture - platform of an intelligent system for monitoring Internet domains by developing a dynamic reputation establishment system (TLDRP)”.

REFERENCE LIST

- Afek, Y., Berger, H., & Bremner-barr, A., (2025) *POPS: From History to Mitigation of DNS Cache Poisoning Attacks*. doi:10.48550/arXiv.2501.13540.
- Almuhaideb, A. M., Aslam, N., Alabdullatif, A., Altamimi, S., Alothman, S., Alhussain, A., Aldosari, W., Alsunaidi, S. J. & Alissa, K. A. (2022) Homoglyph Attack Detection Model Using Machine Learning and Hash Function. *Journal of Sensor and Actuator Networks*. 11(3), art. no. 54. doi: org/10.3390/jsan11030054.
- Anagnostopoulos, M., Kambourakis, G., Konstantinou, E. & Gritzalis, S. (2012) DNSSEC vs. DNSCurve: A Side-by-Side Comparison. Onwubiko, C. & Owens, T. *Situational Awareness in Computer Network Defense: Principles, Methods and Applications*. Pennsylvania, USA, IGI Global Scientific Publishing, pp. 201-220.
- Apostu, A., Gheorghe, S., Hiji, A., Cleju, N., Pătrașcu, A., Rusu, C., Ionescu, R. & Irofti, P. (2025) Detecting and Mitigating DDoS Attacks with AI: A Survey. *arXiv preprint arXiv:2503.17867*.
- Ariyapperuma, S. & Mitchell, C. J. (2007) Security vulnerabilities in DNS and DNSSEC. In: *Proceedings of the Second International Conference on Availability, Reliability and Security (ARES '07), 10-13 April 2007, Vienna, Austria*. New York, USA, IEEE. pp. 335-342.
- Basri, R., Karmakar, G., Newaz, S. S., Kamruzzaman, J., Nguyen, L., Alam, M. M. & Usman, M. (2025) Enhancing IoT security: Assessing instantaneous communication trust to detect man-in-the-middle attacks. *Future Generation Computer Systems*. 166, art. no. 107714 .doi: org/10.1016/j.future.2025.107714.
- Birthriya, S. K., Ahlawat, P. & Jain, A. K. (2025) A Comprehensive Survey of Social Engineering Attacks: Taxonomy of Attacks, Prevention, and Mitigation Strategies. *Journal of Applied Security Research*. 20(2), 244-292. doi: or g/10.1080/19361610.2024.2372986.
- Biswas, M., Singh, S. P. & Shaha, S. K. (2023) Detecting Subdomain TakeOver Threats and Real-Time Alerting for Rapid Response. In: *2023 26th International Conference on Computer and Information Technology (ICCIT), 13-15 December 2023, Cox's Bazar, Bangladesh*. New York, USA, IEEE. doi: org/10.1109/ICCIT60459.2023.10441370.
- Bykov, N. & Chernyshov, Y. (2024) Detecting DNS Tunnels Using Machine Learning. In: *2024 IEEE Ural-Siberian Conference on Biomedical Engineering, Radioelectronics and Information Technology (USBREIT), 13-15 May 2024, Yekaterinburg, Russia*. New York, USA, IEEE. pp. 92-94.



- Chung, T., van Rijswijk-Deij, R., Choffnes, D., Levin, D., Maggs, B. M., Mislove, A. & Wilson, C. (2017) Understanding the role of registrars in DNSSEC deployment. In: *Proceedings of the 2017 Internet Measurement Conference, 1 - 3 November, 2017, London, UK*. New York, USA, Association for Computing Machinery. pp. 369-383.
- Dixon, C. (2024) *Read Write Own: Building the Next Era of the Internet*. New York, USA, Random House.
- Faqrunnisa, S., Adil, S., Arbaaz, S. M., Ali, S. A. & Arifullah, S. (2025) Exploring Web Security Vulnerabilities Considering Man in the Middle and Session Hijacking. *International Journal of Computational Learning & Intelligence*. 4(4), 580-590. doi:org/10.5281/zenodo.15224950.
- Fereidouni, H., Fadeitcheva, O. & Zalai, M. (2025) IoT and Man-in-the-Middle Attacks. *Security and Privacy*. 8(2), art. no. e70016 . <https://doi.org/10.1002/spy2.70016>.
- Hasegawa, K., Kondo, D., Osumi, M. & Tode, H. (2023) Collaborative Defense Framework Using FQDN-Based Allowlist Filter Against DNS Water Torture Attack. *IEEE Transactions on Network and Service Management*. 20(4), 3968 – 3983. doi: org/ 10.1109/TNSM.2023.3277880.
- Houser, R., Hao, S., Li, Z., Liu, D., Cotton, C., & Wang, H. (2021) A Comprehensive Measurement-based Investigation of DNS Hijacking. In: *2021 40th International Symposium on Reliable Distributed Systems (SRDS), 20-23 September 2021, Chicago, USA*. New York, USA, IEEE. pp. 210-221.
- Jadoaa, S. H., Ali, R. H., Abdulsalam, W. H. & Alsaedi, E. M. (2025) The Impact of Feature Importance on Spoofing Attack Detection in IoT Environment. *Mesopotamian Journal of CyberSecurity*. 5(1), 240-255. doi: org/10.58496/MJCS/2025/016.
- Kambourakis, G., Moschos, T., Geneiatakis, D. & Gritzalis, S. (2007) A Fair Solution to DNS Amplification Attacks. In: *Second International Workshop on Digital Forensics and Incident Analysis (WDFIA 2007), 27-28 August 2007, Karlovassi, Greece*. Washington, USA, IEEE Computer Society. pp. 38-47.
- Kusumi, R., Takita, M., Thein, T. T., Mohri, M. & Shiraishi, Y. (2025) Malicious Domain Detection Using Statistical Features of Domain Strings, Public Information, and DNS Logs. In: *2025 International Conference on Artificial Intelligence in Information and Communication (ICAIIIC), 18-21 February 2025, Fukuoka, Japan*. New York, USA, IEEE. pp. 0049-0054.
- Lim, K., Lee, K., Sommesse, R., Jonker, M., Mok, R., Claffy, C. & Kim, D. (2025) Registration, Detection, and Deregistration: Analyzing DNS Abuse for Phishing Attacks. To be published in *arXiv preprint arXiv:2502.09549*.
- Logaprakash, M., Gowtham, A., Madhav, S. & Gokul, S. (2025) Blockchain based DNS modification module for fast flux attack. In: *Hybrid and Advanced Technologies*. Boca Raton, FL, USA, CRC Press, pp. 327-332.
- Mathew, S. E., Vali, Y. S., & Shakkeera, L. (2025) Botnet Detection Methods: A Review and Classification. In: *2025 3rd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), 5-7 February 2025, Bengaluru, India*. New York, USA, IEEE. pp. 497-502.
- Moubayed, A., Injadat, M., Shami, A. & Lutfiyya, H. (2018) DNS Typo-Squatting Domain Detection: A Data Analytics & Machine Learning Based Approach. In: *2018 IEEE Global Communications Conference (GLOBECOM), 9-13 December 2018, Abu Dhabi, United Arab Emirates*. New York, USA, IEEE. doi: org/10.1109/GLOCOM.2018.8647679.
- Panda, D., Padhy, N. & Sharma, K. (2025) Strengthening IoT Resilience: A Study on Backdoor Malware and DNS Spoofing Detection Methods. In: *2025 International Conference on Emerging Systems and Intelligent Computing (ESIC), 8-9 February 2025*. New York, USA, IEEE. pp. 795-800.
- Ramdas, A. & Muthukrishnan, R. (2019) A Survey on DNS Security Issues and Mitigation Techniques. In: *2019 International Conference on Intelligent Computing and Control Systems (ICCS), 15-17 May 2019, Madurai, India*. New York, USA, IEEE. pp. 781-784.
- Rathod, T., Jadav, N. K., Tanwar, S., Alabdulatif, A., Garg, D. & Singh, A. (2025) A comprehensive survey on social engineering attacks, countermeasures, case study, and research challenges. *Information Processing & Management*. 62(1), art. no. 103928. doi: org/10.1016/j.ipm.2024.103928.
- Rawat, R. S., Diwakar, M., Garg, U. & Srivastava, P. (2025). Developing an Intelligent System for Efficient Botnet Detection in IoT Environment. *International Journal of Mathematical, Engineering and Management Sciences*. 10(2), 537 -553. doi: org/10.33889/IJMEMS.2025.10.2.027.
- Rishith, A., Kulkarni, A., Das, T. & Balachandran, V. (2024) Overcoming DNSSEC Islands of Security: A TLS and IP-Based Certificate Solution. In: *2024 IEEE Conference on Engineering Informatics (ICEI), 20-28 November 2024, Melbourne, Australia*. New York, USA, IEEE. doi: org/10.1109/ICEI64305.2024.10912416.
- Rodenbaugh, M. (2009) Abusive Domain Registrations: ICANN Policy Development Efforts (or Lack Thereof?). *The Computer and Internet Lawyer*. 26(5), 17-22. http://news.cnet.com/8301-10784_3-6i70192-7.html.
- Sadegh-Zadeh, S.-A. & Tajdini, M. (2025) An unsupervised machine learning approach for cyber threat detection using geographic profiling and Domain Name System data. *Decision Analytics Journal*. 15, art. no. 100576. doi: org/10.1016/j.dajour.2025.100576.

- Sadeghi Jahromi, A., Abdou, A. R. & van Oorschot, P. C (2024) *DNSSEC+: An enhanced DNS scheme motivated by benefits and pitfalls of DNSSEC*. To be published in 10.48550/arXiv.2408.00968. [Accessed 23th july 2024]
- Sheheryar, M. A. & Sharma, S. (2025) Ensemble Feature Engineering and Deep Learning for Botnet Attacks Detection in the Internet of Things. *Transactions on Emerging Telecommunications Technologies*. 36(3), art. no. e70099. doi: org/10.1002/ett.70099.
- Simpson, G., Moore, T. & Clayton, R. (2020) Ten years of attacks on companies using visual impersonation of domain names. In: *2020 APWG Symposium on Electronic Crime Research (eCrime)*, 16-19 November 2020, Boston, MA, USA. New York, USA, IEEE. doi: org/10.1109/eCrime51433.2020.9493251.
- Sinha, A. (2025) *Web 3.0 Next: Toward a Decentralized Internet Infrastructure Beyond Traditional ISPs*. Authorea Preprints.
- Southam, M (2014) DNSSEC: What it is and why it matters. *Network Security*. 5, 12–15. doi: org/10.1016/S1353-4858(14)70050-9.
- Vevera, A. V. (2018) De la amenințarea cibernetică la acțiunea ostilă în spațiul cibernetic [From cyber threat to hostile action in cyberspace]. *Revista Română de Informatică și Automatică [Romanian Journal of Information Technology & Automatic Control]*. 28(3), 17-30.



This is an open access article distributed under the terms and conditions of the Creative Commons Attribution-NonCommercial 4.0 International License.