International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 12
Article Received: *25 July 2021* ***Revised:*** *12 September 2021* ***Accepted:*** *30 November 2021*

Domain Name System Security Extensions (DNSSEC) for Identification of DNS Vulnerabilities

Lataben J Gadhavi[1], Suresh B Prasad[2]

Lecturer, Information Technology Department, Government Polytechnic Gandhinagar[1]

Lecturer, Computer Engineering Department, Government Polytechnic Gandhinagar[2]

latagpg@gmail.com[1] , sbprasad011@gmail.com[2]

Abstract: On the Internet, Domain Name System Security Extensions (DNSSEC) is continuously communicated. With extended sign, DNSSEC updates the DNS protocol to include two major security properties: validity and honesty. While DNSSEC was established to identify DNS security vulnerabilities, it also introduces a new one: the extended marks significantly increase DNS packet length, making DNSSEC a tempting vector for abuse in the context of spousal abuse. For computerised marks, DNSSEC, of course, employs RSA. In previous research, elective mark schemes based on elliptic bent cryptography have been found to effectively reduce the impact of tags on DNS resolution sizes. DNS provides simple query and interpretation services for converting URLs to IP addresses and IP addresses to URLs. As an outcome of this, DNS is completely unprotected against man-in-the-middle (MITM) attacks & a lot of other threats as an outcome of this. The Web Engineering Task Force suggested DNSSEC to make DNS more reliable (IETF). Beginning with information integrity, DNSSEC employs additional indicators to provide information integrity and reliability. Despite the reality that DNSSEC gives privacy for DNS data; it has real security and functional flaws. The large number of testing exercises on DNS in particular and safety and stability in particular indicate that almost all challenges in this area have been addressed. To identify the DNS vulnerabilities domain name system security extensions methodology is used in this paper.

Keywords: DNS, DNSSEC, DNS Security, Cryptography, DNS Attacks, DNS Firewall, Cloud DNS.

1. Introduction

Domain Name System is an important component of Internet. DNS is used for address lookup to tolerate simple services and translation of URL into IP addresses. As a privilege to the DNS, a file called 'host.txt' was used that served as a lookup table. However as the size grew it became inevitable to have a better and sophisticated system loading to DNS. But as the Internet was growing tremendously, maintaining all the addresses into a single file proved to be very costly and difficult. There were two major problems that were encountered. First, maintaining a very large file was very difficult. Secondly, since the file was a single file, all the websites lookup used to be based on single file and thus too many accesses of a single file were there and because of these problems DNS was introduced. Domain name system otherwise called as DNS is a system that is used for translating the URL into the IP addresses. This was decentralized in nature. This addressed both the issues of the previous method i.e. There wasn't a need to maintain a big and a single file as the DNS is decentralized. Thus the look up problem was solved[1-3]. And as the Internet is growing bigger this method was widely suitable and accepted. The DNS system has an hierarchical structure called as DNS Namespace hierarchy. The structure is shown in the Figure 1. The DNS was far better than the maintaining a single file but it also came up with a problem, Security. Though the DNS is used only for translating the addresses and has no information other than the addresses, these addresses needs to be protected.

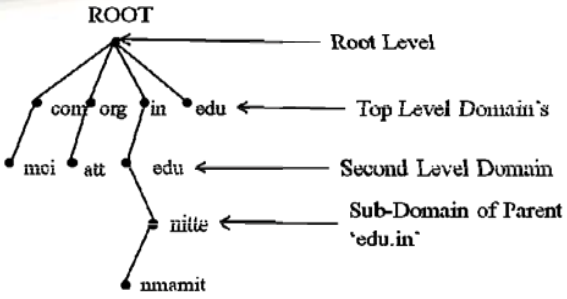

Fig.1. DNS Namespace hierarchy structure

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 12
***Article Received:** 25 July 2021 **Revised:** 12 September 2021 **Accepted:** 30 November 2021*

DNS security is critical since DNS is used by practically everyone on the Internet. And any DNS compromise could result in a significant loss for the user. A number of incidents have been impacted. There have been numerous instances of DNS security. A terror outbreak on Bank of America occurred as a result of a DNS compromise [4]. If the DNS isn't secure enough, an attacker may gain access to these addresses, alter them, and cause a slew of additional issues. As a result, DNS security is an essential matter that requires to be revitalised.

2. Name Servers and Resolvers

In most cases, name servers keep comprehensive name and address details about a district in a file called the zone file. To improve resiliency, redundancy, and load balancing, each zone should have a primary and secondary name server. The zone data is kept in a locally saved zone file by primary master servers. All updates to district data must be made in the prime or first server's database[4]. A source node periodically asks the application, i.e., for a record of the data replication and updates its own database using the information returned. This is referred to as "zone transfer." UDP is the major protocol for DNS communication. TCP, on the other hand, is used for zone transfers.DNS requests are sent to name servers over UDP and TCP port 53. DNS query resolution usually starts with a query to root name servers in the lack of just about any information, which means the root servers are all quite busy[5]. To lessen the burden on the root servers, all name servers use caching extensively.

Resolution of DNS Queries: A name server can operate in two modes, recursive or iterative. A recursive query is sent with the RD (Recursion Desired) flag set to on in the DNS query header. In recursive mode the name server searches through the DNS hierarchy in response to queries and returns either an error or the answer, but never referrals to other name servers. For iterative queries, the queried name server operating in iterative mode consults its own database for the requested data. If it cannot find the answers, it typically gives the IP address of the closest name server that might know the result[6]. The client repeats the request, this times sending it to the server it just learned about. By default, queries to root name servers are iterative.

3. Attacks possible in DNS

DNS is a mostly useful method, but none of us can deny that DNS security is a problem that continues to be one of the most serious difficulties. The protection of DNS is in jeopardy as a result of a few possible DNS-based attacks. Some of these attacks are targeted specifically at DNS, while others are more generic. The following is a list of some of the major assaults identified by DNS:

3.1 IP Sniffing & Spoofing:

IP addressed scanning is a types of threat in which the attacker steals the exact location of a person in question. Catching IP addresses is part of this. When the site is taken, that survivor can do anything he or she wants with it. Following this assault, this next stage is frequently caricaturing[7]. An attack against DNS in which the attacker masks the suspect is known as IP Address satirising. He poses as a genuine client and sends communications on behalf of the individual at issue.

3.2 Denial of Service attack (DoS):

One of the popular & hazardous attacks is the denial of service attack. In this attack, the adversary floods the victim's DNS with queries, causing the victim's system to become overloaded and unresponsive. Other users are inconvenienced in this situation and are thus refused service, i.e., they will be unable to reach the DNS server. A DDoS attack is a kind of attack. The concept of "DDoS" refers to such a generalised denial of service attack. This attack has the same consequence as a DoS attack in that the client is overburdened with ,requests (traffic), causing a system failure, but it is carried out by a collection of systems or attackers with a single point of control. As a result, all of the assailants are members of the same group and have the same goal in mind when they assault the victim[8]. Because it is carried out in a group, this assault is stronger than the DoS attack as shown in the Figure 2 and DDoS attack in Figure 3. This type of attack is prevalent nowadays, and it has been reported in a number of locations around the world. It's going to be difficult to stop this attack.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 12
Article Received: *25 July 2021* ***Revised:*** *12 September 2021* ***Accepted:*** *30 November 2021*

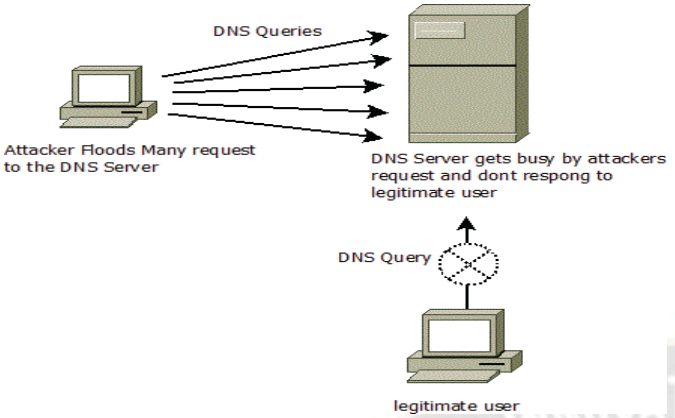

Fig 2. Working of DOS Attack

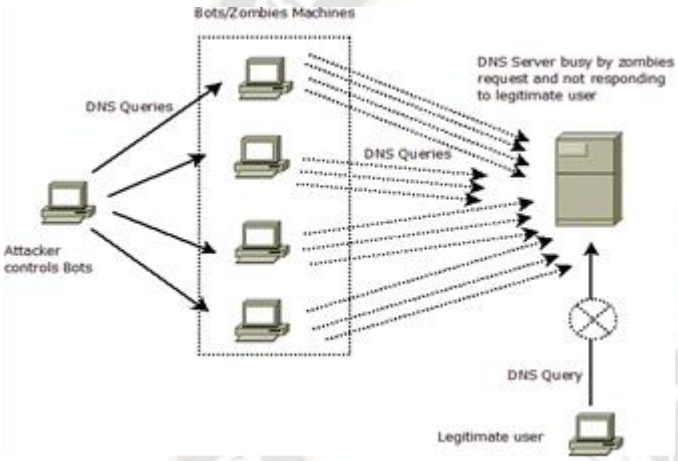

Fig 3. Working of DDoS Attack

3.3 DNS Amplification :

DNS Amplification is the attack which is possible on recursive DNS Servers. Here, the power of the attack is amplified to harm to the victim to the maximum extent possible. This attack is accelerated due to the presence of Recursive servers which allow repeated sending of the queries to the DNS server, thereby increasing the load of the server by manifolds. These servers are usually open servers. Many dynamic DNS servers, which are cyclic in nature, can do recursive query lookups[9]. For whatever reason, the strike will become more powerful over time.The attack takes advantage of the victim's strength in order to cause them harm. The server's requests are usually not legitimate, and the queries can also be delivered by automated devices displayed in the Figure 4.

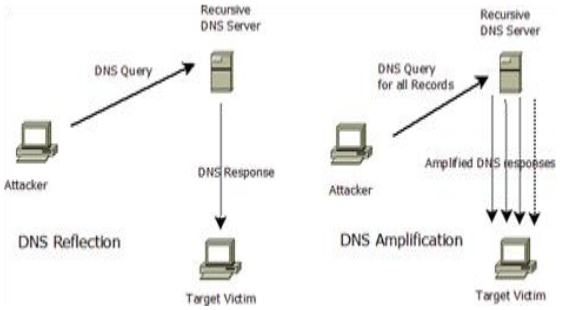

Fig 4. DNS amplification

3.4 Cache Poisoning:

Cache poisoning is one of the common attack that can be carried out quite easily when compared to other DNS attacks. In cache poisoning attack the adversary "poisons" the Name server. The adversary maliciously changes the IP address of the legitimate user i.e. he changes the IP address in the table that is stored in the DNS . As shown in the Figure Thus whenever a DNS lookup is done the DNS would translate the wrong address to the user and will instead redirect all the conversations or queries to the address given by the adversary rather than redirecting it to the original user[10]. Thus the adversary can easily impersonate as the genuine person and can gain complete control over the victims user base as shown in the Figure 5.

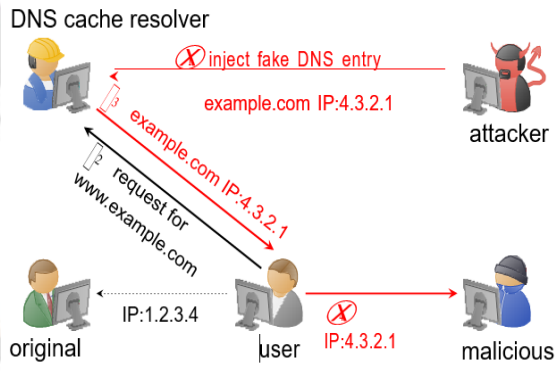

Fig 5. Work flow of Cache Poisoning

3.5 Registrar Hijacking :

In a registrar hijacking attempt, a hostile enemy takes charge of the registrar. The registrant is just the organisation with which the visitor registers to utilise the service. A grouping of registered users is under the control of the registrars[11]. The attacker controls all registration actions in this scenario, including the client. This assault impacts a large number of people, including all registered members. This attack is aimed towards a group of individuals rather than just a single individual.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 12
Article Received: *25 July 2021* ***Revised:*** *12 September 2021* ***Accepted:*** *30 November 2021*

3.6 Man in the middle (MITM) attacks:

The recipient of information from such a DNS name server would have no way of verifying where it came from or validating its accuracy. This is due to the fact that DNS does not include a means for servers to provide the authentication information for the content they send to clients. A resolver doesn't need to review the information sent in by name servers for validity or integrity. The source IP addressed of such a DNS server, destination & source port numbers, DNS transaction ID are the only ways for the resolver to verify the identities of a DNS reply packets. An attacker can easily create a DNS server response packet with these parameters in it. The recipient will have no reason to accept the data given by an attacker as reliable. An attacker can respond with misleading information to valid inquiries.

3.7 DNS Tunnelling:

Internal network data leakage is a method of collecting internal network data by exposing data privacy to the attacker's systems. To do the same, the attackers infect a DNS user with malware that builds a tunnel to the attacker's desk through a recurring DNS server inside that plaintiff's lan, bypassing the firewall. HTTPS traffic can also be transferred through the tunnel under the guise of a DNS query-response, completely circumventing the firewall and ensuring the obscurity of the exfiltrated information outside of any detection devices in the network as shown in the Figure 6.

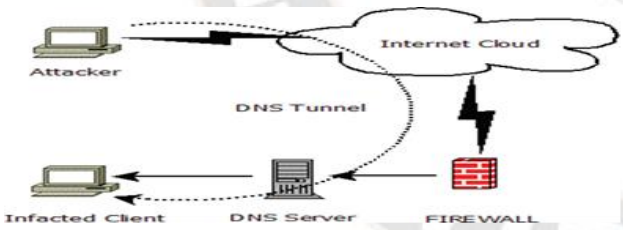

Fig 6:DNS Tunnel Attack

4. Domain Name System Security Extensions (DNSSEC)

DNSSEC enhances DNS protocol security by enabling origin authentication, data integrity, and validated denial of existence for DNS data delivered by a name server. All DNSSEC returns are digitally signed. A DNSSEC resolver can examine the signature to see if the data came from such a trustworthy server and if it is equivalent to the content on the authentic DNS server. An authorised denial is generated if the content is not available on the server. DNSSEC only necessitates minor modifications to the DNS protocol to retain backward compatibility. DNSSEC introduces four new DNS record types: Resource Record Signature (RRSIG), DNS Public Key (DNSKEY), Delegation Signer (DS), & Next Secure (NS) (NSEC). In the DNS query and answer message headers, DNSSEC makes use of two previously empty flag bits (AD and CD). The AD (Authentic Data) bit in such a response indicates that the server has authenticated all of the data in the answer and authority sections of the response. The CD (checking disabled) flag specifies that the resolver submitting the query accepts unauthenticated data .Because the UDP protocol has a 512-bit packets size restriction, DNSSEC needs any use of EDNS0 upgrades to overcome this limitation, allowing for bigger key sizes [12]. DNSSEC adds data origin authentication, transaction, and request authentication to DNS, but it does not prevent MITM attacks. Both providers and resolvers must employ the DNSSEC protocol to preserve data origination authenticity and integrity.

Keys in DNSSEC: For each secured zone, a session key consists of a zone pass code & its corresponding public key. Its zone public key is retained in the secured sector as a career history (type KEY). The public key is used by DNS servers & resolvers to check the location's digital signature.Service records in a secure area are signed using the zone's private key. One or more keys, like key signing keys, must all be obtained to allow sector re-signing & key roll-overs to be easier to deploy (KSKs). Only the sector's topmost KEY RRs will also be confirmed with a KSK. Zone Signing Keys are used to sign all of the RRsets in a sector (ZSKs).

Signatures in DNSSEC: DNSSEC encrypts an RRset by correlating it all with a signature asset record that connects DNS data to an interval and the signer's domain name, making it unforgeable. A RRset is signed using a private key. A hashed version of such an RRset is signed for better speed. This ensures that the data source is verified. If data is changed while being transported, the signature becomes invalid (authenticated data integrity). Only signatures are used in DNSSEC, & nothing is encrypted. MD5 or SHA-1 are now used to compute hashes. A combination of MD5/RSA , DSA , and elliptic curve cryptographic techniques is used to create signatures. Signatures are kept for resource records (type RRSIG) and are used to authorise resource records using the zone's public key.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 12
***Article Received:** 25 July 2021 **Revised:** 12 September 2021 **Accepted:** 30 November 2021*

NSEC Records: A NSEC resource record is assigned per each username in a secured zone, which connects to the next name in the zone. The NSEC resource record chain for a zone determines which resource records are actually present in that zone. The zone private key is also used to sign the NSEC resource records, which prevents the zones from being compromised by unauthorised additions or deletions of zone resource data. When zone records are signed, NSEC research based for that zone are generated automatically.

Time in DNSSEC:In DNS, all times are relative. The refresh, retry, and expiration timers in the Start Of Authority (SOA) resource record are counts that are used to detect how long it has been since a child server synchronised with a master server. After data has indeed been retrieved from an authoritative server, the Time to Live (TTL) value reflects how long a forwarder should store it. DNSSEC adds absolute time to the DNS. In DNS, all times are relative. The refresh, retry, and expiration timers in the Start Of Authority (SOA) resource record are counts that are used to detect how long it has been since a child server synchronised with a master server. After data has indeed been retrieved from an authoritative server, the Time to Live (TTL) value reflects how long a forwarder should store it. DNSSEC adds absolute time to the DNS.

5. Cloud DNS and its Security features

As per the National Institute of Standards and Technology (NIST), cloud computing is a methodology for rapidly provisioning and releasing distributed, suitable, on-demand, network configurable computer resources with no administration effort or network operator contact . From infrastructure to tools to any facility, almost anything in the cloud is offered as a service. Cloud computing's appeal stems from its market-driven nature and pay-as-you-go model, which enables users to use the cloud only if they need it and pay for what they need. As previously said, there are different ways to deliver services, and several significant companies, like Google DNS, Cloud DNS, OpenDNS, and others have begun to shift DNS to the cloud, e.g., they now provide DNS as a service. For example, OpenDNS, for example, is still a company and service that extends the Domain Name System's functions. While they're online, Umbrella, the industry's cloud computing security service, guards the customer base from malware, botnets, and phishing. Similar to many other cloud services, the costs are based on a cost model. All of the advantages of a cloud system are available with these DNS services. In terms of security, it's also much more protected than a separately maintained DNS server[14]. DNS has a substantial level of security. IP spoofing, cache poisoning, registrant hijacking, DNS amplification, and some other DNS-related assaults are all possibilities. As a result, whatever system is used must be protected. From a security aspect, there are multiple reasons to adopt the cloud; e.g., the cloud has several features:

5.1 Features of cloud for security:

Best Distributive Data Security: For handling distributed data, the cloud is the ideal option. Because the cloud is distributed by nature, & DNS is a distributive data service, it is sometimes simple to set up and maintain DNS servers on the cloud. This has an added benefit in terms of security, as the clouds are recognised as different datasets and are thought to be superior to centralised administration, which has a single point of failure.

Security from external sources: The primary goal of DNS security is to keep the system safe from outside threats. Although DNS Server data is critical, it is not as critical as other sorts of data, such as financial or medical data. An assault can be caused by a number of factors. The attacker may be motivated by a desire to harm the DNS server by unintentional or planned assault or any other abuse that involves changing the DNS nameserver's content. This is impractical with a cloud because it is completely protected and cannot be harmed by external systems. Cloud security is only a hazard of its cloud services and the nations under which authority the server is placed.No external party may access the cloud without the authorization of the cloud service & the owner.

Special Attention towards security: The seamless service-based cloud is one of the key benefits of using their facilities. The majority of cloud DNS services are provided by large corporations such as Google, HP, CloudDNS, and others. These businesses spend a lot of money on infrastructure, & they can spend an unlimited sum of money on system upkeep[13]. As a result, these behemoths can afford to invest a lot of money as well as time in security, which is nearly impossible for a smaller private company with its own DNS server. Cloud services have a specialised staff of highly qualified professionals who focus exclusively on DNS security. They go to great lengths to ensure that the system remains secure.

Prevention of DDoS attack: One of the most well-known threats that damages DNS is the DDoS attacks. A DDoS

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 12
***Article Received:** 25 July 2021 **Revised:** 12 September 2021 **Accepted:** 30 November 2021*

assault, also known as a Distributed Denial of Service attacks, aims to stress the DNS server to the same point where it fails and certain other users can't connect to it. This attack is extremely common, and smooth of the most secure DNS servers may be harmed & become victims[15]. This attack is exceedingly difficult to stop, and within time of launching it, the server is completely broken, as clients would be unable to access the server, resulting in service denial. Such cloud DNS providers are experts at preventing DDoS attacks and providing complete protection.

Updated Security Features: Cloud DNS service providers' systems are usually regularly updated.These businesses use the most up-to-date software and are always among the first to implement security measures. These service providers assess the system on a regular basis, correctly configure it, and ensure that there are no security flaws that could cause difficulties. Even the tiniest inconsistencies are addressed. Even if there are any unanticipated security breaches, these systems can be restored to their previous state.

Tolerate Attacks:If a cloud service provider encounters a security breach and discovers it, they can purposefully allow it to occur by securing themselves while analysing the victims' attack. According to the report, the DDoS attack committedon purpose by a cloud DNS use supplier. Despite the attack's great intensity, it had little effect on the system, as well as the service providers let it happen because it wouldn't harm theirs. They did it in order to examine and analyse the attack in order to employ it in the future[16].

Physical security: If a system's actual location is known, it is always possible that it will be compromised.As a result, a DNS internet provider must physically secure the server's location. This security may be questioned at times. The cloud service providers, on the other hand, ensure that no data about their data centres is shared with the public[17]. Their privacy restrictions can even help determine the precise address being stored.These services have a large number of data centres around the world, and it is impossible for a user to know where his or her data is stored. When it comes to DNS data, it is up to the client and service provider to decide whether or not to keep the data transparent[18]. As a result, physical security can be managed.

Transaction Signature (TSIG): Transaction Signatures (TSIG) ensures a secure communication between primary and secondary Domain Name server (DNS) by use of symmetric keys and cryptographic hash functions [6]. TSIG ensures that the data received in sector transfer is authentic & not modified during transit, and also provides for the authenticity of the DNS response[21]. TSIG is a mechanism used to address IP spoofing during a Resource Record (RR) updating operation. It's used to provide a means of authenticating updates to a DNS database. TSIG only protects from "spoofing master attack" discussed earlier[22-23].

DNS Firewall Solution: DNS Firewall is security appliance that filters the DNS traffic to protect various DNS attacks and typically blocks certain type of DNS queries to known bad domains . Most of the DNS Firewall has the feature of malware protection, Response Policy Zones (RPZ) functionality[19-20]. It can detect most of the DNS attacks based on attack signatures and provide defence by dropping the packets if a signature matches. It can monitor live DNS traffic and block specific domains. Following are some of the DNS Firewall Solutions available : Infoblox DNS Firewall, Roksit DNS Firewall, Efficient IP DNS FIREWALL, Cloudflare's DNS Firewall is shown in Figure 7. Most of the IPS (Intrusion Prevention Systems) also claim to provide protection against DNS attacks[24]. Similarly many of the firewalls too claim protection against DNS attacks like, The Cisco PIX, FWSM, ASA Firewall appliance etc.

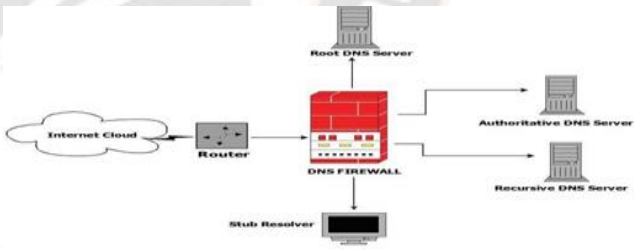

Fig 7: DNS FIREWALL

6. Conclusion

DNS has critical security flaws that must be addressed immediately. Man-in-the-middle attacks and cache feeding are possible as a result of the DNS transaction process's absence of authentication and integrity. Although the cloud is not a novel mechanism, it gives more security when compared to other approaches.A DNS Firewall can protects the DNS infrastructure from DoS/DDoS attacks, DNS amplification attacks by blocking malformed DNS requests, but cannot mitigate from all the DNS attacks listed in this paper.

References

1. Ateniese, Giuseppe, and Stefan Mangard. "A new approach to DNS security (DNSSEC)." Proceedings of the 8th ACM conference on Computer and Communications Security. ACM, 2001.
2. S. Gourley and H. Tewari, "Blockchain Backed DNSSEC", Business Information Systems Workshops Lecture Notes in Business Information Processing, pp. 173-184, 2019.
3. H. Tewari, A. Hughes, S. Weber and T. Barry, "X509Cloud Framework for a ubiquitous PKI", MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM), 2017.
4. S. Y. Chau, O. Chowdhury, V. Gonsalves, H. Ge, W. Yang, S. Fahmy, et al., "Adaptive Deterrence of DNS Cache Poisoning", Lecture Notes of the Institute for Computer Sciences Social Informatics and Telecommunications Engineering Security and Privacy in Communication Networks, pp. 171-191, 2018.
5. K. Chetioui, G. Orhanou and S. El Hajji, "New Protocol E-DNSSEC to Enhance DNSSEC Security", IJ Network Security, vol. 20, no. 1, pp. 19-24, 2017.
6. P. Schmitt, A. Edmundson and N. Feamster, "Oblivious DNS: Practical Privacy for DNS Queries", 2018.
7. Q. Hu, M. R. Asghar and N. Brownlee, "Measuring IPv6 DNS Reconnaissance Attacks and Preventing Them Using DNS Guard", 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2018.
8. X. Luo, L. Wang, Z. Xu, K. Chen, J. Yang and T. Tian, "A Large Scale Analysis of DNS Water Torture Attack", Proceedings of the 2018 2nd International Conference on Computer Science and Artificial Intelligence - CSAI 18, 2018.
9. T. Mahjabin and Y. Xiao, "Mitigation Process for DNS Flood Attacks", 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), 2019
10. S. Sankaran, S. Sanju and K. Achuthan, "Towards Realistic Energy Profiling of Blockchains for Securing Internet of Things", 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), 2018.
11. Y. Takeuchi, T. Yoshida, R. Kobayashi, M. Kato and H. Kishimoto, "Detection of the DNS Water Torture Attack by Analyzing Features of the Subdomain Name", Journal of Information Processing, vol. 24, no. 5, pp. 793-801, 2016.
12. S. Ariyapperuma and C. J. Mitchell, "Security vulnerabilities in DNS and DNSSEC", The Second International Conference on Availability Reliability and Security (ARES07), 2007.
13. D. Zagar and K. Grgic, "IPv6 Security Threats and Possible Solutions", 2006 World Automation Congress, 2006.
14. Anand Nayar, Lata Gadhavi, Noor Zaman, Machine learning in healthcare: review, opportunities and challenges, Science Direct(Elsevier),2021, ISBN 978-0-12-821229- 5,pp.23-45,2021.
15. Fetzer, Christof, Gert Pfeifer, and Trevor Jim. "Enhancing dns security using the ssl trust infrastructure." Object- Oriented Real-Time Dependable Systems, 2005. WORDS 2005. 10th IEEE International Workshop on. IEEE, 2005.
16. Gadhavi, L.J., & Bhavsar, M.D, Efficient and Dynamic Resource Provisioning Strategy for Data Processing Using Cloud Computing, International Review on Computers and Software (I.RE.CO.S.), Vol. 11, 691-700,2016.
17. R. Arends, R. Austein, M. Larson, D. Massey, andS. Rose. DNS security introduction and requirements. RFC 4033, Internet Engineering Task Force, Mar. 2005.
18. Gadhavi, L.J., & Bhavsar, M.D. Adaptive cloud resource management through workload prediction. *Energy Systems, 13*, 601 – 623, 2019.
19. D. Atkins and R. Austein. Threat analysis of the domainname system (DNS). RFC 3833, Internet Engineering Task Force, Aug. 2004.
20. D. E. 3rd. RSA/MD5 KEYs and SIGs in the domainname system (DNS). RFC 2537, Internet Engineering Task Force, Mar. 1999.
21. Gadhavi, L.J., & Bhavsar, M.D, Prediction based efficient resource provisioning and its impact on QoS parameters in the cloud environment, International Journal of Electrical and Computer Engineering (IJECE), Volume 8, No 6,5359- 5370,2018.
22. Gadhavi, L.J., Bhavsar, M.D. Efficient Resource Provisioning Through Workload Prediction in the Cloud System. In: Zhang, YD., Mandal, J., So-In, C., Thakur, N. (eds) Smart Trends in Computing and Communications. Smart Innovation, Systems and Technologies, vol 165. Springer, Singapore, 2020.