IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Impact Factor: 6.252

Volume 2, Issue 1, August 2022

# A Detection Method Against DNS Cache Poisoning Attacks using Machine Learning Techniques

**Shashank Biradar[1], Shramik S Shetty[2], Pradeep Nayak[3], Prajakta Shetty[4], Shwetha R Sharma[5]**
Students, Department of Information Science and Engineering[1,2,4,5]
Assistant Professor, Department of Computer Science and Engineering[3]
Alvas Institute of Engineering and Technology, Mijar, Karnataka, India
4al20is044@gmail.com,4al20is046@gmail.com, 4al20is045@gmail.com,
4al20is047@gmail.com, pradeepnayak@aiet.org.in

**Abstract:** *In this paper, we offer a machine learning-based enhanced detection strategy for DNS cache poisoning attacks. In addition to the standard DNS packet's five basic tuples, we plan to include numerous specific features that were extracted based on The heuristic components, such as the common DNS protocols "trigger," "time related features," and "GeoIP related features" of DNS cached data," etc.[1] By mapping IP and domain name, DNS's principal job is to lead users to the right computers, programmes, and data. Due to some DNS security weaknesses, attackers frequently use DNS-based malware, DNS-amplification, false-positive triggering, DNS tunnelling, etc. as a means of attack.[2] The upcoming effort comprises training with DNS traffic data and evaluations in both a small-scale experimental network and a large-scale real network environment.*

**Keywords:** DNS, Machine Learning.

## REFERENCES

**[1].** A Detection Method Against DNS Cache Poisoning Attacks Using Machine Learning Techniques Yong Jin∗ , Masahiko Tomoishi† , and Satoshi Matsuura‡ Tokyo Institute of Technology, 2-12-1 O-okayama, Meguroku, Tokyo, JAPAN[1]

**[2].** Detecting Malicious DNS over HTTPS Traffic Using Machine Learning Sunil Kumar Singh School and Pradeep Kumar Roy

**[3].** Detection of Hijacked Authoritative DNS Servers by Name Resolution Traffic Classification Yong Jin∗ , Masahiko Tomoishi† , and Satoshi Matsuura‡ Tokyo Institute of Technology, 2-12-1 O-okayama, Meguroku, Tokyo, JAPAN

**[4].** Classifying DNS Servers Based on Response Message Matrix Using Machine Learning Keiichi Shima;Ryo Nakamura;Kazuya Okada;Tomohiro Ishihara;Daisuke Miyamoto;Yuji Sekiya

**[5].** Recovering and Protecting against DNS Cache Poisoning Attacks Xi Yu;Xiaochen Chen;Fangqin Xu

**[6].** Detection of Kaminsky DNS Cache Poisoning Attack Yasuo Musashi;Masaya Kumagai;Shinichiro Kubota;Kenichi Sugitani

DOI: 10.48175/IJARSCT-7033