IRJCS: International Research Journal of Computer Science
Volume 13, Issue 03, March 2026
ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1303.28

# Detection of DNS Tunneling Attack Using Network Traffic Entropy Analysis

**S.Kanmani**
Assistant Professor, Department of CSE (Cyber Security),
Sengunthar Engineering College (Autonomous),Tiruchengode,India
kanmanicse@gmail.com
https://orcid.org/0009-0006-2904-7365
**Bantikumar Goswamy, Bharatkumar, Ragavan.R, Shubham Giri**
UG Students, Department of CSE (Cyber Security),
Sengunthar Engineering College (Autonomous),Tiruchengode, India
bk2009535@gmail.com, 01harshkr@gmail.com, ragavanyuki@gmail.com, history01@gmail.com

**Publication History**
Manuscript Reference: IRJCS/RS/Vol.13/Issue03/CSMR26.MRCS10107
Research Article | Open Access | Double-Blind Peer Reviewed Article ID: IRJCS/RS/Vol.13/Issue03/CSMR26.MRCS10107
Received: 30, January 2026, Revised: 13, February 2026, Accepted: 28 February 2026 Published Online: 25 March 2026
https://www.irjcs.com/volumes/Vol13/iss-03/28.CSMR26.MRCS10107.pdf
**Article Citation:Kanmani,Bantikumar,Bharatkumar,Ragavan,Shubham(2026)**,Detection of DNS Tunneling Attack Using Network Traffic Entropy Analysis, IRJCS: International Research Journal of Computer Science, Volume 13,Issue 03 of 2026 pages 259-265 **Doi:>** https://doi.org/10.26562/irjcs.2026.v1303.28
**BibTeX Key Kanmani@2026Detection**
**Orcid:** https://orcid.org/0009-0004-9398-7488
IRJCS papers should be cited as IRJCS (International Research Journal of Computer Science, AM Publications, India 2026, ISSN 2393-9842, https://doi.org/10.26562/ijrcs.2025.v1303.28 The journal's official abbreviation is IRJCS.


**Abstract:** This study focuses on detecting DNS tunneling attacks using network traffic entropy analysis. Entropy is a statistical measure used to analyze randomness and irregular patterns in network traffic. In normal DNS traffic, domain names follow predictable patterns and contain meaningful words. However, DNS tunneling generates highly random and encoded domain names, which results in higher entropy values. The proposed approach monitors DNS query traffic and calculates entropy values of domain names to identify unusual patterns. By comparing queries and responses. In this attack, the attacker encodes data inside DNS requests and sends them to a malicious DNS server. The server then decodes the information and may send commands back to the compromised system through DNS responses. This technique allows attackers to create a hidden communication channel, which is often used for data exfiltration, remote command execution, and bypassing network security controls. Entropy levels between legitimate and suspicious DNS queries, the system Detecting DNS tunneling attacks is difficult because the traffic appears can effectively detect potential tunneling activities. This method helps in identifying hidden communication channels without significantly affecting network performance.

## INTRODUCTION

The Domain Name System (DNS) is one of the most important components of the Internet. It is responsible for translating human-readable domain names into IP addresses so that computers can similar to normal DNS communication. Traditional security tools such as firewalls and basic intrusion detection systems may fail to detect such attacks since DNS traffic is usually considered legitimate. Therefore, advanced analysis techniques are required to identify abnormal patterns within DNS queries. Communicate with each other. One effective approach for detecting DNS tunneling is network traffic one such malicious technique is known as DNS tunneling.DNS entropy analysis. Entropy is a statistical measure that evaluates. This study focuses on detecting DNS tunneling attacks through network traffic analysis. By analyzing DNS traffic patterns such as randomness or unpredictability of data. In normal DNS traffic, domain names generally contain meaningful and structured words, resulting in lower query length, frequency of requests, unusual domain structures, and entropy values. However, in DNS tunneling, attackers often encode data entropy levels in domain names, suspicious activities can be using random or encrypted strings with in domain names, which leads to tunneling is a method used by attackers to secretly transmit data through DNS identified. Network traffic datasets are examined to distinguish normal DNS behavior from abnormal patterns associated with tunneling attacks. The analysis helps in identifying key indicators of compromise, including excessive DNS requests, long and encoded domain names, and irregular communication patterns. The findings suggest that continuous monitoring of DNS traffic and applying anomaly detection techniques can effectively detect DNS tunneling attempts. Higher entropy values. By analyzing the entropy of DNS queries, it is possible to identify unusual patterns that indicate potential tunneling activity.

## LITERATURE REVIEW

Several researchers have studied different methods to detect DNS tunneling attacks and other malicious activities hidden within DNS traffic. Since DNS is a commonly used protocol in network communication, attackers often exploit it to bypass security mechanisms. As a result, many detection techniques such as traffic analysis, machine learning, and entropy-based methods have been proposed to identify abnormal DNS behavior.

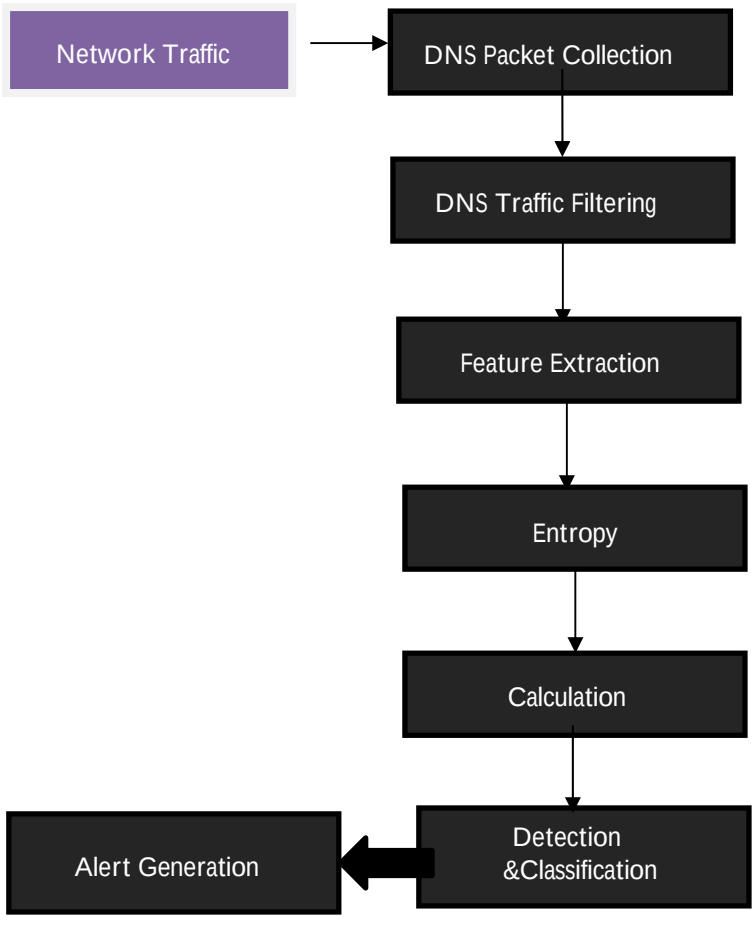
IRJCS: International Research Journal of Computer Science
Volume 13, Issue 03, March 2026
ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1303.28

Early research focused on signature-based detection techniques to identify DNS tunneling. These methods rely on predefined patterns or signatures of known tunneling tools such as Iodine, DNS cat, and TCP-over-DNS. While signature-based systems are effective in detecting known attacks, they have limitations Later studies introduced anomaly-based detection approaches to overcome these limitations. In anomaly detection, the normal behavior of DNS traffic is first analyzed, and any deviation from this behavior is considered suspicious. Researchers found that DNS tunneling of ten produces unusual characteristics such as long domain names, a large number of queries, and encoded strings that differ from normal DNS requests. One of the earliest approaches used for detecting DNS tunneling attacks was rule-based and signature-based detection. In this method, network security systems identify attacks by comparing DNS traffic with known attack patterns stored in a database. If a match is found, the system generates an alert. Although this approach is simple and effective against known attacks, it has limitations in detecting new or unknown tunneling techniques. Attackers can easily modify their tunneling methods to avoid detection, making signature-based approaches less reliable in dynamic network environments.

## PROPOSED METHODOLOGY ARCHITECTURE

The proposed methodology for detecting DNS tunneling attacks using network traffic entropy analysis focuses on monitoring DNS traffic, extracting important features, and identifying abnormal patterns through entropy calculation. The system architecture is designed to analyze DNS queries in real time and detect suspicious domain names that may contain hidden data. The architecture consists of several stages that work together to detect DNS tunneling attacks effectively. The proposed methodology focuses on detecting DNS tunneling attacks by one important approach used in recentre search is entropy-based analyzing the randomness of DNS traffic using entropy analysis. DNS traffic analysis. Entropy is a statistical measure that represents the randomness or unpredictability of data. Researchers observed that domain names generated by DNS tunneling tools contain highly random characters due to encoding techniques such as Base32 or Base64. As a result, the entropy value of such domain names becomes significantly higher than that of normal domain names. By calculating entropy values and comparing them with predefined thresholds, it becomes possible to detect suspicious DNS queries. Several studies have also combined entropy analysis with machine learning algorithms to improve detection accuracy. Machine learning models such as decision trees, random forests, and support vector machines are trained using features extracted from DNS traffic, including domain length, query frequency, and entropy values. These hybrid approaches have shown promising results in identifying both known and unknown DNS tunneling attacks. Overall, the literature indicates that entropy-based DNS traffic analysis is an effective and lightweight method for detecting covert DNS communication channels.

### A. System Architecture Design



ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1303.28

It helps security systems identify suspicious patterns in network traffic and provides an additional layer of protection against data exfiltration and command-and-control activities performed through DNS tunneling. In recent years, the increasing use of the Internet and cloud-based services has led to a rapid growth in network traffic. Among the various network protocols, the Domain Name System (DNS) plays a critical role in enabling communication between devices. However, due to its open and trusted nature, DNS has become a popular target for cyber attackers. Many researchers have focused on identifying techniques to detect malicious activities such as DNS tunneling, which is commonly used for covert communication and data exfiltration. tunneling allows attackers to hide malicious data inside DNS queries and responses. Since DNS traffic is usually trusted and allowed by firewalls, attackers exploit this protocol to create covert communication channels. Therefore, the proposed system monitors DNS traffic continuously and identifies suspicious patterns using statistical analysis.

The System Architecture Design for detecting DNS tunneling Security implementation is an important part of the DNS tunneling attacks is developed to monitor network traffic and identify detection system. It ensures that the network remains protected from suspicious DNS queries using entropy-based analysis and unauthorized access, data leakage, and hidden communication channels classification techniques. The architecture is designed in a created by attackers. The main goal of security implementation is to apply structured manner so that each component performs a specific task proper security measures and mechanisms to detect, prevent, and respond in the detection process. This design helps in efficiently analyzing to DNS tunneling attacks effectively. In the proposed system, security DNS traffic and detecting hidden malicious communication within implementation begins with continuous monitoring of DNS traffic. The entire network. DNS queries and responses passing through the network are observed carefully. By monitoring DNS traffic, the system can identify unusual.

### Network Flow Monitoring Protocol

A Network Flow Monitoring Protocol is used to observe, collect, and analyze network traffic flows between devices in a network. It helps network administrators understand how data moves across the network and identify abnormal activities such as attacks, patterns such as repeated queries, long domain names, or encoded strings that may indicate suspicious activity.

### Performance Validation

Performance validation is an important stage in the proposed DNS intrusions, or unauthorized data transfers. In cyber security tunneling detection system. It is used to evaluate how effectively the systems, network flow monitoring plays an important role in system detects malicious DNS traffic while maintaining efficient network detecting suspicious behavior, including DNS tunneling and other performance. The main goal of performance validation is to measure the covert communication methods. Network flow monitoring works accuracy, reliability, and efficiency of the detection mechanism. In this by capturing information about the communication between stage, the system is tested using a dataset that contains both normal DNS different devices on a network. Instead of storing the entire packet traffic and malicious DNS tunneling traffic. The collected network content, the system records metadata about the flow, such as traffic is processed through the proposed framework, where source IP address, destination IP address, source port, destination preprocessing, feature extraction, entropy calculation, and classification port, protocol type, packet count, and time stamp. This information are performed. By applying these processes, the system attempts to help in analyzing traffic patterns without consuming large storage resources.

### Data Processing Framework

The Data Processing Frame work is an important component in Identify suspicious DNS queries that may indicate tunneling activity.

## TECHNOLOGIES USED

### Python

Python is used as the primary programming language for developing the processing, and analyzing the collected network traffic data in a DNS tunneling detection system. It is widely used in cyber security and organized and efficient manner. The main objective of this data analysis because of its simple syntax and powerful libraries. Python frame work is to transform raw network data into meaningful helps in processing network traffic data, performing entropy calculations, information that can be used for detecting suspicious activities and implementing detection algorithms. Libraries such as NumPy, such as DNS tunneling the frame work begins with the data Pandas, and Scikit-learn are commonly used for data analysis and the DNS tunneling detection system. It is responsible for handling, collection stage, where DNS traffic is gathered from the network using monitoring tools or packet capture systems. The collected data usually contains raw packet information such as DNS queries, responses, time stamps, IP addresses, and domain names. Since raw data may contain large volumes of information, the framework must process it efficiently to make it suitable for analysis.

### Threat Detection System

The threat detection module utilizes machine learning algorithms such as Random Forest, Support Vector Machine (SVM), and Decision Tree classifiers to identify malicious activities. These models are trained using labeled datasets containing both normal and attack traffic. Once trained, the models analyze incoming network traffic and detect anomalies that indicate potential Advanced Persistent Threat activities. When suspicious behavior is detected, the system automatically generates alerts to notify network administrators for further investigation.

### Wireshark / Packet Capture Tools

Wireshark or similar packet capture tools are used to collect DNS network traffic from the network environment.

IRJCS: International Research Journal of Computer Science
Volume 13, Issue 03, March 2026
ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1303.28

These tools capture packets that travel across the network and allow analysts to inspect DNS queries and responses. The captured packet data is then used as input for further processing and analysis in the detection Packet capture tools are software applications that allow network administrators, security analysts, and developers to capture, inspect, and analyze network traffic in real-time.

### Entropy Analysis Technique

Entropy analysis is one of the core technologies used in this system. Entropy is a statistical measurement that determines the level of randomness in a data sequence. In DNS tunneling attacks, attackers encode data into domain names, which produces random strings of characters. These random strings generate higher entropy values compared to normal domain names.

### Machine Learning Algorithms

Machine learning techniques are used to enhance the accuracy of the detection system. Algorithms such as Decision Tree, Random Forest, and Support Vector Machine are commonly used to classify DNS traffic as normal or malicious. These algorithms learn patterns from historical data and apply that knowledge to detect new threats. Machine learning helps improve detection performance and reduces false alarms.

### Network Flow Monitoring Protocols

Network flow monitoring protocols such as NetFlow, sFlow, and IPFIX are used to monitor network traffic flows. These protocols collect metadata about network communication such as source address, destination address, protocol type, and packet counts. Flow monitoring provides an overview of network activity and helps detect unusual traffic patterns that may indicate DNS tunneling.

## IMPLEMENTATIONS AND RESULTS

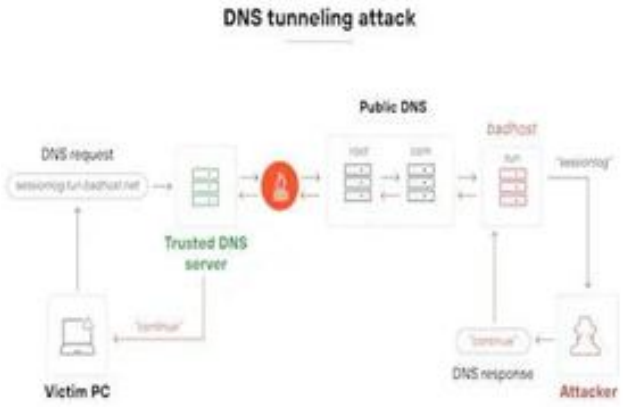



**Fig.2:** The system implementation

### Data Processing Framework

The system implementation focuses on detecting DNS tunneling A data processing framework is used to handle large volumes of DNS traffic data efficiently. The framework performs tasks such as data collection, preprocessing, feature extraction, and analysis. By organizing these processes into a structured workflow, the system can analyze network data more efficiently and detect malicious activities in real time.

### A. Intrusion Detection System (IDS)

An Intrusion Detection System is used to monitor network traffic for suspicious behavior or policy violations. IDS tools analyze incoming and outgoing traffic and generate alerts when abnormal patterns are detected. When integrated with the DNS tunneling detection system, IDS improves the overall security of the network environment.

### B. Database Management System

A database management system is used to store captured DNS traffic data, extracted features, entropy values, and detection results. Storing this information allows researchers and network administrators to analyze historical data and track attack patterns over time. The database also helps in maintaining logs for security monitoring and forensic investigation.

### C. Visualization and Reporting Tools

Visualization tools are used to present analysis results in graphical or tabular form. Charts, graphs, and reports help network administrators understand DNS traffic behavior and identify suspicious activities quickly. Visualization improves the interpretation of detection results and supports decision-making in network security management. attacks by analyzing the entropy of network traffic. The architecture consists of multiple modules that capture, preprocess, analyze, and report suspicious DNS activities. As shown in Fig.2. The Use Case Diagram represents the interaction between the system and the external factors involved in detecting DNS tunneling attacks. It illustrates how the network administrator and security analyst interact with the DNS tunneling detection system to monitor network traffic, analyze anomalies, and respond to potential threats. This diagram helps in clearly understanding the responsibilities of each actor and the functional capabilities of the system as shown in Fig 3. The output of the proposed system displays the analysis of DNS traffic using entropy-based detection techniques. The system monitors DNS queries captured from the network and evaluates them to identify suspicious patterns that may indicate DNS tunneling attacks.

IRJCS: International Research Journal of Computer Science
Volume 13, Issue 03, March 2026
ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1303.28


**Fig.3** Use case Diagram

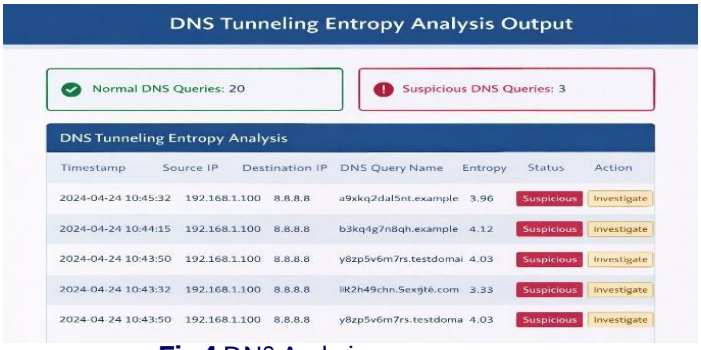



**Fig.4** DNS Analysis

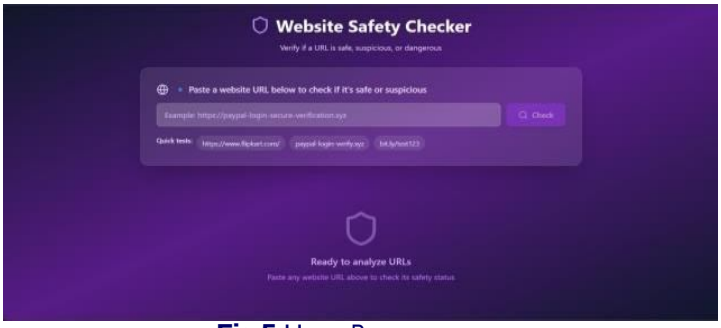



**Fig.5** HomePage

Welcome to the DNS Tunneling Detection System using Network Traffic Entropy Analysis. This system is designed to monitor and analyze DNS traffic in order to identify potential DNS tunneling attacks. DNS tunneling is a technique used by attackers to hide malicious communication within DNS queries and responses, which can lead to data exfiltration and unauthorized network access. Welcome to the DNS Tunneling Detection System using Network Traffic frequency should be carefully chosen to help the machine learning model distinguish between normal and malicious network behavior.

**Model Accuracy and Performance:** The machine learning algorithms used in the system must be optimized to achieve high detection accuracy while minimizing false positives and false negatives. Continuous model evaluation and tuning are required to ensure reliable identification of Advanced Persistent Threat activities.

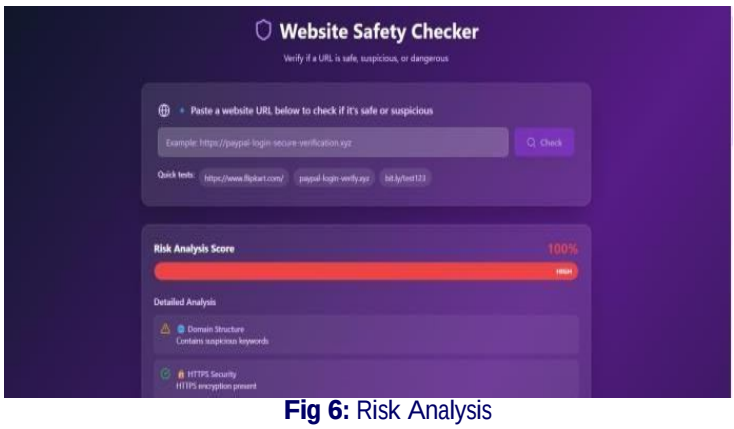



**Fig 6:** Risk Analysis

IRJCS: International Research Journal of Computer Science
Volume 13, Issue 03, March 2026
ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1303.28

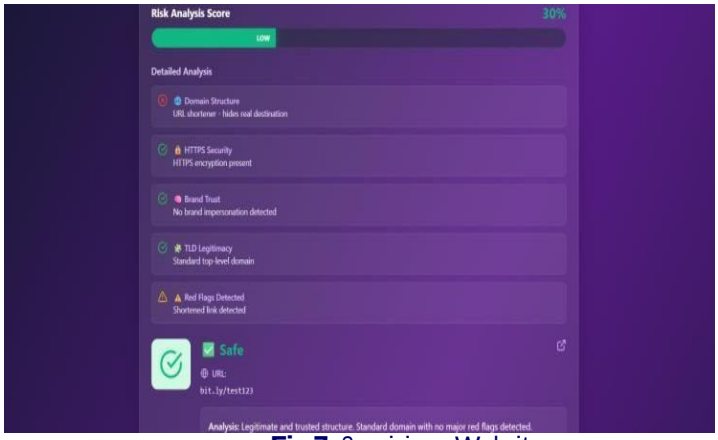



**Fig 7:** Suspicious Website

**Real-Time Detection Capability:** DNS attacks often occur over long periods and involve stealthy communication patterns. Therefore, the detection system must support real-time or near real- time analysis of network traffic to quickly identify suspicious activities and generate alerts.

## CONCLUSION

DNS tunneling is a technique where attackers misuse the Domain Entropy Analysis. This system is designed to monitor and analyze DNS Name System (DNS) protocol to secretly transfer data between a traffic in order to identify potential DNS tunneling attacks. DNS tunneling compromised system and an external server. This method is often is a technique used by attackers to hide malicious communication within used to bypass firewalls and security systems because DNS traffic is DNS queries and responses, which can lead to data exfiltration and usually allowed in most networks. In this study, network traffic unauthorized network access. Welcome to the DNS analysis was used to identify suspicious DNS activities that may Tunneling Detection System using Network Traffic Entropy Analysis. Indicate DNS tunneling attacks. By analyzing different DNS traffic This system is designed to monitor and analyze DNS traffic in order to features such as query length, frequency of requests, unusual domain identify potential DNS tunneling attacks.DNS tunneling is a technique names, and high entropy in DNS queries, it becomes possible to used by attackers to hide malicious communication within DNS queries detect abnormal patterns that differ from normal DNS behavior. The and responses, which can lead to data exfiltration and unauthorized results show that monitoring DNS traffic can effectively help in network access. Key Considerations: identifying potential tunneling activities. Indicators such as a large. Data Quality and Availability: The collected network flow data must be accurate, complete, and properly labeled to ensure reliable threat detection. Poor quality or incomplete data may reduce the effectiveness of the detection system. Feature Selection: Selecting the most relevant network flow features is critical for improving detection accuracy. Features such as packet size, session duration, protocol type, and traffic number of DNS requests, encoded or randomly generated domain names, and long DNS query strings are strong signs of DNS tunneling.

## REFERENCES

1. B.Born and G.Gustafson, "Detecting DNS tunneling using character frequency analysis," in 2010 IEEE International Conference on Communications, 2010, pp. 1–6.
2. M.Kara,K.K.Ramachandran,andB.Sikdar,"Detecting DNS tunnels using statistical analysis of network traffic,"in 2014 IEEE International Conference on Communications, 2014
3. B.W.Yu,X.Niu,andJ.Li,"A survey on DNS-based covert channel detection techniques, "IEEE Communications Surveys & Tutorials,vol.18,no. 2,pp.1232–1246,2016.
4. S.Dietrich,N.Long, and D.Dittrich, "Analyzing distributed denial- of-service tools: The shaft case, "in USENIX Security Symposium, 2000,pp.1–12.
5. A.Nadler,A.Aminov,andA.Shabtai,"Detection of malicious and low throughput data exfiltration over DNS protocol, "Computers & Security, vol. 80, pp. 36–53, 2019.
6. P.Philipp,R.X.M.Georgi,J.Beyerer,andS.Robert,"Analysis of control flow graphs using graph convolutional neural networks," in 2019 6th International Conference on Soft Computing & Machine Intelligence (ISCMI), 2019, pp. 1-5.
7. Q.Wang,H.Yan,andZ.Han,"Explainable APT attribution for malware using NLP techniques,"in 2021IEEE 21st International Conference on Software Quality, Reliability and Security (QRS), 2021, pp. 1-11.
8. T.Fiebig,S.Krishnan,andJ.Waller,"Monitoring DNS traffic for anomaly detection in enterprise networks,"in IEEE Conference on Network Operations and Management Symposium, 2018, pp. 1–5.
9. H.Choi, H.Lee, H.Kim, and H.Kim, "Botnet detection by monitoring group activities in DNS traffic,"in IEEE International Conference on Computer Communications, 2007, pp. 715–720.
10. M.Antonakakis, R. Perdisci, and W. Lee, "Building a dynamic reputation system for DNS," in USENIX Security Symposium, 2010, pp. 1–16.
11. J.Jung, E.Sit, H.Balakrishnan, and R.Morris, "DNS performance and the effectiveness of caching, "IEEE/ACM Transactions on Networking, vol. 10, no. 5, pp. 589–603, 2002.
12. P.Mockapetris,"Domain names-concepts and facilities," InternetEngineeringTaskForce(IETF)RFC1034,1987.

ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1303.28

13. D.Plonka and P.Barford, "Context-aware clustering of DNS query traffic," in Internet Measurement Conference, 2008,pp. 1–10.
14. R.State, O.Festor, and A.Dulaunoy, "Entropy-based anomaly detection in network traffic,"in International Conference on Network and Service Management, 2014, pp. 1–6.
15. L.Bilge, E.Kirda, C.Kruegel, andM. Balduzzi, "Exposure: Finding malicious domains using passive DNS analysis," in Network and Distributed System Security Symposium (NDSS), 2011, pp. 1–17.
16. C.Rossow,"Amplification hell: Revisiting network protocols for DDoS abuse," in Network and Distributed System Security Symposium (NDSS), 2014, pp. 1–15.
17. J.Francois, S.Wang, R.State, and T.Engel, "Botcloud: Detecting botnets using DNS traffic analysis," in IEEE Global Communications Conference (GLOBECOM), 2011, pp. 1–6.
18. S.Yu,W.Zhou, R. Doss, andW. Jia, "Traceback ofDDoS attacks using entropy variations,"IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 3, pp. 412–425, 2011.
19. A.Shabtai,U.Kanonov,Y.Elovici,C.Glezer,andY.Weiss, "Andromaly: A behavioral malware detection framework for Androiddevices,"Journal of Intelligent InformationSystems, vol. 38, no. 1, pp. 161–190, 2012.
20. G.Gu, R.Perdisci, J.Zhang, and W. Lee, "BotMiner: Clustering analysis of network traffic for protocol and structure-independent botnet detection," in USENIX Security Symposium, 2008, pp. 139–154