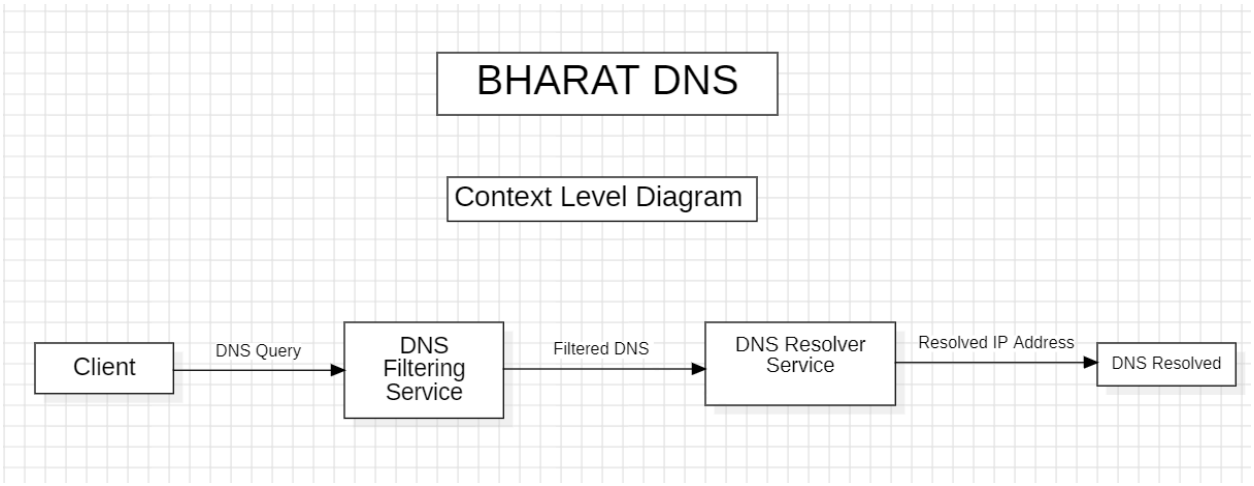
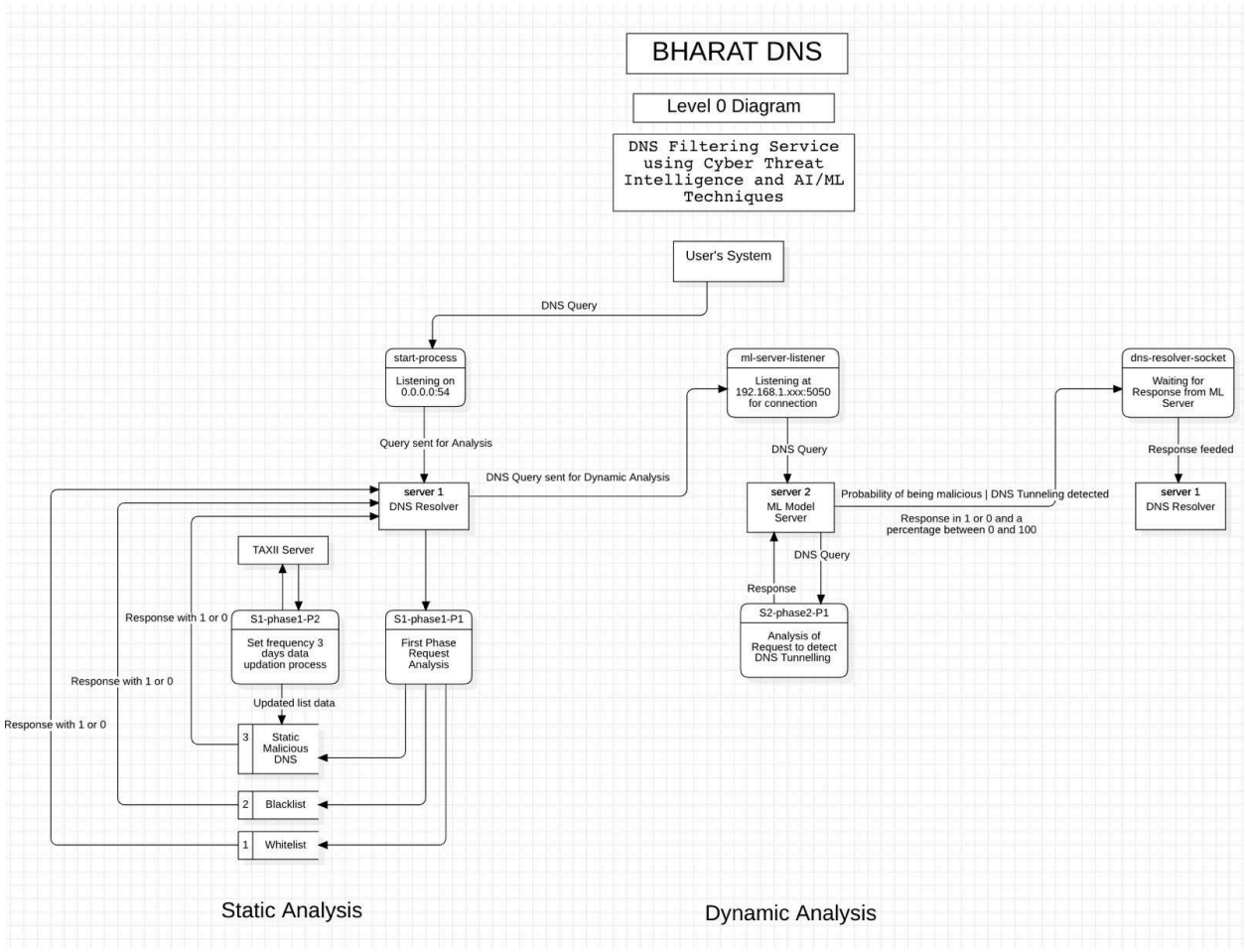
Data flow Diagrams for Bharat DNS

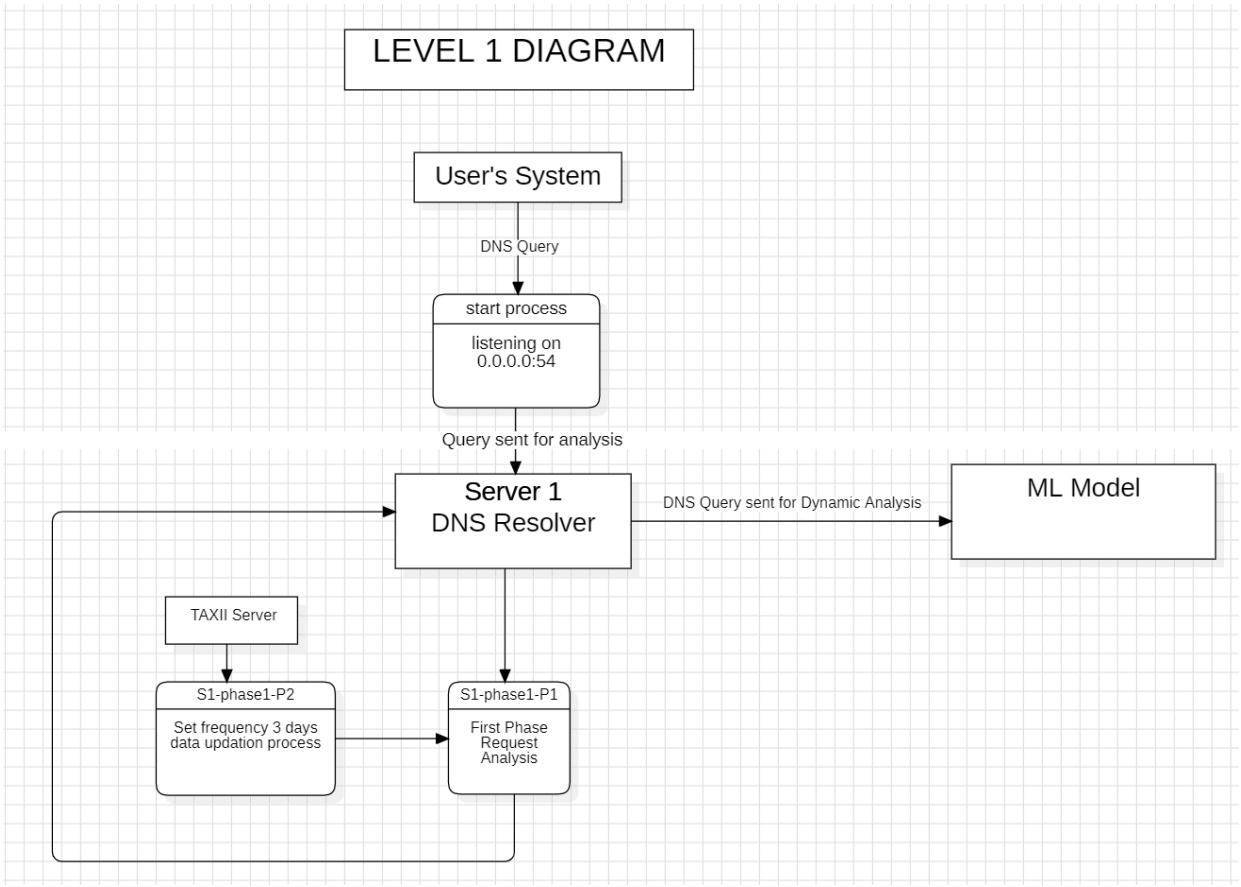
Context Level Diagram:



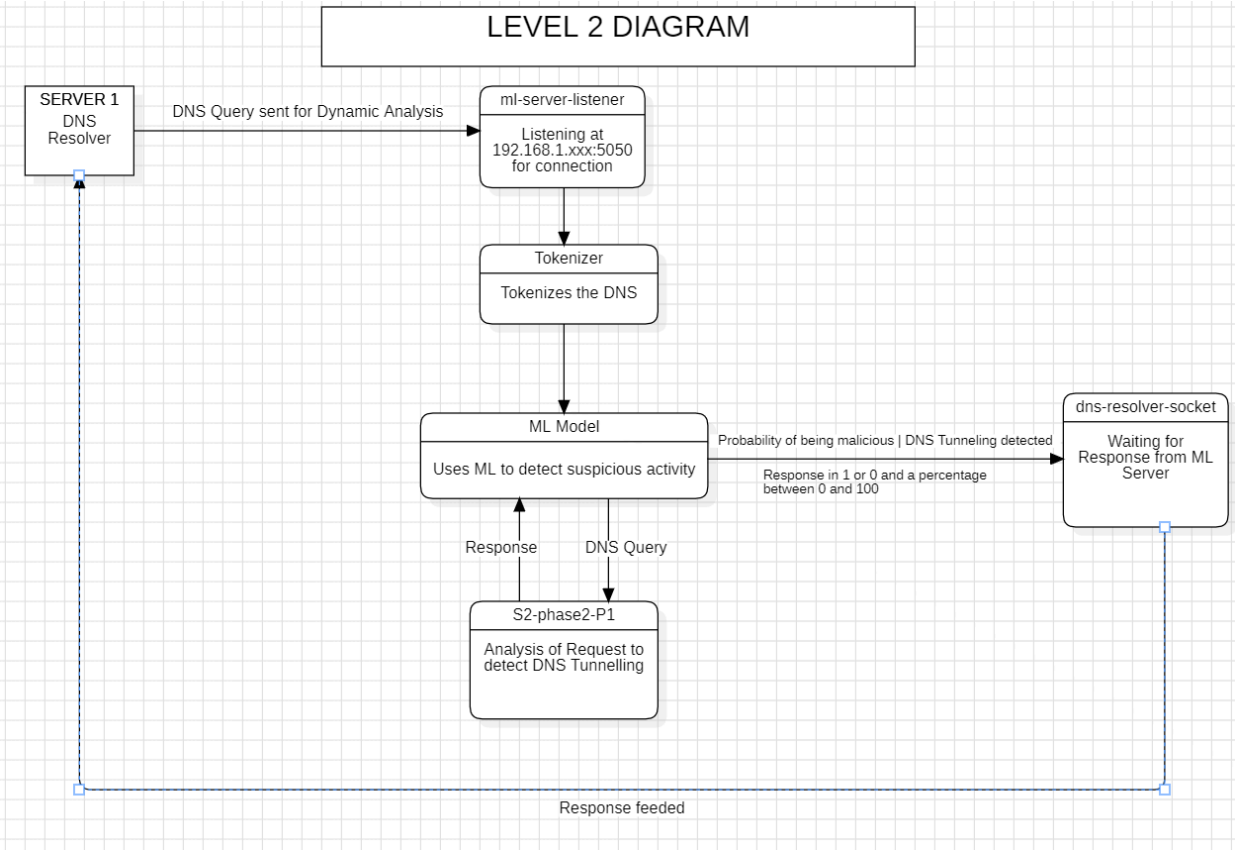
Level 0:


BHARAT DNS
Level 0 Diagram
DNS Filtering Service using Cyber Threat Intelligence and AI/ML Techniques
User's System
DNS Query
start-process
Listening on 0.0.0.0:54
Query sent for Analysis
server 1
DNS Resolver
DNS Query sent for Dynamic Analysis
ml-server-listener
Listening at 192.168.1.xxx:5050 for connection
DNS Query
server 2
ML Model Server
Probability of being malicious | DNS Tunneling detected
Response in 1 or 0 and a percentage between 0 and 100
dns-resolver-socket
Waiting for Response from ML Server
Response feeded
server 1
DNS Resolver
DNS Query
Response
S2-phase2-P1
Analysis of Request to detect DNS Tunnelling
TAXII Server
Response with 1 or 0
S1-phase1-P2
Set frequency 3 days data updation process
S1-phase1-P1
First Phase Request Analysis
Response with 1 or 0
Updated list data
Response with 1 or 0
3
Static Malicious DNS
2
Blacklist
1
Whitelist
Static Analysis
Dynamic Analysis

Level 1:


LEVEL 1 DIAGRAM
User's System
DNS Query
start process
listening on
0.0.0.0:54
Query sent for analysis
Server 1
DNS Resolver
DNS Query sent for Dynamic Analysis
ML Model
TAXII Server
S1-phase1-P2
Set frequency 3 days
data updation process
S1-phase1-P1
First Phase
Request
Analysis

Level 2:


LEVEL 2 DIAGRAM
SERVER 1
DNS Resolver
DNS Query sent for Dynamic Analysis
ml-server-listener
Listening at 192.168.1.xxx:5050 for connection
Tokenizer
Tokenizes the DNS
ML Model
Uses ML to detect suspicious activity
Probability of being malicious | DNS Tunneling detected
Response in 1 or 0 and a percentage between 0 and 100
dns-resolver-socket
Waiting for Response from ML Server
Response
DNS Query
S2-phase2-P1
Analysis of Request to detect DNS Tunnelling
Response feeded