Metadata Analysis & Application Identification using Deep packet Inspection (DPI) or other techniques in High-Speed Internet Traffic

1	**Problem Statement**	Metadata Analysis & Application Identification using Deep packet Inspection (DPI) or other techniques in High-Speed Internet Traffic
2	**Technology Area**	Cybersecurity
3	**Project Introduction**	At CDOT, a premier government R&D institute, we are engaged in a pioneering project aimed at developing advanced deep packet inspection (DPI) technologies for the identification of applications within internet traffic at the ingress and egress points of Internet Service Providers (ISPs). The continuous growth in internet traffic and the increasing complexity of applications have created a significant challenge for ISPs and network operators. Traditional traffic management and security tools are no longer sufficient to handle the volume and variety of traffic, especially with the widespread adoption of encrypted and obfuscated data transmission methods. The increasing volume and complexity of internet traffic have underscored the need for precise and efficient traffic analysis tools, capable of handling data rates up to 200/400Gbps.
4	**Problem Description**	To achieve this ambitious goal, we seek collaboration with other government agencies, private sector partners, and research institutions with expertise in DPI, traffic analysis, and related technologies. The specific feature sets and capabilities we aim to develop as part of this collaboration is given below: a. **Traffic Volume and Complexity:** o Modern networks experience exponential growth in traffic volumes, reaching hundreds of gigabits per second. This surge in data transmission is coupled with increasingly complex application behaviors, including the use of encryption and obfuscation techniques that hinder traditional traffic analysis methods. b. **Need for Granular Visibility:** o ISPs and network operators require deep visibility into network traffic to ensure efficient management and security. The ability to identify and classify applications at a granular level, even when encrypted or using non-standard protocols, is crucial for maintaining network performance and security. c. **Performance and Scalability:** o Existing DPI solutions often struggle to scale effectively with the increasing demands of high-throughput environments. There is a need for a DPI solution that can maintain high performance without sacrificing accuracy, even when processing traffic at 200/400Gbps. d. **Real-Time Threat Detection:** o With the rise of sophisticated cyber threats, there is a critical need for real-time detection and mitigation of malicious activities within network traffic. The proposed DPI solution must integrate advanced threat detection capabilities to safeguard network integrity. e. **Interoperability and Flexibility:** o The solution must be flexible enough to integrate with a wide range of existing network infrastructure and security tools. It should also be adaptable to future technological developments, including the adoption of 5G and cloud-native environments.

5	**Feature Sets and Capabilities**	**a. Advanced Protocol and Application Identification** **Overview:** One of the primary objectives of our DPI solution is to achieve accurate identification of protocols and applications across all layers of the OSI model. This includes analyzing both metadata and payload information, even in scenarios where data is encrypted or obfuscated. **Capabilities:** ● **Protocol Parsing:** The DPI engine must be capable of parsing a broad range of protocols, including HTTP, HTTPS, FTP, DNS, and more. This includes recognizing standard, non-standard, and proprietary protocols. ● **Application Signatures:** The solution should maintain an extensive database of application signatures, enabling the identification of numerous applications, including web apps, P2P networks, VoIP services, and mobile apps. ● **Behavioral Analysis:** The system should incorporate behavioral analysis techniques to identify applications based on traffic patterns, which is particularly useful for detecting encrypted traffic. ● **Contextual Awareness:** The DPI solution should offer the ability to correlate traffic flows with user sessions, device types, and geolocation data, providing a comprehensive view of application usage. **b. Scalability and High-Performance Processing** **Overview:** Handling traffic rates of 200/400Gbps requires a DPI solution that can scale both horizontally and vertically, leveraging hardware acceleration, multi-threading, and efficient memory management. **Capabilities:** ● **Hardware Acceleration:** The DPI solution should integrate with hardware accelerators like FPGA or ASIC to offload computationally intensive tasks, such as packet filtering, encryption/decryption, and pattern matching. ● **Parallel Processing:** It should utilize multi-core processors and parallel processing techniques to distribute the workload efficiently across multiple processing units. ● **Load Balancing:** The DPI engine should include load balancing mechanisms that distribute traffic across multiple nodes, ensuring no single node becomes a bottleneck. ● **High-Throughput Architecture:** The solution should feature a modular architecture that supports high-throughput data processing, with minimal latency and jitter, even under peak traffic conditions. **c. Real-Time Traffic Analysis and Threat Detection** **Overview:** Beyond application identification, our DPI solution aims to provide real-time traffic analysis and threat detection capabilities. This includes identifying anomalies, detecting malicious traffic, and providing actionable insights for network security. **Capabilities:** ● **Anomaly Detection:** The DPI engine should detect deviations from normal traffic patterns, indicating potential security threats such as DDoS attacks, botnets, or data exfiltration. ● **Malware Detection:** The solution should incorporate signature-based and heuristic analysis methods to identify and block malware, spyware, and other malicious payloads embedded within traffic flows.

		● **Intrusion Detection System (IDS) Integration:** The DPI engine should integrate with existing IDS solutions, enhancing their capabilities with deep packet inspection for more accurate threat detection. ● **Real-Time Alerts and Reporting:** The system should provide real-time alerts and detailed reports on detected threats, with the ability to correlate events across multiple data sources for comprehensive threat analysis. **d. Flexible Deployment and Integration Options** **Overview:** Given the diverse environments in which DPI solutions must operate, from large-scale ISPs to enterprise networks, our solution should offer flexible deployment and integration options. **Capabilities:** ● **Cloud and On-Premises Deployment:** The DPI solution should support deployment in both cloud-based and on-premises environments, providing flexibility based on the needs of the organization. ● **API and SDK Availability:** It should offer comprehensive APIs and SDKs to facilitate integration with existing network management and security tools, ensuring seamless interoperability. ● **Customizable Policies and Rules:** The DPI engine should allow administrators to define custom policies and rules for traffic classification, prioritization, and filtering based on specific organizational requirements. ● **Ease of Management:** The solution should feature a user-friendly management interface that allows for easy configuration, monitoring, and maintenance, with support for automated updates and scalability. The DPI solution we envision at CDOT aims to be at the forefront of traffic analysis technology, offering unparalleled capabilities in protocol and application identification, scalability, real-time threat detection, and flexible deployment. We believe that through collaboration with other government agencies, private sector partners, and research institutions, we can achieve this vision and create a solution that addresses the challenges of modern internet traffic at unprecedented scales.
6	**Roles & Responsibilities of C-DOT**	C-DOT will provide technical development assistance, and financial support to the project partner(s) selected through a process of evaluation and due diligence conducted by a committee of subject experts. Wherever deemed necessary and depending upon the project type (i.e. co-development or fully outsourced), C-DOT may arrange resources, equipment, training, testing infrastructure, mandatory clearances, statutory permissions, and provide gap funding to the partner(s) in realizing the respective target deliverables. Development costs of the module, whether developed from scratch or derived from existing background technology of partner(s), shall be borne by C-DOT. C-DOT shall use the final solution for integration with production grade software. C-DOT reserves the right to modify and enhance the solution and provide it to C-DOT customers or another Partner(s). C-DOT shall engage with Partner(s) on a non-exclusive basis and shall retain its right to develop similar projects/products through other developmental programs.
7	**Roles & Responsibilities of Partner(s)**	The Partner(s) may build the required module afresh or by modifying pre-existing background technologies available with them. As per the project demand or project

		type, the Partner(s) may utilize the available test and infrastructure facilities offered by C-DOT with no/some financial implication for its usage. All commercial proposals shall include necessary cloud infrastructure cost as per requirements, manpower and cost breakup (Capital, Consumables, Travel, DA, Training, Contingency, Overhead, GST etc.). The proposal should include minimum of two years support for enhancements and capacity building for future enhancements in the product. Participation in the project shall be on a non-exclusive basis. All partner(s) shall be required to demonstrate commitment to the project by entering into a formal agreement with C-DOT as per the CCRP policy.
8	**Expected Deliverables**	DPI solution with feature set and capabilities enumerated in sl. No. 5 **Timeline: 1 year**
9	**Ownership of Background & Foreground IP**	All technologies created during the project shall be owned by the respective development partner(s), individually or collectively as the case may be. Any agreement required for collective ownership shall be settled directly by the concerned partners, but the ownership/IPR of the final solution shall rest with C-DOT only with all the deliverables including complete source code etc.