Proposal No. 06

(Proposal details for the R&D scheme of USOF)

Subject: Solution for Telecom self-correcting Network

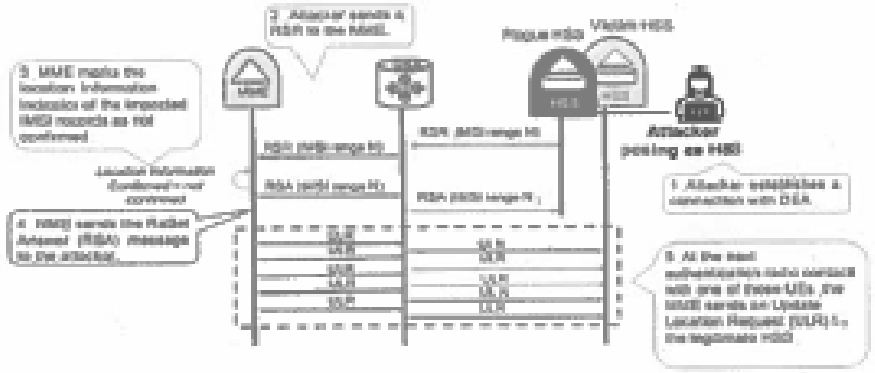
a)	Description of Product / Concept/Idea (in detail)	This software solution will identify anomaly in network. It will, based on training model using AI/ML , will predict fault and fraud in the network. Any network can have following challenges 1. Signaling attack (Some example attacks are shown in figure 1) 2. Revenue loss by traffic that bypass rules 3. Performance degrade 4. Fault This software solution will do analysis on logs and based of rules and training model it will predict possible 1. anomaly 2. attack 3. fault Solution suit may comprise 1. interfaces to network nodes (log access of nodes) 2. Data collection , segregation 3. ML Models 4. Forecasting Algorithms 5. Indicators 6. Dashboard
a)	Objective	Develop SW solution for 1) Anomaly Detection in Telecommunication Network 2) Fraud Detection, Prevention and Prediction
a)	Key deliverable	1. SW for Anomaly detection
a)	How did the idea originate	Product portfolio of following companies gave idea of this product . Figure 2 shows reference architecture f these products **Mavenir** https:// www.mavenir.com/portfolio/ mavepps/fraud-security/ **Ericsson** https://www.ericsson.com/en/blog/2021/8/p roactive-anomaly-detection
	Potential demand	Following may require this products 1) Telcos (MTNL, BSNL, JIO, AIRTEL) for making their network safe from fraud, attack and failures 2) Govt agencies (Defense, Space, Railways) may require for the safety and security

	Alternate competing technology /& product available / under development locally / outside India	Following companies are working in the area of Anomaly detection 1) Mavenir 2) Ericsson
	How they compare in performance / features / cost with what you are proposing	Not Known Now, need KRA ,people to study
	What makes your proposal different and unique	No difference
a)	Will it serve any value addition to any current CDOT's product? If so, how?	Security being generic so required with every product of CDOT
b)	Key technology to be used	1. AI/ML for decision making 2. DB (SQL, NoSQL both) 3. Web Infrastructure (Application Server, WebServer) 4. Backend (Java), Python 5. Security (TLS/SSL etc) 6. Linux OS
a)	What kind of application areas/market/segment it will serve	• Telecom network security • Performance and fault detection in telecom network • For web based solutions so that security vulnerability like unwanted access can be predicted anytime
a)	What kind of social/ security impact will it have on society/Nation?	1. Security Impact . Indigenous so safe (same reason for which GOI opted for indigenous Core of CDOT in LTE-ENH) . Can be used in border and other areas of security concern
a)	Budget requirement (approx.)	(Rs. in Lakhs)
	Component & Consumables	Not Known Now, need KRA ,people to study
	Computing Equipment	Not Known Now, need KRA ,people to study
	prototype development	Not Known Now, need KRA ,people to study
	Software Licensees / AMCs	Not Known Now, need KRA ,people to study
	Deployment / Rollout planned	Not Known Now, need KRA ,people to study
b)	Approximate timelines for prototype readiness or conducting a PoC (Proof of Concept)	Not Known Now, need KRA ,people to study
c)	What kind of resources would you require from C-DOT	1. Manpower 2. Capital 1. SW 1. Open Source Security Solutions 2. AI,ML framework 3. Training , Certification in Security, ML/AI 3. Mentoring & Leadership from Board Seniors
1.	Requisite support required from other design and service groups in C-DOT	Design : Review/Feedback Service : Not Known Now, need time ,people to study

d)	Will it be an Application Oriented Solution/Product or will it require certain hardware to be developed?	It will be a software product
e)	Are the hardware equipment, PCBs, components and chipsets required for the product development readily available from vendors?	NA
f)	Use existing hardware or with minor changes in PCBs only	NA
g)	List out the expected IPRs, if any on the development of proposed technology / product	Copyright , Publications Papers on new Algorithms, Patent on System
h)	What will be the Utility of infrastructure built up after project completion?	The expertise developed will be useful for future security, ML/AI based products.

Figure 1: Attack on Diameter protocol leading to denial of services

Source: Ericson



Format of Response

Companies / organizations / institutions / individuals developing enabling technologies / modules / components / subsystems / products are required to respond in the format provided in Annexure-A, on the DOT website (link address provided- refer “format of response”)