ACTION TAKEN REPORTS

Name of the Host Institute: IIT KANPUR

Name of the TIH: IHUB NTIHAC FOUNDATION

Technology Vertical: CYBER SECURITY AND CYBER SECURITY FOR PHYSICAL INFRASTRUCTURE

	Problem Area/details	**Name of line ministries/States Govt/PSUs/industries**	**Collaborating TIH**	**Collaborating Partner other than TIH**	**Projects undertaken**	**Technology/product developed (current status)**	**Any other update**
W.r.t. problem statement shared by MO on 20.07.2021	5) As per para 23.13 of the National Educational Policy 2020, focus has been insisted on the laws and standards associated with data handling and data protection as it is vulnerable to both physical and online threats as personal and other confidential data has to be considerably secured. 6) In NDEAR, as a part of student registry infrastructure, cyber security plays an eminent role in the design principles it must ensure that data is exchanged in a secured manner with well-defined privacy rules and in alignment with access allowed by data owner and issuer. Necessary work will be done accordingly with the frameworks and coordination with IIT Kanpur may also be initiated.	Department of School Education and Literacy, Ministry of Education, Government of India	No	None	No		
	Technologies for Internet of Things and Internet of Everything 36) There are security challenges in the deployment of IoT devices that pose severe threats not only to its operations but also can potentially harm the entire internet. There were several instances where the IoT devices were used as malwares to target other systems such as DNS, Web Servers etc. 37) Another challenge in the area of IoT was the Privacy of the end users and most of the IoT device vendors try to monetize the data collected from these IoT devices. 38) A solution should be available so that IoT devices can trust each other anonymously that may protect the privacy of the end users in the deployment. **Cyber Security and Cyber Security for Physical Infrastructure**	Intelligence Bureau (Ministry of Home Affairs), Government of India	No	None	No		

	41) Focus area should be 'cyber security solutions'. 42) Presently, all cyber security solutions are developed by multinational OEMs. Therefore, a customized solution needs to be developed to meet specific requirements pertaining to network and data security. **Autonomous Navigation and Data Acquisition Systems (UAVs, RoVs etc)** 45) Now-days, unconventional Low Slow Small (LSS) air threats pose serious challenges that cause deep concerns among military and civilian security organizations. Consequently, there is a high demand for robust and reliable counter unmanned aerial vehicles (C-UAV) solutions. However, traditional air defence systems may be unable to detect, identify and defeat some types of potentially hostile UAVs. 46) Detection challenges such as small RCS values of air targets, unconventional flight patterns in low airspaces, terrain masking effects, or complex urban environments lead to high false alarm rates. 47) In addition, the evolution of advanced LSS air threats such as signature reduced drones or swarms have to be considered in the development of the second generation of C-UAV.						
	59)**Application of AI/ML for cryptanalysis:** It is learnt that the Computer Science Department of IIT Kharagpur have already been working on cryptanalysis of AES, which is used in most of the modern end-to-end encrypted applications. **Decrypting Https/TLS 1.2 sessions:** 60) Understanding the nature of encryption algorithms including AES/DES 256 & key exchange mechanisms used in the intercepted internet traffic. 61) Developing technologies to exploit the vulnerabilities available in the encryption algorithms/ key exchange mechanism used. 62) In case of symmetric encryptions, identifying the public key and decrypting the session. 63) In case of asymmetric encryptions, developing technological solutions to obtain private key for decrypting the session. This may include mechanisms such as packet alteration/packet corruption etc. **Decrypting VOIP/VC sessions:**	Research & Analysis Wing (Cabinet Secretariat)	No	None	No		

	64) Identifying weak encryption techniques being used by various OTT service providers including those providing video conferencing solutions. 65) Developing mechanisms to identify such traffic flowing over the network and decrypt these traffic. 66) Research on identifying vulnerabilities in latest encryption algorithms used by popular OTT platforms and developing Proof of Concepts for these vulnerabilities. **Technologies for "Internet of Things & Internet of Everything"** 67) IoT security- Developing complete Proof of Concepts for identified/known vulnerabilities in Smart TVs and Smart Watches. To illustrate, there an know vulnerability in Samsung Smart TVs which were exploited to turn them into silent listening devices. A fake off mode was also developed to make it appear that the TV was off, while it was silently recording audio and using the TV's WiFi capability to transmit the recorded files. Similar such latest vulnerabilities could be identified and PoC may be developed for each of these identified ones. **Cyber Security & Cyber Security for Physical Infrastructure** 69) Development of a tool vulnerability assessment and penetration testing of Big Data Systems. **Sensors, Networking, Actuator and controls** 70) Identification of vulnerabilities in Huawei and ZTE networking devices and developing complete Proof of Concepts for these vulnerabilities.						
Other direct Initiatives							