Minutes of the Meeting of the
Brainstorming Session on Artificial Intelligence & Cyber Security (AI&CS)

Date: 17th November, 2018, Time: 10 AM to 1:30 PM Venue: SETS, Chennai

A Brainstorming session on Artificial Intelligence & Cyber Security (AI&CS) was held at SETS on 17th November 2018 under the chairmanship of Dr. K. VijayRaghavan.

Members present:

1. Prof. K. VijayRaghavan , Principal Scientific Adviser to Govt. of India and President, SETS
2. Dr. N. Sarat Chandra Babu, Executive Director, SETS
3. Dr. Hemant Darbari, Director General, C-DAC
4. Dr P V Ananda Mohan, Technology Advisor, CDAC, Bangalore
5. Prof. Arvind, Director, IMSC
6. Prof. Ravindran, IIT Madras & Head, Robert Bosch Centre for Data Science and AI
7. Prof. B. Mehetre, IDRBT
8. Dr. N. Subramanian, Associate Director, C-DAC, Pune
9. Dr. Ajay Kumar, Associate Director, C-DAC, Pune
10. Dr. M. Prem Laxman Das, Sr. Scientist, SETS
11. Ms. A. Suganya, Scientist, SETS
12. Mr. Kunal Abhishek, Scientist, SETS
13. Dr. Lakshmi Devi K., Scientist, SETS
14. Mr. K. Thiruppathi, Sr. Network Analyst, SETS
15. Mr. Karthikeyan, Systems& Networks In-Charge, SETS
16. Mr. Muthukumaran, Project Associate, SETS

The following are the deliberations of AI&CS brainstorming session:

Agenda Item No 1: Welcome Address by ED, SETS

1. Dr Sarat, on behalf of SETS, extended a warm welcome to Prof. K. VijayRaghavan, PSA to GoI, and to the distinguished members who participated from different organizations and thanked them for accepting the invitation and making their presence in this important meeting. He informed that SETS initiated this Brainstorming meet motivated by the special interest shown by PSA "in applying AI aspects in the context of cyber security". Dr. Sarat added that the objective of the meet is to get insights on the subject matter and synergize the efforts of experts to explore the possible AI enablement to cyber security solutions.

   A handout material was shared with all members to help in initiating the discussions.

Agenda Item No 2: Opening Remarks by Prof. K. VijayRaghavan, PSA to GoI

2. Prof. K. VijayRaghavan, Chairman of the AI&CS meet welcomed all the participants and then expressed his expectations from AI&CS. He expressed his happiness for organizing this brain-storming session and appreciated SETS team for preparing the appropriate handout material with the requisite background content.

3. Prof. VijayRaghavan expressed that the AI technologies and their applications in different domains is fast growing and wished to know where India stands in these areas and how much we are equipped with such niche technologies to solve well defined problems across various domains. He mentioned that there are reports from three task forces/ Committees, constituted by GoI departments. While these reports addressed certain issues, the resource requirements are not clearly articulated. He emphasized the need for formulating mechanisms to address the generation and allocation of resources.

4. He felt that the immediate attention is to address capacity building in terms of education, training and skills development in the fields of AI and ML. He said that this can be addressed in two folds: Firstly to identify experts world-over including India and to develop an eco-system to enhance the knowledge and skills of student community at various levels (foundation level to advanced level). He told that this is the right time to connect with world class subject experts and create a pool of highly specialized resources in this area.

5. He added that we need to find out the experts available in the country in ML and AI domain at one side and Cyber Security on the other side to enable each other to produce best solutions to a range of existing problems. He further added that we have now challenges, mainly to create mechanisms and resources for initiating Cyber Security and AI based solutions and we should apply these techniques efficiently to specific kind of projects which may be of open or confidential natures.

6. He also expressed that at this point of time, there is no significant participation of experts from India to participate in International events. It is felt that this aspect needs to be improved by participating in structured manner in meetings at various levels.

7. He emphasised on the following key aspects for nurturing AI for Cyber security:

    i. **Open System Initiative**: To be created by researchers focussing in computer science and mathematics departments

    ii. **Top Down Approach**: To identify and take specific projects which needs to be implemented in mission mode.

    iii. **Structured International Participation**: Indian participation in Top AI conferences are very low and this can be addressed only through structured methodology. We need to carryout filtering and ensure high quality large number of participation in such International events. We need to evolve a model to ensure this is carried out effectively easing out such travel for participation.

Agenda Item No 4: Presentation by ED SETS on intent & the need of the Meet

8. A comprehensive presentation was made by Dr. Sarat covering the evolving threat scenario, importance of AI, International/ National status, importance of standards, industry capabilities & solutions across the globe, available expertise and gaps. He mentioned the need of Artificial Intelligence for various applications and specifically for Cyber Security. He felt that in the context of ever changing threat landscape, application of AI becomes very important to devise effective mechanisms towards detection, deterrence and prevention of Cyber Attacks. He emphasised on the need to focus on Standards apart from publications. He presented the consolidated views on the key aspects which were tabled for brainstorming related to AI for Security and Security for AI. He also provided the intent of the meet and the points for discussion to arrive at a possible plan of action and a way forward.

Agenda Item No 5: Inputs by the participating members

9. Dr Ananda Mohan, an expert in Cryptology and Cyber security made a presentation bringing-out various views of experts on the AI as a domain and its impact on society. Dr. Ananda Mohan presented the details of various challenges in the field of network security and insisted that we need to have mechanisms for dataset creation and contribution. He brought out the challenges faced by humans Vs computers. He informed that there are pockets of excellence in the area of Cryptology at ISI, Kolkata, IISc, IITs and in labs like SETS, C-DAC. He impressed upon the importance of having trained cyber security professionals and also a Chief Information Security Officer in every enterprise.

10. Prof Mehtre, IDRBT, briefly touched upon how IDRBT is contributing to the AI and cyber security. He brought out specific challenges being faced by Financial domain through advanced persistent threats (APTs) and highlighted key initiatives of RBI and IDRBT such as the Indian Banks - Centre for Analysis of Risks and Threats (IB-Cart) program, Cyber drills to various banks to deal with cyber-attacks, and R&D outcomes. He conveyed that as on IDRBT has produced about 15 PhDs and on date 25 PhDs are in progress in the area Banking technology, and some of them are in Cyber security. He also informed that IDRBT was actively involved in collecting 35,000 incidents of cyber-attacks by their Cyber threat intelligence (CTI) wing.

11. Prof. Ravindran, IIT-Madras has indicated that the number of Ph.Ds are continually growing in the area of Cyber Security and AI/ML/DL related technologies. As per his experience the participation of research community in the International events such as conferences, workshops is also growing, though the numbers are still small compared to the similar participation from China. . He added that sufficient incentives and budget is required at this point of time for investing it in to the research and related activities. He indicated that testing of AI systems and components is a big challenge and needs immediate action. Also creating quality data set to train the AI Learning Systems is the need of the hour.

12. Dr Hemant Darbari, DG, C-DAC and Dr Subrahanyam from C-DAC made a presentation bringing-out C-DAC's capabilities in the area of cyber security and AI&ML. Dr. Hemant, presented various AI techniques being applied for High Speed Network & System security, HoneyNet & Botnet analysis, Steganalysis, Digital Forensics and SCADA Security. He also brought out the challenges of AI security and newer evolving opportunities in 5G/SDN and Edge computing. He also shared point wise response and inputs as sought for the brainstorming related to AI for cyber security and emphasised the need to have a national level test bed and creation of data-sets for researchers.

13. Prof. Arvind gave an account of PhDs produced by China in Cyber security, which is much more compared to that of India. He felt that steps needs to be taken to improve this situation. He was also keen to understand the possibility of creating professorships for International experts in Indian organizations.

Agenda Item No 6: Discussions / Deliberations to arrive at next steps

14. It was felt by Chairman and members that the contributions of Indian experts in international fora in the areas of cyber security and AI/ML/DL is abysmally poor. Prof. Ravindran informed that while the participation of Indian community is growing in such events, the same can be improved. He also said that very few faculty exist even in IITs in the area of AI/ML/DL. He also brought to the notice of members that present 40% of research articles on AI are from Chinese researchers. In India, TCS group have around 15 AI experts. He conveyed to that more incentives are required to seed the AI development programme in the country.

15. Prof. VijayRaghavan wished to know if any international conference participation from premier institutions like DRDO, CSIR, C-DAC, to which Dr. Hemant conveyed that C-DAC is encouraging their technical staff to participate in international conferences such as Super Computing 2018 (SC-2018). It was in general agreed that the members need to be encouraged to participate by simplifying the process with a focus on ease of travelling and provision of financial support.

16. Prof. Ravindran conveyed that participations in such niche areas can be made through frequent workshops in which different players like TCS Innovation Lab and others can contribute to a meaningful outcome. Prof. VijayRaghavan also opined that high quality participation of students and faculties are desired.

17. Dr. Sarat indicated that Visweshwarya Fellowship Scheme, Information Security Education & Awareness (ISEA) programs are working towards increasing the number of Ph.Ds. Similar programs in AI &ML area will add value to create talent in the country and to deliver high quality products.

18. Prof. VijayRaghavan wished to know how AI and Cyber Security activity can be pushed in a big way, Prof. Ravindran conveyed that a high quality of International Conference in India will attract foreign experts. He also felt that attracting International experts to visit India is a tedious process and needs to be addressed.

19. Prof. VijayRaghavan concluded that immediate need is to create resources in this area at least at a nodal centre and escalate it to other parts of the country. He told to establish Cyber Physical Systems in India and also to prepare project proposals in AI and Cyber Security and get it funded from O/o PSA.

20. Dr. Anand Mohan conveyed that it is time to create a big data set to train our AI systems. He added that developing Test Vectors in AI is also required at present.

21. Prof. Mehtre conveyed that IDRBT is actively proceeding with 2 patents in the APT and produced 15 Ph.Ds in this area. They have also collected 35000 incidents and developed Cyber Threat Intelligence (CTI) and quarterly organize SISO Forum every quarter of the year. Prof. VijayRaghavan felt that if there is any International effort to look at financial, banking frauds where different nation's could be members and share the incidents and possible counter measures for different cyber-attacks.

22. Prof. VijayRaghavan directed ED, SETS to look at more closely on the specific requirements of banking sector in terms of training, manpower needs etc. in the area of cyber security by working closely with IDRBT.

23. Prof. VijayRaghavan queried with regard to who monitors & controls cyber security activities in India. Dr. Subramanian responded to this and informed that there are national organizations working in the area of Cyber Security and regulating them. These organizations include, CERT-IN, NTRO/ NCIIPC, CCA etc.

24. Dr. Subramanian conveyed that CDAC has done a considerable amount of work in AI technologies and cyber security and arrived at some useful solutions, especially in the AI enabled Cyber Forensics.

25. Prof. Ravindran conveyed that now challenge lies in testing the AI systems and giving guarantee for their safe operations. He told that we need to work towards devising new models for AI and Cyber Security.

26. Prof. VijayRaghavan suggested that a budgeted Umbrella programme in AI and Cyber Security can be proposed to O/o PSA in the peripheral interactive areas with focused programmes to lay foundation at all levels with a long-term goals.

27. Prof. VijayRaghavan suggested that Prof. Ravindran can identify the top talent who would be useful for developing AI/ ML based technologies for cyber security and other related areas. He suggested that conducting workshops may be an interface for the same. He also added that we need to look into how resources can be used to do research activities in this area. He also suggest to have help from experts like Dr. Prateek Jain of Microsoft Research in the area of Machine Learning areas.

Agenda Item No 7: Recommendations & Concluding Remarks (towards Plan of action: way forward and action items)

28. The main goal of AI&CS brainstorming session was to bring together AI and cyber security experts and to chart future course of action and way forward. The following are the recommendations/ action points emanated from the discussions and concluding remarks of Prof.VijayRaghavan.

29. Recommendations

- Training the trainers focussing on excellence at foundational level and having in place an amplifying mechanisms. Can adopt combined approach roping in faculty from reputed academic institutes and offer online training materials.

- Cyber Security Research Program: To groom PhDs through a solution driven model where the focus is not just on doing incremental research but to create new frontiers and development. Lessons learnt from ISEA and Networking initiatives in the past to be taken in cognizance.

- To create a high quality node as a model with all AI&CS facilities to begin with. This model could be replicated to meet the needs of the nation in due course of time. The details related to this aspect can be done taking inputs from Prof. Ravindran, IIT Madras.

- To create quality data for training of AI research. Creation of data-sets in our country is essential and throwing open the same through announcement of cyber challenge across the globe is required to bring in visibility and recognitions for such data set created by our country. Visual data analytics is very important to present the useful data alone to the user based on AI to enable immediate actions by humans.

- Creation of National level test bed for carrying out cyber security and attack experiments to study and understand attack behaviour is very much required.

- Testing of AI system is by itself an area to be researched thoroughly and needs sufficient focus towards the same.

30. Plan of action and way forward:

- To setup the PMG (Project Management Group) which shall play the nodal agency to collate and coordinate experts from across country in CS, Mathematics, Statistics, AI and sector specific leaders (NSM,CPS, Banking, Defence, ICS/SCADA etc).

- PSA office shall provision seed resources towards Project Management and towards Consultancy Contract to group of people (or) to a nodal agency. Fund support shall be extended to monitor and implement the entire programme. However PMG will work towards generating more funds beyond seed funding from the programs such as NSM, CPS; Cyber security funding agencies; or from user agencies like Banking, Defence.

- It is recommended to encourage world class collaborations in these technologies to develop core competencies in the country. As part of this recommendation to identify and choose at least Top 5 Experts abroad and invite them to spend quality time with researchers.

- To identify 4-5 young leaders (from Government, academia, industry and R&D labs) to drive the AI&CS program and SETS to spearhead the program and manage the PMG nodal agency to have all facilities and resources to begin with.

The meeting ended with vote of thanks to Chairman and experts from various organizations by ED, SETS.