ERCIM "ALAIN BENSOUSSAN"
FELLOWSHIP PROGRAMME

Scientific Report

First name / Family name	Adnan Akhunzada
Nationality	Pakistan
Name of the *Host Organisation*	RISE SICS Vasteras Sweden
First Name / family name of the *Scientific Coordinator*	Hans Hanson
Period of the fellowship	01/06/2018 to 01/06/19

I – SCIENTIFIC ACTIVITY DURING YOUR FELLOWSHIP

I have done the following scientific activities during my fellowship.

1. **Initially, I worked on SALLP project. I have completed first SALLP Project Report on Cyber Security that is** 'Smart Automation Living Lab for Process industry (SALLP) Cyber Security Recommendation Report'. **(i.e., after the successful completion of this report and acknowledgement, SALLP 1 project have been awarded.**

Executive Summary of the report: Smart Automation living lab for process industry (SALLP) is a prioritized testbed project within the innovation partnership programme financed by the Swedish government through Vinnova and together with Swedish industry. We believe that creating an innovative, long-term, and accessible arena for process industry that enables an easier and faster way to test new industrial innovations, functions and solutions in an environment that mimics real production conditions is the need of the day. Since the project spectators are varied network major stake holders that are process industries, system suppliers, equipment suppliers, academia and other various institutions. SALLP project to be scalable and more effective needs to be deployed on Cloud systems. Utilizing the concept of Cloud Computing (CC) for creating and analyzing virtual Cloud-based test systems are highly scalable and efficient. However, this paradigm shift may bring

serious cyber security concerns. The purpose of the cyber security recommendation report is to assist the executive team in developing a strategy for designing, developing, evaluating and managing cyber security apprehensions of the Smart Automation living lab for process industry (SALLP). To appropriately avoid any future cyber security related mishaps, a step by step secure design of the SALLP starting from the very initialization till the deployment is also on the agenda of this report. The report also identifies and highlight some of the major online trends and possible sophisticated attacks on SALLP. A summary of cyber security recommendations is provided. Finally, the recommendations are mainly categorized as Technical (T), Non-Technical (NT), and Physical (P).

2. **Further on continuation of the SALLP project, I worked on SALLP1. I have designed Cyber Security Application Programming Interfaces (APIs) for SALLP1.**

3. **I have also contributed to an EU funding that is 'dynamic encountering of cyber-attacks'. I worked as a WP lead of detection and mitigation of dynamic encountering of Cyber Attacks. Though, we did not get that project, but I worked practically to have some results and that I published in the following papers.**

4. **Moreover, I was also involved with IoTSP project team.**

II – PUBLICATION(S) DURING YOUR FELLOWSHIP

1. **I have published a journal paper (i.e., Journal of Parallel and Distributed Computing) having high impact factor with RISE affiliation. I am also the corresponding author of this paper**

Title of the Paper: **Towards augmented proactive cyberthreat intelligence**

Tanveer Khan [a,b], Masoom Alam [a], Adnan Akhunzada [a,d,*], Ali Hur [b], Muhammad Asif [a,b], Muhammad Khurram Khan [c]
[a] COMSATS Institute of Information Technology, Islamabad, Pakistan
[b] Trillium Information Security, Islamabad, Pakistan
[c] Center of Excellence in Information Assurance (CoEIA), King Saud University, Saudi Arabia
[d] RISE SICS Vasteras AB, Sweden

Abstract - In cyber crimes, attackers are becoming more inventive with their exploits and use more sophisticated techniques to bypass the deployed security system. These attacks are targeted and are commonly referred as Advanced Persistent Threats (APTs). The currently available techniques to tackle these attacks are mostly reactive and signature based. Security Information and Event Management (SIEM), a proactive approach is the best solution. However, the major problem with SIEM is tackling huge amount of data in real time that makes it a time consuming and tedious task for security analyst. The use of threat intelligence caters to such issue by prioritizing the level of threat. In this paper, we assign risk score and confidence value to each feed generated at our product ''T-Eye platform". On the basis of these values, we assign a severity score to each feed type.

Severity score assigns a level to the threat means prioritize the threat. The results, we achieved for prioritizing the threat is more apparent and accurate. In addition, we optimize the rules of IBM-Q-Radar by using threat feeds generated at T-Eye platform. Furthermore, a huge amount of false positive alarms generated at IBM Q-Radar is reduced to a certain extent.

2. **I have also got an acceptance of Conference Paper on Intrusion Detection using Deep Learning in Software Defined Networks**

Title of the Paper: **INTELIGENT INTRUSION DETECTION SYSTEM USING DEEP LEARNING IN SOFTWARE DEFINED NETWORK**

Jahanzaib Malik[1], Iram Bibi[1], Adnan Akhunzada[1,2]

[1]COMSATS Institute of Information Technology, Islamabad, Pakistan
[2] RISE SICS Vasteras AB, Sweden

Abstract- Traditional network architecture proved cumbersome in terms of dynamic network configuration, agile network measurement, and flexible network deployment. Due to unchanged architecture of legacy networks for past few decades, Software Defined Networks (SDNs) has envisioned as emerging approach providing programmability, adaptiveness and flexibility. Despite its promising architecture, it also introduces new attack possibilities and potential security threats. In this paper, we propose an intelligent deep learning-based intrusion detection system (IDS) that provide scalable threat detection in SDN by implementing Long-Short-Term Memory (LSTM), a Recurrent Neural Networks (RNN) based algorithm. The performance of the proposed algorithm has been thoroughly evaluated with standard parameters using state-of-the-art (i.e., ISCXIDS2012) dataset that is purely a Flow-based SDN dataset for network-based intrusions. Our proposed approach outperforms with 99.36 % detection accuracy. After exhaustive experimentation and evaluation, we endorse that deep learning approach has great potential to be used as a Flow-based intrusion detection mechanism in emerging SDN environments.

III – ATTENDED SEMINARS, WORKHOPS, CONFERENCES

I have attended several local seminars in Kista, Stockholm. However, I have never attended any conference abroad.

IV – RESEARCH EXCHANGE PROGRAMME (REP)

I did not avail research exchange programme.