



ERCIM "ALAIN BENSOUSSAN"
FELLOWSHIP PROGRAMME



Scientific Report

First name / Family name

Ankur Shukla

Nationality

India

Name of the *Host Organisation*

NTNU, Norway

First Name / family name
of the *Scientific Coordinator*

Basel Katt

Period of the fellowship

01/04/2019 to 30/04/2020

I – SCIENTIFIC ACTIVITY DURING YOUR FELLOWSHIP

With the time, software systems become more complex, connected and dynamic in nature. Cloud platform provides both economic and technological advantages in smooth operation on these software systems. Cloud computing is a new computing paradigm which provides numerous benefits to customers, service providers and developers in terms of flexibility, availability and scalability. It enables wide ranges of uses including storages, databases, servers and networking for both home and business users. We use cloud-based services in our daily routine such as email, watching online videos, designing online project, editing documents, exploring online images, and so on. Nowadays, top leading companies like Amazon, Google, IBM, Oracle, Microsoft, Adobe and Dropbox provide cloud services. Cloud platform has many advantages to construct and maintain modern IT infrastructure, however it comes with some disadvantages also. The major concern of these cloud platforms is security. Cloud platforms need to be conduct rigorous security check with the time and update to prevent the threats. Assurance of security is very important to protect the crucial data and information present and controlled by the cloud platforms. Security assurance provides the confidence that the system has met, will meet and continuing to meet its required security objectives. Considering this fact, a quantitative approach has been developed to measure the security assurance metric of a private cloud platform, Skyhigh. In this proposed approach two important metrics, i.e., security requirements and vulnerabilities are incorporated. Moreover, it is important for security testing team to detect the

components of the software system which are not much secure and the vulnerabilities which are more severe. Therefore, a detailed analysis to rank the various component of the Skyhigh based on security risk has been done.

Web browsers are primary targets of attacks because of their extensive uses and the fact that they interact with sensitive data. Vulnerabilities present in a web browser can pose serious risk to millions of users. Thus, it is pertinent to address these vulnerabilities to provide adequate protection for personally identifiable information. Research done in the past has showed that few vulnerability discoveries models (VDMs) highlight the characterization of vulnerability discovery process. In these models, severity which is one of the most crucial properties has not been considered. Vulnerabilities can be categorized into different levels based on their severity. The discovery process of each kind of vulnerabilities is different from the other. Hence, it is essential to incorporate the severity of the vulnerabilities during the modelling of the vulnerability discovery process. A VDM is proposed to assess the vulnerabilities present in the software quantitatively with consideration for the severity of the vulnerabilities. It is possible to apply the proposed model to approximate the number of vulnerabilities along with vulnerability discovery rate, future occurrence of vulnerabilities, risk analysis, etc. Vulnerability data obtained from one of the major web browsers (Google Chrome) is deployed to examine goodness-of-fit and predictive capability of the proposed model. Experimental results justify the fact that the model proposed herein can estimate the required information better than the existing VDMs.

On the other hand, I have submitted a book proposal on “Recent Development in Reliability and Security Assurance” with Dr. Basel Katt (Scientific Coordinator) and Professor Hoang Pham, Rutgers University, U.S.A. I attended weekly seminar and lectures organized by Center for Cyber and Information Security, NTNU during the fellowship. I actively participated in various activities organized by Norwegian Cyber Range and System Security Group. I am an active member of System Security Group. I attended a conference entitled “Postdoc Career Conference” on 30th August 2019 in the Trondheim campus of NTNU. I also attended various seminar and lectures on research proposal writing. NTNU also provided great assistantship regarding research proposals.

II – PUBLICATION(S) DURING YOUR FELLOWSHIP

Published/Accepted

- **Ankur Shukla**, Basel Katt, and Livinus Obiora Nweke (2019) “*Vulnerability Discovery Modelling with Vulnerability Severity*”, Proceeding of 3rd IEEE Conference on Information & Communication Technology, December 6-8, 2019, IIIT Allahabad, India.
- **Ankur Shukla** and Basel Katt, (2019) “*Change Point Problem in Security Vulnerability Discovery Model*”, Proceeding of 5th International Conference on Software Security and Assurance, July 25-26, 2019, St. Pölten, Austria
- Subhashis Chatterjee, Bhagyashree Chaudhuri, Chandan Bhar and **Ankur Shukla**, (2019) “*Optimal Release Time Determination Using FMOCCP Involving*

Randomized Cost Budget for FSDE Based Software Reliability Growth Model, International Journal of Reliability, Quality and Safety Engineering, 205004, 27(1). (World Scientific)

Under preparation

- **Ankur Shukla**, Basel Katt, A Quantitative Security Assurance Assessment Methodology of Cloud.
- **Ankur Shukla**, Basel Katt, Livinus Obiora Nweke, Prosper Yeng, Goitom Kahsay Weldehawaryat, Systematic Literature Review on System Security Assurance

III – ATTENDED SEMINARS, WORKHOPS, CONFERENCES

- Oral Presentation in 5th International Conference on Software Security and Assurance, July 25-26, 2019, St. Pölten, Austria. on “Change Point Problem in Security Vulnerability Discovery Model”.
- Oral Presentation in 3rd IEEE Conference on Information & Communication Technology, December 6-8, 2019, IIIT Allahabad, India on “Vulnerability Discovery Modelling with Vulnerability Severity”.
- Attended Sikkerhetsfestivalen 2019 (Safety Festival) organized by the Norwegian Information Security Forum (ISF), August 26-28, 2019, Lillehammer, Norway

IV – RESEARCH EXCHANGE PROGRAMME (REP)

I visited VTT, Oulu Finland for research exchange program during 21st October to 30th October 2019. In VTT, I visited to Reijo Savola, Principal Scientist, Cybersecurity, VTT Technical Research Centre of Finland and Pekka Savolainen, Scientist, Cybersecurity, VTT Finland.

The main motive of my visit to enhance and establish the concrete future research collaboration between System Security Group, NTNU and Cyber Security Group of VTT. I had several meetings with the members of cyber security group of VTT, I given detailed description about our Department of Information Security and Communication Technology (IIK) including various infrastructures and facilities. I also discussed our motivation, our research objectives, various research areas in which we are working, various running projects, our research partners, our business partners, our teaching skills and so on. In this visit, we agreed to work on the automation of vulnerabilities testing in a software system and to measure the security assurance of the software system quantitatively. We also discussed about the possibilities to evaluate the security assurance of mobile based applications.