ERCIM "ALAIN BENSOUSSAN"
FELLOWSHIP PROGRAMME

ERCIM
European Research Consortium
for Informatics and Mathematics

Scientific Report

First name / Family name	Shubham Gupta
Nationality	Indian
Name of the *Host Organisation*	NTNU, Trondheim, Norway
First Name / family name of the *Scientific Coordinator*	Prof. Stig Frode Mjølsnes and Prof. Colin Alexander Boyd
Period of the fellowship	01/11/2019 to 31/12/2020

I – SCIENTIFIC ACTIVITY DURING YOUR FELLOWSHIP

I stared to work in the designing of private identification and authentication of crypto-protocols suitable for 5G lightweight mobility management.

To protect the privacy and integrity of users involved in communications across these networks, 3GPP designed the AKA protocol that mutually authenticates a device consisting of the Universal Subscriber Identity Module (USIM) card and established keys to encrypt these communications. However, taking into consideration the attacks and breaches involved with the security of the various AKA protocols and their versions, the 5G network is vulnerable to the IMSI catching attack. Hence, it is recommended to re-approach the 5G-AKA scheme for implementing the identity preservation of the user equipment/ mobile device (UE/MD) during the communication process.

After that, I started to work in group-based authentication protocol suitable for evolved Machine Type Communication (eMTC) devices in 5G communication network.

As the development of the next generation of mobile communication networks (5G), the 3rd Generation Partnership Project (3GPP) committee has standardized a new 5G-AKA protocol to ensure the access security of a mobile equipment. However, there are still some security vulnerabilities in 5G-AKA protocol and there is no authentication protocol proposed for mass device simultaneous connection by the 3GPP. In this work, I attempt to propose the lightweight and secure authentication protocol for group of eMTC devices. The proposed protocol can achieve several security functionalities including mutual authentication, session key establishment, identity privacy protection, and key forward/backward secrecy (KFS/KBS). In addition, the protocol is lightweight in nature compared with the 5G-AKA. In order to comprehensively and accurately evaluate the protocol, I carried out formal security analysis and informal security analysis. Further, I evaluate the performance of the proposed protocol with regard to authentication signalling cost, authentication communication cost, authentication computational cost and authentication storage cost. The security evaluation and performance analysis results show that the proposed protocol can provide better security and high efficiency.

Apart from that, I submitted the Marie Skłodowska-Curie Actions (MSCA) fellowship proposal 2020; “Colosseum 5G: Generic construction of lightweight security mechanisms for static IoT devices in 5G communication network" with Prof. Stig Frode Mjølsnes.

The project will handle the challenging issues such as identity privacy-preservation of eMTC devices, signalling congestion, and key forward/ backward secrecy in IoT-based applications. Simultaneously, the proposed mechanism can simplify the authentication process, reduce the signalling, storage, and communication overhead. We aim to construct a software application for the static IoT devices (smart home/building) in the 5G communication network. The software application will be installed in the IoT devices and build secure communication with the server/home network by using the lightweight authentication and key agreement mechanism. The mechanism will consist of various security properties such as privacy-preservation, key-establishment, and the freshness of session key, anonymity, untraceability, confidentiality, and integrity that suits for resource-constrained and energy-efficient IoT devices.

Primarily, the following deliverables are desired.

1. We will perform the simulation test-bed/setup to evaluate the proposed system in real-world environment
2. We will keep available the development of project for the researchers and provide place to the research community for further enhancements
3. The successful implementation of software will strengthen the confidence in proposing the new software for various applications such as smart grid, smart agriculture, smart city etc.

II – PUBLICATION(S) DURING YOUR FELLOWSHIP

1. LE2S: Lightweight End-to-End Security Mechanism for Evolved Machine Type Communication Devices in 5G Network; Shubham Gupta and Stig Frode Mjølsnes; work in progress.

2. Private Identification in 5G communication network; Stig Frode Mjølsnes, Sonu K. Jha, Shubham Gupta; pending work.

3. ISAG: IoT-enabled and Secrecy Aware Group-based Handover Scheme for e-Health Services in M2M Communication Network; Shubham Gupta, B.L.Parne, and N.S. Chaudhari; submitted in Future Generation Computer Systems; Revision Submitted

4. SEDI: Secure and Efficient Development of Inter-gNB Handover Authentication and Key Agreement Protocol in 5G Communication Network; Shubham Gupta, B.L.Parne, N.S. Chaudhari, and S. Saxena; about to submit in Peer to Peer Network and Applications springer; Work completed

5. Submitted the Marie Skłodowska-Curie Actions (MSCA) fellowship proposal 2020; "Colosseum 5G: Generic construction of lightweight security mechanisms for static IoT devices in 5G communication network".

III – ATTENDED SEMINARS, WORKHOPS, CONFERENCES

1. I attended the Gemini IoT PhD online seminar at Trondheim, Norway on 28 May 2020. I talked my work on the Group-based Lightweight Authentication Protocol for Evolved Machine Type Communication Devices in 5G Networks.

2. I attended the online workshop supervised by Prof. Radhakrishna Ganti on Overview of 5G technology and 5G testbed work at IIT Madras, India from 23-25 April 2020

3. I attended the IEEE International Conference on Advanced Networks and Telecommunications Systems, IIIT Delhi, India from 14-17 Dec 2020

4. Attended the weekly seminar of NTNU Applied Cryptology Lab (NaCl) group members. Also, I talked on the topic "Group-based authentication protocols" in one of the seminar presentation.

IV – RESEARCH EXCHANGE PROGRAMME (REP)

1. I started the online REP with Prof. Vasos Vassiliou who is the Associate Professor and Co-Director Networks Research Laboratory (NetRL), Chairman, Cyprus Academic and Research Network (CYNET) Department of Computer Science University of Cyprus from 02 Oct 2020 to 16 Oct 2020. In this REP, I discussed my work on private identification

in 5G network with his team. The discussion was very fruitful for both of us and we also discussed about possible collaboration on future work.

2. I stared the 2nd online REP with Prof. Christos Koulamas and Dimitrios Serpanos who are the Research Director at Industrial Systems Institute ATHENA Research & Innovation Centre Patras Science Park Bldg., GREECE. The professors share their working projects and I met online with their team members from 05 Oct 2020 to 12 Oct 2020.

3. I started the 3rd REP with Prof. Shahid Raza who is the Director of Cyber security Unit at RISE Research Institutes of Sweden and his team from 16 Oct 2020 to 22 Oct 2020. In this REP, I discussed my work group-based authentication protocols with his team.

   The discussion was good and his team discussed about possible collaboration/ work in future.

Apart from this, I was involved in following short term programs:

1. I attended the TM8107 - Cryptographic Protocols and Their Applications course under the supervision of Prof. Stig Frode Mjølsnes

2. I attended the NFUT0104 - Norwegian for Foreigners Level-1 under the supervision of Prof. Kjell Heggvold Ullestad

I confirm this report, Trondheim 6/1/21
Stig Frode Mjølsnes