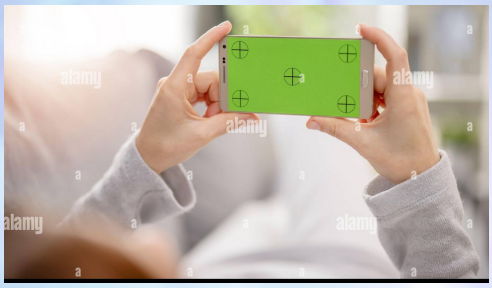
MAGAZINE

ISSUE NO:103
MARCH, 2022

Department of CSE

Byte Quest



RESTRAIN

THOR FI

FLEXMON

REPS-AKA3

Department Vision

To be a center for academic excellence in the field of Computer Science and Engineering education to enable graduates to be ethical and competent professionals.

Department Mission

To enable students to develop logic and problem solving approach that will help build their careers in the innovative field of computing and provide creative solutions for the benefit of society.

FACULTY COORDINATORS

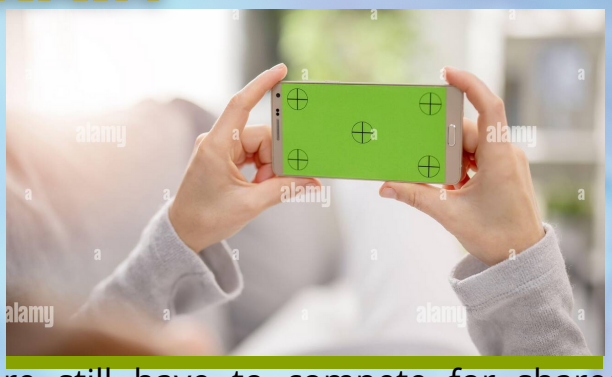
S. KOMAL KAUR
(ASST. PROFESSOR)
T. NISHITHA
(ASST. PROFESSOR)

STUDENT COORDINATORS

CHANDRASHEKAR (2/4) CSE B
ANISHA (4/4) CSE B
AKASH (3/4) CSE C

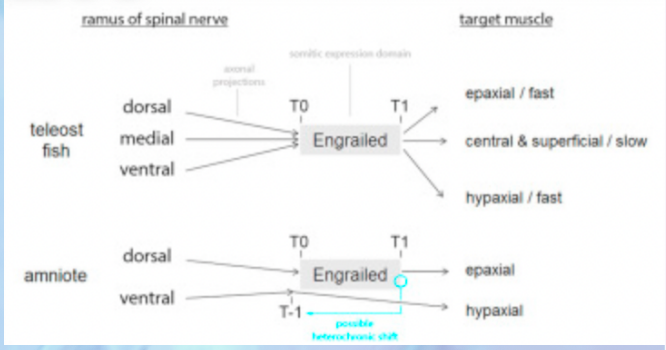
Byte Quest

RESTRAIN



Network Functions Virtualization (NFV) replaces the conventional middleboxes by their software counterparts known as Virtual Network Functions (VNFs) which run on general-purpose hardware platforms and promise several benefits like reduced cost, ease of deployment, flexibility, etc. However, NFV faces some critical challenges as VNFs running on the same physical hardware still have to compete for shared resources such as Last Level Cache (LLC) and different levels of Memory Bandwidth (MB) (between L2 cache & LLC and LLC & main memory), which might result in unpredictable and variable performance interference to the co-located VNFs deployed. Some recent works have explored mechanisms for allocating LLC dynamically using Cache Allocation Technology (CAT) but they did not look into MB contentions among the co-located VNFs.

THOR FI



In this work, we present a novel fault injection solution (ThorFI) for virtual networks in cloud computing infrastructures. ThorFI is designed to provide non-intrusive fault injection capabilities for a cloud tenant, and to isolate injections from interfering with with other tenants on the infrastructure. We present the solution in the context of the OpenStack cloud management platform, and release this implementation as open-source software. Finally, we present two relevant case studies of ThorFI, respectively in an NFV IMS and of a high-availability cloud application. The case studies show that ThorFI can enhance functional tests with fault injection, as in 4%–34% of the test cases the IMS is unable to handle faults; and that despite redundancy in virtual networks, faults in one virtual network segment can propagate to other segments, and can affect the throughput

Byte Quest

FLEXMON

Accurate and fine-grained traffic measurements are crucial for various network management tasks. Recent researches introduce counter-based and sketch-based approaches to traffic measurement.However,implementing accurate and fine grained traffic measurements is very challenging due to the rigid constraints of measurement resources. The counter-based approaches are limited by the memory space constraints that prevent covering each flow in the network, and the sketch-based approaches produce inefficient throughput and lower measurement accuracy. Emerging programmable networking techniques provide programmable, flexible, and fine-grained traffic control capabilities, paving the way for realizing fine-grained and accurate traffic measurements. In this paper, we aim to design efficient traffic measurement schemes for programmable networks. We first propose a single-node traffic measurement scheme called FlexMon to accurately measure fine-grained flows in a single network node. The FlexMon separates large flows from small ones and uses dedicated flow rules and sketches to measure large and small flows, respectively. Then, to further improve the measurement performance by efficiently leveraging the network-wide measurement resource, we propose a network-wide traffic measurement scheme and extend FlexMon to support network-wide measurement. We implement the FlexMon on FPGA and CPU to process five typical measurement tasks. Experimental results show that both the single-node and network-wide measurement schemes can achieve much faster speed and higher accuracy compared to the state-of-the-art.

Byte Quest

REPS-AKA3

Key agreement and authentication are the most significant phases in LTE systems since many malicious attacks may occur in these systems. For this reason, the LTE system employs standard EPS-AKA protocol to provide security of the communication system. However, the LTE system still suffers from different security threats such as Impersonation,DoS,MitM and replay attacks. In this paper, a Robust Authentication and Key Agreement protocol (REPS-AKA3) has been suggested to resolve the security issues in LTE systems. The proposed REPS-AKA3 combines the Public Key Infrastructure, symmetric key Infrastructure, and full mutual authentication between all network nodes. First, we propose an efficient AKA protocol to enable mutual authentication between the users (i.e., UE) and the LTE network (i.e., MME and HSS nodes). Then, we present a secure procedure to enable key agreement in NAS and AS layers properly. Finally, we suggest a secure and fast re-Authentication procedure to reduce the AKA latency in the next attach. Thus, the REPS-AKA3 method provides the security goals (i.e., strong mutual authentication, and adequate confidentiality) in AS and NAS layers appropriately. Formal verification of the proposed REPS-AKA3 protocol is checked and validated using the AVISPA tool. The evaluation results illustrate that the REPS-AKA3 can achieve all the security goals, and it is secure against different malicious attacks.

BROUGHT TO YOU BY

Department of Computer Science and Engineering

Vasavi College of Engineering