Rana Abu Bakar

ABOUT ME

Dedicated PhD with over 12 years in IT, focusing on networks, network security, and system administration. Experienced researcher with 5 years in advanced European projects and 3 years in academia, teaching computer science subjects. Skilled in Linux administration, C, Python, and machine learning, with a strong analytical mindset. I am seeking a challenging role as a Network Researcher to apply expertise in network protocols and secure system architectures.

WORK EXPERIENCE

01/01/2023 – CURRENT PISA, Italy
RESEARCHER CNIT

As a researcher at the National Inter-University Consortium for Telecommunications (CNIT), my work has focused extensively on cutting-edge network security solutions, particularly within various European projects aimed at advancing telecommunications and cybersecurity technologies. My involvement in key projects such as **SMARTEDGE**, **DESIRE6G**, **CLEVER**, **NATWORK**, and **SMARTY** has allowed me to contribute to the development and implementation of secure, resilient, and efficient network architectures, with a focus on both wired and wireless systems.

20/08/2020 – 31/10/2022 Bangkok, Thailand
RESEARCH ASSISTANT CHULALONGKORN UNIVERSITY

1. Writing literature review
2. Conducting research on hardware-based scanners and summarizing findings.
3. Attending weekly group and one to one meetings
4. Checking the work progress of master's projects
5. Performs various job-related duties as assigned by supervisor

19/07/2015 – 01/10/2022 KASUR, Pakistan
ASSISTANT MANAGER CENTURY PAPER & BOARD MILLS

60 Network designs, 40 network support jobs per day, Network traffic monitoring, supporting and developing new Security mechanisms, I.T documenting and enforcing ISO system standards in the I.T department.

31/08/2018 – 01/09/2022 Sahiwal, Pakistan
VISITING LECTURER UNIVERSITY OF SAHIWAL

Conducted lectures on Operating Systems, Cyber Security, Cloud Computing, Data Structure, Data Warehouse and Databas, delivered 12 hours per week of instructions in theory and hands on labs.

EDUCATION AND TRAINING

01/10/2022 – CURRENT Pisa, Italy
PHD STUDENT Scuola Sant'Anna Pisa

Address Piazza Martiri della Libertà, 33, 56127, Pisa, Italy | **Website** https://www.santannapisa.it/

30/09/2015 – 05/06/2018 Lahore, Pakistan
MSCS Virtual University of Pakistan

As an M.S student, I developed a particular interest in the machine learning research gaps and limitations which affect large-scale businesses and economic outcomes worldwide. Progressing toward the interest, I have used a machine-

learning-based optimized technique to detect DDoS attacks in real-time traffic and mitigated attacks at the initial attack stage by using SNORT-based IPS in my Master's project.

Field of study Computer Science | **Final grade** 3.66/4.0 |

Thesis SMART ROUTING BASED ON DDOS DETECTION WITH INTELLIGENT SURVIVABLE CENTRIC NETWORK AGENT

31/08/2013 – 22/07/2015 Islamabad, Pakistan
MCS Comsats University

In my undergraduate M.C.S, I have studied a broad mixture of science and engineering subjects. Various courses like Artificial Intelligence (Robotics), Programming Languages (C, C++, JAVA, Android, Assembly), Software Engineering, Assembly, Algorithm Analysis and Design, Data Structure, Computer Networks, Computer graphics, and multimedia. Computer Simulation and Modelling gave me an excellent background in the theoretical concept of Computer Science and Engineering.

Field of study Computer Science | **Final grade** 3.20/4.0 | **National classification** 1 | **Number of credits** 72

DIGITAL SKILLS

OS: Windows OS, Linux, MAC OS | Programming Languages: C, C++, C#, Python | Penetration Testing | Virtulization (Red Hat Virtualization Ovirt KVM VMware) | Simulation/Emulation frameworks (NS3, Mininet, OMNeT++ ...) | Ability to manage security solutions (email gateway, WAF, DLP, endpoint security, network firewall) | Zabbix Server, Pfseanse, Kerio Control, Mikrotik, Radius Server AAA, Cisco FMC FTD | Routing protocols OSPF-EIGRP-BGP-ECMP | Switching Protocols(STP,RSTP and MSTP) | Ansible network automation

LANGUAGE SKILLS

Mother tongue(s): **URDU**

Other language(s):

	UNDERSTANDING		SPEAKING		WRITING
	Listening	Reading	Spoken production	Spoken interaction	
ENGLISH	C1	C1	C1	C1	C1

Levels: A1 and A2: Basic user; B1 and B2: Independent user; C1 and C2: Proficient user

PUBLICATIONS

2024
A Secure and Green Cognitive Routing Protocol for Wireless Ad-Hoc Networks

We propose an efficient and intelligent Cognitive (COG) Protocol to address routing issues and ensure optimized and secure routing. The proposed protocol is based on cognitive behavior and utilizes the extension header field of IPv6 for route selection in wireless ad hoc networks.

M. Saqib Javed and R. A. Bakar, "A Secure and Green Cognitive Routing Protocol for Wireless Ad-Hoc Networks," in IEEE Access, vol. 12, pp. 194989-195004, 2024, doi: 10.1109/ACCESS.2024.3519976.

2024
VRPR: A New Data Center Protocol for Enhanced Network Performance, Resilience and Recovery

We propose the Versatile Resilience Packet Ring (VRPR) protocol. VRPR leverages a dual-connectivity approach to manage network traffic efficiently. It is implemented alongside P4-enabled network adapters on servers, allowing them to seamlessly utilize both wired and wireless links. Servers can choose the optimal link type based on load and potential interference. In case of a wired link failure, servers can seamlessly transition to wireless links, minimizing downtime and ensuring application availability. VRPR's rapid recovery times further enhance network robustness. The protocol integrates seamlessly with P4, a programmable network architecture. This enables efficient packet duplication, rerouting, and fault tolerance mechanisms within the VRPR framework. The P4-based approach allows for the integration of security measures like flow entry verification and additional security checks, ensuring robust protection of sensitive data within the network.

Muzaffar, et al. 2024 IEEE ACCESS

2024
Wireless and Fiber-Based Post-Quantum-Cryptography-Secured IPsec Tunnel

In this work, we report on the first experimental IPsec tunnel secured by the PQC algorithms Falcon, Dilithium, and Kyber. We deploy our IPsec tunnel in two scenarios. The first scenario represents a high-performance data center environment where many machines are interconnected via high-speed networks. We achieve an IPsec tunnel with an AES-256 GCM encrypted east–west throughput of 100 Gbit/s line rate. The second scenario shows an IPsec tunnel between a wireless NVIDIA Jetson and the cloud that achieves a 0.486 Gbit/s AES-256 GCM encrypted north–south throughput.

Lawo, et al. "Wireless and Fiber-Based Post-Quantum-Cryptography-Secured IPsec Tunnel."

2024

FTG-Net-E: A hierarchical ensemble graph neural network for DDoS attack detection

This paper proposes a new DDoS attack detection approach that uses Graph Neural Networks (GNN) ensemble learning. GNN ensemble learning is a type of machine learning that combines multiple GNN models to improve the detection accuracy. We evaluated our approach on the Canadian Institute for Cybersecurity Intrusion Detection Evaluation Dataset (CICIDS2018) and CICIDS2017 datasets, a benchmark dataset for DDoS attack detection.

Bakar, et al. "FTG-Net-E: A hierarchical ensemble graph neural network for DDoS attack detection

2024

5GDAD: A Deep Learning Approach for DDoS Attack Detection in 5G P4-based UPF

We propose a novel framework for collecting and processing large amounts of telemetry data in 5G networks leveraging state-of-the-art technologies, including data-plane programmability in P4-based User-Plane Function (UPF) and Data Processing Unit (DPU). Furthermore, we propose an anomaly-detection method for performing live deep learning analysis on network traffic using a Convolutional Neural Network (CNN) to detect DDoS attacks. Our results demonstrate the effectiveness of our framework, achieving an impressive 98.6% accuracy and 98% F1-score

Bakar, et al. "5GDAD: A Deep Learning Approach for DDoS Attack Detection in 5G P4-based UPF."

2024

DPUAUT: Secure Authentication Protocol with SmartNiC Integration for Trustworthy Communications in Intelligent Swarm Systems

In this paper, we propose a provably secure authentication protocol using a Bluefield Data Processing Unit (DPU), enabling one-round mutual authentication while preserving anonymity and preventing physical attacks using PUF. We conduct security analyses comprehensively, which provide evidence of its strong resilience against attacks. Experimental evaluation confirms its dominance over existing solutions. The DPUAUT swarm authentication protocol has a low computational overhead of 6.1 ms, and the communication overhead is 1052bits.

Bakar, et al. IEEE Access (2024).

2024

First Line-rate End-to-End Post-Quantum Encrypted Optical Fiber Link Using Data Processing Units (DPUs)

We demonstrate the first 92.3-Gbits/s line-rate, end-to-end post-quantum cryptography optical fiber link based on HW accelerators and processing offloading.

Aguilera, et al. OFC 2024

2024

Programmable Packet-Optical Networks using Data Processing Units (DPUs) with Embedded GPU

Data Processing Units (DPUs) with embedded GPU have the potential to rev-olutionize optical networks functionalities at the edge. Use cases are presented for optical data monitoring with local AI processing and embedded security.

Piero, et al. OFC 2024

2023

Cascaded Look Up Table Distillation of P4 Deep Neural Network Switches

This paper proposes an innovative knowledge distillation technique that maps a DNN into a cascade of lookup tables (i.e., flow tables) with limited entry size. The proposed mapping avoids stateful elements and maths operators, whose requirement prevented the deployment of DNNs within hardware switches up to now. The evaluation is carried out considering a cyber security use case targeting a DDoS mitigator network function, showing negligible impact due to the lossless mapping reduction and feature quantization.

Lorenzo, et al. "Cascaded Look Up Table Distillation of P4 Deep Neural Network Switches." GLOBECOM

2023

Enhancing Network Visibility and Security with Advanced Port Scanning Techniques

In this paper, we develop and implement advanced techniques such as protocol-specific probes and evasive scan techniques to enhance the visibility and security of networks. We also evaluate network scanning performance and scalability using programmable hardware, including smart NICs and DPDK-based frameworks, along with in-network processing, data parallelization, and hardware acceleration. Additionally, we leverage application-level protocol parsing to accelerate network discovery and mapping, analyzing protocol-specific information. In our experimental evaluation, our proposed DPDK-based scanner demonstrated a significant improvement in target scanning speed, achieving a 2× speedup compared to other scanners in a target scanning environment.

Abu Bakar, R.; Kijsirikul, Sensors 2023, 23, 7541

2023

An Intelligent Agent-Based Detection System for DDoS Attacks Using Automatic Feature Extraction and Selection

This paper proposes an intelligent agent system for detecting DDoS attacks using automatic feature extraction and selection. We used dataset CICDDoS2019, a custom-generated dataset, in our experiment, and the system achieved a 99.7% improvement over state-of-the-art machine learning-based DDoS attack detection techniques. We also designed an agent-based mechanism that combines machine learning techniques and sequential feature selection in this system.

Bakar, et al. Sensors 23.6 (2023): 3333.

2023

LSNCP: Lightweight and Secure Numeric Comparison Protocol for Wireless Body Area Networks

We propose the lightweight and secure NCP (LSNCP) which requires less scalar multiplication than the NCP in Bluetooth. New logic expressions and rules are proposed to verify the security of LSNCP in GNY logic. The proof shows that LSNCP is secure. We conduct a provable security analysis by integrating the commitment scheme and short hash function. The result shows that LSNCP is secure in the modified Bellare–Rogaway model.

Haotian Yin et al IEEE Internet of Things Journal. 2023

2020

An effective mechanism to mitigate real-time DDoS attack

In this paper, we provide a mechanism that not only detects the presence of a DDoS attacks but also identifies the route of attack and commences a process of mitigation at the initial stage of identification.

R. Abubakar et al., "An Effective Mechanism to Mitigate Real-Time DDoS Attack," in IEEE Access

ONLINE COURSES

31/03/2020 – 30/04/2020

Data Science:Machine learning from Harvard

https://www.coursera.org/account/accomplishments/certificate/5N422AJ839YQ

31/12/2018 – 05/12/2019

Machine Learning from Stanford University

Information Security: Context and Introduction course organized by the University of London, Royal Holloway, the University of London at Coursera.

Link https://www.coursera.org/account/accomplishments/certificate/5N422AJ839YQ

01/12/2019 – 01/04/2020

Information Security: Context and Introduction

Link https://www.coursera.org/account/accomplishments/certificate/8BF8E9FL2KBG

01/09/2019 – 01/11/2019

AI For Everyone

Link https://www.coursera.org/account/accomplishments/certificate/QNDH8AGV6XPD

01/08/2019 – 01/11/2019
AWS Fundamentals: Going Cloud-Native

Link https://www.coursera.org/account/accomplishments/certificate/YBMKYVFKT6F3

CONFERENCES AND SEMINARS

04/12/2023 – 08/12/2023 Kuala Lumpur, Malaysia
IEEE GLOBECOM

I have presented our paper titled "Cascaded Look Up Table Distillation of P4 Deep Neural Network Switches".

Link https://globecom2023.ieee-globecom.org/

14/12/2021 – 16/12/2021 Bangkok, Thailand
The 16th Asian Internet Engineering Conference (AINTEC)

17/12/2019 – 23/12/2019 Lahore, Pakistan
IEEE International conference Open-Source Software (ICOSST)

COMMUNICATION AND INTERPERSONAL SKILLS

Communication Skills

Good communication skills were gained through my experience as a visiting lecturer and as a presenter at conferences.

TRAININGS

10/06/2021 – 12/03/2022
Certified Information Systems Auditor (CISA) training

NUST College of Electrical & Mechanical Engineering (CEME) organized Certified Information Systems Auditor (CISA) training.

04/05/2016 – 07/12/2016
PLC HMI SCADATraining

COMSATS Institute of Information Technology and IEEE CIIT Lahore (Industrial Automation Lab Training & Skill Development Programmes) organized PLC HMI SCADA training

VOLUNTEERING

09/07/2015 – CURRENT Kasur, Pakistan
Volunteer at Human Rights Commission

I am providing voluntary services for the Establishment of Human Rights Information Management System at our district office of HRC. Also take part of awareness on international human rights principle and take part in survey to promote tolerance and respect for human rights in our distric.

RECOMMENDATIONS

Piero Castoldi Professor

He is a Full Professor at the Institute of Telecommunications, Computer Science and Photonics at Scuola Superiore Sant'Anna, Italy.

Email piero.castoldi@santannapisa.it

Muhammad Saqib Javed Lecturer

Lecturer Computer Science at Virtual University of Pakistan

Email saqibjaved@vu.edu.pk | **Phone** (+92) 042111880880

PROJECTS

01/01/2023 – CURRENT

SMARTEDGE

This project centers on enhancing the security of autonomous systems, especially in vehicular networks. I have been responsible for integrating SmartNIC-based solutions for real-time attack detection and mitigation, leveraging programmable DPUs to improve the system's responsiveness and security while maintaining minimal latency in communication between edge devices.

01/01/2023

DESIRE6G

As part of this project, I contributed to developing security protocols for 6G network infrastructures. I worked on creating scalable and flexible solutions to secure ultra-dense, low-latency 6G environments, focusing on enhancing the robustness of wireless communications against cyber-attacks.

01/10/2022 – CURRENT

CLEVER

In CLEVER, I designed secure communication protocols for connected devices within IoT ecosystems. The project explored the potential of cognitive and AI-based techniques for detecting and mitigating cyber threats in real time, with a special focus on low-power and resource-constrained IoT devices.

01/01/2024 – CURRENT

NATWORK

My role in NATWORK EU project revolved around network function virtualization (NFV) and integrating SmartNIC technology for DDoS attack detection and mitigation. I led the efforts in building a secure, programmable infrastructure capable of handling high-speed network traffic, providing real-time monitoring and rapid response to threats.