Azhar Ghafoor

Lecturer Cyber Security

Chatta Bakhtawar, Islamabad

Dec 10, 1996

azhar.ghafoor@mail.au.edu.pk

+92 305 5125974

https://azharghafoor.netlify.app/

Professional Summary

I am a highly skilled cybersecurity analyst with expertise in cyber deception, web attacks detection, phishing, compliance, pen testing, and data analytics. My passion for staying up-to-date with the latest technologies and best practices, combined with my broad skill set, enables me to approach challenges creatively and provide effective solutions for my clients. My goal is to advance my career in cybersecurity by obtaining certifications in advanced techniques and technologies, as well as pursuing opportunities to lead and manage cybersecurity projects. I am committed to contributing to the cybersecurity community through research, education, and mentorship, and I am excited to take on new challenges and opportunities in the field.

Social Network

linkedin.com/azhar-ghafoor

medium.com/GhafoorAzahr

researchgate.net/AzharGhafoor

github.com/AzharGhafoor

Languages

Urdu	●●●●●
English	●●●●○

Working Experience

2022-2023 **Cybersecurity Analyst** Cytomate Solutions & Services

- Spearheaded the creation of a cutting-edge compliance tool utilizing the NIA Policy Framework, measuring compliance for SMEs nationwide, resulting in a 50% increase in compliance rates for clients.
- Led a team of four cybersecurity professionals to create a post-attack assessment system using machine learning models to detect undetected attacks. This system was 40% more effective than competing systems in the market.
- Played a leading role in an attack surface management project to protect the organization by detecting, preventing, and containing critical assets and information in a timely manner. Expected to be implemented across multiple clients.
- Led a phishing awareness project where different exploits were created to steal users' emails and hijack their accounts. Created a machine learning-based tool to reduce password harvesting attacks by more than 80% than previous statistics.
- Led the development and deployment of advanced cyber deception systems, resulting in a remarkable 70% decrease in successful attacks on client networks.
- Conducted in-depth log analysis using advanced machine learning models to uncover hidden malicious patterns and identify threats in their early stages. Strengthened overall security posture and reduced detection time for attacks by 70%.
- Deployed network protection technologies such as IDS/IPS and firewalls and integrated them with different SIEM solutions such as QRadar, Wazuh, and Splunk. Created a post-attack assessment system to reduce the detection time for attacks by 60%. Successfully integrated IDS/IPS technology with SIEMs QRadar and Wazuh to enhance endpoint visibility and cybersecurity measures, resulting in a 50% reduction in successful attacks on client networks.
- Collaborated with cross-functional teams on multiple cybersecurity projects, showcasing excellent communication and teamwork skills.

2021 – 2022 **Cybersecurity Researcher** Cybersecurity Lab

- Contributed to advanced cybersecurity projects aimed at luring attackers away from real organizational assets by deploying decoy-based deception systems.
- Profiling threat actors based on their malicious intents and level of severity for any firm.
- Investigated adversaries' collaborative efforts to launch attacks.
- Developed models with advanced capabilities for classifying web attacks using machine learning.

2019 – 2019 **Intern** AKSA-SDS

- Completed research, compiled data, updated spreadsheets and produced timely reports.
- Developed and maintained relationships with key internal stakeholders.
- Maintained accurate records and documentation of projects to inform stakeholders of progress and updates.
- Optimized Google knowledge panel and developed a chat application.
- Wrote technical documents related to software development and deployment.

Education

2020 – 2022 **MS Information Security** COMSATS University Islamabad

CGPA: *3.83 (91.8%)*

Thesis: *Measuring The Effectiveness Of Geotagging In Cyber Deception.*

2015 – 2019 **BS Information Technology** Quaid-i-Azam University

CGPA: *3.10 (70.3 %)*

Azhar Ghafoor

Lecturer Cyber Security

Technical Skills

- Cyber deception with advanced geo-tagging
- Data analytics for in-depth threat analysis
- Web attacks detection leveraging machine learning
- Phishing detection and response
- Penetration testing methodologies and techniques
- Compliance experience including tool development for SMEs

Soft Skills

- Effective communication and collaboration skills
- Project execution and management
- Development of lab modules for cybersecurity students
- Passion for staying up to date with latest technologies and best practices

Hands-On Tools

- ISO-27001
- NIA Policy 2.0
- NIST
- Splunk
- QRadar
- Wazuh
- Snort
- Suricata
- Nmap
- Cuckoo Sandbox
- Linux (Kali, Ubuntu)
- Google Dorks
- theHarvester
- Amass
- mimikatz
- Metasploit
- httpX
- Metasploitable
- Recon-ng
- Censys
- Shodan
- Gophish
- W3af
- Nuclei
- Wapiti
- Dalfox
- Wappalyze
- Burpsuite
- Zap
- Sublist3r
- Subfinder
- VMware
- Virtual Box
- Whois
- Wireshark
- Anaconda Distribution
- Ettercap
- Ffuf
- Dirbuster
- wfuzz
- Hydra
- Medusa
- Hashcat
- XSStrike
- PwnXSS
- Sqlmap
- Ghouri
- Dionaea
- Cowrie
- Snare&Tanner
- Office
- Teams

Interests

- GRC and Compliance
- Cybersecurity Community Engagement
- Cybersecurity Training and Education

Professional Development

SkillFront	ISO 9001 Quality Management Systems Associate™
Google	Foundations of Cybersecurity
CodeRed	Ethical Hacking Essentials
PFTP	Certified Ethical Hacker (CEH)
Huawei	Huawei Certified ICT Associate of Security
Skill Front	ISO/IEC 27001 Information Security Associate
arcX	Cyber Threat Intelligence 101
Cyber Triage	Intro to DFIR: The Divide and Conquer Process
(ISC)^2	Certified in Cybersecurity (in Progress)
Microsoft	Microsoft Security, Compliance, and Identity Fundamentals
LetsDefend	Phishing Email Analysis
OPSWAT	OPSWAT Email Security Associate
OPSWAT	OPSWAT Network Security Associate
OPSWAT	OPSWAT Web Traffic Protection Associate
OPSWAT	OPSWAT Endpoint Compliance Associate
LinkedIn	Microsoft Powerpoint
LinkedIn	Linux Assessment

Personal Projects

The following is a selection of my personal projects, which showcase my expertise in cybersecurity and computer science:

- Developed a comprehensive hands-on guidebook for cybersecurity enthusiasts and an autonomous emotion-based music recommender system.
- Built several cybersecurity tools, such as a machine learning-based phishing email detector, a tool for customized templates for phishing campaigns, an email header analyzer, and a web attack detector for identifying vulnerabilities like XSS, CMDI, LFI, and SQLI.
- Developed a smart auth system, integrated various SIEMs, IDSs, and firewalls, and built a robust sub-domains finder tool, an easy-to-use ARP spoofer, a Python-based web application enumeration tool, and a port scanner.

Publications

Published	5G Security Threats Affecting Digital Economy and Their Countermeasures
Published	The Internet of Medical Things (IOMT): Security Threats and Issues Affecting the Digital Economy Forecasting
Published	The Trends and Patterns of Crime In San Francisco Using Machine Learning Model
Accepted	Insider Threats in The Cybersecurity Landscape: A Call for Cultural Transformation

Academic Excellence

Distinction — Completed Master's Degree in Information Security with academic excellence, achieving a CGPA of 3.83 and securing the top position in the batch.

References

Pro. Dr. Munam Ali Shah — Associate Professor

Incharge Huawei Lab, COMSATS University Islamabad
Email: *mshah@comsats.edu.pk*

Pro. Dr. Farhana Jabeen Khan — Associate Professor

Incharge Cybersecurity Program, COMSATS University Islamabad
Email: *farhanakhan@comsats.edu.pk*