



RIPHAH
INTERNATIONAL UNIVERSITY



Prospectus

**RIPHAH INSTITUTE OF
SYSTEMS ENGINEERING**



Our Mission

“To create a center of excellence for Information Security and Data Sciences. Facilitate the market with the best talent in information security, Data Sciences and positively contribute to the academic, public and private sectors. Ingrain the spirit of national competitiveness and be a catalyst for change in the field of Information Security and Data Sciences”

Riphah Institute of Systems Engineering (RISE)

RISE is a special initiative by Riphah International University to impart quality in education, professional trainings & consultancy in the field of Information Security. With a unique construct this institute outshines all the other educational institutes as it is the first institute that has academia, R&D, training & consulting specializing in information security technology solutions and dedicated to providing information security professionals & delivering cost-effective services that span Information Security Management, Data Sciences for all industries.

Dr. Saad Naeem Zafar

(CISA, CISM, CRISC, CGEIT)

Professor, Riphah Institute of Systems Engineering



Dr. Saad Zafar is currently working as Research Professor, Riphah Institute of Systems Engineering, at Riphah International University (RIU), Islamabad, Pakistan. He has been affiliated with the field of Information Technology for more than twenty years. His area of specialization is Information Security.

At Riphah, he is leading a Secure and Dependable Systems research group. He has been teaching Information Security Management, Security Engineering and Application Security, both at the undergraduate and postgraduate level. He has been Director of Information Technology at Riphah International University and has provided Information Technology consultancy to a number of organizations. Dr. Zafar started his career working as a Software Engineer at Phoenix Technologies and Polysar Incorporated in the USA. Since then he has been involved in many projects related to software acquisition, development and implementation as software engineer, project manager and chief information officer.

He has received his PhD from Griffith University, Australia. His research is in the area of Information Security. He was affiliated with the Dependable Complex Computer-based System (DCCS) research group which was funded by the Australian Research Council. He was also associated with the Software Quality Institute and the Institute of Integrated and Intelligent Systems at Griffith University. He has received Masters in Software Engineering from Griffith University, Australia. He was awarded Academic Excellence Award for his educational performance at the Griffith University.

Khurram Javed

(CEI, CEH, ECSA, CHFI, LPT, CCAI)

Assistant Director, Riphah Institute of Systems Engineering

Cyber Security Consultant/Penetration Tester

Master Trainer, Cyber Security Training



Khurram Javed is currently serving as Assistant Director, RISE. He is a renowned Cyber Security professional leading the strategic development, planning, analysis and execution of diversified projects for clientele varying from defence, strategic, financial, multi-national and telecommunication/internet security related organizations across the globe. Khurram is also an acclaimed academician and has been attached with academia for over a decade and has served as permanent faculty in many prestigious universities in Pakistan. His areas of specialization are Social Engineering, Wireless and Offensive Security.

In addition to managerial responsibilities, he has been delivering as Cyber Security Consultant/Penetration Tester & Master Trainer, under the Professional Development Center at RISE. He is a prolific cyber security mentor and has trained over 1000 professionals from leading companies through numerous security training sessions conducted across Pakistan. He is a Certified EC-Council Instructor (CEI), Certified Ethical Hacker (CEH), Computer Hacking Forensics Investigator (CHFI), EC-Council Certified Security Analyst (ECSA) and a Licensed Penetration Tester (LPT) from EC-Council Academy, Kuala Lumpur, Malaysia and is enlisted amongst their Roll of Honor. His competence as a Security Analyst is well acknowledged by the industry through deliverance in training and consultancy projects. He leads the Penetration Testing and Digital Forensics teams at RISE. His other trainings include Cyber Security Assessment of Industrial control systems, International Innovative ICT Management in Artificial Intelligence & Big Data (Mayor's Scholarship, Government of China), Block Chain Technologies Cisco Certified Academy Instructor (CCAI), Virtualization Security, Network Analysis & Forensics, Panda Gate Defender Integra-Performa, VoIP design, installation & configuration, CCNA Discovery, FTTH technology and creating an effective CSOC.

Khurram is also an active researcher focusing in the areas of Wireless Security, Social Engineering, Malware Development & Analysis, BOTNETs, Offensive Security and Digital Forensics. He has also contributed towards architecting multiple flavors of Cyber Security Awareness training programs. Khurram is an enthusiastic speaker at Cyber Security conferences, symposiums and seminars and has professional memberships with EC-Council, IEEE, Cisco Network Academy, ISOC, CSTA-ACM and PISA.

Creating Knowledge Beyond Chronology

RISE Research

The objective of research initiatives is to educate future leaders which will enable them to unveil knowledge and generate fresh ideas. Our research groups work in liaison with varied international research consortiums. The key areas of research are:

Secure and Dependable Systems Research Group

This research group is led by Dr. Saad Naeem Zafar. Active research areas of this group are: Secure Software Engineering, Information Security Management, Information Security Policies, IT Governance.

Offensive Security Research Group:

This research group is led by Mr. Khurram Javed. Active Research areas of the group are: Wireless Security, Ethical Hacking, Social Engineering, Penetration Testing, Offensive Security, Digital Forensics, Malware Research, BOTNETS & Android exploitation framework.

Network Security Research Group:

The members of the Network Security Research Group (NSRG) are committed to design, analyze and implement the security services and mechanisms in order to achieve the following two primary objectives: i) to contribute towards enhancing the security of network infrastructure, security protocols, and network applications, ii) to contribute towards discouraging cyber-attacks through network forensics readiness and sophisticated attack detection schemes. Dr. Muhammad Yousaf leads the NSRG group. Following are the active research projects currently going on in the NSRG group: Network Traffic Analysis, Next Generation Firewalls, Intrusion Detection and Prevention Systems, Public Key Infrastructure based Smart Card Authentication Systems, Secure VoIP Infrastructures, Secure IoT Infrastructures, Secure Group Communication Systems, User Profiling Techniques, Privacy Preserving Techniques. www.facebook.com/groups/nsrgp



Health Data Analytics Research Group

The health data analytics research group at Riphah Institute of Systems Engineering (RISE) is actively engaged in cutting-edge research in the field of healthcare and data science. The recent explosion in health data coupled with the advances in the field of artificial intelligence has created tremendous opportunities for healthcare improvement. The group aims to provide a platform for collaborative multidisciplinary research in healthcare by providing support through expertise in large-scale data science techniques to researchers in the medical field. The group has a keen interest to address the global health challenges in the local context of Pakistan, as the healthcare indicators in the country are one of the lowest in the region. To this end, as one of the key initiatives, the research center is in the process of establishing a permanent source of data through our collaborative partners to collect, store and process health data to support research in the areas of: (i) diagnostics—data mining and analysis to identify causes of illness; (ii) prevent medicine – predictive analytics and data analysis of genetic, lifestyle, and social circumstances to prevent disease; (iii) precision medicine – leveraging aggregate data to drive hyper-personalized care; (iv) medical research – data-driven medical and pharmacological research to cure disease and discover new treatments and medicines; (v) reduction of adverse medication events – harnessing of big data to spot medication errors and flag potential adverse reactions (vi) cost reduction – identification of value that drives better patient outcomes for long-term savings; (vii) population health – monitor big data to identify disease trends and health strategies based on demographics, geography, and socio-economics.

International Research Grants

Strategic Support for Accreditation of Programs and Internationalization at South Asian Higher Education Institutes (HEIs)

Start: 15-01-2021 - End: 14-01-2024

Project Reference: 619438-EPP-1-2020-1-PK-EPPKA2-CBHE-JP

EU Grant: 876206 EUR

Programme: Erasmus+

Key Action: Cooperation for innovation and the exchange of good practices

Action Type: Capacity Building in higher education

Because of globalization, standardization leading to accreditation of academic programs has become an increasingly dominant theme in higher education. In order to achieve it, there are various challenges faced by Asian partner country Higher Education Institutions, which resulted in creating the motivation towards undertaking this project. The partner countries face the challenge of strong competition with international institutions because of the easy and wide access to higher education abroad. The institutions cannot delay any further to address it, otherwise they risk the severe issues of comparability of quality of education locally and abroad, and other issues relating to recognition of qualification. Moreover, the increased proportion of students entering university-level education has increased the complexity of higher education systems across the entire partner countries, thereby also giving rise to the need of standardization and accreditation. In spite of huge student population in Asia, unfortunately very few universities from Asia are seen in good positions in global world ranking of universities.



Map of project partner countries

Network Security Training and Workshops across Selected Women Universities in Pakistan

The employees and students in women's universities across Pakistan are girls. As Pakistan's government is planning to have more women universities in the country, there is a need to trained women to serve in newly established universities to ensure the security of networks of those universities. Moreover, there isn't any cybersecurity or network security program or department in women's universities in Pakistan.

Moreover, Women in Pakistan face isolation, and due to cultural and religious implications, they are

unable to go to big cities to get themselves trained on network and cybersecurity. There is a dire need to conduct hands-on training and workshops at their doorsteps and campuses.

RISE Secured a Grant amount of 76650/- Euros from European Commission through TEIN*CC via 4th Call of its Asi@connect programs. It consists of seven "five days hands-on network security training and workshops" for Pakistani women network engineers at their doorstep and place. Dr Syed Muhammad Sajjad was the Principal Investigator of the Project.

Asi@Connect 4th Call for Proposals Result - 16 Programmes

- 157 concept notes received
- Selected: 16 Programmes

Security Training for Women engineers	Linux System	Routing and Security management
Nuclear Medicine	OF@TEIN++	Federated Identity Roaming & E-Infrastructure
Platform for Agricultural Management	LandSAGE- Monitoring Natural Disaster	Agriculture for Disaster Risk Reduction
Real-Time Emission Mapping	Helping to bridge the digital divide in Pakistan and Bhutan	

Deployment of Collaborative Modern HoneyNet to improve Regional Cyber security Landscape (CMoHN)

Landscape (CMoHN)The project deployed and established the core skills required to manage and integrate different honeynets and designed new honeypots for countering cyber-attacks. The project connected with other honeynets in the

region to form a regional collaborative honeynet network, and promoted R&D activities to secure network infrastructure through publications and conducting community awareness seminars. Grant amount for this research project is AUD 30,000. Dr. Muhammad Yousaf was the principal investigator of the project.

isif asia GRANTS 2016

CATEGORIES

- APNIC Internet Operations Research Grants
- Internet Society Cybersecurity Grant
- Community Impact Grants
- Technical Innovation Grants

APPLICATIONS REVIEWED

300+

10 INITIATIVES SELECTED

Australia, India, Myanmar, New Zealand, Pakistan, Philippines, Singapore, Thailand and Tonga



National Research Grants

- Development of interactive online “cyber-security and privacy awareness training program for students”**
 “The proposed project helps to curtail the threats/vulnerabilities associated with cyberspace by developing and evaluating cyber-security awareness course for vulnerable segments of society (School and College/ University going Students)”. Grant amount for this research project is PKR 4.6 M. Dr. Saad Naeem Zafar is the principal investigator of the project.
- Establishment of Cyber Range using Open Source Technologies**
 Project funded by National Engineering and Scientific Commission (NESCOM), Directorate

of Research and Academic Coordination (RAC). Awarded to Principal Investigator Dr. Muhammad Yousaf, Riphah Institute of Systems Engineering, Riphah International University Islamabad. 2017 - 2019.

- Secure Sandbox Orchestration**
 Project funded by National Engineering and Scientific Commission (NESCOM), Directorate of Research and Academic Coordination (RAC). Awarded to Principal Investigator Dr. Muhammad Yousaf, Riphah Institute of Systems Engineering, Riphah International University Islamabad. 2019 to 2020 – Continue.

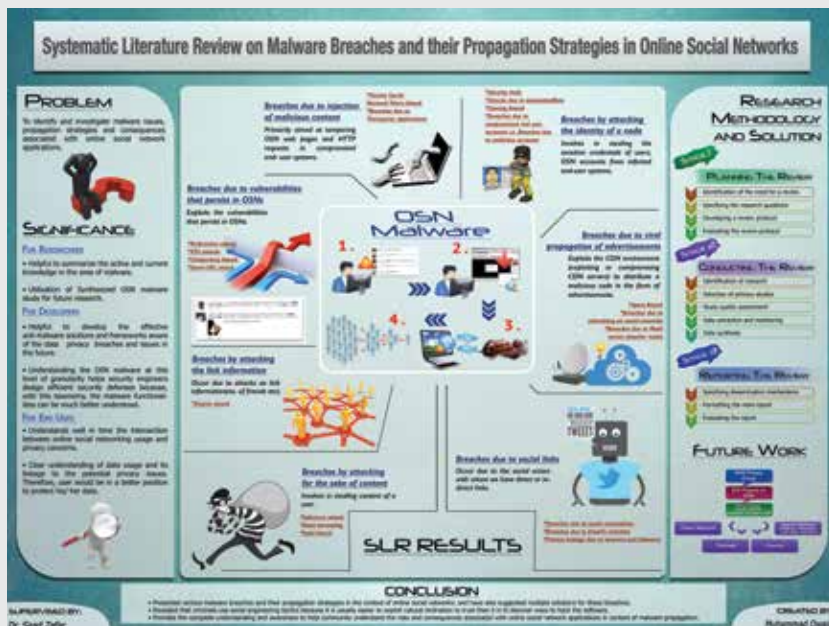
Industrial Projects

Ministry of Information Technology (IT) & Pakistan Software Export Board (PSEB) Government of Pakistan has granted a project titled “Free IT Training and Certification” to a joint venture of MetaPi Private limited and Riphah Institute of Systems Engineering (RISE) worth PKR. 270 Million for providing trainings and certifications to 1700 students, professionals, and government employees across all over Pakistan (2022) for the following professional certifications.

- Certified Ethical Hacking (CEH)
- Computer Hacking Forensics Investigation (CHFI)

- Microsoft Azure
- AWS Solutions Architect-Associate (SAA)
- AWS Solutions Architect-Professional (SAP)
- Cisco Certified Network Associate (CCNA)
- Certified Associate in Python Programming Certification (PCAP)

The project will be executed in two phases. In the first phase, 800 professionals are targeted to be trained. So far, team RISE has trained 700+ professionals in the following cities of Pakistan. Islamabad, Lahore, Peshawar, Quetta, and Karachi.



Exposing Android Vulnerabilities through Malicious Payload Binder

AndroBinder

Research Approach & Design

- Decompile Target**
 - Obtainable APKs from Android App Store
 - APK Extraction
 - Extract Common Resources of APK
 - Generate Smali code
 - Smali is bytecode equivalent of assembler
- Code Analysis**
 - APKs are analyzed for Malicious App
 - Analyze the smali code of both Apps
 - String resources for finding conflicts
 - Compare Smali of both apps
- Code Injection**
 - Describe the Execution Events and Permissions
 - Injection in application Context and injection in the form of Smali
- Agent Preparation**
 - APKs are analyzed for Malicious App
 - APKs are analyzed for Malicious App
 - APKs are analyzed for Malicious App
- Build APK**
 - Recompile the resultant code
 - Sign the APK for distribution
 - Publish the signed APK

Strengths

- Control & Control Server can:
 - get OS version and specs
 - read entire address book
 - get call history
 - get all the messages (SMS/IMES)
 - activate the device's microphone
 - activate the device's front/back camera
 - initiate outgoing video streams
 - visit any given URL
 - kill all the running processes

The Challenge

is to develop malicious app, that deploys itself on the target of Evaluation while keeping itself Stealthy and doesn't raise any flags of concern on the remote end.

Motivation:

Android is the most popular operating system being shipped now a days. Hence the development of a toolkit to generate vulnerability - explosive apps can be of mutual benefit for security agencies and for research community.

Android Packaging Flow

Future Works

- Research Publication (Journal)
- Patent Registration - IPO
- Development of Plug-ins
- Web based Command & Control server
- Customized Payload
- Reporting

Experimental results

showed that its possible by integration of different payloads with reverse engineered existing android applications, to exploit android vulnerabilities for remote administration.

Offence is the best Defense

It's a challenge for National Security Agencies to penetrate in Target's Territory

DESIGN AND IMPLEMENTATION OF A LIGHTWEIGHT PRIVACY EXTENSION OF DNSSEC PROTOCOL

INTRODUCTION

IETF RFC 7258, describes pervasive monitoring as a technical attack on the Internet user's privacy that should be mitigated in all networking protocols.

- Domain Name System (DNS) has always been a soft target for the attackers.
- RFC 8333 describes the threat analysis of the Domain Name System.
- In order to mitigate these threats, DNS Security Extensions were proposed in RFC 4033, 4034, 4035. These security extensions provide the integrity and origin authentication services to the DNS.
- But, these extensions largely ignored the confidentiality service for the DNS request/response messages.

OBJECTIVE

The primary objective of this research work is to provide a lightweight privacy extension of DNS. Privacy regarding DNS messages can be considered from the two perspectives.

- One is the user privacy.
- And the other is the network privacy.

Moreover, the solution proposed in this research work incorporates built-in security mechanism in the DNS messages thus avoiding its dependence on the heavyweight TLS and DTLS.

METHODOLOGY

PROPOSED DNS HEADER

The proposed header is the modification of current DNS protocol header in such a way that the modified header shouldn't violate the principle functionality of DNS protocol.

RESULTS

This solution used an independent widely used tool 'Wireshark' for capturing and analyzing DNS traffic. The results are calculated for two different aspects of DNS Server behavior.

- Cache response
- Iterative recursive response

Encrypted vs Plaintext DNS Message Exchange

Encrypted vs Plaintext DNS Message Exchange cache reply

EXPERIMENTATION TESTBED SETUP

- The most common and widely used DNS Name Server open source software solution is Berkeley Internet Name Domain (BIND).
- In this experimentation BIND is deployed and configured on the server side.

ACTUAL TESTBED DEPLOYMENT

The actual experimentation Testbed setup is composed of two DNS machines configured with Ubuntu operating system. Both of these DNS VMs are termed as Server VM and Client VM.

DISCUSSION

The primary objective of this research work is to provide a lightweight privacy extension of DNS. Privacy regarding DNS messages can be considered from the two perspectives. One is the user privacy. And the other is the network privacy. Moreover, the solution proposed in this research work incorporates built-in security mechanism in the DNS messages thus avoiding its dependence on the heavyweight TLS and DTLS.

Each of these results is observed in the experimental results of the proposed solution DNS server. Further, arrival of these results only one goal remain in the user's interest to avoid any intruder's attempt to intercept it with the malicious intention. This is why the implementation presented is always higher results than the other compared more than 1 second.

SUMMARY

In this research study, the discussion is made regarding the threat to end-user privacy proposed by an attacker through Pervasive Monitoring DNS. Currently, there is no solution exists to be developed to detect the PMA's and thus in this research work a lightweight solution is presented.

The performance of the proposed solution is measured by analyzing the results in both web server query resolution mechanisms which are of Recursive and of Cache response.

The traffic during this analysis is captured by the use of an independent well-known tool Wireshark. Results indicate that in the privacy of query resolution when iterative resolutions are involved can lead to time consumption of almost double in its same cases to be with respect to a Cache response process.

As once the destination for a particular domain is performed by the DNS server, the rest of the query resolution process the same will remain at the intermediate level until the TTL of an answer resource record is not expired.

The domain 'google.com' for the first time may take approximately 1.5 seconds, but later on if queried more 1000 times, it will respond in the later response with approximately half or less than a half seconds. Thus the occurrence of a second reply can be acquired in 1.0000 ms.

Programs Offered

MS Information Security (MSIS)

The program aims to develop core competencies in various areas of information security like information security management, application security, computer networks security, and digital forensics. Students will have the opportunity of learning the technical aspects of information security by understanding current threats and vulnerabilities and examining ways of developing effective countermeasures. In order to cater for wide range of professional and academic interests, students have the option of selecting their course work according to their specific needs. Currently, RISE is offering three degree programs that are: i) MS (Information Security), ii) MS (Data Science), and iii) Ph.D. Computing with area of specialization as Information Security and Data Science.

Duration 4 Semesters (2 Years)

Eligibility

- 16-years of education in science/engineering discipline preferably with 4 years degree program of BS (SE/CS/IT/EE) or equivalent from HEC recognized university or degree awarding institute with at least 60% marks or CGPA of at least 2.0 (on a scale of 4.0). (NOTE: candidates may have to complete the deficiency coursework as determined by the admissions committee).
- Two years of relevant work experience is recommended.

Admission Criteria

- Qualify GRE General type admission test conducted by the university or a valid NTS GRE General test
- Qualify the admission interview.
- Admission will depend to the candidate's overall score in previous academic degree, admission test and performance in the interview.

Intake: Spring (January) & Fall (July)

Class Timings:

05:30 pm – 08:30 pm (Monday – Friday)

Scholarships: Talent & need based scholarship (upto 100% on tuition fee)

List of Core Courses

Code	Course Name	Cr. Hrs
IS-5063	Cryptography	3
IS-5073	Information Privacy and Security	3

University Mandatory Courses

Code	Course Name	Cr. Hrs
CM-5011	Ethics in Practice-2	2

Some Elective Courses

Code	Course Name	Cr. Hrs
IS-6013	Information Systems Auditing	3
IS-6023	Risk Management	3
IS-6033	Information Security Management	3
IS-6043	IT Governance	3
IS-6063	Strategic Management, Leadership & Governance	3
IS-5023	Network Security	3
IS-6233	Wireless Networks Security	3
IS-6203	Ethical Hacking	3
IS-6213	Penetration Testing	3
IS-6253	Distributed and Cloud Computing	3
IS-6283	Security of Internet of Things	3
IS-5053	Application Security	3
IS-6403	Secure Software Development	3
IS-6433	Malware Analysis	3
IS-6443	Programming for Security Professionals	3
IS-6453	Machine Learning for Security Applications	3
IS-6463	Database Security	3
IS-6473	Security Testing	3
IS-6483	Trusted Computing	3
IS-6633	Applied Cryptography	3
IS-6663	Digital Forensics	3
IS-6703	Data Analysis and Quantitative Techniques	3
IS-6723	Ethics in Information Security	3
IS-6803	Advanced Topics in Applied Cryptography	3
IS-6813	Quantum Computing & Information Security	3
IS-6823	Quantum Cryptography	3
IS-5433	Research Methods	3

Degree Completion

For award of MS degree, a student must have:

- a. Passed courses totaling at least 32 credit hours, including two core courses.
- b. Obtained a CGPA of 2.5 or more.

MS Data Science (MSDS)

Data science is an interdisciplinary field of scientific methods, processes and systems for understanding the modern-age data sources, modelling the data behavior, extracting the business insight from that data, predicting the future behavior and delivering the useful data-driven business applications.

In 2013, IBM estimated that two and a half million terabytes of data are created every day. Some of the sources, generating the data are:

- a) Individuals (through social networks and smartphones for the reflection of society)
- b) Machines (through real-time, network connected sensors – “the internet of things”)
- c) Business and commerce (e.g. transaction records and financial data)
- d) Education (e.g. academics, literature, research)
- e) Medical / Healthcare (personal health records, health insurance)
- f) Justice (crime statistics for a city for the sake of efficient resource deployment)
- g) Transportation (Vehicle, pedestrians, trains, airlines, movement data)

The challenge is to make sense of this ever-increasing source of data for the use and benefit of society. A lot many companies and higher education institutions are already planning and implementing for this data tsunami. Data science has emerged as an interdisciplinary paradigm that draws upon the traditionally distinct areas of computer science, applied mathematics and statistics, applications from natural and social science, engineering, and business for developing solutions for gathering, cleaning, archiving, analyzing and visualizing data for the purposes of making informed decisions.

The Master of Science in Data Science (MS-DS) program aims to develop core competencies in various areas of data science like understanding data products, data extraction, data cleaning, data modeling, classification, clustering, predictions, etc. Students will have the opportunity of learning the technical aspects of data science by understanding the trends in the current data products and preparing for the required data analysis skillset for the upcoming information processing systems. To cater for wide range of professional and academic interests, students have the option of selecting their course work according to their specific needs. Riphah Institute of Systems Engineering (RISE) is currently offering MS (Information Security) program and the proposed MS (Data Science)

program is expected to not only complement the existing program but also it will open new opportunities for coping with the challenges of the near future.

Duration: 4 Semesters (2 Years)

Eligibility

- 16-years of education in computing/science/engineering discipline preferably with 4 years degree program of BS (Computer Science, Software Engineering, Information Technology, Applied Mathematics, Mathematics, Statistics, Computer Engineering, and Electrical Engineering) or equivalent from HEC recognized university or degree awarding institute.
- At least CGPA of 2.0 on the scale of 4.0 or 60% marks in the previous degree.
- Two years of relevant work experience is recommended.
- Candidates may have to complete the deficiency coursework as determined by the admissions committee. List of deficiency courses is:
 1. Programming Fundamentals
 2. Data Structures and Algorithms / Design and Analysis of Algorithms
 3. Database Systems

Admission Criteria

- Qualify GRE General type admission test conducted by the university or a valid NTS GRE General test.
- Qualify the admission interview.
- Admission will depend on the candidate's overall score in previous academic degree, admission test and performance in the interview.

Intake: Spring (January) & Fall (July)

Class Timings

05:30pm – 08:30pm (Monday – Friday)

Scholarships

Talent & need based scholarship (upto 100% on tuition fee)

List of Core Courses

Code	Course Name	Cr. Hrs
DS-5013	Statistical and Mathematical Methods for Data Science	3
DS-5023	Tools and Techniques in Data Science	3
DS-5033	Machine Learning	3

University Mandatory Courses

Code	Course Name	Cr. Hrs
CM-5011	Ethics in Practice-2	2

List of Specialization Courses

Choose any two from the following specialization courses of data science.

Code	Course Name	Cr. Hrs
DS-5513	Big Data Analytics	3
DS-5523	Deep Learning	3
DS-5533	Natural Language Processing	3
DS-5543	Distributed Data Processing	3

Some Elective Courses

Code	Course Name	Cr. Hrs
DS-6113	Data Classification	3
DS-6123	Data Clustering	3
DS-6133	Predictive Analytics	3
DS-6143	Data Visualization	3
DS-6153	Advanced Database Systems	3
DS-6163	Advanced Data Structures	3
DS-6173	High Performance Computing	3
DS-6213	Data ware Housing	3

Code	Course Name	Cr. Hrs
DS-6223	Cloud Computing	3
DS-6233	Datacenter Design	3
DS-6313	Data Mining	3
DS-6323	Distributed Machine Learning	3
DS-6333	Time Series Analysis and Prediction	3
DS-6343	Social Network Analysis	3
DS-6353	Applied Text Analysis	3
DS-6363	Modelling and Reasoning in Bayesian Networks	3
IS-5043	Information Systems Security	3
IS-6013	Information Systems Auditing	3
DS-6433	Data Analytics for Security Applications	3
DS-6513	Health Data Analytics	3
DS-6613	Data Privacy Laws and Regulations	3
DS-6623	Ethics for Data Scientists	3
DS-6633	Optimization Methods in Data Science	3
IS-5433	Research Methods	3

Degree Completion

For award of MS degree, a student must have:

- Passed courses totaling at least 32 credit hours, including three core courses and two specialization courses.
- Obtained a CGPA of 2.5 or more.

Graduate Diploma

The Graduate Diploma program has been designed to offer a higher degree of flexibility, especially for the professionals, in order to meet their targeted learning requirements in constrained time limits. Additionally, the students successfully completing the Graduate Diploma will have the opportunity to upgrade their earned diploma into MS program. The knowledge areas include Information Security, Data Science, Software Engineering, and Computer Science.

Eligibility Criteria

16-years of education in Computer Science or Software Engineering or any other 16-years degree in computing discipline preferably with 4 years degree program of BS (Computer Science or Software Engineering) or equivalent from HEC recognized university or degree awarding institute.

1. At least CGPA of 2.0 on the scale of 4.0 or 60 % marks in the previous degree.
2. An industrial experience of two years is recommended.

Requirements for the Award of Graduate Diploma

After successful completion of 5 courses each of 3 credit hours, the student can claim his/her diploma. Duration of diploma is 1 year or maximum 2 years.

Conversion Options

The students completing the graduate certificate and graduate diploma will have the following conversion options.

1. A student who enrolled and successfully completed graduate diploma will have the right to enroll in the MS program later on such that the earned credit hours in diploma will be

counted towards relevant MS program under the rules, outlined by university.

2. A student who enrolled in MS program and partially completed the coursework requirements and is not willing to continue, will have option to get certificate(s) or graduate diploma depending upon the successfully completed credit hours. One successfully completed course will equate one graduate certificate while five successfully completed courses will be equivalent to graduate diploma.
3. A student who enrolled in graduate diploma and is not willing to continue, will have the right to get graduate certificates equal to the successfully completed courses.

Intake and Class Timings

It will be one semester long i.e. Spring (February-June) or Fall (August - January) Evening Classes, Monday to Friday, 05:30 PM to 08:30 PM.

Titles to Offer

Broadly, any candidate who fulfils the admission criteria can enroll for graduate diploma and can study any course, offered at the graduate level in the department of software engineering & computer science or the department of cyber security and data science. Specifically, the department(s) can offer specialized graduate certificate(s) / graduate diploma(s) according to the requirements of a group of professionals. For more information about the specific titles to be offered please refer to list of courses provided in MS programs.

Graduate Certificate

The Graduate Certificate program has been designed to offer a higher degree of flexibility, especially for the professionals, in order to meet their targeted learning requirements in constrained time limits. Additionally, the students successfully completing the Graduate Certificate will have the opportunity to upgrade their earned certificate into diploma and MS program. The knowledge areas include Information Security, Data Science, Software Engineering, and Computer Science.

Eligibility Criteria

16-years of education in Computer Science or Software Engineering or any other 16-years degree in computing discipline preferably with 4 years degree program of BS (Computer Science or Software Engineering) or equivalent from HEC recognized university or degree awarding institute.

1. At least CGPA of 2.0 on the scale of 4.0 or 60 % marks in the previous degree.
2. An industrial experience of two years is recommended.

Requirements for the Award of Certificate

After successful completion of 3 credit hours course work the student can claim his/her certificate. Duration of certificate is 18 weeks.

Conversion Options

The students completing the graduate certificate and graduate diploma will have the following conversion options.

1. A student who enrolled and successfully completed graduate certificate will have

the right to enroll in diploma and in the MS program later on such that the earned credit hours in certificate will be counted towards relevant diploma/MS program under the rules, outlined by university.

2. A student who enrolled in MS program and partially completed the coursework requirements and is not willing to continue, will have option to get certificate(s) or graduate diploma depending upon the successfully completed credit hours. One successfully completed course will equate one graduate certificate while five successfully completed courses will be equivalent to graduate diploma.
3. A student who enrolled in graduate diploma and is not willing to continue, will have the right to get graduate certificates equal to the successfully completed courses.

Intake and Class Timing

It will be one semester long i.e. Spring (February-June) or Fall (August - January) Evening Classes, Monday to Friday, 05:30 PM to 08:30 PM.

Titles to Offer

Broadly, any candidate who fulfils the admission criteria can enroll for graduate certificate and can study any course, offered at the graduate level in the department of software engineering & computer science or the department of cyber security and data science. Specifically, the department(s) can offer specialized graduate certificate(s) / graduate diploma(s) according to the requirements of a group of professionals. For more information about the specific titles to be offered please refer to list of courses provided in MS programs.

PhD Computing

Students enrolled in the PhD Computing program are required to complete minimum 48 credit hours of course/research work. Students are required to take minimum 18 credit hours (typically 6 courses) as part of their course work. Objective of these 6 courses is to cover the breadth as well as depth of the knowledge of their interest area. At the completion of these 6 courses, students are expected to cover the issues, best practices, standards, research gaps and challenges of their interest area. On the completion of the course work, students are required to pass the comprehensive / doctoral qualifying exam as well.

Furthermore, students are required to take minimum of 30 credit hours as part of their research work. During this phase, students initially are required to defend their PhD synopsis / proposal defense. Students are required to publish their research work in ISI indexed impact factor journals. Minimum of 1 ISI indexed impact factor journal paper and 2 conference papers in high quality international research conferences are required as part of the PhD degree program. However, this number can be increased by the concerned research supervisor. Later on, student is required to defend his/her PhD pre-final defense. Student's research thesis is also evaluated by 2 foreign experts from technologically developed countries. Finally, student is required to defend his/her PhD final public defense.

Generally, students complete their PhD degree requirements in 4 years. However, in some rare cases this duration can last up to maximum 8 years. Students failing to complete their PhD degree requirements in 8 years will be disqualified.

Eligibility Criteria

- 18 years of education in science / engineering discipline preferably with MS/MPhil (IS/SE/CS/IT/EE) or equivalent from HEC recognized university or degree awarding institute.

(NOTE: candidates may have to complete the deficiency coursework as determined by the admissions committee.)

- CGPA of 3.0/4.0 or above in MS/MPhil degree.
- Two years of relevant work experience is recommended.

Admission Criteria:

- A valid GAT (Subject) type score of minimum 70% is required
- Interview

Intake: Spring & Fall (Twice a year)

Timings: Evening Classes

Duration: 3 to 8 years

Active Research Areas:

- Cyber Security Management
- Malware Analysis
- Security Assessment
- Digital Forensics
- Network Security
- Machine Learning
- Natural Language Processing
- Data Governance

Program Compliance and Accreditation

PhD program is structured to meet the requirements of Higher Education Commission (HEC), Pakistan. The programs are offered by Riphah International University, which is a Federally Chartered University based in Islamabad, Pakistan. Programs are approved by the relevant university authorities.

Courses Details	Cr. Hrs
University Mandatory Course (Ethics in Practice II)	02
Elective Courses	18
Research Credit Hours	30
Total Ph.D Credit Hours	50

Trainings

RISE provides following world recognised certifications and trainings



CEH provides a comprehensive ethical hacking and network security hands-on training program to meet the standards of highly skilled security professionals. Hundreds of SMEs and authors have contributed towards the content presented in the CEH courseware. Our researchers have invested thousands of man hours researching the latest trends and uncovering the covert techniques used by the underground community.



Computer forensics include the application of computer investigation and analysis techniques in the interests of determining potential legal evidence. CHFI enables trainees to acquire necessary hands-on experience on various forensic investigation techniques and standard forensic tools necessary to successfully carry out a computer forensic investigation leading to prosecution of perpetrators.



Computer forensics include the application of computer investigation and analysis techniques in the interests of determining potential legal evidence. CHFI enables trainees to acquire necessary hands-on experience on various forensic investigation techniques and standard forensic tools necessary to successfully carry out a computer forensic investigation leading to prosecution of perpetrators.



CISMs understand the business. Its assists to know how to manage and adapt technology to the enterprise and industry. The uniquely management - focused CISM certification promotes international security practices and recognizes the individual who manages designs, and oversees and assesses an enterprise's Information Security.



This course is designed to prepare the participants for the CISA examination. It covers the unique aspects of managing an audit and the knowledge necessary to complete the task. The course focuses on the design and implementation of general computer control, application level control auditing as well as introducing the risk based management approach. While disseminating information about Information Systems auditing standards, this course enables the trainee to perform Information System audits.

CISSP

The Certified Information Systems Security Professional (CISSP) is the most globally recognized certification in the information security market. CISSP validates an information security professional's deep technical and managerial knowledge and experience to effectively design, engineer, and manage the overall security posture of an organization.

The broad spectrum of topics included in the CISSP Common Body of Knowledge (CBK®) ensure its relevance across all disciplines in the field of information security. Successful candidates are competent in the following eight domains:

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management (IAM)
- Security Assessment and Testing
- Security Operations
- Software Development Security

PCAP

This intermediate Certified Associate in Python Programming training prepares learners to take the PCAP exam, which is the one exam required to earn the PCAP certification.

Python is one of the simplest, most accessible programming languages around today, and it's hard to imagine a developer who won't benefit from knowing it. Python always seems to show up everywhere.

Developers who work with data scientists and researchers rely on the hundreds of scientific libraries to extend Python for their work. Developers working with tech startups love Python's ease of use and scalability -- perfect for building simple solutions that you know can explode when the company does.

AZURE

Designing and Implementing a Data Science Solution on Azure offers a set of related services to address the day-to-day workflow of a data scientist. This skill teaches how these Azure services work together to enable various parts of this workflow. This path is designed to address the Microsoft DP-100 certification exam. After completing this course, students will be able to understand and build AI solutions on Azure, learn about various Azure Machine Learning services usage & integration, and understand the profound impacts Machine Learning is making in smart business decisions.

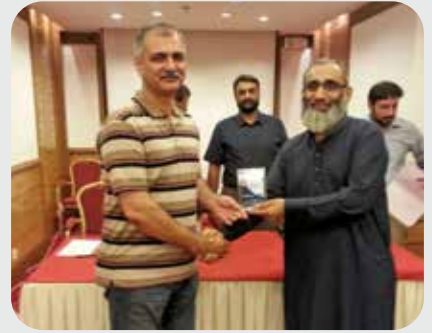
TEAM MEMBERS

Names	Designation
Dr. Muhammad Yousaf PhD Computer Engineering (CASE) MS Computer Engineering (CASE) CISSP Member (ISC) ² Founding Member ISOC Islamabad Chapter Leader: Network Security Research Group (NSRG) muhammad.yousaf@riphah.edu.pk	Director RISE
Dr. Muhammad Zubair Ph.D. Electrical Engineering (IIUI), MS Information Technology (Hamdard University) muhammad.zubair@riphah.edu.pk	Dean Faculty of Computing
Dr. Saad Naeem Zafar Ph.D – Software Engineering (Australia), MS – Software Engineering (Australia), CISA, CISM, CRISC, Member IEEE, ISACA saad.zafar@riphah.edu.pk	Research Professor
Dr. Naveed Ikram PhD - Computer Science (University of Salford, UK) M.Sc - Computer Science (University of Salford, UK) Chartered IT Professional, Senior Member ACM, Member IEEE, AIS, CSP Leader: Empirical Software Engineering Research Group naveed.ikram@riphah.edu.pk	Professor, Associate Dean, Graduate Program
Dr. Musharif Ahmed Ph.D. - Computing (Riphah International University) MS - Systems and Software Engineering (MAJU), musharif.ahmed@riphah.edu.pk	Assistant Professor HoD, Software Engineering & Computer Science
Dr. Adeel Zafar Ph.D. - Computing Science (NU-Fast, Islamabad) MS - Computing Science (NU-Fast, Islamabad) BS - Software Engineering (Riphah International University)	Assistant Professor In-Charge DS Program
Dr. Syed Muhammad Sajjad PhD Computing (Riphah International University) MS Electrical Engineering (Networks Engineering) BSc Electrical Engineering (Electronics) (FUUAST, Islamabad) muhammad.sajjad@riphah.edu.pk	Assistant Professor
Mr. Khurram Javed PhD Scholar - Wireless Security (UTM, Malaysia) MS - Computer Networks (IIUI, Islamabad) Certified EC-Council Instructor (CEI), Certified Ethical Hacker (CEH) Certified Hacking Forensics Investigator (CHFI) EC-Council Certified Security Analyst (ECSA) Licensed Penetration Tester (LPT), Virtualization Security Network Analysis & Forensics, CCAI & CCNA 4.0 discovery Leader: Offensive Security Research Group khurram.javed@riphah.edu.pk	Assistant Director RISE Assistant Professor, Head Commercialization & Trainings Cyber Security Consultant/ Analyst, Master Trainer Cyber Security
Mr. Obaid ur Rehman Certified Ethical Hacker (CEH) Trained for: ISMS 27001 Lead Auditor Computer Hacking Forensic Investigator (CHFI) CSOC - SIEM Installation, Configuration and Administration CCNA, VMWare 3.5 ESX, ITIL v3 Foundation PANDA Gate Defender Performa V3.02 & Panda Security for Business PANDA Gate Defender Integration obaid.rehman@riphah.edu.pk	Manager Security & Compliance
Ms. Komal Batool PhD Computing (Riphah International University) (In Progress), MS-Information Security (Military College of Signal, (NUST) CHFI (Certified Hacker Forensic Investigator), CASE (Certified Application Security Engineer) komal.batool@riphah.edu.pk	Senior Lecturer

Names	Designation
Mr. Mirza Muhammad Touseef PhD Computing (In Progress)(Riphah International University) MS – Software Engineering (Riphah International University) mirza.touseef@riphah.edu.pk	Senior Lecturer
Mr. Obaid Ullah MS - Information Security (Riphah International University) BS - Computer Science (Sarhad University, Peshawar) CHFI (Computer Hacking Forensics Investigator) Trainer CEH (Certified Ethical Hacker) Trainer CSFPC (Cyber Security Foundation Professional Certificate) ISO/IEC 27001 Information Security Associate, CNSS Certified Network Security Specialist, CISCO Cisco Certified Network Associate obaid.ullah@riphah.edu.pk	Research Associate
Shehab Abdo Ali MS - Information Security (Riphah International University) BS - Computer Science Hons. (Preston University) CEI - (Certified Ec-Council Instructor) CHFI - (Computer Hacking Forensics Investigator) CEH - (Certified Ethical Hacker) Master, Practical CSFPC - (Cyber Security Foundation Professional Certificate) ICSI - Certified network security specialist shehab.abdoali@riphah.edu.pk	Teaching Fellow
Mr. Arslan Ali Khan MS - Information Security (Riphah International University) BS - Telecom Engineering (National University of Computer & Emerging Sciences) arslan.ali@riphah.edu.pk	Teaching Fellow
Ms. Kinza Naseer MS – Software Engineering (Riphah International University) kinza.naseer@riphah.edu.pk	Teaching Fellow
Ms. Afia Ishaq MS – Data Sciences (Riphah International University) (In Progress) BS – Software Engineering (Riphah International University) afia.ishaq@riphah.edu.pk	Teaching Fellow
Mr. Furqan Amjad MS – Data Sciences (Riphah International University) BS - Electronics and Electrical Systems (Power) University of Lahore Data Visualization with Python, IBM, Data Analysis with Python, IBM Pytohon 101 for Data Science, IBM, Data Science & Matchine Learning, DICE Analytics furqan.amjad@riphah.edu.pk	Teaching Fellow
Mr. Irfan Ahmad MBA - Finance (International Islamic University, Islamabad) irfan.ahmad@riphah.edu.pk	Program Coordinator
Mr. Aslam Malik B.Com (Allama Iqbal Open University, Islamabad) aslam.malik@riphah.edu.pk	Assistant Program Coordinator
Mr. Ahsan Ilyas MBA - HRM (Arid Agriculture University, Rawalpindi (PMP) ahsan.ilyas@riphah.edu.pk	Assistant Manager Administration
Mr. Nadeem Ahmed MBA, Hamdard University, Islamabad nadeem.awan@riphah.edu.pk	Finance Officer

Corporate Training Sessions





Testimonials

I and my colleagues participated in the training of CEHv8 and we found Mr. Khurram Javed as instructor of CEHv8 is not only instructor but true mentor for security professional. Moreover, he turned computer scientist into cyber security professional. RISE as institute provide us state of the art resources for CEHv8 training. I recommend computer & IT professionals to attend CEHv8 at RISE and see yourself a new world of wonder.

M. Shakil (NESCOM).

In modern era of information, its security at all the levels individual, organizational, national; now it has become a very need of the time. Training was up to the mark and RISE really is contributing at all the mentioned levels to induce security expertise to cope with up-coming threats.

M. Sohail Iqbal (NESCOM).

Training comprises of many good workshops, topics, labs, tutorials and all above conducted by very learned Mr. Khurram Javed. Instructor is a very professional and instrumental in his field and tried his level best to impart training to the participant. His support Mr. Ahmed is also well trained, experienced and having required knowledge to conduct such trainings and maintain lab environment.

Muzammel Hussain (Pak Navy).

The CEH training helped me boost my confidence towards my aim of CEH Exam. The trainer was very proficient and kept a healthy environment. CEH training gave a set of direction towards exam preparation and moreover provided a clearer range and concepts, roadmap, and strategy to the skills at hand.

Noushin Ahson (Systems Ltd).

Mr. Khurram teaching skills is excellent. I have been through many trainings but the friendly way with practical and live examples he trained us it's fabulous. I am very happy to being a student of him. The course material is really good and the moreover the way he delivers it made us to take interest. In last I wish him best of luck to Mr. Khurram Javed and RIPHAAH International University.

Sohaib Naqi (Kaspersky).

The training met our expectations, especially in form of course contents, material provided and most important trainer knowledge and the way of knowledge sharing. Labs and related material was

excellent, discussions were often open and based on knowledge sharing. I hope provided material/source information (dumps etc) will help us to get certified. From improvement perspective, if facilities provided at training campus are taken care, it will further facilitate participants to focus on learning.

Muhammad Qaiser Iqbal (Ufone).

The CEH training by Khurram was one of the best training I have received in my life. These 5 days contained a wealth of knowledge related to technical hacking, offensive and of course, defensive reason. The training not only broadened my vision on digital security but also opened horizon of various land of security measures that should have been undertaken by me, but were ignored due to lack of knowledge.

It is usually said that 'ignorance of bliss' but not in this case. Khurram Javed for alleviating our sense of security and opening our eyes to the dark that security instant until you is not connected to the internet.

Mustafa Shiraz Ahmed (SBP).

This was an excellent experience for me. The training has been provided by skilled trainer i.e. Mr. Khurram Javed. He shared his professional experiences & provided a real time insight into practical scenarios.

I absolutely enjoyed all parts of training setup including the meals & interaction with other participants. I hope to apply all the knowledge gained & improve my skills on top of the kick start and platform that this training has provided.

I will definitely recommend this to my colleagues. Thank you Mr. Khurram, Mr. Ahmad & Riphah for this wonderful experience.

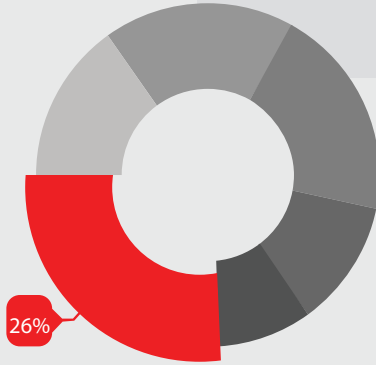
Waqas Arshed (Systems Ltd).

The training was very good. It does not only improved my knowledge but also enhanced my vision by looking at things from different perspective. The lab content was excellent and tools and material which was provided are also sufficient for self-training and exam preparation. The training arrangement, including equipment and environment were excellent as well. Khurram is very knowledgeable and have complete grip and command over the topic. Ahmed was very helpful and humble and was always there to help us.

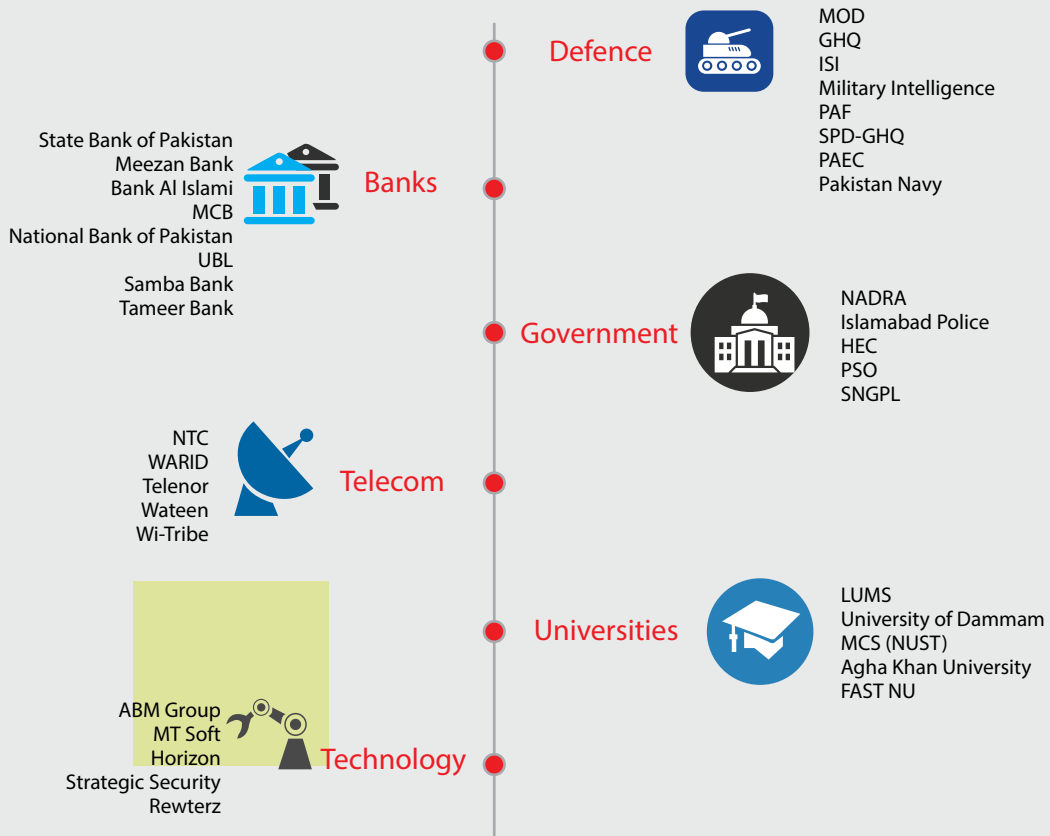
Syed Jaffer Zaidi.

Clientele

Our clientele is from different sectors of Pakistan including Defense, government, telecom, banks and IT industry. Almost 26 % of participation is from the defense sector. Higher level defense and governmental officials have participated in our training programs.
























■ Banks (15%) ■ Government (18%) ■ IT Industry (20%) ■ Telecom (12%)
 ■ Other (9%) ■ Defence (26%)



So far we have trained numerous personnel form different sectors like Defence, IT Companies, Banking, Education, Energy Sector etc.

				
Ministry of Defense	GHQ (Armed Forces)	Inter Services Intelligence	Military Intelligence	SPD-GHQ
				
Air Weapon Complex	NDC/NESCOM	Pakistan Air Force	MCS-NUST	State Bank of Pakistan
				
NADRA	Pakistan Atomic Energy Commission	National Telecom	Kaspersky Lab (U.A.E)	Ufone Telecom
				
Ernst and Young	Meezan Bank	PARCO	Bank Al-Islami	Islamabad Police
				
Warid Telecom	Telenor Telecom	Wateen	Muslim Commercial Bank	Higher Education Commission
				
NIFT	PERN	Suparco	LUMS	University of Dammam (Saudi Arabia)
				
Wi-Tribe	CureIT	A.F. Ferguson	KPMG (U.K)	GulfCap Investment (U.A.E)
				
Systems Limited	Pakistan Navy	Nakheel (U.A.E)	Pakistan State Oil	National Bank of Pakistan

				
United Bank Limited	Samba Bank	Tameer Bank	Agha Khan University	SNGPL
				
Central Depository Company of Pakistan	NRTC	Rewterz	CMA CGM Systems (U.A.E)	NLC
				
NCCPL	National Foods Limited	Horizon Technologies	TRG	FAST-NU
				
Toyota-Indus Motors	Strategic Security	FireEye	NetSoft	I2c inc
				
Junaid Jamshed	ABM Group	Tullo	Axvoice	Bata
				
PNEC	Muller and Phipps	Aptech	Dawn Media Group	Dubai Immigration
				
CASE	Kualitatem	Coeus	Infini Logic	Deltasoft
				
Fariya Network	GIZ International	GulfCap Investments	ISRA University	IP 360
				
Infogistic	Institute of Chartered Accountants of Pakistan	Institute of Space and Technology	Risk Associated	LMKR

				
Pacific Delta Shipping	NIB Bank	Sui Northern Gas Pipelines Limited SNGPL	Sonari Bank	Sita Aero
				
Nest Bridge	Siemens	Server4sale	Lucky Cement	Tanchulas
				
CUST	voizar	NCCPL	PTCL	KFUEIT
				
A.F. Ferguson & Co	BTMU	Agar International (Pvt.) Limited	Fatima Group	Air-University
				
Haniya Technologies	Askari Bank	FFC	SELA-PASS	CTD

ISLAMABAD / RAWALPINDI

Al-Mizan Campus:

Al-Mizan IIMCT Complex,
274-Peshawar Road, Rawalpindi.

UAN: +92 (51) 111-510-510

Phone: +92 (51) 512 5162-7

I-14 Campus:

Sector I-14, Haji Camp, Islamabad.

Phone: +92 (51) 844 6000-7

UAN: +92 (51) -111-747-424

G-7 Campus:

RIU, 7th Avenue, G-7/4, Islamabad.

Phone: +92 (51) 289 1835-8

Fax: +92 (51) 289 0690

Gulberg Green Campus:

Plot No PB-02 Gulberg Expressway,
Gulberg Green (IBECHS), Islamabad

Phone: +92 (51) 5912890-5

ETB Campus:

Suite No 7, Ground Floor, Evacuee
Trust Complex, Agha Khan Road,
Sector F-5/1, Islamabad.

Phone: +92 (51) 843 8370-7

Westridge Campus:

Potohar Plaza, main Peshawar Road,
Rawalpindi.

Phone: +92 (51) 5166 813-4, 5166 917-8

IIMCT Pakistan Railway Hospital:

Westridge, Rawalpindi.

Phone: +92 (51) 425 9795-8

Fax: +92 (51) 425 9793

Riphah International Hospital:

Main Expressway opposite DHA II,
Sihala, Islamabad.

Phone: +92 (51) 448 6064

Islamic International Dental Hospital:

IIDH, 7th Avenue, G-7/4, Islamabad.

Phone: +92 (51) 289 1835-8

Fax: +92 (51) 289 0690

MaxHealth Hospital:

2-K Markaz Road, G-8 Markaz,
Islamabad

Phone: +92 (51) 8094760-65

LAHORE

Raiwind Campus:

Raiwind Road Campus,
13-Km, Raiwind Road, Lahore.

Phone: +92 (42) 111- 747-424

Quaid-e-Azam Campus

28-M, Quaid-e-Azam, Industrial
Estate, Kot Lakhpat, Lahore.

UAN: +92 (42) -111-747-424

Gulberg Campus:

26-M, Gulberg - III,
Ferozepur Road, Lahore

UAN: +92 (42) -111-747-424

FAISALABAD

Faisalabad Campus:

Satiana Road, Adjacent Fish Farm,
Faisalabad.

Phone: +92 (41) 8777- 210 & 310

MALAKAND

Malakand Campus:

Chakdara Road, Malakand.

Phone: 0314-3019495



Find us on facebook
/RiphahUniversity



RIPHAH
FM102.2