REVA UNIVERSITY
Bengaluru, India

School of Computing and Information Technology

M.Tech. in Cyber Security

2021-23 Batch

HANDBOOK

Rukmini Knowledge Park

Kattigenahalli, Yelahanka, Bengaluru – 560064

www.reva.edu.in

REVA UNIVERSITY
Bengaluru, India

SCHOOL OF COMPUTING AND INFORMATION TECHNOLOGY

HANDBOOK

M. Tech. in Cyber Security

2021-23

Rukmini Knowledge Park,

Kattigenahalli, Yelahanka, Bangalore - 560 064

Phone No: +91-080-46966966

Rukmini Educational
Charitable Trust

Chancellor's Message

"Education is the most powerful weapon which you can use to change the world."

- Nelson Mandela.

There was a time when survival depended on just the realization of physiological needs. We are indeed privileged to exist in a time when 'intellectual gratification' has become indispensable. Information is easily attainable for the soul that is curious enough to go look for it. Technological boons enable information availability anywhere anytime. The difference, however, lies between those who look for information and those who look for knowledge.

It is deemed virtuous to serve seekers of knowledge and as educators it is in the ethos at REVA University to empower every learner who chooses to enter our portals. Driven by our founding philosophy of 'Knowledge is power', we believe in building a community of perpetual learners by enabling them to look beyond their abilities and achieve what they assumed impossible.

India has always been beheld as a brewing pot of unbelievable talent, acute intellect and immense potential. All it takes to turn those qualities into power is a spark of opportunity. Being at a University is an exciting and rewarding experience with opportunities to nurture abilities, challenge cognizance and gain competence.

For any University, the structure of excellence lies in the transitional abilities of its faculty and its facility. I'm always in awe of the efforts that our academic board puts in to develop the team of subject matter experts at REVA. My faculty colleagues understand our core vision of empowering our future generation to be ethically, morally and intellectually elite. They practice the art of teaching with a student-centered and transformational approach. The excellent infrastructure at the University, both educational and extra-curricular, magnificently demonstrates the importance of ambience in facilitating focused learning for our students.

A famous British politician and author from the 19th century - Benjamin Disraeli, once said 'A University should be a place of light, of liberty and of learning'. Centuries later this dictum still inspires me and I believe, it takes team-work to build successful institutions. I welcome you to REVA University to join hands in laying the foundation of your future with values, wisdom and knowledge.

Dr. P. Shyama Raju

The Founder and Hon'ble Chancellor, REVA University

Vice-Chancellor Message

The last two decades have seen a remarkable growth in higher education in India and across the globe. The move towards inter-disciplinary studies and interactive learning have opened up several options as well as created multiple challenges. India is at a juncture where a huge population of young crowd is opting for higher education. With the tremendous growth of privatization of education in India, the major focus is on creating a platform for quality in knowledge enhancement and bridging the gap between academia and industry.

A strong believer and practitioner of the dictum "Knowledge is Power", REVA University has been on the path of delivering quality education by developing the young human resources on the foundation of ethical and moral values, while boosting their leadership qualities, research culture and innovative skills. Built on a sprawling 45 acres of green campus, this 'temple of learning' has excellent and state-of-the-art infrastructure facilities conducive to higher teaching-learning environment and research. The main objective of the University is to provide higher education of global standards and hence, all the programs are designed to meet international standards. Highly experienced and qualified faculty members, continuously engaged in the maintenance and enhancement of student-centric learning environment through innovative pedagogy, form the backbone of the University.

All the programs offered by REVA University follow the Choice Based Credit System (CBCS) with Outcome Based Approach. The flexibility in the curriculum has been designed with industry-specific goals in mind and the educator enjoys complete freedom to appropriate the syllabus by incorporating the latest knowledge and stimulating the creative minds of the students. Bench marked with the course of studies of various institutions of repute, our curriculum is extremely contemporary and is a culmination of efforts of great think-tanks - a large number of faculty members, experts from industries and research level organizations. The evaluation mechanism employs continuous assessment with grade point averages. We believe sincerely that it will meet the aspirations of all stakeholders – students, parents and the employers of the graduates and postgraduates of REVA University.

At REVA University, research, consultancy and innovation are regarded as our pillars of success. Most of the faculty members of the University are involved in research by attracting funded projects from various research level organizations like DST, VGST, DBT, DRDO, AICTE and industries. The outcome of the research is passed on to students through live projects from industries. The entrepreneurial zeal of the students is encouraged and nurtured through EDPs and EACs.

REVA University has entered into collaboration with many prominent industries to bridge the gap between industry and University. Regular visits to industries and mandatory internship with industries have helped our students. REVA University has entered into collaboration with many prominent industries to bridge the gap between industry and University. Regular visits to industries and mandatory internship with industries have helped our students become skilled with relevant to industry requirements. Structured training programs on soft-skills and preparatory training for competitive exams are offered here to make students more employable. 100% placement of eligible students speaks the effectiveness of these programs. The entrepreneurship development activities and establishment of "Technology Incubation Centers" in the University extend full support to the budding entrepreneurs to nurture their ideas and establish an enterprise. With firm faith in the saying, "Intelligence plus character –that is the goal of education" (Martin Luther King, Jr.), I strongly believe REVA University is marching ahead in the right direction, providing a holistic education to the future generation and playing a positive role in nation building. We reiterate our endeavour to provide premium quality education accessible to all and an environment for the growth of over-all personality development leading to generating "GLOBAL PROFESSIONALS".

Welcome to the portals of REVA University!

Dr.M.Dhanamjaya

Vice-Chancellor, REVA University

Director's – Message

I congratulate and welcome all the students to the esteemed school of Computing and Information technology (IT). You are in the right campus to become a computer technocrat. The rising needs of automation in Industry 4.0 and improvising living standards have enabled rapid development of computer software and hardware technologies. Thus providing scope and opportunity to generate more human resources in the areas of computers and IT. The B.Tech and M.Tech program curriculum and Ph.D areas in the school are designed to cater to the requirements of industry and society. The curriculum is designed meticulously in association with persons from industries (TCS, CISCO, AMD, MPHASIS, etc.), academia and research organizations (IISc, IIIT, Florida University, Missouri S & T University, etc).

This handbook presents the M.Tech in Cyber Security program curriculum. The program is of 2 years duration and split into 4 semesters. The courses are classified into foundation core, hard core, and soft core courses. Hard core courses represent fundamentals study requirements of CSE. Soft courses provide flexibility to students to choose the options among several courses as per the specialization. Theoretical foundations of engineering, science, and computer science are taught in first two Semesters. Later, advanced courses and recent technologies are introduced in subsequent semesters for pursuing specialization.

The important features of the M.Tech Cyber security are as follows: 1) Choice based course selection and teacher selection,

2) Studies in emerging areas like cyber security programming, cyber forensics, cryptography, Ethical hacking, Python/R Programming, Genetic Engineering, Swarm Intelligence, Cyber security, -Deep Learning and Re-enforcement Learning, Knowledge Representation and Reasoning, Block Chain Technology, Virtual and Augmented Reality, Natural Language Processing, Robotic Process Automation and Internet of Things. 3) Short and long duration Internships 4) Opportunity to pursue MOOC course as per the interest in foundation and soft core courses, 5) Attain global and skill certification as per the area of specialization, 6) Self-learning components,

7) Experiential, practice, practical, hackathons, and project based learning, 8) Mini projects and major projects with research orientation and publication, 9) Soft skills training and 10) Platform for exhibiting skills in cultural, sports and technical activities through clubs and societies.

The school has well qualified faculty members in the various areas of Computing and IT including cloud computing, security, Internet of Things, Artificial IIntellegence, Machine Learning and Deep Learning, Software Engineering, Computer Networks, Cognitive Computing, etc. State of art laboratories are available for the purpose of academics and research.

Dr. Mallijkarjun M Kodabagi

Director, School of Computing and IT

CONTENTS

RUKMINI EDUCATIONAL CHARITABLE TRUST

It was the dream of late Smt. Rukmini Shyama Raju to impart education to millions of underprivileged children as she knew the importance of education in the contemporary society. The dream of Smt. Rukmini Shyama Raju came true with the establishment of Rukmini Educational Charitable Trust (RECT), in the year 2002. Rukmini Educational Charitable Trust (RECT) is a Public Charitable Trust, set up in 2002 with the objective of promoting, establishing and conducting academic activities in the fields of Arts, Architecture, Commerce, Education, Engineering, Environmental Science, Legal Studies, Management and Science & Technology, among others. In furtherance of these objectives, the Trust has set up the REVA Group of Educational Institutions comprising of REVA Institute of Technology & Management (RITM), REVA Institute of Science and Management (RISM), REVA Institute of Management Studies (RIMS), REVA Institute of Education (RIE), REVA First Grade College (RFGC), REVA Independent PU College at Kattigenahalli, Ganganagar and Sanjaynagar and now REVA University. Through these institutions, the Trust seeks to fulfill its vision of providing world class education and create abundant opportunities for the youth of this nation to excel in the areas of Arts, Architecture, Commerce, Education, Engineering, Environmental Science, Legal Studies, Management and Science & Technology.

Every great human enterprise is powered by the vision of one or more extraordinary individuals and is sustained by the people who derive their motivation from the founders. The Chairman of the Trust is Dr. P. Shyama Raju, a developer and builder of repute, a captain of the industry in his own right and the Chairman and Managing Director of the DivyaSree Group of companies. The idea of creating these top notched educational institutions was born of the philanthropic instincts of Dr. P. Shyama Raju to do public good, quite in keeping with his support to other socially relevant charities such as maintaining the Richmond road park, building and donating a police station, gifting assets to organizations providing accident and trauma care, to name a few.

The Rukmini Educational Charitable Trust drives with the main aim to help students who are in pursuit of quality education for life. REVA is today a family of ten institutions providing education from PU to Post Graduation and Research leading to PhD degrees. REVA has well qualified experienced teaching faculty of whom majority are doctorates. The faculty is supported by committed administrative and technical staff. Over 13,000 students study various courses across REVA's three campuses equipped with exemplary state-of-the-art infrastructure and conducive environment for the knowledge driven community.

ABOUT REVA UNIVERSITY

REVA University has been established under the REVA University Act, 2012 of Government of Karnataka and notified in Karnataka State Gazette No. 80 dated 27thFebruary, 2013. The University is empowered by UGC to award degrees any branch of knowledge under Sec.22 of the UGC Act. The University is a Member of Association of Indian Universities, New Delhi. The main objective of the University is to prepare students with knowledge, wisdom and patriotism to face the global challenges and become the top leaders of the country and the globe in different fields.

REVA University located in between Kempegowda International Airport and Bangalore city, has a sprawling green campus spread over 45 acres of land and equipped with state-of-the-art infrastructure that provide conducive environment for higher learning and research. The REVA campus has well equipped laboratories, custom-built teaching facilities, fully air-conditioned library and central computer centre, the well planned sports facility with cricket ground, running track & variety of indoor and outdoor sports activities, facilities for cultural programs. The unique feature of REVA campus is the largest residential facility for students, faculty members and supportive staff.

REVA consistently ranked as one of the top universities in various categories because of the diverse community of international students and its teaching excellence in both theoretical and technical education in the fields of Engineering, Management, Law, Science, Commerce, Arts, Performing Arts, and Research Studies. REVA offers 28 Undergraduate Programmes, 22 Full-time and 2 Part-time Postgraduate Programmes, 18 Ph. D Programmes, and other Certificate/ Diploma/Postgraduate Diploma Programmes in various disciplines.

The curriculum of each programme is designed with a keen eye for detail by giving emphasis on hands-on training, industry relevance, social significance, and practical applications. The University offers world-class facilities and education that meets global standards.

The programs being offered by the REVA University are well planned and designed after detailed study with emphasis with knowledge assimilation, applications, global job market and their social relevance. Highly qualified, experienced faculty and scholars from reputed universities / institutions, experts from industries and business sectors have contributed in preparing the scheme of instruction and detailed curricula for this program. Greater emphasis on practice in respective areas and skill development to suit to respective job environment has been given while designing the curricula. The Choice Based Credit System and Continuous Assessment Graded Pattern (CBCS – CAGP) of education has been introduced in all programs to facilitate students to opt for subjects of their choice in addition to the core subjects of the study and prepare them with needed skills. The system also allows students to move forward under the fast track for those who have the capabilities to surpass others. These

programs are taught by well experienced qualified faculty supported by the experts from industries, business sectors and such other organizations. REVA University has also initiated many supportive measures such as bridge courses, special coaching, remedial classes, etc., for slow learners so as to give them the needed input and build in them confidence and courage to move forward and accomplish success in their career. The University has also entered into MOUs with many industries, business firms and other institutions seeking their help in imparting quality education through practice, internship and also assisting students' placements.

REVA University recognizing the fact that research, development and innovation are the important functions of any university has established an independent Research and Innovation division headed by a senior professor as Dean of Research and Innovation. This division facilitates all faculty members and research scholars to undertake innovative research projects in engineering, science & technology and other areas of study. The interdisciplinary-multidisciplinary research is given the top most priority. The division continuously liaisons between various funding agencies, R&D Institutions, Industries and faculty members of REVA University to facilitate undertaking innovative projects. It encourages student research projects by forming different research groups under the guidance of senior faculty members. Some of the core areas of research wherein our young faculty members are working include Data Mining, Cloud Computing, Image Processing, Network Security, VLSI and Embedded Systems, Wireless Censor Networks, Computer Networks, IOT, MEMS, Nano- Electronics, Wireless Communications, Bio-fuels, Nano-technology for coatings, Composites, Vibration Energies, Electric Vehicles, Multilevel Inverter Application, Battery Management System, LED Lightings, Renewable Energy Sources and Active Filter, Innovative Concrete Reinforcement, Electro Chemical Synthesis, Energy Conversion Devices, Nano-structural Materials, Photo-electrochemical Hydrogen generation, Pesticide Residue Analysis, Nano materials, Photonics, Nana Tribology, Fuel Mechanics, Operation Research, Graph theory, Strategic Leadership and Innovative Entrepreneurship, Functional Development Management, Resource Management and Sustainable Development, Cyber Security, General Studies, Feminism, Computer Assisted Language Teaching, Culture Studies etc.

The REVA University has also given utmost importance to develop the much required skills through variety of training programs, industrial practice, case studies and such other activities that induce the said skills among all students. A full-fledged Career Development and Placement (CDC) department with world class infrastructure, headed by a dynamic experienced Professor& Dean, and supported by well experienced Trainers, Counselors and Placement Officers.

The University also has University-Industry Interaction and Skill Development Centre headed by a Senior Professor & Director facilitating skill related training to REVA students and other unemployed students. The University has been recognised as a Centre of Skill Development and Training by NSDC (National Skill Development Corporation) under Pradhan Mantri Kaushal VikasYojana. The Centre conducts several add-on courses in challenging areas of development. It is always active in facilitating student's variety of Skill Development Training programs.

The University has collaborations with Industries, universities abroad, research institutions, corporate training organizations, and Government agencies such as Florida International University, Okalahoma State University, Western Connecticut University, University of Alabama, Huntsville, Oracle India Ltd, Texas Instruments, Nokia University Relations, EMC2, VMware, SAP, Apollo etc, to facilitate student exchange and teacher–scholar exchange programs and conduct training programs. These collaborations with foreign universities also facilitates students to study some of the programs partly in REVA University and partly in foreign university, viz, M.S in Computer Science one year in REVA University and the next year in the University of Alabama, Huntsville, USA. The University has also given greater importance to quality in education, research, administration and all activities of the university. Therefore, it has established an independent Internal Quality division headed by a senior professor as Dean of Internal Quality. The division works on planning, designing and developing different quality tools, implementing them and monitoring the implementation of these quality tools. It concentrates on training entire faculty to adopt the new tools and implement their use. The division further works on introducing various examination and administrative reforms.

To motivate the youth and transform them to become innovative entrepreneurs, successful leaders of tomorrow and committed citizens of the country, REVA organizes interaction between students and successful industrialists, entrepreneurs, scientists and such others from time to time. As a part of this exercise great personalities such as Bharat Ratna Prof. C. N. R. Rao, a renowned Scientist, Dr. N R Narayana Murthy, Founder and Chairman and Mentor of Infosys, Dr. K Kasturirangan, Former Chairman ISRO, Member of Planning Commission, Government of India, Dr. Balaram, Former Director IISc., and noted Scientist, Dr. V S Ramamurthy, Former Secretary, DST, Government of India, Dr. V K Aatre, noted Scientist and former head of the DRDO and Scientific Advisor to the Ministry of Defence Dr. Sathish Reddy, Scientific Advisor, Ministry of Defence, New Delhi and many others have accepted our invitation and blessed our students and faculty members by their inspiring addresses and interaction. REVA organises various cultural programs to promote culture, tradition, ethical and moral values to our students. During such cultural events the students are given opportunities to unfold their hidden talents and motivate them to contribute innovative ideas for the progress of the society. One of such cultural events is REVAMP conducted every year. The event not only gives opportunities to students of REVA but also students of other Universities and Colleges. During three days of this mega event students participate in debates, Quizzes, Group discussion, Seminars, exhibitions and variety of cultural events. Another important event is Shubha Vidaaya, - Graduation Day for the final year students of all the programs, wherein, the outgoing students are felicitated and are addressed by eminent personalities to take their future career in a right spirit, to be the good citizens and dedicate themselves to serve the society and make a mark in their respective spheres of activities. During this occasion, the students who have achieved top ranks and won medals and prizes in academic, cultural and sports activities are also recognised by distributing awards and prizes. The founders have also instituted medals and prizes for sports

achievers every year. The physical education department conducts regular yoga class'severyday to students, faculty members, administrative staff and their family members and organizes yoga camps for villagers around.

REVA University

Vision

REVA University aspires to become an innovative university by developing excellent human resources with leadership qualities, ethical and moral values, research culture and innovative skills through higher education of global standards.

Misson

- To create excellent infrastructure facilities and state-of-the-art laboratories and incubation centers
- To provide student-centric learning environment through innovative pedagogy and education reforms.
- To encourage research and entrepreneurship through collaborations and extension activities.
- To promote industry-institute partnerships and share knowledge for innovation and development.
- To organize society development programs for knowledge enhancement in thrust areas.
- To enhance leadership qualities among the youth and enrich personality traits, promote patriotism and moral values.

Objectives

- Creation, preservation and dissemination of knowledge and attainment of excellence in different disciplines.
- Smooth transition from teacher - centric focus to learner - centric processes and activities.
- Performing all the functions of interest to its major constituents like faculty, staff, students and the society to reach leadership position.
- Developing a sense of ethics in the University and Community, making it conscious of its obligations to the society and the nation.
- Accepting the challenges of globalization to offer high quality education and other services in a competitive manner.

About the School of Computing and Information Technology (C & IT)

The School has a rich blend of experienced and committed faculty who are well-qualified in various aspects of computing and information technology apart from the numerous state-of-the-art digital classrooms and laboratories having modern computing equipment. The School offers five undergraduate programs: B Tech in Computer Science and Engineering, B Tech in Computer Science and Engineering (Artificial Intelligence and Machine Learning), B Tech in Computer Science and Information Technology, B Tech in Information Science and Engineering. Three postgraduate programs offered in the school are: M Tech in Artificial Intelliigence. In addition, the school has a unique academic collaboration with the University of Alabama in Huntsville to jointly offer an MS program in Computer Science. In addition, the school has a research center in which students can conduct cutting edge research leading to a PhD degree.

Curricula of both undergraduate and postgraduate programs have been designed through a collaboration of academic and industry experts in order to bridge the growing gap between industry and academia. This makes the program highly practical-oriented, and thus industry-resilient. The B Tech program aims to create quality human resources to play leading roles in the contemporary, competitive industrial and corporate world. The masters' degrees focus on quality research and design in the core and application areas of computing to foster a sustainable world and to enhance the global quality of life by adopting enhanced design techniques and applications. This thought is reflected in the various courses offered in the masters' programs.

Vision

To produce excellent quality technologists and researchers of global standards in computing and Information technology who have potential to contribute to the development of the nation and the society with their expertise, skills, innovative problem-solving abilities, strong moral and ethical values.

Mission

- To create state of the art computing labs infrastructure and research facilities in information technology.
- To provide student-centric learning environment in Computing and Information technology through innovative pedagogy and education reforms.

- To encourage research, innovation and entrepreneurship in computing and information technology through industry/academia collaborations and extension activities
- Organize programs through club activities for knowledge enhancement in thrust areas of information technology.
- To enhance leadership qualities among the youth and enrich personality traits, promote patriotism, moral and ethical values.

Quality Policy

The School of Computing and Information Technology is committed to excellence through following policies.

1. Impart quality education by providing state of art curriculum, experimental learning, and state of the art labs.
2. Enhance skill set of faculty members through faculty development programmes and interaction with academia and industries.
3. Inculcate the competency in software/hardware design and programming through co-curricular activities like Hackathon, Project exihibition, Internship and Enterpreneuship Programme.
4. Provide soft skill and skill development training for personality development and better placement.
5. Promote innovation and research culture among students and support faculty members for better research and development activity.

MEMBERS OF BOARD OF STUDIES

Sl. No.	Name		Correspondence Address
1	**Dr. Mallikarjun M Kodabagi** Professor and Director School of Computing and InformationTechnology REVA University,Bangaluru	Chairperson	Rukmini Knowledge Park, Kattigenahalli, Yelahanka, Bengaluru, Karnataka 560064
2.	**Dr. Vishwanath R Hulipalled** Professor School of Computing and Information Technology	Member	Rukmini Knowledge Park, Kattigenahalli, Yelahanka, Bengaluru, Karnataka 560064
3.	**Dr. Udaya Rani V** Professor School of Computing and Information Technology	Member	Rukmini Knowledge Park, Kattigenahalli, Yelahanka, Bengaluru, Karnataka 560064
4.	**Dr. Parthasarthy** Associate Professor, School of Computing and Information Technology	Member	Rukmini Knowledge Park, Kattigenahalli, Yelahanka, Bengaluru, Karnataka 560064
5.	**Dr. Venkatesh Prasad** Associate Professor, School of Computing and Information Technology	Member	Rukmini Knowledge Park, Kattigenahalli, Yelahanka, Bengaluru, Karnataka 560064
6.	**Sreenivasa Ramanujam Kanduri** Academic Relationship Manager, TCS	Member (Industry Expert)	Academic Relationship Manager, Tata Consultancy Services, Bangalore.
7.	**Dr. Sundar K S** Associate Vice-President & Head, IMS Academy at Infosys	Member (Industry Expert)	Associate Vice-President & Head, IMS Academy at Infosys, Mysore
8.	**Dr. Ramabrahmam Gunturi** Consultant, TCS	Industry Expert	Tata Consultancy Services, Hyderabad.
9.	**Dr. S. A. Angadi** Professor, School of CSE VTU	Academic Expert	Professor, School of CSE Visvesvaraya, Belagavi
10.	**Dr. Bharati Arakeri** Professor**,** School of CSE BMSIT, Bangalore.	Academic Expert	Professor**,** School of CSE BMSIT, Bangalore
11.	**Abhishek Revanna Swamy** Associate Project Manager, Robert Bosch	Alumni-Member	Associate Project Manager, Robert Bosch, Bangalore

Program Overview

M. Tech. in Cyber Security

The M.Tech in Cyber Security programme is designed to provide an outcome-driven and skill-based learning to make students become proficient cyber security professionals. Experiential learning with proprietary and open software programmes is the one of the best academic facilities of this programme. The School offers state-of-the art infrastructure to reproduce a real-time simulator-like environment to defend against cyberattack scenarios.

Computers have become ubiquitous part of modern life, and new applications are introduced every day. The use of computer technologies is also commonplace in all types of organizations, in academia, research, industry, government, private and business organizations. As computers become even more pervasive, the potential for computer-related careers will continue to grow and the career paths in computer-related fields will become more diverse. Since 2001, global information and communication technologies (ICTs) have become more powerful, more accessible, and more widespread. They are now pivotal in enhancing competitiveness, enabling development, and bringing progress to all levels of society.

Designed keeping in mind the exponential growth in the usage of information technology and the demand for huge number of cyber security professionals to counter measure online cyber-attacks.

Meet the demands of the future job market especially demand for cyber security professionals.

Designed with inputs from industry professionals and academic experts from various universities in India and abroad.

Some of the important courses of study include: cryptography, cloud security, block chain technology, cyber physical systems, Firewall and UTM architecture, digital forensics, ethical hacking, security architecture with solid theoretical foundation and project-based skills.

The career opportunities o Cyber Security are Cybersecurity Analyst,Security Engineer,Security Architect,Security Administrator,Security Software Developer ,Cryptanalyst,Digital Forensic Analyst,Vulnerability Assessor,Cloud Security Architect,Intrusion Detection Specialist,Cybercrime Investigator,Malware Analyst, Data Privacy Officer,Computer Security Incident Responder,Governance Compliance & Risk (GRC) Manager,Security Consultant.

May even go for pursuing higher studies in Cyber Security or go for doctorate degree.

The School of Computing and Information Science at REVA UNIVERSITY offers M.Tech, Cyber Security programme to create motivated, innovative, creative thinking graduates to fill ICT positions across sectors who can conceptualize, design, analyse, and develop ICT applications to meet the modern day requirements.

The M.Tech, in Cyber Security curriculum developed by the faculty at the School of Computing andInformation Science, is outcome based and it comprises required theoretical concepts and practical skills in the domain. By undergoing this programme, students develop critical, innovative, creative thinking and problem solving abilities for a smooth transition from academic to real-life work environment. In addition, students are trained in interdisciplinary topics and attitudinal skills to enhance their scope. The above mentioned features of the programme, advanced teaching and learning resources, and experience of the faculty members with their strong connections with ICT sector makes this programme unique.

Program Educational Objectives (PEO's)

After few years of graduation, the graduates of M. Tech (Cyber Security) will be able to:

PEO-1: Demonstrate skills as a Cybersecurity professional and perform duties with ethical and moral values.

PEO-2: Engage in active research for professional development with an attribute of lifelong learning.

PEO-3: Be an active and useful member of the society contributing to the economic and technological development of the nation and the world.

PEO-4: Take up entrepreneurship.

Program Outcomes (POs)

On successful completion of the programme, graduates of M.Tech (Cyber security) programme will be able to:

PO1:

Demonstrate in-depth knowledge of specific discipline or professional area, including wider and global perspective, with an ability to discriminate, evaluate, analyse and synthesise existing and new knowledge, and integration of the same for enhancement of knowledge.

PO 2:

Analyse complex engineering problems critically, apply independent judgment for synthesizing information to make intellectual and/or creative advances for conducting research in a wider theoretical, practical and policy context.

PO 3:

Think laterally and originally, conceptualize and solve engineering problems, evaluate a wide range of potential solutions for those problems and arrive at feasible, optimal solutions after considering public health and safety, cultural, societal and environmental factors in the core areas of expertise.

PO 4:

Extract information pertinent to unfamiliar problems through literature survey and experiments, apply appropriate research methodologies, techniques and tools, design, conduct experiments, analyze and interpret data, demonstrate higher order skill and view things in a broader perspective, contribute individually/in group(s) to the development of scientific/technological knowledge in one or more domains of engineering.

PO 5:

Create, select, learn and apply appropriate techniques, resources, and modern engineering and IT tools, including prediction and modeling, to complex engineering activities with an understanding of the limitations.

PO 6:

Possess knowledge and understanding of group dynamics, recognize opportunities and contribute positively to collaborative-multidisciplinary scientific research, demonstrate a capacity for self-management and teamwork, decision-making based on open-mindedness, objectivity and rational analysis in order to achieve common goals and further the learning of themselves as well as others.

PO 7:

Demonstrate knowledge and understanding of engineering and management principles and apply the same to one's own work, as a member and leader in a team, manage projects efficiently in respective disciplines and multidisciplinary environments after consideration of economic and financial factors.

PO 8:

Communicate with the engineering community, and with society at large, regarding complex engineering activities confidently and effectively, such as, being able to comprehend and write effective reports and design documentation by adhering to appropriate standards, make effective presentations, and give and receive clear instructions.

PO 9:

Recognize the need for, and have the preparation and ability to engage in life-long learning independently, with a high level of enthusiasm and commitment to improve knowledge and competence continuously.

PO 10:

Acquire professional and intellectual integrity, professional code of conduct, ethics of research and scholarship, consideration of the impact of research outcomes on professional practices and an understanding of responsibility to contribute to the community for sustainable development of society.

Program Specific Outcomes (PSOs)

On successful completion of the programme, graduates of M.Tech. (Cybersecurity) will be able to:

PSO-1: Develop an in-depth knowledge and skill sets in Cyber Security to monitor, prepare, predict, detect and respond and prevent cyber-attacks and ensure enterprise security.

PSO-2: Identify, assess and protect the enterprise IT assets and risks, perform risk analysis and develop policies and procedures based on compliance and able to define the architecture, design, and management of the security of an organisation.

PSO-3: Monitor, detect, respond, remediate cyber security threat using latest hardware and software tools and technologies, along with analytical and managerial skills to arrive at cost effective and optimum solutions either independently or as a team.

PSO-4: Review scholarly work by referring journals, define a new problem, design, model, analyse and evaluate the solution and report as a project in the area of Cybersecurity.

REVA University Regulations for Choice Based Credit System (CBCS) and Continuous Assessment Grading Pattern (CAGP) for Post Graduate Degree Program (M.Tech) – w.e.f Academic Year 2021-2023

Teaching and Learning Process

The teaching and learning process under CBCS-CAGP of education in each course of study will have three components, namely-

(i) L= Lecture (ii) T= Tutorial (iii) P= Practice, where:

L stands for **Lecture** session consisting of classroom instruction.

T stands for **Tutorial** session consisting participatory discussion / self-study/ desk work/ brief seminar presentations by students and such other novel methods that make a student to absorb and assimilate more effectively the contents delivered in the Lecture classes.

P stands for **Practice** session and it consists of Hands on Experience / Laboratory Experiments / Field Studies / Case Studies/ Project Based Learning/ Self Study / Online courses from listed portals that equip students to acquire the much required skill component.

Classification of Courses: A course shall have either or all the three components. That means a course may have only lecture component, or only practical component or combination of any two or all the three components.

Various course of s**tudy** are labeled and defined as: (i) Core Course (CC) (ii) Hard Core Course (HC), (iii) Soft Core Course (SC), (iv) Foundation Core Course (FC) and (v) Open Elective Course (OE).

(i) **Core Course:** A course which should compulsorily be studied by a candidate as a core-requirement is termed as a Core course.

(ii) Foundation Course (FC):

The foundation Course is a core course which should be completed successfully as a part of graduate degree program irrespective of the branch of study.

(iii) Hard Core Course (HC):

The **Hard Core Course** is a Core Course in the main branch of study and related branch (es) of study, if any that the candidates have to complete compulsorily.

(iv) Soft Core Course (SC):

A Core course may be a **Soft Core** if there is a choice or an option for the candidate to choose a course from a pool of courses from the main branch of study or from a sister/related branch of study which supports the main branch of study.

(v) Open Elective Course:

An elective course chosen generally from other discipline / subject, with an intention to seek exposure is called an O**pen Elective Course.**

Project Work:

Project work is a special course involving application of knowledge in solving / analyzing /exploring a real life situation / difficult problem.

Minor Project:

A project work up to TWO to FOUR **credits** is called **Minor Project** work. A Minor Project work may be a hard core or a Soft Core as decided by the BOS / concerned.

Major Project / Dissertation:

A project work of SIX or **EIGHT or TEN credits** is called **Major Project** work. The Major Project / Dissertation shall be Hard Core.

Minimum Credits to be earned:

A candidate has to earn 72 credits for successful completion of M Tech degree with a distribution of credits for different courses as prescribed by the University.

A candidate can enroll for a maximum of 24 credits per Semester. However s/he may not successfully earn a maximum of 24 credits per semester. This maximum of 24 credits does not include the credits of courses carried forward by a candidate.

Only such full time candidates who register for a minimum prescribed number of credits in each semester from I semester to IV semester and complete successfully 72 credits in 4 successive semesters shall be considered for declaration of Ranks, Medals, Prizes and are eligible to apply for Student Fellowship, Scholarship, Free ships, and such other rewards / advantages which could be applicable for all full time students and for hostel facilities.

Add- on Proficiency Certification:

In excess to the minimum of 72 credits for the M. Tech Degree program, a candidate can opt to complete a minimum of 4 extra credits either in the same discipline/subject or in different discipline / subject to acquire **Add on Proficiency Certification** in that particular discipline / subject in his / her subject of study or in other subjects / discipline along with the M .Tech degree.

Add on Proficiency Diploma:

In excess to the minimum of 72 credits for the M. Tech degree program, a candidate can opt to complete a minimum of 18 extra credits either in the same discipline/subject or in different discipline / subject to acquire Add on Proficiency Diploma in that particular discipline / subject along with the B. Tech degree. The A**dd -on Proficiency Certification / Diploma** so issued to the candidate contains the courses studied and grades earned.

Continuous Assessment, Earning of Credits and Award of Grades.

The assessment and evaluation process happens in a continuous mode. However, for reporting purpose, **a Semester is divided into 3 components as IA1, IA2 and SEE.** The performance of a candidate in a course will be assessed for a maximum of 100 marks as explained below.

(i) Component IA1:

The first Component (IA1), of assessment is for 25 marks. This will be based on test, assignment / seminar. During the first half of the semester (i.e. by 8th week), the first 50% of the syllabus (Unit 1&2) will be completed. This shall be consolidated during the first three days of 8th week of the semester. A review test based on IA1 will be conducted and completed in the beginning of the 9th week. In case of

courses where test cannot be conducted, the form of assessment will be decided by the concerned school and such formalities of assessment will be completed in the beginning of the 9th week. The academic sessions will continue for IA2 immediately after completion of process of IA1.

The finer split - up for the award of marks in IA1 is as follows:

Assignment & Seminars .....10 marks for the **first 20% of the syllabus**
Test (Mid-Term) ..... 15 marks forthe **first 30% of the syllabus**
Total.....25 marks

(ii) Component IA2:

The second component (IA2), of assessment is for 25 marks. This will be based on test, assignment /seminar. The continuous assessment and scores of second half of the semester (9th to 16th week) will be consolidated during 16th week of the semester. During the second half of the semester the remaining units in the course will be completed. A review test based on IA2 will be conducted and completed during 16th week of the semester. In case of courses where test cannot be conducted, the form of assessment will be decided by the concerned school and such formalities of assessment will be completed during 16th week.

The 17th week will be for revision of syllabus and preparation for the semester - end examination.

The finer split - up for the award of marks in IA2 is as follows:
Assignment/Seminar ..... 10 marks for the **second 20% of the syllabus**
Review Test (Mid-Term)..... 15 marks for the **second 30% of the syllabus**
Total.....25 marks

(iii) Component SEE:

The Semester End Examination of 3 hours duration for each course shall be conducted during the 18th & 19th week. **This forms the third / final component of assessment (SEE) and the maximum marks for the final component will be 50.**

The Assessment of MOOC and Online Courses shall be decided by the concerned School Board of Studies (BOS).

For> 3 credit courses

i	IA-I	25 marks
ii	IA-2	25 marks
iii	Semester end examination by the concern school board (demo, test, viva voice etc)	50 marks
	Total	**100 marks**

For 1 & 2 credit courses

i	IA-I	15 marks
ii	IA-2	15 marks
iii	Semester end examination by the concern school board (demo, test, viva voice etc)	20 marks
	Total	**50 marks**

The 50 marks meant for Internal Assessment (IA) of the performance in carrying out practical shallfurther be allocated as under:

i	Conduction of regular practical / experiments throughout the semester	20 marks
ii	Maintenance of lab records / Activities /Models / charts etc	10 marks
iii	Performance of mid-term test (to be conducted while conducting second test for theory courses); the performance assessments of the mid-term test includes performance in the conduction of experiment and write up about the experiment.	20 marks
	Total	**50 marks**

Setting Questions Papers and Evaluation of Answer Scripts:

There shall be three sets of questions papers set for each course. Two sets of question papers shall be set by the internal and one set by external examiner for a course. The Chairperson of the BoE shall get the question papers set by internal and external examiners.

The Board of Examiners shall scrutinize and approve the question papers and scheme of valuation.

There shall be single valuation for all theory papers by internal examiners. In case, the number of internal examiners falls short, external examiners may be invited. The answer scripts evaluated both by internal and external examiners shall be moderated by the external examiner / moderator.

The examination for Practical work/ Field work/Project work will be conducted jointly by two examiners (internal and external). However, in case of non-availability of external examiner or vice versa, the Chairperson BoE at his discretion can invite internal / external examiners as the case may be, if required.

If a course is fully of (L=0):T: (P=0) type, then the examination for SEE Component will be as decided by the BoS concerned.

In case of a course with only practical component a practical examination will be conducted with two examiners and each candidate will be assessed on the basis of: a) Knowledge of relevant processes, b) Skills and operations involved, and c) Results / Products including calculation and reporting.

The duration for Semester-End practical examination shall be decided by the Controller of Examinations.

5.4. Evaluation of Minor Project / Major Project / Dissertation:

Right from the initial stage of defining the problem, the candidate has to submit the progress reports periodically and also present his/her progress in the form of seminars in addition to the regular discussion with the supervisor. At the end of the semester, the candidate has to submit final report of the project / dissertation, as the case may be, for final evaluation. The components of evaluation are as follows:

Component – I	(IA1)	Periodic Progress and Progress Reports (25%)
Component – II	(IA2)	Results of Work and Draft Report (25%)
Component– III	(SEE)	Final Evaluation and Viva-Voce (50%). Evaluation of the report is for 30% and the Viva-Voce examination is for 20%.

5.4. The schedule of continuous assessment and examinations are summarized in the following Table below.

Component	Period	Syllabus	Weightage	Activity
IA1	1st Week to 8th Week	First 50% (two units)		Instructional process and Continuous Assessment
	Last 3 days of 8th Week		25%	Consolidation of IA1
IA2	9th week to 16th week	Second 50% (remaining two units)		Instructional process and Continuous Assessment
	Last 3 days of 16th week		25%	Consolidation of IA2
SEE	17th and 18th week			Revision and preparation for Semester end examination
	19th week to 20th week	Entire syllabus	50%	Conduct of semester end examination and Evaluation concurrently
	21st week			Notification of Final Grades
***Evaluation shall begin very first day after completion of the conduct of examination of the first course and both examination and evaluation shall continue concurrently. The examination results / final grades be announced latest by 21st week**				

Note: 1. Practical examination wherever applicable shall be conducted before conducting of IA2 examination. The calendar of practical examination shall be decided by the respective school.

2. Finally**, awarding the Grades** be announced latest by 5 days after completion of the examination.

6.0 Requirements to Pass a Course

A candidate's performance from all 3 components will be in terms of scores, and the sum of all three scores will be for a maximum of 100 marks (25 + 25 + 50). A candidate who secures a minimum of 40% in the SEEand an overall 40% (IA1+IA2+SEE) in a course is said to be successful.

Eligibility to Appear for SEE (Semester -End Examination) and Provision to Drop the Course.

Only those students who fulfill 75% attendance requirement and who secure minimum 30% marks in IA1

and IA2 together in a course are eligible to appear for SEE examination in that course.

Those students who have 75% of attendance but have secured less than 30% marks in IA1 and IA2 together in a course are not eligible to appear for SEE examination in that course. They are treated as dropped the course and they will have to repeat that course whenever it is offered.

Teachers offering the courses will place the above details in the School Council meeting during the last week of the Semester, before the commencement of SEE, and subsequently a notification pertaining to the above will be brought out by the Director of the School before commencement of SEE examination. A copy of this notification shall also be sent to the office of the Controller of the Examinations.

In case a candidate secures more than 30% in IA1 and IA2 together but less than 40% in aggregate of IA1, IA2 and SEE in a course is considered as unsuccessful and such a candidate may either opt to DROP that course or appear for SEE examination during the subsequent semesters / years within the stipulated period.

In such a case wherein he / she opts to appear for just SEE examination, then the marks secured in IA1 and IA2 shall get continued. Repeat SEE examination will be conducted in respective semesters.

In case a candidate opts to drop the course he / she has to re-register for the dropped course only in subsequent semesters whenever it is offered if it is Hard Core Course and he / she may choose alternative course if it is Soft Core Course or Open Elective course or Skill Development Course. **The details of any dropped course will not appear in the Grade Card.**

Provision to Withdraw Course:

A candidate can withdraw any course within ten days from the date of notification of final results. Whenever a candidate withdraws a course, he/she has to register for the same course in case it is hard core course, the same course or an alternate course if it is soft core/open elective. **A DROPPED course is automatically considered as a course withdrawn.**

Provision for Supplementary Examination

In case a candidate fails to secure a minimum of 40% (20 marks) in Semester End Examination (SEE) and a minimum of 40% marks overall (IA and SEE together), such candidate shall seek supplementary examination of only for such course(s) wherein his / her performance is declared unsuccessful. The supplementary examinations are conducted after the announcement of even semester examination results. The candidate who is unsuccessful in a given course(s) shall appear for supplementary examination of odd and even semester course(s) to seek for improvement of the performance.

Re-Registration and Re-Admission:

A candidate's class attendance in aggregate of all courses in a semester is less than 75% or as stipulated by the University and is considered as dropped the semester and is not allowed to appear for semester end examination (SEE) shall have to seek re-admission to that semester during subsequent semester / year within a stipulated period.

In case a candidate fails in more than 2 courses in odd and even semesters together in a given academic year, he / she may either drop all the courses and repeat the semester or reappear (SEE-semester end examination) to such of those courses where in the candidate has failed during subsequent semester / year within a stipulated period.

In such a case where in a candidate drops all the courses in semester due to personal reasons, it is considered that the candidate has dropped the semester and he / she shall seek re-admission to such dropped semester.

Requirements to Pass the Semester andProvision to Carry Forward the Failed Subjects / Courses:

A candidate who secures a minimum of 40% in the SEE and an overall 40% (IA1+IA2+SEE) in a course is said to be successful.

7.5. Provision to Carry Forward the Failed Subjects / Courses:

A student who has failed in 4 courses in 1st and 2nd semesters together shall move to 3rd semester. And he / she shall appear for SEE examination of failed courses of the said semesters concurrently with 3rd semester end examinations (SEE) and 4th semester end examinations (SEE) of second year of study.

8.0 **Attendance Requirement:**

All students must attend every lecture, tutorial and practical classes.

In case a student is on approved leave of absence (e g:- representing the university in sports, games or athletics, placement activities, NCC, NSS activities and such others) and / or any other such contingencies like medical emergencies, the attendance requirement shall be minimum of 75% of the classes taught.

Any student with less than 75% of attendance in a course during a semester shall not be permitted to appear in the semester end examination.

Absence during mid semester examination

In case a student has been absent from a mid-semester examination due to the illness or other contingencies he / she may give a request along with necessary supporting documents and certification from the concerned class teacher / authorized personnel to the concerned Head of the School, for make-up examination. The Head of the School may consider such request depending on the merit of the case and after consultation with course instructor and class teacher, and permit such student to appear for make-up mid semester examination.

Absence during Semester End Examination:

In case a student is absent for Semester End Examination on medical grounds or such other exigencies, the student can submit request for make-up examination, with necessary supporting documents and certification from the concerned class teacher / authorized personnel to the concerned Director of the School. The Director of the School may consider such request depending on the merit of the case and after consultation with class teacher, course instructor and permit such student to appear for make-up mid semester examination

Provisional Grade Card:

The tentative / provisional Grade Card will be issued by the Controller of Examinations at the end of every Semester indicating the courses completed successfully. The provisional grade card provides **Semester Grade Point Average** (SGPA).This statement will not contain the list of DROPPED courses.

Challenge Valuation:

A student who desires to apply for challenge valuation shall obtain a Xerox copy of the answer script by paying the prescribed fee within 10 days after the announcement of the results. He / She can challenge the Grade awarded to him/her by surrendering the Grade Card and by submitting an application along with the prescribed fee to the Controller of Examination (COE) within 15 days after the announcement of the results. This challenge valuation is only for SEE component.

The answer scripts for which challenge valuation is sought for shall be sent to another external examiner. The marks awarded will be the higher of the marks obtained in the challenge valuation and in maiden valuation.

Final Grade Card: Upon successful completion of the Post Graduate Degree a Final Grade card consisting of grades of all courses successfully completed by the Candidate will be issued by the COE.

The Grade and the Grade Point: The Grade and the Grade Point earned by the candidate in the subjectwill be as given below.

Marks P	Grade G	Grade Point (GP=V x G)	Letter Grade
90-100	10	v*10	O
80-89	9	v*9	A
70-79	8	v*8	B
60-69	7	v*7	C
50-59	6	v*6	D
40-49	5	v*5	E
0-39	0	v*0	F

O - Outstanding; A-Excellent; B-Very Good; C-Good; D-Fair; E-Satisfactory; F - Fail;

Here, P is the percentage of marks (P=[(IA1+IA2)+SEE] secured by a candidate in a course which is **rounded to nearest integer**. v is the credit value of course. G is the grade and GP is the grade point.

Computation of SGPA and CGPA

The Following procedure to compute the Semester Grade Point Average (SGPA)

The SGPA is the ratio of sum of the product of the number of credits with the grade points scored by a student in all the courses taken by a student and the sum of the number of credits of all the courses undergone by a student, i.e

SGPA (Si) = ∑(Ci x Gi) / ∑Ci

Where Ci is the number of credits of the ith course and Gi is the grade point scored by the student in the ith course.

Illustration for Computation of SGPA and CGPA

Illustration No. 1

Course	Credit	Grade letter	Grade Point	Credit Point (Credit x Grade)
Course 1	**3**	**A**	**9**	**3X9=27**
Course 2	**3**	**B**	**8**	**3X8=24**
Course 3	**3**	**C**	**7**	**3X7=21**
Course 4	**3**	**O**	**10**	**3X10=30**
Course 5	**3**	**D**	**6**	**3X6=18**
Course 6	**3**	**O**	**10**	**3X10=30**
Course 7	**2**	**A**	**9**	**2X 9 = 18**
Course 8	**2**	**B**	**8**	**2X 8 = 16**
	22			**184**

Thus, **SGPA = 184 ÷ 22 = 8.36**

Cumulative Grade Point Average (CGPA):

Overall Cumulative Grade Point Average (CGPA) of a candidate after successful completion of the required number of credits (72) for two year post graduate degree in a specialization is calculated taking into

account all the courses undergone by a student over all the semesters of a program, i. e **CGPA = ∑(Ci x Si) / ∑Ci**

Where Si is the SGPA of the ith semester and Ci is the total number of credits in that semester.

The SGPA and CGPA shall be rounded off to 2 decimal points and reported in the transcripts.

Illustration:

CGPA after Final Semester

Semester (ith)	**No. of Credits (Ci)**	**SGPA (Si)**	**Credits x SGPA (Ci X Si)**
1	22	8.36	22 x 8.36 = 183.92
2	22	8.54	22 x 8.54 =187.88
3	16	9.35	16x9.35=149.6
4	12	9.50	12x9.50=114
Cumulative	72		635.4

Thus, **CGPA** = $\frac{22x8.36+22x8.54+16x9.35+12x9.50}{72}$ = 8.83

CONVERSION OF GRADES INTO PERCENTAGE:

Conversion formula for the conversion of CGPA into Percentage is:

Percentage of marks scored = CGPA Earned x 10

Illustration: CGPA Earned 8.83 x 10=88.30

Classification of Results

The final grade point (FGP) to be awarded to the student is based on CGPA secured by the candidate and is given as follows.

CGPA	Numerical Index	FGP Qualitative Index
> 4 =CGPA < 5	**5**	SECOND CLASS
5 > = CGPA < 6	6	
6 >= CGPA < 7	7	FIRST CLASS
7 >= CGPA < 8	8	
8 >= CGPA < 9	9	DISTINCTION
9 >= CGPA 10	10	

Overall percentage=10*CGPA

Provision for Appeal

If a candidate is not satisfied with the evaluation of IA1 and IA2 components, he/she can approach the grievance cell with the written submission together with all facts, the assignments, test papers etc, which were evaluated. He/she can do so before the commencement of semester-end examination. The grievance cell is empowered to revise the marks if the case is genuine and is also empowered to levy penalty as prescribed by the university on the candidate if his/her submission is found to be baseless and unduly motivated. This cell may recommend taking disciplinary/corrective action on an evaluator if he/she is found guilty. The decision taken by the grievance cell is final.

Grievance Committee

For every program there will be one Grievance Committee. The composition of the grievance committee is as follows:-

- The Controller of Examinations - Ex-officio Chairman / Convener
- One Senior Faculty Member (other than those concerned with the evaluation of the course concerned) drawn from the school / department/discipline and/or from the sister schools / departments/sister disciplines – Member.

- One Senior Faculty Members / Subject Experts drawn from outside the University school /department – Member.

M.Tech in Cyber Security

Scheme of Instructions for 2021-23

(Effective from the Academic Year 2021-22)

Sl. No	Course Code	Course Title	Course Type	Credit Pattern and Credit Value				No. of Hrs.
				L	T	P	C	
First Semester								
1	M21TF0101	Cyber Security and Programming	HC	3	0	1	4	5
2	M21TF 0102	Mathematics for Cyber Security	HC	4	0	0	4	4
3	M21TF 0103	Cyber Forensics	HC	3	0	1	4	5
4	M21TF 0104	Security and investigation of the block chain	HC	4	0	0	4	4
5	M21TF 0105	Ethical Hacking and Network Defense	HC	3	0	1	4	5
6	M21TF 0106	Mini Project	HC	0	0	2	2	4
Total Credits for the First Semester							**22**	**27**
Second Semester								
1	M21TF0201	Cloud security	HC	3	0	1	4	5
2	M21TF0202	Cyber security with ML and AI	HC	3	0	1	4	5
3	M21TF0203	Security Analytics	HC	3	0	1	4	5
4	M21TFS204	Firewall & UTM architecture	SC	3	0	0	3	3
	M21TFS205	Malware Analysis and Detection						
	M21TFS206	Web Security						
5	M21TFS207	Secure Communications	SC	3	0	0	3	3
	M21TFS208	Penetration testing & incident response						
	M21TFS209	Mobile and Wireless security						
6	M21TF0206	Forensics and VAPT Lab	HC	0	0	2	2	4
7	M21TF0207	Mini Project	HC	0	0	2	2	4
Total Credits for the Second Semester							**22**	**29**

Sl. No	Course Code	Course Title	Course Type	Credit Pattern and Credit Value				No. of Hrs.
THIRD SEMESTER								
1	M21TFS301	Security and Resilience	SC	4	0	0	4	4
	M21TFS302	IOT Security						
	M21TFS303	Advanced topics in cyber security						
2	M21TFO3XX	Open Elective	MC	4	0	0	4*	4
3	M21TF0303	Project Phase-1	HC	0	0	4	4	8
4	M21TF0304	Internship/Global Certification	HC	0	0	4	4	8
	Total Credits for the Third Semester						**12**	20
	*(MC)This course must be completed but it will not be graded and not considered for computing CGPA/SGPA							
FOURTH SEMESTER								
1	M21TF0401	Project Phase -2 and Dissertation	HC	0	0	16	16	32
	Total Credits for the Fourth Semester						**16**	32
Total Number of Credits for all Four Semesters is 72.								

Note:

Internship should be carried out in a reputed /Tier-1/R & D organization, preferably, internship should be with stipend. The internship should be approved by the REVA University authorities before completion of 3rd semester and the students should obtain the permission for the same by producing the necessary details of company, selection process, and the offer letter issued by the company. At the end of the Internship, detailed report must be submitted.

Open Electives offered to other schools

1. M21CB3021 Fundamentals of cyber security
2. M21CB3022 Ethical Hacking
3. M21CB3023 Blockchain Technology

<table>
<tr><td>Course Title</td><td colspan="4">Cyber Security And Programming</td><td colspan="2">Course type</td><td colspan="2">Integrated</td></tr>
<tr><td>Course Code</td><td>M21TF0101</td><td>Credits</td><td colspan="2">4</td><td colspan="2">Class</td><td colspan="2">VII Semester</td></tr>
<tr><td rowspan="5">Course Structure</td><td>TLP</td><td>Credits</td><td>Contact Hours</td><td>Work Load</td><td colspan="2" rowspan="2">Total Number of Classes Per Semester</td><td colspan="2" rowspan="2">Assessment in Weightage</td></tr>
<tr><td>Theory</td><td>3</td><td>3</td><td>3</td></tr>
<tr><td>Practice</td><td>1</td><td>2</td><td>2</td><td rowspan="2">Theory</td><td rowspan="2">Practical</td><td rowspan="2">CIE</td><td rowspan="2">SEE</td></tr>
<tr><td>-</td><td>0</td><td>-</td><td>-</td></tr>
<tr><td>Total</td><td>4</td><td>5</td><td>5</td><td>39</td><td>26</td><td>50%</td><td>50%</td></tr>
</table>

Course Overview:

The Cyber Security and Programming course gives an awareness of software Vulnerabilities in computer systems that can be used to crack the frontier problems of the current day. The C /C++ programming concepts are covered in this course are at the forefront of commercial practice in solving real-time problems. They are applicable in Exception handling – Mitigation Strategies, stack randomization, vulnerabilities in Cybersecurity. This course is designed to understand the software security concepts in cyber security to handle real world applications.

Course Objective (s):

The Objectives of this course are to:

1. Understand the most frequent programming errors to software vulnerabilities.
2. Identify and analyze security problems in software and integral security issues.
3. Apply the knowledge to the common vulnerabilities associated with file I/O.
4. Apply the specific development practices for improving the overall security of the application.

COURSE OUTCOMES (COs)

After the completion of the course, the student will be able to:

CO#	Course Outcomes	POs	PSOs
CO1	Discuss the software security concepts for cybersecurity	1, 2, 3, 4, 5	1
CO2	Analyze Exception Handling - Mitigation Strategies in computer systems.	1, 2, 3, 4, 5	2
CO3	Applying Stack Randomization-Mitigation Strategies to Notable Vulnerabilities in cybersecurity	1, 2, 3, 4, 5	2,3
CO4	Demonstrate Stack Randomization, Mitigation Strategies and Vulnerabilities	1, 2, 3, 4, 5	2,3

CO5	Design the Security Development Lifecycle for Cybersecurity	1, 2, 3, 4, 5	1
CO6	Analyze File I/O Interfaces, Access Control and File Identification	1, 2, 3, 4, 5	1,2

BLOOM'S LEVEL OF THE COURSE OUTCOMES

CO#	Bloom's Level					
	Remember (L1)	Understand (L2)	Apply (L3)	Analyze (L4)	Evaluate (L5)	Create (L6)
CO1		√				
CO2				√		
CO3			√			
CO4						√
CO5				√		
CO6			√			

COURSE ARTICULATION MATRIX

CO#/ POs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	2	2	2	2	1								3		
CO2	3	2	3	1	2									3	
CO3	3	1	2	2	3									3	3
CO4	2	2	2	1	1									3	3
CO5	2	2	2	1	1									3	3
CO6	2	2	2	1	1									3	3

Note: 1-Low, 2-Medium, 3-High

Course Contents:

Unit-1

SOFTWARE SECURITY CONCEPTS : Gauging the Threat - Security Concepts - C and C++ - Development Platforms - Strings - Character Strings - Common String manipulation Errors - String Vulnerabilities and Exploits - Mitigation Strategies - String handling functions - runtime protection strategies - notable vulnerabilities

Unit-2

POINTER SUBTERFUGE AND INTEGER SECURITY : Data Locations - Function Pointers - Object Pointers - Modifying the Instruction Pointer - Global Offset Table - The .dtors Section - Virtual Pointers - The atexit() and on_exit() Functions - The longjmp() Function - Exception Handling - Mitigation Strategies - Integer Security - Integer Conversions - Integer Operations - Integer Vulnerabilities - Mitigation Strategies

Unit-3

FORMATTED OUTPUT FUNCTIONS: Variadic Functions - Exploiting Formatted Output Functions - Stack Randomization-Mitigation Strategies - Notable Vulnerabilities

Unit-4

File I/O: File I/O Basics - File I/O Interfaces - Access Control - File Identification - Race Conditions - Mitigation Strategies, Recommended practices: The Security Development Lifecycle - Security Training -Requirements - Design- Implementation – Verification.

Self-learning component:

Python, Java

PRACTICE:

Sl. No	**Title of the Experiment**	**Tools and Techniques**	**Expected Skill /Ability**
1.	Thread is an execution unit which consists of its program counter, a stack, and a set of registers**.** Write a c program for multi-threading and thread synchronization on a kernel such that, each thread occupied an independent memory slot.	Windows/Linux OS, IDE, C,C++	Thread operations.
2.	Demonstrate how to pass array of pointers to the thread such that, each pointer is independent to another.	Windows/Linux OS, IDE, C,C++	**Pointer operations**
3.	Demonstrate a program that is vulnerable to a buffer overflow.	Windows/Linux OS, IDE, C,C++	**Buffer overflow vulnerability**

4.	Demonstrate the concept of Signal Handler with respect to multi-threading optimization in C or C++	Windows/Linux OS, IDE, C,C++	**Multi-Threading**
5.	Demonstrate the following functions: atexit() and onexit() in C.	Windows/Linux OS, IDE, C,C++	**Standard functions**
6.	Stack may grow downward or upward depending on environment for which code is compiled. Demonstrate the growth of Stacks in C/C++.	Windows/Linux OS, IDE, C,C++	**Stacks**
7.	Integer overflow based on a real-world vulnerability in the handling of the comment field in JPEG files. Demonstrate Integer overflow vulnerability.	Windows/Linux OS, IDE, C,C++	**Integer overflow vulnerability**
8.	Write a C Programming to demonstrate mitigation strategies	Windows/Linux OS, IDE, C,C++	**Mitigation strategies**
9.	Write a C/C++ programming on File IO operation management	Windows/Linux OS, IDE, C,C++	**Files**
10.	Develop a C Program to Read content of a File and Display it	Windows/Linux OS, IDE, C,C++	**Files**

Text books:

1. Seacord, R. C., Secure Coding in C and C++, Addison c for Software Engineering Institute, 2nd edition, 2013.
2. Howard, M., LeBlanc, D., Writing Secure Code, 2nd Edition. Pearson Education, 2002

Reference books:

1 Daswani N., Kern C., Kesavan A., Foundations of Security, Apress, 2007.

2 https://www.newhorizons.com/promotions/cybersecurity-ebooks

3 https://www.coursera.org/learn/introduction-cybersecurity-cyber-attacks#syllabus

JOURNALS/MAGAZINES:

1 IEEE Transactions on Cybersecurity

2 Springer Journal of Cybersecurity.

SWAYAM/NPTEL/MOOCS:

1. https://www.udemy.com/Cybersecurity/
2. https://www.coursera.org/learn/Cybersecurity
3. https://nptel.ac.in/courses/cybersecurity/

Course Title	**Mathematics for Cyber Security**				**Course Type**		**Theory**	
Course Code	M21 TF 0102	**Credits**	**4**		**Class**		**I Semester**	
Course Structure	TLP	Credits	Contact Hours	Work Load	Total Number of Classes Per Semester		Assessment in Weightage	
	Theory	4	4	4				
	Practice	0	0	0	Theory	Practical	IA	SEE
	Tutorial	-	-	-				
	Total	**4**	**4**	**4**	**52**	**-**	**50%**	**50%**

COURSE OVERVIEW

The course **Mathematics for Cyber Security** with the basic aspects of number theory like, GCD, Divisibility, Prime number etc. This course includes algebraic structure for Groups, Discrete logarithms . Probability theory is important to understand the concept of probability and conditional probability. Coding theory is important for liner code, hamming code and syndrome decoding. Pseudorandom number is used for Next bit predictor and Blum-Blum-Shub Generator. All mathematical concepts are highly important for the mathematical foundation and calculation of Cyber Security for to develop strong foundations on these concepts.

COURSE OBJECTIVE (S):

The objectives of this course are to:

1. Explain the basics maths used for information security.
2. Illustrate how to Design and analyse security protocols.
3. Describe the concepts of Probability and Statistics are used in many commercial, industrial as well as web Application.
4. Demonstrate the use of the coding theory concepts will help them to develop security model.

COURSE OUTCOMES (COs)

After the completion of the course, the student will be able to:

CO#	Course Outcomes	POs	PSOs
CO1	Effectively express the concepts and results of Number Theory. Understand basic concepts of various algebraic structures and theorems like Euler's theoerem for designing security algorithm.	1-6	1,2
C02	Apply Euclidean algorithm, Fermat's theorem to the real world application.	1-6	1,2
CO3	Describe introduction to probability concepts, random variables, probability distributions (continuous and discrete),	1-6	2
CO4	Identify and evaluate the probability based on Baye's theorem.	1-6	1,2
CO5	Make use of concept of Coding Theory in real world problem.	1-6	1,2
CO6	Apply Cryptographic Hash Functions for given data	1-6	2

BLOOM'S LEVEL OF THE COURSE OUTCOMES

CO#	Bloom's Level					
	Remember (L1)	Understand (L2)	Apply (L3)	Analyze (L4)	Evaluate (L5)	Create (L6)
CO1			√			
CO2			√			
CO3		√				
CO4			√			
CO5		√				
CO6			√			

COURSE ARTICULATION MATRIX

CO#/ POs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	3	3	2	2	3	1						3	3	
CO2	3	3	3	3	3	1						3	3	
CO3	3	3	2	2	3	1							2	
CO4	2	3	2	3	3	1						1	1	

CO5	2	3	2	3	3	1						1	1	
CO6	2	3	2	3	3	1							1	

Note: 1-Low, 2-Medium, 3-High

COURSE CONTENT

THEORY:

UNIT – 1

NUMBER THEORY : Logic, Mathematical reasoning, Sets, Basics of counting, Relations.

Introduction - Divisibility - Greatest common divisor - Prime numbers - Fundamental theorem of arithmetic - Mersenne primes - Fermat numbers - Euclidean algorithm.

Graph Theory: Euler graphs, Hamiltonian paths and circuits, planar graphs, trees, rooted and binary trees, distance and centres in a tree, fundamental circuits and cut sets, graph colorings and applications.

UNIT – 2

Linear Algebra: vector spaces and subspaces, linear independence, basis and dimensions, linear transformations and applications.

Pseudorandom Number Generation: Stream Ciphers Principles of Pseudorandom Number Generation, Principles of Pseudorandom Number Generation using a Block Cipher.

UNIT – 3

Probability Theory: introduction to probability concepts, random variables, probability distributions (continuous and discrete), Bayesian approach to distributions, mean and variance of a distribution, joint probability distributions, theory of estimation,

UNIT – 4

CODING THEORY: Introduction - Basic concepts: codes, minimum distance, equivalence of codes, Linear codes - Linear codes - Generator matrices and paritycheck matrices - Syndrome decoding – Hamming codes.

Cryptographic Hash Functions: Application of Cryptographic Hash Functions, Two Simple Hash Functions, Requirements and Security.

TEXT BOOKS:

1. R.P.Grimaldi, ”Discrete and Combinatorial Mathematics”, Fifth edition, Pearson Education, 2007.
2. K. H. Rosen, “Discrete Mathematics and its applications”, Seventh Edition, Tata MCGraw-Hill Publishing company limited, New Delhi, 2007.
3. H. Anton, “Elementary Linear Algebra”, John Wiley & Sons, 2010.
4. N. Deo, “Graph theory with applications to Engineering and Computer Science”, Prentice Hall of India, New Delhi, 1974.
5. T. M. Apostol, “Introduction to Analytic Number Theory”, Springer, 1976.

REFERENCE BOOKS:

1. Douglas C. Montgomery and George C. Runger, "Applied Statistics and Probability forEngineers", Third Edition, John Wiley & Sons Inc., 2003.
2. A. Papoulis and U. Pillai, Probability, "Random Variables and Stochastic Processes", Fourth Edition, McGraw Hill, 2002.
3. Ronald E. Walpole, Raymond H Myres, Sharon.L.Myres and Kying Ye, "Probability andStatistics for Engineers and Scientists", Seventh Edition, Pearson Education, 2002.
4. D. S. Malik, J. Mordeson, M. K. Sen, Fundamentals of abstract algebra, Tata McGraw Hill
5. P. K. Saikia, Linear algebra, Pearson Education, 2009.
6. I. Niven, H.S. Zuckerman and H. L. Montgomery, An introduction to the theory of numbers, John Wiley and Sons, 2004.
7. D P Bersekas and J N Tsitsiklis, Introduction to probability, Athena Scientific, 2008
8. Douglas Stinson, 'Cryptography – Theory and Practice', CRC Press, 2006.
9. Sheldon M Ross, "Introduction to Probability Models", Academic Press, 2003.
10. C.L. Liu, 'Elements of Discrete mathematics', McGraw Hill, 2008.
11. Behrouz A. Forouzan, " Cryptography and Network Security ", TMH Publication.

JOURNALS/MAGAZINES

1. https://ocw.mit.edu/courses/mathematics/

2. http://homes.soic.indiana.edu/yh33/Teaching/I231-2016/syllabus.html

SWAYAM/NPTEL/MOOCs:

1. http://nptel.ac.in/syllabus/106105031/

2. http://nptel.ac.in/syllabus/syllabus_pdf/106105031.pdf

3. http://nptel.ac.in/syllabus/106101004/

4 https://eliademy.com/catalog/physical-science/elementary-number-theory.html

<table>
<tr><td>Course Title</td><td colspan="4">Cyber Forensics</td><td colspan="2">Course Type</td><td colspan="2">Integrated</td></tr>
<tr><td>Course Code</td><td>M21 TF 0103</td><td colspan="2">Credits</td><td>4</td><td colspan="2">Class</td><td colspan="2">II Semester</td></tr>
<tr><td rowspan="6">Course Structure</td><td>TLP</td><td>Credits</td><td>Contact Hours</td><td>Work Load</td><td colspan="2" rowspan="2">Total Number of Classes Per Semester</td><td colspan="2" rowspan="2">Assessment in Weightage</td></tr>
<tr><td>Theory</td><td>3</td><td>3</td><td>3</td></tr>
<tr><td>Practice</td><td>1</td><td>2</td><td>2</td><td>Theory</td><td>Practical</td><td>CIE</td><td>SEE</td></tr>
<tr><td>-</td><td>-</td><td>-</td><td>-</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Total</td><td>4</td><td>5</td><td>5</td><td>39</td><td>26</td><td>50</td><td>50</td></tr>
</table>

COURSE OVERVIEW

The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information. The course aims to give insight on Digital Forensic Evidence Collection and Processing,

Fundamentals of Host Forensics for Microsoft Windows. UNIX derivatives. It gives an overview of Forensic Database Systems and Network Forensics.

COURSE OBJECTIVE (S):

The objectives of this course are to:

1. Understand methodology and procedures associated with digital forensic analysis in a network environment.
2. Explain Digital Forensic Framework, Fundamentals of Host Forensics for Microsoft Windows and UNIX derivatives.
3. Illustrate Forensic Analysis of Database Systems.
4. Discuss protection of consumer web.

COURSE OUTCOMES (COs)

After the completion of the course, the student will be able to:

CO#	Course Outcomes	POs	PSOs
CO1	Apply digital information for possible use as evidence in civil, criminal or administrative cases.	1 to 4, 8, 9 , 12	1
CO2	Identify importance of digital forensic principles and procedures, legal considerations, digital evidence controls	1 to 3, 5,9,12	1
CO3	Make use of concepts of forensics for UNIX derivatives - Linux operating system and File systems	1 to 5, 9, 12	2
CO4	Illustrate Forensic analysis of Database Components,	3,4,5,9,12	2
CO5	Analyze network Forensics with case studies and tools	1,4,5,9,12	1
CO6	Classify the types of Steganography and Image file Forensics	1 to 5	2,3

BLOOM'S LEVEL OF THE COURSE OUTCOMES

CO#	Bloom's Level					
	Remember (L1)	Understand (L2)	Apply (L3)	Analyze (L4)	Evaluate (L5)	Create (L6)
CO1			√			

CO2			√			
CO3			√	√		
CO4			√			
CO5		√	√			
CO6				√		

COURSE ARTICULATION MATRIX

CO#/ POs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	1	1	2				1	1			1	3		
CO2	3	2	3		2				1			1	2	3	
CO3	3	1	2	1	2				1			1		2	
CO4	3			2	2				1			1	3		
CO5	3			2	2				1			1		3	
CO6	3			2	2				1			1		3	3

Note: 1-Low, 2-Medium, 3-High

COURSE CONTENT

THEORY:

UNIT – 1

Digital Forensic : Framework for Digital Forensic Evidence Collection and Processing, Fundamentals of Host Forensics for Microsoft Windows - Kernel and Device driver architecture, registry, auditing and security architecture File system handling - Reconstruction of files and directory structures on the FAT and NTFS.

UNIT – 2

Linux operating system and File system: Fundamentals of Host Forensics for UNIX derivatives - Linux operating system, Kernel and Device drives architecture, Security and audit mechanisms, file system and pseudo file systems, the reconstruction of file and directory structures using UFS and Ext2/3fs as exemplars.

UNIT – 3

Forensic Database Systems: Forensic Analysis of Database Systems, Database Tampering, Forensic analysis of Database Components, table storage, transaction log, indexes, Forensic recovery for table storage.

UNIT – 4

Network Forensics: Network Forensics, investigating logs, network traffic and web attacks, Mobile Device and Wireless Forensics, Anti-Forensics. Steganography and Image file Forensics, Email investigation, Investigating Copiers, IVR, Video Surveillance, RFID and Vehicular tracking (GPS) devices, Case studies and Tools.

No	Title of the Experiment
1.	Creating a Forensic Image using FTK Imager/Encase Imager : - Creating Forensic Image - Check Integrity of Data - Analyze Forensic Image
2.	Data Acquisition: - Perform data acquisition using: - USB Write Blocker + FTK Imager
3.	Forensics Case Study : -Solve the Case study (image file) provide in lab using Encase Investigator or Autopsy
4.	Capturing and analyzing network packets using Wireshark (Fundamentals) : - Identification the live network - Capture Packets - Analyze the captured packets
5	Analyze the packets provided in lab and solve the questions using Wireshark : - What web server software is used by www.snopes.com? - About what cell phone problem is the client concerned? - According to Zillow, what instrument will Ryan learn to play? - How many web servers are running Apache?

6.	Using Sysinternals tools for Network Tracking and Process Monitoring : - Check Sysinternals tools - Monitor Live Processes - Capture RAM - Capture TCP/UDP packets - Monitor Hard Disk - Monitor Virtual Memory - Monitor Cache Memory
7	Recovering and Inspecting deleted files - Check for Deleted Files - Recover the Deleted Files - Analyzing and Inspecting the recovered files
8	Acquisition of Cell phones and Mobile devices
9	:- Email Forensics - Mail Service Providers - Email protocols
10	Web Browser Forensics . -Web Browser working -Forensics activities on browser

Text Books/References:

1. E. P. Dorothy, Real Digital Forensics for Handheld Devices , Auerback Publications, 2013.

2. J. Sammons, The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics, Syngress Publishing, 2012.

3. E. Casey, Handbook of Digital Forensics and Investigation, Academic Press, 2010 L T P C 3 0 0 3 Page 32 of 44

4. C. H. Malin, E. Casey and J. M. Aquilina, Malware Forensics Field Guide for Windows Systems: Digital Forensics Field Guides, Syngress, 2012 5. J. Wiles and A.Reyes,

5. J. Wiles and A.Reyes, The Best Damn Cybercrime and Digital Forensics Book Period, Syngress, 2007.

Online Resources:

1. https://github.com/wtsxDev/Machine-Learning-for-Cyber-Security
2. https://github.com/jivoi/awesome-ml-for-cybersecurity#-books
3. https://github.com/RegaipKURT/CyberSecurity

JOURNALS/MAGAZINES

1. https://www.journals.elsevier.com/journal-of-information-security-and-applications
2. https://www.journals.elsevier.com/computers-and-security
3. http://scholar.google.co.in/scholar_url?url=https://www.profsandhu.com/cs6393_s19/Solms-Niekerk- 3.pdf&hl=en&sa=X&ei=6QpBYLmcH5X0yATMxJGADQ&scisig=AAGBfm122ujljJW_s9W8QhWP-HQUU- uNQw&nossl=1&oi=scholarr

SWAYAM/NPTEL/MOOCs:

1. https://www.classcentral.com/course/swayam-digital-forensic-19842 2. https://nptel.ac.in/courses/106/106/106106182/

3, https://onlinecourses.swayam2.ac.in/cec20_ge10/preview **Self-Learning Exercises:**

3. **https://onlinecourses.swayam2.ac.in/ugc19_hs25/preview**

1. More exploration on GIThub
2. Data Visualization packages

Course Title	Security and investigation of the block chain				**Course Type**		**Integrated**	
Course Code	M21 TF 0104	**Credits**	**4**		**Class**		**I Semester**	
Course Structure	TLP	Credits	Contact Hours	Work Load	Total Number of Classes Per Semester		Assessment in Weightage	
	Theory	4	4	4				
	Practice	0	0	0	Theory	Practical	CIE	SEE
	-	-	-	-				
	Total	**4**	**4**	**4**	**52**	**0**	**50**	**50**

COURSE OVERVIEW

The widespread popularity of digital cryptocurrencies has led the foundation of Blockchain, which is fundamentally a public digital ledger to share information in a trustworthy and secure way. The concept and applications of Blockchain have now spread from cryptocurrencies to various other domains, including business process management, smart contracts, IoT and so on. This course is a joint venture from academia and industry, where the target is to cover both the conceptual as well as application aspects of Blockchain. This includes the fundamental design and architectural primitives of Blockchain, the system and the security aspects, along with various use cases from different application domains.

COURSE OBJECTIVE (S):

The objectives of this course are to:

1. Understand the mechanism of Blockchain and Cryptocurrency.
2. Explain functionality of current implementation of blockchain technology.
3. Describe the required cryptographic background.

4. Explore the applications of Blockchain to cryptocurrencies and understanding limitations of current Blockchain and recent research.

COURSE OUTCOMES (COs)

After the completion of the course, the student will be able to:

CO#	Course Outcomes	POs	PSOs
CO1	Apply the fundamentals of Cryptography in Cryptocurrency	1 to 4, 8, 9 , 12	1
CO2	Make use of various operations associated with the life cycle of Blockchain and Cryptocurrency	1 to 3, 5,9,12	1
CO3	Explain methods for verification and validation of Bitcoin transactions	1 to 5, 9, 12	2
CO4	Explain Bitcoin as an Append only Log, Smart Property and Secure Multi Party	1 to 5	2
CO5	Analyze principles, practices and policies associated Bitcoin business and demonstrate the general ecosystem of several Cryptocurrency	1,4,5,9,12	1
CO6	Illustrate the Relationship Between Bitcoin and Altcoins	1 to 5	1

BLOOM'S LEVEL OF THE COURSE OUTCOMES

CO#	Bloom's Level					
	Remember (L1)	Understand (L2)	Apply (L3)	Analyze (L4)	Evaluate (L5)	Create (L6)
CO1			√			
CO2			√			
CO3			√	√		
CO4		√				
CO5			√			
CO6			√			

COURSE ARTICULATION MATRIX

CO#/ POs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	1	1	2				1	1			1	3		
CO2	3	2	3		2				1			1	3		
CO3	3	1	2	1	2				1			1		3	
CO4	3			2	2				1			1	3		

CO5	3			2	2				1				2		
CO6	3			2	2				1				2		

Note: 1-Low, 2-Medium, 3-High

COURSE CONTENT

THEORY:

UNIT – 1

Introduction to Cryptography and Cryptocurrencies

Cryptographic Hash Functions, Hash Pointers and Data Structures, Digital Signatures, Public Keys as Identities, A Simple Cryptocurrency, Decentralization-Centralization vs. Decentralization-Distributed consensus, Consensus with- out identity using a blockchain, Incentives and proof of work. Simple Local Storage, Hot and Cold Storage, Splitting and Sharing Keys, Online Wallets and Exchanges, Payment Services, Transaction Fees, Currency Exchange Markets.

UNIT – 2

Mechanics of Bitcoin, Mining and Anonymity

Bitcoin transactions, Bitcoin Scripts, Applications of Bitcoin scripts, Bitcoin blocks, The Bit- coin network, Limitations, and improvements. The task of Bitcoin miners, Mining Hardware, Energy consumption and ecology, Mining pools, Mining incentives and strategies Anonymity Basics, How to De-anonymize Bitcoin, Mixing, Decentralized Mixing, Zerocoin and Zerocash.

UNIT – 3

Community, Politics, and Regulation

Consensus in Bitcoin, Bitcoin Core Software, Stakeholders: Who's in Charge, Roots of Bitcoin, Governments Notice on Bitcoin, Anti Money Laundering Regulation, New York's Bit License Proposal. Bitcoin as a Platform: Bitcoin as an Append only Log, Bitcoins as Smart Property, Secure Multi Party Lotteries in Bitcoin, Bitcoin as Public Randomness, Source-Prediction Markets, and Real-World Data Feeds.

UNIT – 4

Altcoins and the Cryptocurrency Ecosystem

Altcoins: History and Motivation, A Few Altcoins in Detail, Relationship Between Bitcoin and Altcoins, Merge Mining-Atomic Cross chain Swaps-6 Bitcoin Backed Altcoins, Side Chains, Ethereum and Smart Contracts. Blockchain Use Cases – Finance, Industry

TEXT BOOKS:

1. Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press.

REFERENCE BOOKS:

1. Antonopoulos, A. M. (2014). Mastering Bitcoin: unlocking digital cryptocurrencies. OReilly Media, Inc.".
2. Franco, P. (2014). Understanding Bitcoin: Cryptography, engineering and economics. John Wiley and Sons.

JOURNALS/MAGAZINES

4. https://www.inderscience.com/jhome.php?jcode=ijbc(Inderscience)
5. https://www.journals.elsevier.com/blockchain-research-and-applications(Elsevier)
6. https://www.frontiersin.org/journals/blockchain
7. https://ledgerjournal.org/ojs/ledger

SWAYAM/NPTEL/MOOCs:

4. Coursera – Blockchain technology
5. https://nptel.ac.in/courses/106/104/106104220/
6. https://www.edx.org

Self-Learning Exercises:

1. Blockchain By IBM Source: IBM Blog
2. Blockchain And Deep Learning: Future Of AI Source: Udemy
3. Bitcoin And Cryptocurrency Technologies Source: Coursera
4. Bitcoin And Cryptocurrencies Source: edX Blog
5. Introduction To Cryptocurrencies And Blockchain Source: Udemy

<table>
<tr><td>Course Title</td><td colspan="3">Ethical Hacking and Network Defense</td><td colspan="2">Course Type</td><td colspan="2">HARD CORE</td></tr>
<tr><td>Course Code</td><td>M21 TF 0105</td><td>Credits</td><td colspan="2">4</td><td colspan="2">Class</td><td colspan="2">I Semester</td></tr>
<tr><td rowspan="5">Course Structure</td><td>TLP</td><td>Credits</td><td>Contact Hours</td><td>Work Load</td><td colspan="2" rowspan="2">Total Number of Classes Per Semester</td><td colspan="2" rowspan="2">Assessment in Weightage</td></tr>
<tr><td>Theory</td><td>3</td><td>3</td><td>3</td></tr>
<tr><td>Practice</td><td>1</td><td>2</td><td>2</td><td>Theory</td><td>Practical</td><td>CIE</td><td>SEE</td></tr>
<tr><td>-</td><td>-</td><td>-</td><td>-</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Total</td><td>4</td><td>5</td><td></td><td>39</td><td>26</td><td></td><td></td></tr>
</table>

COURSE OVERVIEW

Ethical Hacking and Network Defense deals with the systematic evaluation and study of various technical aspects, approaches and paradigms of ethical hacking and networking defense properties. This course on ethical hacking has been designed to learn the fundamentals of ethical hacking. You will understand how ethical hacking plays a very important role in the present-day scenario. In this course, you will learn about the basic concepts of networking defense, ethical hacking fundamentals, various secure communication protocols and security patches.

COURSE OBJECTIVE (S):

The objectives of this course are to:

1. Explain the fundamentals of Ethical Hacking and its application front in validating networks
2. Inculcate knowledge of various secure communication protocols and ethical hacking tools
3. Gain expertise in evaluating and analyzing spoofed properties and attacks
4. Evaluating and monitoring the Networking properties via ethical hacking approaches.

COURSE OUTCOMES (COs)

After the completion of the course, the student will be able to:

CO#	Course Outcomes	POs	PSOs
CO1	Evaluating the fundamentals learning's of ethical hacking and its organizational benefits.	1 to 5	2, 3
CO2	Develop ethical hacking approaches, techniques and programming patches to encounter malicious activity by ethical hacking	1 to 5	2, 3
CO3	Validating various secure communication protocols for building reliable networking defense systems	1 to 5	2, 3
CO4	Describe Building a Kali Web Server and Linux and Python server models	1 to 5	2, 3
CO5	Create and validating networking patches for various hacking attacks via ethical hacking approaches,	1 to 5	2, 3
CO6	Illustrate Information Assurance Model in detail	1 to 5	2, 3

BLOOM'S LEVEL OF THE COURSE OUTCOMES

CO#	Bloom's Level					
	Remember (L1)	Understand (L2)	Apply (L3)	Analyze (L4)	Evaluate (L5)	Create (L6)
CO1			√	√		
CO2					√	
CO3			√	√	√	
CO4			√			
CO5						√
CO6			√			

COURSE ARTICULATION MATRIX

CO#/ POs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3

CO1	2	3	2	3	2									2	3
CO2	2	3	3	3	2									2	3
CO3	3	3	2	3	2									2	3
CO4	2	3	2	2	2									2	3
CO5	3	2	3	3	3									3	2
CO6	2	3	3	2	2									2	3

Note: 1-Low, 2-Medium, 3-High

COURSE CONTENT

THEORY:

UNIT – 1

Introduction: Legal Side of Hacking, Hacking Environment, Installing Virtual Box, Kali Linux server, Python and Ethical Hacking, General Syntaxes, variables, objects and Loops

UNIT – 2

Regular Expressions, Exceptions, Catching Errors, Classes and Databases, Sockets and Networking, Building NMAP Scanner, Dark WEB and Tor, Proxy chains, Virtual Private Networks (VPN), MAC Addresses, Security Trends

UNIT – 3

Penetration Testing: Setup of Networking Security Lab, Know Your Network, Building a Kali Web Server, Kali Linux and Python

UNIT – 4

SQL Mapping, Vulnerability Analysis, Information Assurance Model, Hashes and Passwords, Classic Modern Encryption, Exploiting Targets

PRACTICE:

No	Title of the Experiment	Tools and Techniques	Expected Skill /Ability
1.	Installation of Virtual Box, Metasploitable, Kali	Windows, VMWare	Ability to learn the process of setting up a virtual lab devices for ethical hacking

2.	Write a hashed (md5) format plain text re-representing program for capturing passwords using dictionary attack.	Windows / VmWare/ python	Tracking passwords from the regular un-texted format.
3.	Write a python script to change the MAC Address and demonstrate the following a) demonstrate spoofing attack bypassing b) demonstrate to avoid device tracking in public networks	Windows / VmWare/ python	Changing the MAC Address and validate skills of ethical hacking.
4.	Demonstrate the process of Network Scanner in Python IDE using three basic methods of ICMP Echo Request, Three-way hand shaking Method and TCP Scan	Windows / VmWare/ python	Validating the network setting skills and scanning of node information
5.	Demonstrate the process Network Scanning using scapy module	Windows / VmWare/ python	Validating the network setting skills and scanning of node information
6.	Demonstrate the process of Intrusion detection and spoofing attack in Address Resolution Protocol (ARP) in KALI LINUX	Windows / VmWare/ python	Validating ARP attacks and network defense process

TEXT BOOKS:

1. Sanjib Sinha, "Beginning Ethical Hacking with Python" Apress, 2018
2. Sanjib Sinha, "Beginning Ethical Hacking with Kali, Computational Techniques for resolving security issues" Apress, 2018

REFERENCE BOOKS:

1. Patrick Engebretson, "Basics of Hacking and Penetration Testing", Second Edition, Elsevier.

Self-Learning Exercises:

1. Introduction to Ethical Hacking: https://www.tutorialspoint.com/ethical_hacking/index.htm

SECOND SEMESTER

Course Title	Cloud Security				**Course Type**		**Integrated**	
Course Code	M21TF0201	**Credits**	**4**		**Class**		**II Semester**	
Course	TLP	Credits	Contact Hours	Work Load	Total Number of Classes Per Semester		Assessment in Weightage	
	Theory	3	2	2				
	Practice	1	2	2	Theory	Practical	CIE	SEE

Structure	-	-	-	-				
	Total	**4**	**4**	**4**	**39**	**26**	**50**	**50**

COURSE OVERVIEW

Python is a Programming Language that can be treated in a procedural way, an object-orientated way or a functional way. It can be used on a server to create web applications, create workflows, connect to database systems, read and modify files, handle big data and perform complex mathematics. It can implement object oriented features and exception handling, It can parse the strings using regular expressions. It can be used for implementing the machine learning algorithms to develop solutions for interdisciplinary problems apart from any general problems leading to automation.

COURSE OBJECTIVE (S):

The objectives of this course are to:

1. Understanding of the security challenges in the cloud environment.
2. Understanding of the issues regarding privacy and manage risks associated with it.
3. Knowledge of security standards and the audit processes to follow and ensure better cloud security.

COURSE OUTCOMES (COs)

After the completion of the course, the student will be able to:

CO#	Course Outcomes	POs	PSOs
CO1	State the security challenges of cloud infrastructure.	1 to 4, 8, 9 , 12	1
CO2	Illustrate the application security mechanisms.	1 to 3, 5,9,12	1
CO3	Make Use of concepts of standards to define a management policy.	1 to 5, 9, 12	2
CO4	Design solutions for risk management and security threats	1,4,5,9,12	1
CO5	Analyze a cloud security audit report.	1,4,5,9,12	2
CO6	Categorize record generation, reporting and management and service level agreement models	1,4,5,9,12	2

BLOOM'S LEVEL OF THE COURSE OUTCOMES

CO#	Bloom's Level					
	Remember (L1)	Understand (L2)	Apply (L3)	Analyze (L4)	Evaluate (L5)	Create (L6)

CO1			√			
CO2			√			
CO3			√	√		
CO4						√
CO5			√			
CO6				√		

COURSE ARTICULATION MATRIX

CO#/ POs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	1	1	2				1	1			1	3		
CO2	3	2	3		2				1			1	2	3	
CO3	3	1	2	1	2				1			1		3	3
CO4	3			2	2				1			1	3		
CO5	3			2	2				1			1		2	
CO6	3			2	2				1			1		2	

Note: 1-Low, 2-Medium, 3-High

COURSE CONTENT

THEORY:

UNIT – 1

Cloud Security Fundamentals:

Cloud computing security challenges – cloud computing security architecture–data security life-cycle-Security Patterns and architectural elements - Planning key Strategies for secure operation.

Cloud Application Security

Encryption techniques – homomorphic encryption - securing data Redaction - secure bitcoin – Public key infrastructure (PKI) – key management - open web application security project (OWASP) Cloud Top 10 Security Risks - Security as a service (SECaaS)

UNIT –2

Cloud Infrastructure Security

Virtualization security – securing hypervisor - securing virtual machines - designing virtual network for security - Network Security in the cloud - software-defined security - secure isolation strategy - anti- fragile cloud infrastructure - Failure as a service.

Security Management & Privacy

Managed Security Service Provider (MSSP): Availability management – configuration management - vulnerability management - identity management. - Privacy: privacy, compliance and the cloud - privacy enhancing encryption

UNIT-3

Risk Management & Security Threats

Risk management – principles - assessing the risk – strategies for managing risk – risk analysis framework – security threats – intrusion detection

Cloud Standards and Compliance

Cloud security alliance – cloud controls matrix - cloud security standards guidance – security compliance - NIST – PCI data security standards – SAS 70 - ISO 27001 **–** HIPAA – ITIL - FISMA - FIPS 140-2.

UNIT-4

Audit

Cloud-Based IT Audit Process – System and Infrastructure lifecycle management for the cloud -governance, risk management and compliance (GRC) – cloud audit assurance – auditing –record generation, reporting and management- tamper-proofing audit logs service level agreement (SLA) – legal safeguards - cloud morphing.

PRACTICE:

1.	AWS Account Setup and Services Overview
2.	AWS Resource Discovery and Instance Setup
3.	Platform/Application Provisioning and Auto Scaling Adaptation
4.	Demonstrate Intrusion Detection System (IDS) using any tool (snort or equivalent software)
5.	Installation of rootkits and study about the variety of options
6.	Demonstrate how a sniffer attack is done using Wireshark Tool.
7.	Install Jcrypt Tool (or any equivalent) to demonstrate Asymmetric and Symmetric Crypto algorithm.
8.	Demonstrate how to inject JavaScirpt using Cross Site Scripting (XSS).

TEXT BOOKS:

1. Tim Mather, Subra Kumaraswamy, Shahed Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O'Reilly Media Inc, 2009.
2. Dave Shackleford, Virtualization security:Protecting virtualized environments, John Wiley & sons, 2013.
3. Vic (J.R.) Winkler, Securing the Cloud: Cloud Computer Security Techniques and Tactics, Syngress; 1st edition (April 29, 2011).
4. Raghu Yeluri, Enrique castro-leon, Building the infrastructure for cloud security:A Solutions view, Apress, 2014.
5. Krutz, R.L. (2010), Cloud Security A Comprehensive Guide to Secure Cloud Computing, Wiley
6. Ben Halpert , "Auditing Cloud Computing: A Security and Privacy Guide: ", John Wiley & Sons, 2011.
7. Shao ying zhu, Richard Hill, Guide to security assurance for cloud computing, Springer 2015.
8. John Rittinghouse, James F.Ransome, Cloud computing implementation, Management, security, CRC Press, 2010.
9. Stefan Rass, Daniel Slamanig, Cryptography for security and Privacy in cloud computing, Artech House, 2014.
10. OWASP - https://www.owasp.org/images/4/47/Cloud-Top10-Security-Risks.pdf
11. JOURNALS/MAGAZINES

    https://journalofcloudcomputing.springeropen.com/

    https://www.journals.elsevier.com/journal-of-information-security-and-applications

    https://www.journals.elsevier.com/computers-and-security

    https://www.journals.elsevier.com/computer-fraud-and-security

SWAYAM/NPTEL/MOOCs:

https://onlinecourses.nptel.ac.in/noc21_cs14/preview

https://nptel.ac.in/courses/106/105/106105167/

https://onlinecourses.swayam2.ac.in/cec20_cs09/preview

Self-Learning Exercises:

1. Introduction to **Cloud Computing** with Amazon Web Services. ...
2. **Cloud Computing**: The Big Picture By David Chappell. ...
3. Getting Started with **Cloud Computing** — Level 1. ...
4. **Cloud Computing** Concepts by Coursera. ...
5. AWS Certified Solutions Architect — Associate.

Course Title	Cyber security with ML and AI				Course Type		Integrated	
Course Code	M21TF0202	Credits	4		Class		II Semester	
Course Structure	TLP	Credits	Contact Hours	Work Load	Total Number of Classes Per Semester		Assessment in Weightage	
	Theory	3	3	3				
	Practice	1	2	2	Theory	Practical	CIE	SEE
	-	-	-	-				
	Total	**4**	**5**	**5**	**39**	**26**	**50**	**50**

COURSE OVERVIEW

Machine learning has become a vital technology for cyber security. Machine learning preemptively stamps out cyber threats and bolsters security infrastructure through pattern detection, real-time cybercrime mapping and thorough penetration testing. The course aims to give insight on how machine learning has contributed to the success of modern spam filters, Quickly detect anomalies, including breaches, fraud, and impending system failure. It gives an overview of how to conduct malware analysis by extracting useful information from computer binaries, uncover attackers within the network by finding patterns inside datasets.

COURSE OBJECTIVE (S):

The objectives of this course are to:

1. Explain the fundamentals of machine learning and their applications in cyber security.
2. Gain knowledge on anomaly detection with respect to cyber security.
3. Analyze malware using static analysis and analyze network traffic analysis.
4. Discuss protection of consumer web.

COURSE OUTCOMES (COs)

After the completion of the course, the student will be able to:

CO#	Course Outcomes	POs	PSOs
CO1	Explain the fundamentals of machine learning and their applications in cyber security.	1 to 4, 8, 9 , 12	1
CO2	Develop programs for anomaly detection using suitable machine learning algorithms	1 to 3, 5,9,12	1
CO3	Understand malware analysis and network traffic analysis.	1 to 5, 9, 12	2
CO4	Build a Predictive Model to Classify Network Attacks	1 to 5, 9, 12	2
CO5	Create data science solutions for consumer web	1 4,5, 9, 12	1

CO6	Demonstrate Supervised Learning for Abuse Problems and Labeling Data	1 4,5, 9, 12	2

BLOOM'S LEVEL OF THE COURSE OUTCOMES

CO#	Bloom's Level					
	Remember (L1)	Understand (L2)	Apply (L3)	Analyze (L4)	Evaluate (L5)	Create (L6)
CO1			√			
CO2			√			
CO3			√	√		
CO4						√
CO5						√
CO6					√	

COURSE ARTICULATION MATRIX

CO#/ POs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	1	1	2				1	1			1	3		
CO2	3	2	3		2				1			1	2		
CO3	3	1	2	1	2				1			1		3	
CO4	3			2	2				1			1		3	
CO5	3			2	2				1			1	3		
CO6	3			2	2				1			1		3	

Note: 1-Low, 2-Medium, 3-High

COURSE CONTENT

THEORY:

UNIT – 1

Why Machine Learning and Security? Cyber Threat Landscape, The Cyber Attacker's Economy, What Is Machine Learning? Real-World Uses of Machine Learning in Security, Spam Fighting: An Iterative Approach, Limitations of Machine Learning in Security

Classifying and Clustering: Machine Learning: Problems and Approaches, Machine Learning in Practice: A Worked Example, Training Algorithms to Learn, Supervised Classification Algorithms, Practical Considerations in Classification, Clustering

UNIT – 2

Anomaly Detection: When to Use Anomaly Detection Versus Supervised Learning, Intrusion Detection with Heuristics, Data-Driven Methods, Feature Engineering for Anomaly Detection, Anomaly Detection with Data and Algorithms, Challenges of Using Machine Learning in Anomaly Detection, Response and Mitigation, Practical System Design Concerns

Malware Analysis: Understanding Malware, Feature Generation, From Features to Classification

UNIT – 3

Network Traffic Analysis: Theory of Network Defense, Access Control and Authentication, Intrusion Detection, Detecting In-Network Attackers, Data-Centric Security, Honeypots, Machine Learning and Network Security, From Captures to Features, Threats in the Network, Botnets and You, Building a Predictive Model to Classify Network Attacks, Exploring the Data, Data Preparation, Classification, Supervised Learning, Semi-Supervised Learning, Unsupervised Learning, Advanced Ensembling

UNIT – 4

Protecting the Consumer Web: Monetizing the Consumer Web, Types of Abuse and the Data That Can Stop Them, Authentication and Account Takeover, Account Creation, Financial Fraud, Bot Activity

Supervised Learning for Abuse Problems, Labeling Data, Cold Start Versus Warm Start, False Positives and False Negatives, Multiple Responses, Large Attacks, Clustering Abuse, Example: Clustering Spam Domains, Generating Clusters, Scoring Clusters

PRACTICE:

No	Title of the Experiment
1.	Regression (or prediction) is simple. The knowledge about the existing data is utilized to have an idea of the new data. Take an example of house prices prediction. In cyber security, it can be applied to fraud detection. The features (e.g., the total amount of suspicious transaction, location, etc.) determine a probability of fraudulent actions.. Write a program to perform linear regression on any dataset.

2.	Classification is also straightforward. Imagine you have two piles of pictures classified by type (e.g., dogs and cats). In terms of cybersecurity, a spam filter separating spams from other messages can serve as an example. Spam filters are probably the first ML approach applied to Cybersecurity tasks. type (e.g., dogs and cats). In terms of cybersecurity, a spam filter separating spams from other messages can serve as an example write a program to perform classification of any suitable data using any suitable classification algorithm
3.	Clustering is similar to classification with the only but major difference. The information about the classes of the data is unknown. There is no idea whether this data can be classified. This is unsupervised learning. Implement clustering on a suitable dataset using k means
4.	Forensic Challenge You receive a letter from a friend, who is suspicious that a neighbor is up to no good. Your friend has not heard anything from the neighbor in a while. However, your friend did capture some of the neighbor's packets about a week ago. Putting the ethical sides of the problem aside, help your friend figure out where the neighbor has gone and what the neighbor is up to. What is the neighbor's name? What is the neighbor's email address? What is the neighbor's email password? What are the email addresses (at least two) of the neighbor's correspondents? What is the email of the correspondent the neighbor is most likely have gone to visit? What is the name of the file containing the meeting location? Bonus: where are they meeting and what is the correspondent bringing?
5	Touch Biometrics In this question, we explore continuous authentication methods for users who are using a smartphone. Our friends across the bay built 30 features on top of the raw data. You can find the details of the approach and the data at http://www.mariofrank.net/touchalytics/index.html Implement two more features in addition to the 30 found in the database. Do they have positive information gain? That is, are the features useful? Report correlation of these feature to the rest of the implemented features. Train your model on a binary classifier of your choice ("true user" or "false user" classification problem) using the following 4 scenarios in which you use a feature selection method to choose top 10 features. Describe this process. Use 10-fold cross validation to compute precision and recall in the following scenarios. Try to maximize F1 score when optimizing your classifier. Report F1 and any methods you used to optimize your classifier. i) 10 top features, ii) 10 top features & your features iii) 30 computed features, iv) 30 computed features & your features Qualitatively describe which family of features are most discriminating in your classifier.

6.	Merits of Entropy in Attack Detection/Diagnostics (30 points) Consider the following dataset: http://web.stanford.edu/class/cs259d/hw/server-log.txt ii) Two attacks happened this unfortunate day, both somewhere around 8am and 8pm noon. Please identify the exact date and time. What approach did the attackers use? iii) Columns for the server log are the following: iv) Start Start Src Dest Src Dest v) Date Time Duration Serv Port Port IP IP
7	There has been significant literature discussing how entropy can be used to detect these attacks. To do it effectively, approximation schemes are usually used. You do not have to implement these approximation techniques, but do present an analysis of whether entropy is useful and which combinations you tried, e.g. src ip, dest ip, src-port, dst-port, etc. Do any reveal anomalies when the two attacks happen? i) Sources for literature: ii) Lall, et all 2013. Data Streaming Algorithms for Estimating Entropy of Network Traffic. iii) Clifford, Cosma, 2013. A simple sketching algorithm for entropy estimation over streaming data
8	Supposedly, the best task for clustering is forensic analysis. The reasons, course, and consequences of an incident are obscure. It's required to classify all activities to find anomalies. Solutions to malware analysis (i.e., malware protection or secure email gateways) may implement it to separate legal files from outliers.
9	Another interesting area where clustering can be applied is user behavior analytics. In this instance, application users cluster together so that it is possible to see if they should belong to a particular group.

TEXT BOOKS:

1. Clarence Chio, David Freeman, "Machine Learning and Security", O'Reilly Media, Inc, 2018.

REFERENCE BOOKS:

1. Soma Halder , Sinan Ozdemir, "Machine Learning for Cybersecurity Cookbook", Packt publisher, 2018
2. Joshua Saxe and Hillary Sanders " Malware Data Science, Attack Detection and Attribution", No starch press publishers, 2018
3. The Cylance Data Science Team, " Introduction to Artificial Intelligence for Security Professionals", Apple Inc publishers, 2017
4. Sumeet Dua and Xian Du, " Data Mining and Machine Learning in Cybersecurity", 2011
5. "Machine Learning and Data Mining for Computer Security", Springer 2006
6. Network Anomaly Detection: A Machine Learning Perspective
7. Machine Learning for Hackers: Case Studies and Algorithms to Get You Started

Online Resources:

1. https://github.com/wtsxDev/Machine-Learning-for-Cyber-Security
2. https://github.com/jivoi/awesome-ml-for-cybersecurity#-books

JOURNALS/MAGAZINES

8. https://www.journals.elsevier.com/journal-of-information-security-and-applications
9. https://www.journals.elsevier.com/computers-and-security
3. Journal of big data, springer

SWAYAM/NPTEL/MOOCs:

7. https://iisc.talentsprint.com/deeplearning/?utm_source=googlesearch&utm_medium=tcpa&utm_campaign=ts-googlesearch-iisc-dl-tcpa-people-looking-for-training-programs-for-ai-and-deep-tech-deep-learning&utm_content=deep-learning-certification&utm_term=Deep%20learning%20certificate&gclid=Cj0KCQiApsiBBhCKARIsAN8o_4gcH-BYIAUHBTD27DFDoiCGFCkuG7eOi3wnLfXlXerEFWq06DtMRggaAtFkEALw
8. https://www.udemy.com/course/cybersecurity-data-science/
9. https://nptel.ac.in/courses/106/106/106106182/
10. https://www.edx.org/learn/python

Self-Learning Exercises:

3. More exploration on GIThub
4. Data Visualization packages

Course Title	Security Analytics				**Course Type**		**Integrated**	
Course Code	M21TF0203	**Credits**	**4**		**Class**		**IISemester**	
Course Structure	TLP	Credits	Contact Hours	Work Load	Total Number of Classes Per Semester		Assessment in Weightage	
	Theory	3	3	3				
	Practice	1	2	2	Theory	Practical	CIE	SEE
	-	-	-	-				
	Total	**4**	**5**	**5**	**39**	**26**	**50**	**50**

COURSE OVERVIEW

Security analytics is the process of using data collection, aggregation, and **analysis** tools for **security** monitoring and threat detection. Depending on the types of tools installed, **security analytics** solutions can incorporate large and diverse data sets into their detection algorithms.

COURSE OBJECTIVE (S):

The objectives of this course are to:

1. Understanding basics of IAM
2. Able to understand cloud Resources
3. Understanding basics of IAM Covering ML Modelling around use cases.
4. Knowledge on use cases using Tensor flow/Python and Pyspark.

COURSE OUTCOMES (COs)

After the completion of the course, the student will be able to:

CO#	Course Outcomes	POs	PSOs
CO1	Must be able to run the programming and data structures required for data analysis with Python	1 ,3, 8, 9	1
CO2	Identify Source of Data and how to capture Test and Training Sets from the data.	1 , 3, 5	2
CO3	Develop important ML models to predict intrusion detection and User behavior analysis	1 ,3,5, 9,12	2
CO4	Describe end user behavior model	1 ,3,5, 9,12	3
CO5	Assess insider threat model for an attack	1 ,3,5, 9,12	3
CO6	Build ML model for creating data lake	1 ,3,5, 9,12	3

BLOOM'S LEVEL OF THE COURSE OUTCOMES

CO#	Bloom's Level					
	Remember (L1)	Understand (L2)	Apply (L3)	Analyze (L4)	Evaluate (L5)	Create (L6)
CO1			√			
CO2	√	√	√	√		
CO3		√	√	√		
CO4		√	√			
CO5					√	√
CO6					√	√

COURSE ARTICULATION MATRIX

CO#/ POs	**PO1**	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**	**PSO1**	**PSO2**	**PSO3**
CO1	3	1	1	2				1	1			1	2		
CO2	3	2	3		2				1			1		2	
CO3	3	1	2	1	2				1			1		3	
CO4	3		2	1	2				1			1			3

CO5	3		2		2				1			1			3
CO6	3		2		2				1			1			3

Note: 1-Low, 2-Medium, 3-High

COURSE CONTENT

THEORY:

UNIT – 1

Primitive data structures – (constants, variable, data types), Advanced data structures –(list, tuples, dictionary), selection logic, looping logic, functions/methods, file handling Pandas – object model – data loading-exploration – visualization – sampling – data manipulation Project – Network Intrusion Detection System (IDS) data analysis.

UNIT – 2

Data Sources – Network via Access Logs and IPS IDS Training Set and Test Set creation, Install Tensor flow and start creating a model via Python.

UNIT – 3

Build ML models using Tensor flow and python for user behavioral analysis Bot Analysis End User behavior monitoring.

UNIT – 4

Build ML models using Tensor flow and python for, Data Exfiltration, Insider Threats, Threat Hunting Basics, Creating your Data Lake.

LEARNING RESOURCES:

1. Security Analytics For Dummies Securonix Special Edition

2. Machine Learning Approaches In Cyber Security Analytics; Springer; Tony Thomas, Athira P Vijayaraghavan, Sabu Emmanuel

JOURNALS/MAGAZINES:

1. https://ieeexplore.ieee.org/document/6725337
2. https://ieeexplore.ieee.org/document/8258128

SWAYAM/NPTEL/MOOCs:

1. Security analytics | Coursera

2. Security analytics tools | Coursera

Self-Learning Exercises:

5. Explore primitive data structures
6. More exploration on Security challenges
7. Explore on Network Intrusion Detection System (IDS) data analysis

Lab Components:

1. Install Tensor flow and start creating a model via Python.

2. Build ML models using Tensorflow.

<table>
<tr><td>Course Title</td><td colspan="3">Firewall & UTM architecture</td><td colspan="2">Course Type</td><td colspan="2">Softcore</td></tr>
<tr><td>Course Code</td><td>M21TFS204</td><td>Credits</td><td colspan="2">3</td><td colspan="2">Class</td><td colspan="2">II Semester</td></tr>
<tr><td rowspan="6">Course Structure</td><td>TLP</td><td>Credits</td><td>Contact Hours</td><td>Work Load</td><td colspan="2" rowspan="2">Total Number of Classes Per Semester</td><td colspan="2" rowspan="2">Assessment in Weightage</td></tr>
<tr><td>Theory</td><td>3</td><td>3</td><td>3</td></tr>
<tr><td>Practice</td><td>0</td><td>0</td><td>0</td><td rowspan="2">Theory</td><td rowspan="2">Practical</td><td rowspan="2">CIE</td><td rowspan="2">SEE</td></tr>
<tr><td>-</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td>Total</td><td>3</td><td>3</td><td>3</td><td>36</td><td></td><td>50</td><td>50</td></tr>
</table>

COURSE OVERVIEW

For every class of security problem, there is almost certainly either an open source or proprietary solution designed to combat it. This is particularly true in the areas of network intrusion detection systems and network access control devices—firewalls, filtering routers, and the like. A trend in firewall technology is to combine application layer inspection techniques from the intrusion detection world with the ability to filter network traffic, something firewalls have been doing for a long time. It is the goal of this subject to show that the iptables firewall on Linux systems is well positioned to take advantage of this trend, especially when it is combined with some additional software designed to leverage iptables from an intrusion detection standpoint.

COURSE OBJECTIVE (S):

The objectives of this course are to:

1. Gain expertise in Designing secure firewall protected networks.
2. Inculcate knowledge of types of firewalls and how filtering is done..
3. Gain expertise in Evaluating firewalls.
4. Implement UTM architecture and configure firewalls.

COURSE OUTCOMES (COs)

After the completion of the course, the student will be able to:

CO#	Course Outcomes	POs	PSOs
CO1	Make use of opensource platform to secure firewall.	1 to 4, 8, 9 , 12	1
CO2	Compare different firewalls and will be able to apply filtering.	1 to 3, 5,9,12	1
CO3	Design and develop a open source firewall and evaluate it.	1 to 5, 9, 12	2
CO4	Create UTM architecture and configure based on requirements.	1,4,5,9,12	1
CO5	Demonstrate UTM security concepts	1,4,5,9,12	3
CO6	Appraise UTM firewall rules	1,4,5,9,12	3

BLOOM'S LEVEL OF THE COURSE OUTCOMES

CO#	Bloom's Level					
	Remember (L1)	Understand (L2)	Apply (L3)	Analyze (L4)	Evaluate (L5)	Create (L6)
CO1			√			
CO2			√			
CO3			√	√		
CO4					√	√
CO5				√	√	
CO6				√	√	

COURSE ARTICULATION MATRIX

CO#/ POs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	1	1	2				1	1			1	3		
CO2	3	2	3		2				1			1	2		
CO3	3	1	2	1	2				1			1		3	
CO4	3			2	2				1			1	3		
CO5	3			2	2				1			1			3
CO6	3			2	2				1			1			3

Note: 1-Low, 2-Medium, 3-High

COURSE CONTENT

THEORY:

UNIT – 1

Firewall Fundamentals: What is firewall, why do you need firewall, How firewalls work, Types of firewalls, Individual and SOHO firewall Options, Uses for Host Software Firewall, Next Generation Firewalls, Types of Filtering, Selecting right firewall for your needs , the difference between buying firewall and building a firewall.

UNIT – 2

Firewall implementation: examining your network and it's security needs, proper firewall implementation procedure, constructing, configuring, and managing a firewall, PF sense requirements, planning a firewall implementation with PF sense, installing the be up since firewall configuring a firewall with PF sense .

UNIT – 3

Firewall deployment considerations: common security strategies for firewall deployment's, authentication authorization and accounting, placement of network hardware firewalls, benefit and purpose of rivers proxy use and benefit of port forwarding.

Configuring firewalls, firewall rules, composing firewall rules, ordering firewall rules, what should you allow and what should you block , Essential elements of firewall policy limitations of firewalls improving performance,

UNIT – 4

UTM Architecture Sophos: basic UTM security concepts, getting to basic SOPHOS UTM configuration, installing SOPHOS UTM VM, basic system settings configuration, interfaces basic configuration, network definition configuration, DNS configuration, SOPHOS with OSP F routing protocol, Sophos UTM with firewall rules.

TEXT BOOKS:

3. Network Security, Firewalls And VPNs, J. Michael Stewart, Jones & Bartlett Learning, 2013, ISBN-10: 1284031675, ISBN-13: 978-1284031676.
4. Unified Threat Management For Dummies®, 2nd Fortinet Special Edition, Published by John Wiley & Sons, Inc.

REFERENCE BOOKS:

1. Network Security: Private Communications in a Public World, M. Speciner, R. Perlman, C. Kaufman, Prentice Hall, 2002.
2. Linux iptables Pocket Reference, Gregor N. Purdy, O'Reilly, 2004, ISBN-13: 978-0596005696.
3. Linux Firewalls, by Michael Rash, No Starch Press, October 2007, ISBN: 978-1-59327-141-1.
4. The Network Security Test Lab: A Step-By-Step Guide, Michael Gregg, Dreamtech Press, 2015, ISBN-10:8126558148, ISBN-13: 978-8126558148.

<table>
<tr><td>Course Title</td><td colspan="3">Malware Analysis and Design</td><td colspan="2">Course Type</td><td colspan="2">Integrated</td></tr>
<tr><td>Course Code</td><td>M21TFS205</td><td>Credits</td><td>3</td><td colspan="2">Class</td><td colspan="2">II Semester</td></tr>
<tr><td rowspan="5">Course Structure</td><td>TLP</td><td>Credits</td><td>Contact Hours</td><td>Work Load</td><td colspan="2" rowspan="2">Total Number of Classes Per Semester</td><td colspan="2" rowspan="2">Assessment in Weightage</td></tr>
<tr><td>Theory</td><td>3</td><td>3</td><td>3</td></tr>
<tr><td>Practice</td><td>0</td><td>0</td><td>0</td><td>Theory</td><td>Practical</td><td>CIE</td><td>SEE</td></tr>
<tr><td>-</td><td>-</td><td>-</td><td>-</td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td></tr>
<tr><td>Total</td><td>3</td><td>3</td><td>3</td><td>39</td><td>0</td><td>50</td><td>50</td></tr>
</table>

COURSE OVERVIEW

Malware analysis is the art of dissecting malware to understand how it works, how to identify it, and how to defeat or eliminate it. And you don't need to be an uber-hacker to perform malware analysis. Malware analysis is critical for anyone who responds to computer security incidents. And, with a shortage of malware analysis professionals, the skilled malware analyst is in serious demand. The course aims to give insights about Introduction to Malware Analysis, Data collection methods, windows basics. Dynamic malware analysis, basic static analysis, android malware analysis and recent trends.

COURSE OBJECTIVE (S):

The objectives of this course are to:

1. Explain the types of malware through analysis methods
2. Illustrate basics and advanced malware analysis techniques
3. Demonstrate the android malware analysis techniques for real world applications
4. Illustrate the various tools of malware analysis

COURSE OUTCOMES (COs)

After the completion of the course, the student will be able to:

CO#	Course Outcomes	POs	PSOs
CO1	Identify various malwares and understand the behavior of malwares in real world applications.	1 to 4, 8, 9 , 12	1
CO2	Implement different malware analysis techniques.	1 to 3, 5,9,12	1
CO3	Analyze the malware behavior in windows and android.	1 to 5, 9, 12	2
CO4	Identify the various tools for malware analysis.	1,4,5,9,12	1
CO5	Illustrate File System and Directory structure and Registry	1,4,5,9,12	3
CO6	Demonstrate masterkey vulnerability structure	1,4,5,9,12	3

BLOOM'S LEVEL OF THE COURSE OUTCOMES

CO#	Bloom's Level					
	Remember (L1)	Understand (L2)	Apply (L3)	Analyze (L4)	Evaluate (L5)	Create (L6)
CO1			√			
CO2			√			
CO3			√	√		
CO4					√	√
CO5					√	√
CO6					√	√

COURSE ARTICULATION MATRIX

CO#/ POs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	1	1	2				1	1			1	3		
CO2	3	2	3		2				1			1	2		
CO3	3	1	2	1	2				1			1		3	
CO4	3			2	2				1			1	3		
CO5	3			1	2				1			1			3
CO6	3			2	2				1			1			3

Note: 1-Low, 2-Medium, 3-High

COURSE CONTENT

THEORY:

UNIT – 1

Introduction: Malware Analysis Goals of Malware Analysis, Techniques Static and Dynamic Analysis, Types of Malware Backdoor, Botnet, Downloader, Information Stealing malware, Launcher, Rootkit, Scareware, Worm or Virus.

Data Collection Methods: Volatile Data Collection Methodology-Preservation of Volatile Data, Physical Memory Acquisition on a Live Windows System, Identifying Users Logged into the System, Non-Volatile Data Collection Inspect Prefetch Files, Examine the File System, Remote Registry Analysis, Examine Web Browsing Activities, Examine Cookie Files.

UNIT – 2

Windows Basics: Introduction to Windows Malware - Windows Basics Relevant to Malware Behavior-File System and Directory structure, Registry, Boot Sequence, Malware payloads.

Dynamic Malware Analysis: Malware activities, Self-Start techniques, Essential setup for executing malware, Executing DLL files, Classifying Malware Based on their Behavior

UNIT – 3

Basic Static Analysis: Number System Static Analysis with File Attributes and PE Header Packet Identification

Advanced Static Analysis Reverse Engineering: Advanced Static Analysis Reverse Engineering Assembly level computing Standard x86 instructions, Introduction to IDA, OllyDbg, Advanced Malware Analysis Virus, Trojan. Parsing Basic Analysis of an APK.

UNIT – 4

Android Malware Analysis: APK File Structure Security Model Android Root Brief Description of Spreading and Dis- tribution Introduction to Android Debugging Tools and Their Usage Dex Structure Parsing Basic Analysis of an APK. Exploits MasterKey VulnerabilityFileNameLength Vulnerability Introduction to Obfuscation DEX code obfuscation. Recent Trends.

TEXT BOOKS:

5. Cameron H. Malin, Eoghan Casey, James M. Aquilina and Curtis W. Rose, Malware Forensics Field Guide for Windows Systems, Syngress, Elsevier, 2012.
6. Christopher C. Elisan , Advanced Malware Analysis, Tata McGraw Hill, 2015 3.Cameron H. Malin, Eoghan Casey, James M. Aquilina and Curtis W. Rose, Malware

REFERENCE BOOKS:

1. Cameron H. Malin, Eoghan Casey, James M. Aquilina and Curtis W. Rose, Malware Forensics Field Guide for Linux Systems, Syngress, Elsevier, 2014.
2. Ken Dunham, Saeed Abu-Nimeh, Michael Becher and Seth Fogie, Mobile Malware Attacks and Defense, Syngress, Elsevier, 2009
3. John Aycock, Computer Viruses and Malware, Springer, 2006.
4. ErciFiliol, Computer Viruses: from theory to applications, Springer, 2005

JOURNALS/MAGAZINES

5. Abhinav Singh, Metasploit Penetration Testing Cookbook, PACKT Publishing, 2012. ISBN 978-1-84951-742-3
6. Ken Dunham, Mobile Malware Attacks and Defence, Syngress Publisher 2009. ISBN: 978-1-59749-298-0

SWAYAM/NPTEL/MOOCs:

1. Anti-Virus/Anti-Malware - Detection and Prevention tools | Coursera
2. Malware Continued - Understanding Security Threats | Coursera
3. Malware and Ransomware - A brief overview of types of actors and their motives | Coursera

Self-Learning Exercises:

1. Set up of Kali Linux in a Virtual machine and setup with DNS info and collection of local network
2. Scan the network for Windows XP and Windows 7 Target machines in local network and virtual network
3. Identify the open ports and firewall rules setup

Course Title	Web Security				Course Type		Soft Core	
Course Code	M21TFS206	Credits	3		Class		II Semester	
Course Structure	TLP	Credits	Contact Hours	Work Load	Total Number of Classes Per Semester		Assessment in Weightage	
	Theory	3	3	3				
	Practice	0	0	0	Theory	Practical	CIE	SEE
	-	-	-	-				
	Total	**3**	**3**	**0**	**39**	**0**	**50**	**50**

COURSE OVERVIEW

Web is the platform of choice for writing complex, interactive applications such as from mail clients to image editors to computer games and a medium reaching hundreds of millions of casual users around the globe. The resulting issues have quickly emerged as some of the most significant and prevalent threats to data security today. It provides a systematic and thorough analysis of the current state of affairs in the world of web application security, it aims to shed light on the uniqueness of the security challenges for web security engineers, web developers, and users have to face every day.

COURSE OBJECTIVE (S):

The objectives of this course are to:

1. Outline common web application security vulnerabilities.
2. Identify different web application design assumptions and threats.
3. Discover the capabilities of various Browser scripts and proxies.
4. Illustrate to detect Authentication and Session Vulnerabilities

COURSE OUTCOMES (COs)

After the completion of the course, the student will be able to:

CO#	Course Outcomes	POs	PSOs
CO1	Identify underlying security principles of the web.	1,2,5	1
CO2	Outline the different concrete threats against web applications	1	2
CO3	Examine common web application attacks and countermeasures	1	2
CO4	Interpret the current best practices for secure web applications	1,2, 5	1
CO5	Categorize extrinsic site priviledges	1,2,3,4,5	3

CO6	Analyze Security Model Extension Frameworks and Security Model Restriction Frameworks	1,2,3,4,5	3

BLOOM'S LEVEL OF THE COURSE OUTCOMES

CO#	Bloom's Level					
	Remember (L1)	Understand (L2)	Apply (L3)	Analyze (L4)	Evaluate (L5)	Create (L6)
CO1			√			
CO2		√				
CO3				√		
CO4		√				
CO5					√	
CO6					√	

COURSE ARTICULATION MATRIX

CO#/ POs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	3			1								1		
CO2	2													2	
CO3	3													1	
CO4	2	2			1								1		
CO5	2	3	3	2	1										3
CO6	2	3	3	2	1										3

Note: 1-Low, 2-Medium, 3-High

COURSE CONTENT

THEORY:

UNIT – 1

Security in the World of Web Applications: Information Security in a Nutshell, a Brief History of the Web, the Evolution of a Threat.

It Starts With A URL: Uniform Resource Locator Structure, Reserved Characters and Percent Encoding, Common URL Schemes and Their Function, Resolution of Relative URLs, Security Engineering Cheat Sheet.

Hypertext Transfer Protocol: Basic Syntax of HTTP Traffic, HTTP Request Types, Server Response Codes, Keepalive Sessions, Chunked Data Transfers, Caching Behavior, HTTP Cookie Semantics, HTTP Authentication, Protocol-Level Encryption and Client Certificates.

UNIT – 2

Hypertext Markup Language: Basic Concepts Behind HTML Documents, Understanding HTML Parser Behavior, Entity Encoding, HTTP/HTML Integration Semantics, Hyperlinking and Content Inclusion.

C**ascading Style Sheets:** Basic CSS Syntax, Parser Resynchronization Risks, Character Encoding.

Browser-Side Scripts: Basic Characteristics of JavaScript, Standard Object Hierarchy, Script Character Encoding, Code Inclusion Modes and Nesting Risks, The Living Dead: Visual Basic.

Non-Html Document Types: Plaintext Files, Bitmap Images, Audio and Video, XML-Based Documents, A Note on Nonrenderable File Types.

UNIT – 3

Content Rendering With Browser Plug-Ins: Invoking a Plug-in, Document Rendering Helpers, Plug-in-Based Application Frameworks, ActiveX Controls, Living with Other Plug-ins.

Content Isolation Logic: Same-Origin Policy for the Document Object Model, Same-Origin Policy for XML Http Request, Same-Origin Policy for Web Storage, Security Policy for Cookies, Plug-in Security Rules, Coping with Ambiguous or Unexpected Origins.

Life outside Same-Origin Rules: Window and Frame Interactions, Cross-Domain Content Inclusion, Privacy-Related Side Channels, Other SOP Loopholes and Their Uses.

Other Security Boundaries: Navigation to Sensitive Schemes, Access to Internal Networks, Prohibited Ports, Limitations on Third-Party Cookies.

UNIT – 4

Content Recognition Mechanisms: Document Type Detection Logic, Character Set Handling.

Dealing with Rogue Scripts: Denial-of-Service Attacks, Window-Positioning and Appearance Problems, Timing Attacks on User Interfaces.

Extrinsic Site Privileges: Browser- and Plug-in-Managed Site Permissions, Form-Based Password Managers, Internet Explorer's Zone Model.

New and Upcoming Security Features: Security Model Extension Frameworks, Security Model Restriction Frameworks, Other Developments.

TEXT BOOKS:

1. Michal Zalewski, "The Tangled Web: A Guide to Securing Modern Web Applications", No Starch Press, 2011.

REFERENCE BOOKS:

1. Dafydd Stuttard, Marcus Pinto," The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws", Wiley publications, 2008.
2. O'Reilly, "Web Security, Privacy & Commerce", 2nd Edition, O'Reilly Media, Inc, 2001.

JOURNALS/MAGAZINES

1. https://ieeexplore.ieee.org/abstract/document/8342469
2. https://link.springer.com/referenceworkentry/10.1007/978-1-4419-5906-5_1235
3. https://link.springer.com/book/10.1007/978-3-319-12226-7

SWAYAM/NPTEL/MOOCs:

11. https://www.coursera.org/projects/web-application-security-testing-with-owsap-zap
12. https://www.coursera.org/projects/web-application-security-testing-burp-suite
13. https://www.coursera.org/learn/ibm-cybersecurity-analyst-assessment

Self-Learning Exercises:

8. origin inheritance
9. Other Browser Mechanisms
10. Common Web Vulnerabilities

<table>
<tr><td>Course Title</td><td colspan="4">Secure Communications</td><td colspan="2">Course Type</td><td colspan="2">Integrated</td></tr>
<tr><td>Course Code</td><td>M21TFS207</td><td>Credits</td><td colspan="2">3</td><td colspan="2">Class</td><td colspan="2">II Semester</td></tr>
<tr><td rowspan="5">Course Structure</td><td>TLP</td><td>Credits</td><td>Contact Hours</td><td>Work Load</td><td colspan="2" rowspan="2">Total Number of Classes Per Semester</td><td colspan="2" rowspan="2">Assessment in Weightage</td></tr>
<tr><td>Theory</td><td>3</td><td>3</td><td>3</td></tr>
<tr><td>Practice</td><td>0</td><td>0</td><td>0</td><td rowspan="2">Theory</td><td rowspan="2">Practical</td><td rowspan="2">CIE</td><td rowspan="2">SEE</td></tr>
<tr><td>-</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td>Total</td><td>3</td><td>3</td><td>3</td><td>39</td><td>0</td><td>50%</td><td>50%</td></tr>
</table>

COURSE OVERVIEW

Secure communication is when two entities are communicating and do not want a third party to listen in. In order for this to be the case, entities need to communicate in a way unsusception to eavesdropping or interception. Secure communication includes means by which people can share information with varying degrees of certainty that third parties cannot intercept what is said. Other than spoken face-to-face communication with no possible eavesdropper, it is probably safe to say that no communication is guaranteed

to be secure in this sense, although practical obstacles such as legislation, resources, technical issues (interception and encryption), and the sheer volume of communication serve to limit surveillance.

With many communications taking place over long distance and mediated by technology, and increasing awareness of the importance of interception issues, technology and its compromise are at the heart of this debate. For this reason, this article focuses on communications mediated or intercepted by technology.

COURSE OBJECTIVE (S):

The objectives of this course are to:

1. Understand the importance and goals of communication network and information security and introduce him to the different types of attacks.
2. Expose the different approaches to handling security and the algorithms in use for maintaining data integrity and authenticity.
3. Enable to appreciate the practical aspects of security features design and their implementation in wired and wireless internetworking domains.

COURSE OUTCOMES (COs)

After the completion of the course, the student will be able to:

CO#	Course Outcomes	POs	PSOs
CO1	Demonstrate an understanding of the ways in which communication network security may get compromised and the basic principles of security algorithm design.	1,2,3,4	1,2
CO2	Exposed to the different approaches that handle security and the algorithms in use for maintaining data integrity and authenticity.	1,2,3,4	1,2
CO3	Implement and analyze the different algorithms and compare their performances.	1,2,3,4	1,2
CO4	Apply his knowledge for designing or modifying existing algorithms and implementing them at least by simulation.	1,2,3,4	1,2
CO5	Illustrate key management technique in RSA algorithm	1,2,3,5	1,2
CO6	Demonstrate password management techniques	1,2,3,5	1,2

BLOOM'S LEVEL OF THE COURSE OUTCOMES

CO#	Bloom's Level					
	Remember (L1)	Understand (L2)	Apply (L3)	Analyze (L4)	Evaluate (L5)	Create (L6)
CO1	√	√	√			
CO2	√		√	√		
CO3			√	√	√	
CO4			√	√		
CO5				√	√	
CO6				√	√	

COURSE ARTICULATION MATRIX

CO#/ POs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	3	3	1									3	2	
CO2	2	3	3	2									3	2	
CO3	3	3	2	2									3	2	
CO4	3	3	2	2									3	2	
CO5	3	3	2		2								3	2	
CO6	3	3	2		2								3	2	

Note: 1-Low, 2-Medium, 3-High

COURSE CONTENT

THEORY:

UNIT – 1

Introduction on security, security goals and types of attacks: Passive attack, active attack, attacks on confidentiality, attacks on integrity and availability, Security services and mechanisms.

Modular arithmetic: Groups, Ring, Fields. The Euclidean algorithm, Finite fields of the form GF(p)

UNIT – 2

Polynomial arithmetic: Finite fields of the form GF (2n).

Symmetric Ciphers, Symmetric Cipher Model, Substitution Techniques, Caesar Cipher, Mono alphabetic Cipher, Play fair cipher, Hill cipher, Poly alphabetic Cipher, one time pad

UNIT – 3

Transposition techniques, Block Ciphers, Data encryption Standards, DES Encryption, DES decryption, Differential and Linear Crypt analysis Advanced Encryption standard, The AES Cipher, substitute bytes transformation, Shift row transformation, Mix Column transformation.

Public key cryptosystem, Application for Public key cryptosystem requirements

UNIT – 4

RSA algorithm, Key management, Distribution of public key, public key certificates, Distribution of secret keys.

Intruders: Intrusion techniques, Intrusion detection, Statistical anomaly detection, Rule based intrusion detection, Distributed intrusion detection, Honey pot, Intrusion detection exchange format.

Password management: Password protection, password selection strategies.

TEXT BOOKS:

7. Behrouz A. Forouzan , “Cryptography and Network security” Tata McGraw-Hill, 3rd Edition, 2015
8. William Stallings, “Cryptography and Network security: principles and practice", 7th Edition, Prentice Hall of India, New Delhi, 2017

REFERENCE BOOKS:

7. David S. Dummit & Richard M Foote, "Abstract Algebra", 3rd Edition, Wiley India Pvt. Ltd., 2011.
8. Douglas A. Stinson, "Cryptography, Theory and Practice", 2/e, Chapman & Hall, CRC Press Company, Washington, 4th Edition, 2019.
9. Lawrence C. Washington, "Elliptic Curves: Theory and Cryptography", Chapman & Hall, CRC Press Company, Washington, 2008.
10. N. Koeblitz: "A course in Number theory and Cryptography", 2008.
11. Thomas Koshy:" Elementary Number Theory with Applications", 2/e, Academic Press, 2007
12. Tyagi and Yadav , "Cryptography and network security", Dhanpatrai, 2012

JOURNALS/MAGAZINES

1. https://ieeexplore.ieee.org/document/809184
2. https://ieeexplore.ieee.org/document/1221784
3. https://www.journals.elsevier.com/computers-and-security
4. https://www.springer.com/journal/10207

SWAYAM/NPTEL/MOOCs:

14. https://nptel.ac.in/courses/106/105/106105082/
15. https://onlinecourses.swayam2.ac.in/nou19_cs08/preview
16. Coursera – Cryptography, University of MaryLand

<table>
<tr><td>Course Title</td><td colspan="3">Penetration testing & incident response</td><td colspan="2">Course Type</td><td colspan="2">SC</td></tr>
<tr><td>Course Code</td><td>M21TFS208</td><td>Credits</td><td colspan="2">3</td><td colspan="2">Class</td><td colspan="2">II Semester</td></tr>
<tr><td rowspan="5">Course Structure</td><td>TLP</td><td>Credits</td><td>Contact Hours</td><td>Work Load</td><td colspan="2" rowspan="2">Total Number of Classes Per Semester</td><td colspan="2" rowspan="2">Assessment in Weightage</td></tr>
<tr><td>Theory</td><td>3</td><td>3</td><td>3</td></tr>
<tr><td>Practice</td><td>0</td><td>0</td><td>0</td><td rowspan="2">Theory</td><td rowspan="2">Practical</td><td rowspan="2">CIE</td><td rowspan="2">SEE</td></tr>
<tr><td>-</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td>Total</td><td>3</td><td>3</td><td>3</td><td>39</td><td>0</td><td>50</td><td>50</td></tr>
</table>

COURSE OVERVIEW

This course gives background needed to gain Cybersecurity skills, students will learn about the different phases of penetration testing, how to gather data for penetration test and popular penetration testing tools. Furthermore, they will also learn the phases of an incident response, important documentation to collect, and the components of an incident response policy and team.

This course is intended for anyone who wants to gain a basic understanding of cybersecurity.

COURSE OBJECTIVE (S):

The objectives of this course are to:

1. Explain the fundamental concepts of penetration testing and the different steps involved.

2. Inculcate the knowledge of different phases in penetration testing and ethical hacking.
3. Introduce the concept of incident and incident management.
4. Introduce different types of cyberattacks, and develop understanding of cyber forensics.

COURSEOUTCOMES(COs)

After the completion of the course, the student will be able to:

CO#	Course Outcomes	POs	PSOs
CO1	Understanding of fundamental concepts of penetration testing and the different steps involved	1,2,5	1
CO2	Students would have the knowledge of different phases in penetration testing and ethical hacking.	1,4,6	1
CO3	Understanding of incident and incident management.	2,3,8	2
CO4	Understanding of different types of cyberattacks and cyber forensics	1,4,5,9	1
CO5	Analyze Disk and Network forensics and Log analysis	1,4,5,9	3
CO6	Demonstrate Malware identification and Analysis, Lateral Movement and Side Channel Attack Analysis	1,4,5,9	3

BLOOM'S LEVELOF THECOURSE OUTCOMES

CO#	Bloom's Level					
	Remember (L1)	Understand (L2)	Apply (L3)	Analyze (L4)	Evaluate (L5)	Create (L6)
CO1			√			
CO2			√			
CO3			√	√		
CO4	√	√				
CO5				√	√	
CO6				√	√	

COURSE ARTICULATION MATRIX

CO#/ POs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	1	1	2				1	1			1	3		

CO2	3	2	3		2				1			1	3		
CO3	3	1	2	1	2				1			1		2	
CO4	3			2	2				1			1	3		
CO5	3			2	2				1						3
CO6	3			2	2				1						3

Note:1-Low,2-Medium,3-High

COURSE CONTENT

THEORY:

UNIT – 1

Introduction to penetration testing, Scope, roles and responsibilities of a penetration tester, Scoping and Exclusions in a Penetration Testing Assignment, Steps of Penetration Testing, Threat Modeling, Using Kali Linux as Penetration testing Tool kit, Web penetration Testing, OWASP top10, network penetration Testing, Network Penetration Testing, Application penetration Testing

UNIT – 2

Penetration Testing phases/Testing Process, types and Techniques, Blue/Red Teaming, Strategies of Testing, Non Disclosure Agreement Checklist, Phases of hacking, Open-source/proprietary Pentest Methodologies

UNIT – 3

Introduction to Incident - Incident Response Methodology – Steps - Activities in Initial Response Phase after detection of an incident.

UNIT – 4

Indicators of Compromise, Attack Motivations and Attack Methods, Profiling an Adversary, Incident readiness- Tools, Techniques and Procedure, Triaging tools, Memory, Disk and Network forensics and Log analysis, Malware identification and Analysis, Lateral Movement and Side Channel Attack Analysis, Lessons Learnt, Mitigation Efforts

TEXTBOOKS:

9. Kali Linux Wireless Penetration Testing Beginner's Guide by Vivek Ramachandran, Cameron Buchanan, 2015 Packt Publishing
10. Travis E. Oliphant, “Guide to NumPy”, Trelgol publishers,2006.

11. Kevin Mandia, Chris Prosise, “Incident Response and computer forensics”, Tata McGrawHill,2006.

REFERENCEBOOKS:

13. Kali Linux 2: Windows Penetration Testing, By Wolf Halton, Bo Weaver , June 2016 Packt Publishing
14. Mastering Modern Web Penetration Testing By Prakhar Prasad, October 2016 Packt Publishing.
15.

JOURNALS/MAGAZINES

10. https://www.springer.com/de/book/9781484218563
11. http://courses.ncirl.ie/index.cfm/page/module/moduleId/68126
12. https://site.ieee.org/spokane/2017/01/23/cyber-security-incident-response-february-16-2017-2/
13. https://journal-bcs.springeropen.com/articles/10.1186/s13173-017-0051-1

SWAYAM/NPTEL/MOOCs:

17. https://www.classcentral.com/course/ibm-penetration-testing-incident-response-forensi-20194
18. https://www.coursera.org/learn/ibm-penetration-testing-incident-response-forensics
19. https://www.coursera.org/lecture/ibm-penetration-testing-incident-response-forensics/penetration-testing-discovery-oS1qL

Self-LearningExercises:

11. http://www.cyberforensics.in/?AspxAutoDetectCookieSupport=1
12. https://www.cdac.in/index.aspx?id=cyber_security

Course Title	**Mobile and Wireless Security**				**Course Type**		**Softcore**	
Course Code	M21TFS209	**Credits**	**3**		**Class**		**II Semester**	
Course Structure	TLP	Credits	Contact Hours	Work Load	Total Number of Classes Per Semester		Assessment in Weightage	
	Theory	3	3	3				
	Practice	0	0	0	Theory	Practical	CIE	SEE
	-	-	-	-				
	Total	**3**	**3**	**3**	**39**	**0**	**50**	**50**

COURSE OVERVIEW

Wireless security is the prevention of unauthorized access or damage to computers or data using wireless networks, which include Wi-Fi networks. The most common type is Wi-Fi security, which includes Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). Mobile security is the protection of smartphones, tablets, laptops and other portable computing devices and the networks they connect to, from threats and vulnerabilities associated with wireless computing.

COURSE OBJECTIVE (S):

The objectives of this course are to:

1. Explain network security protocols.
2. Gain knowledge about Wireless Network and Security.
3. Shed light on Mobile Networks and security.
4. Gain insights into Mobile Application Security.

COURSE OUTCOMES (COs)

After the completion of the course, the student will be able to:

CO#	Course Outcomes	POs	PSOs
CO1	Summarize concepts of Network Security and Security in Wireless Networks.	1 to 4, 8, 9 , 12	1
CO2	Illustrate the concepts of Wireless Network Security.	1 to 3, 5,9,12	1
CO3	Use to solve problems in Mobile Network Security.	1 to 5, 9, 12	2
CO4	Develop security systems for Mobile application.	1,4,5,9,12	1
CO5	Demonstrate Android security model	1,4,5,9,12	3
Co6	Illustrate Mobile Geolocation and Mobile Web Security models	1,4,5,9,12	3

BLOOM'S LEVEL OF THE COURSE OUTCOMES

CO#	Bloom's Level					
	Remember (L1)	Understand (L2)	Apply (L3)	Analyze (L4)	Evaluate (L5)	Create (L6)
CO1	√					
CO2	√	√				
CO3			√	√		

CO4			√	√		
CO5				√	√	
Co6				√	√	

COURSE ARTICULATION MATRIX

CO#/ POs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	1	1	2				1	1			1	3		
CO2	3	2	3		2				1			1	2		
CO3	3	1	2	1	2				1			1		3	
CO4	3			2	2				1			1	3		
CO5	3			2	2				1			1			3
Co6	3			2	2				1			1			3

Note: 1-Low, 2-Medium, 3-High

COURSE CONTENT

THEORY:

UNIT – 1

Network Security: Network Security Protocols, Security and Layered Architecture, Voice-Oriented Wireless Networks, Data-Oriented Wireless Networks.

UNIT – 2

Wireless Network Security: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Robust Secure Network (RSN) and Virtual Private Network (VPN).

UNIT – 3

Mobile Security: Security of GSM Networks, Security of UMTS Networks, LTE Security, Wi-Fi and Bluetooth Security, SIM/UICC Security.

UNIT – 4

Mobile Malware and App Security: Android Security Model, IOS Security Model, Security Model of the Windows Phone, SMS/MMS, Mobile Geolocation and Mobile Web Security, Security of Mobile VoIP Communications, Emerging Trends in Mobile Security.

TEXT BOOKS:

1. **Sunilkumar S. Manvi and Mahabaleshwar S. Kakkasageri,"**Wireless and Mobile Networks", Concepts and Protocols, 2nd Ed. Wiley Publications, 2010. (Unit 3).

2. **Man Ho Au and Kim-Kwang Raymond Choo**, "Mobile Security and Privacy", Syngress publications, 2016.
3. **Himanshu Dwivedi, Chris Clark and David Theil**, "Mobile Application Security", Tata McGraw-Hill Publication, 2010.

REFERENCE BOOKS:

16. Steven Furnell, "Mobile Security – A Packet Guide", IT Governance Publications, 2009.
17. Noureddine Boudriga, "Security of Mobile Communications", CRC Press Publications, 2009.
18. N Asokan, Lucas Davi, "Mobile Platform Security", M & C Publishers, 2014.

JOURNALS/MAGAZINES

14. https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=7742
15. http://www.ieee-security.org/TC/SPW2017/MoST/

SWAYAM/NPTEL/MOOCs:

20. https://www.coursera.org/learn/network-security-database-vulnerabilities
21. **https://www.coursera.org/learn/smart-device-mobile-emerging-technologies**

Self-Learning Exercises:

13. Web Security
14. Firewall
15. DoS Attack
16. Email Security

<table>
<tr><td>Course Title</td><td colspan="3">Forensics and VAPT Lab</td><td colspan="2">Course Type</td><td colspan="2">Integrated</td></tr>
<tr><td>Course Code</td><td>M21TF0206</td><td>Credits</td><td colspan="2">2</td><td colspan="2">Class</td><td colspan="2">II Semester</td></tr>
<tr><td rowspan="6">Course Structure</td><td>TLP</td><td>Credits</td><td>Contact Hours</td><td>Work Load</td><td colspan="2" rowspan="2">Total Number of Classes Per Semester</td><td colspan="2" rowspan="2">Assessment in Weightage</td></tr>
<tr><td>Theory</td><td>0</td><td>0</td><td>0</td></tr>
<tr><td>Practice</td><td>2</td><td>2</td><td>2</td><td rowspan="2">Theory</td><td rowspan="2">Practical</td><td rowspan="2">CIE</td><td rowspan="2">SEE</td></tr>
<tr><td>-</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td>Total</td><td>2</td><td>2</td><td>2</td><td>0</td><td>2</td><td>20</td><td>30</td></tr>
</table>

PRACTICE:

No	Title of the Experiment
1.	Study of Computer Forensics and different tools used for forensic investigation
2.	How to Recover Deleted Files using Forensics Tools
3.	Study the steps for hiding and extract any text file behind an image file/ Audio file using Command Prompt.

4.	How to Extract Exchangeable image file format (EXIF) Data from Image Files using Exifreader Software
5.	How to make the forensic image of the hard drive using EnCase Forensics.
6.	How to Restoring the Evidence Image using EnCase Forensics
7	How to Collect Email Evidence in Victim PC
8	How to Extracting Browser Artifacts
9	How to View Last Activity of Your PC
10	Find Last Connected USB on your system (USB Forensics)
11	Comparison of two Files for forensics investigation by Compare IT software
12	Live Forensics Case Investigation using Autopsy

THIRD SEMESTER…

Course Title	**Security and Resilience**				**Course Type**		**Integrated**	
Course Code	M21TFS301	**Credits**	**3**		**Class**			
Course Structure	TLP	Credits	Contact Hours	Work Load	Total Number of Classes Per Semester		Assessment in Weightage	
	Theory	3		3				
	Practice	0	0	0	Theory	Practical	CIE	SEE
	-	-	-	-				
	Total	**3**	**3**	**3**	**39**	**-**	**50**	**50**

COURSE OVERVIEW

The course provides an overview a Cybersecurity and Cyber Resiliency strategies. This course discusses all the steps required from conception of the plan from preplanning, project management directives, cyber threat and vulnerability analysis, cyber risk and controls assessment to reporting and measurement techniques for plan success and overall strategic plan performance. Also guides to implement a truly resilient Cybersecurity framework.

COURSE OBJECTIVE (S):

The objectives of this course are to:

1. Understand the purpose of cyber resilience strategy and the associated control objectives
2. Develop Cybersecurity and Cyber Resiliency strategies
3. Demonstrates a methodology to target high risk threats
4. Evaluation of risk assessment methodologies

COURSE OUTCOMES (COs)

After the completion of the course, the student will be able to:

CO#	Course Outcomes	POs	PSOs
CO1	Understand the methodologies for efficient utilization of resources and target high risk threats	1,2,5	1
CO2	Develop a unified Cybersecurity and Cyber Resiliency strategies	1,2,3,4,5,9,12	1,2
CO3	Implement security improvement plan, including all risk assessments and project plan	1,2,3,4,5,9,12	1,2
CO4	Evaluating the performance against various risk and performance indicators	1,2,3,4,5,9,12	1,2
CO5	Develop project strategy management flow	1,2,3,4,5,9,12	1,2
CO6	Demonstrate RACI strategy development matrix	1,2,3,4,5,9,12	1,2

BLOOM'S LEVEL OF THE COURSE OUTCOMES

CO#	Bloom's Level					
	Remember (L1)	Understand (L2)	Apply (L3)	Analyze (L4)	Evaluate (L5)	Create (L6)
CO1		√				
CO2			√			√
CO3				√		
CO4				√	√	
CO5				√	√	
CO6				√	√	

COURSE ARTICULATION MATRIX

CO#/	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	2			2								3		
CO2	3	2	3	2	2				1			1	3	3	
CO3	3	1	1	1	2				1			1	3	3	
CO4	3	2	1	2	2				1			1	3	3	
CO5	3	2	1	2	2				1			1	3	3	
CO6	3	2	1	2	2				1			1	3	3	

Note: 1-Low, 2-Medium, 3-High

COURSE CONTENT

THEORY:

UNIT – 1

Why Cybersecurity and Cyber Resiliency Strategies *:The Value Proposition, The 6 STEPs for Developing and Maintaining a Cyber security and Cyber Resiliency Strategy, Cybersecurity and Cyber Resiliency Strategy Key Players, Initiating the Strategy, Triggers to Create a Corporate Cybersecurity and Cyber Resiliency Strategy, Information Security vs. Cybersecurity, Cyber Resiliency vs. Traditional Resiliency, Cybersecurity and Cyber Resiliency Strategy Life Cycle, Cyber Strategies and Cyber programs, Cybersecurity and Cyber Resiliency Architecture: Standards and Frameworks, Cyber Program Preplanning, Technical Areas of Concentration for a Cyber Program*

UNIT – 2

Steps in Developing and Maintaining a Cybersecurity and Cyber Resiliency Strategy*: Preplanning: Preparation for Strategy Development, Strategy Project Management, Cyber Threats, Vulnerabilities, and Intelligence Analysis, Cyber Risks and Controls, Assessing Current and Target States, Measuring Strategic Plan Performance and End of Year (EoY) Tasks***,** *Governance Cycles and Processes,* P*roposing New Initiatives to Mitigate Threats and Reduce Risk, Checklists and Templates*

Strategy Project Management: *Vision to Initiative Flow, Strategy Project Charter, Strategy Preparation Checklist, Strategy Timeline, Strategy Gantt Chart, Strategy Swimlane, Data Flow Diagrams for STEPs 2, 3, 4, 5, and 6, RACI Strategy Development Matrix, NIST CSF Initiative Mapping, The Final Strategy Deliverable*

UNIT – 3

Cyber Threats, Vulnerabilities, and Intelligence Analysis: *Cyber Threats, Vulnerabilities*

Cyber Risks and Controls: *Cyber Risk, IT Controls, Cyber Insurance*

Current and Target State Assessments: *Introduction to Assessments, Current State Assessments, Conducting a Current State Assessment, Unmapped Initiatives Discussion, Target State Assessment, How to Rate Current and Target States*

UNIT – 4

Measuring Strategic Plan Performance and End of Year (EoY) Tasks: *Evaluating the Strategy Against the Critical Success Factors, Key Risk Indicators (KRIs), Key Performance Indicators (KPIs), Reporting on the Strategies, Determining New Initiatives for the Next Year, End of Year Tasks*

Checklists and Templates to Help Create an Enterprise-Wide Cybersecurity and Cyber Resiliency Strategy: *Guides to Strategy Preparation, STEP 1: Preplanning: Preparation for Strategy Development, STEP 2: Strategy Project Management, STEPs 3 and 4: Cyber Threats, Vulnerabilities, Intelligence Analysis, Risks, and Controls, STEP 5: Current and Target State Assessments, TEP 6: Measuring Plan Performance and EoY Tasks*

TEXT BOOKS:

1. Carol A. Siegel Mark Sweeney, Cyber Strategy: Risk-Driven Security and Resiliency, CRS Press, Taylor & Francis Group, Auerbach Publications,2020
2. Alexander Kott ,Igor Linkov , Cyber Resilience of Systems and Networks (Risk, Systems and Decisions) 1st ed. 2019 Edition

SWAYAM/NPTEL/MOOCs:

1. Coursera – Introduction to Cyber Security Specialization
2. https://onlinecourses.nptel.ac.in/noc21_cs30/preview

<table>
<tr><td>Course Title</td><td colspan="4">IOT Security</td><td colspan="2">Course Type</td><td colspan="2">Integrated</td></tr>
<tr><td>Course Code</td><td>M21TFS302</td><td>Credits</td><td colspan="2">4</td><td colspan="2">Class</td><td colspan="2">III Semester</td></tr>
<tr><td rowspan="5">Course Structure</td><td>TLP</td><td>Credits</td><td>Contact Hours</td><td>Work Load</td><td colspan="2" rowspan="2">Total Number of Classes Per Semester</td><td colspan="2" rowspan="2">Assessment in Weightage</td></tr>
<tr><td>Theory</td><td>4</td><td>4</td><td>4</td></tr>
<tr><td>Practice</td><td>0</td><td>0</td><td>0</td><td>Theory</td><td>Practical</td><td>CIE</td><td>SEE</td></tr>
<tr><td>-</td><td>-</td><td>-</td><td>-</td><td colspan="2" rowspan="2"></td><td colspan="2" rowspan="2"></td></tr>
<tr><td>Total</td><td>4</td><td>4</td><td>4</td><td>52</td><td>00</td><td>50</td><td>50</td></tr>
</table>

COURSE OVERVIEW

IoT security is the act of securing **Internet** of Things devices and the networks they're connected to. Hardware, software and connectivity will all need to be **secure** for **IoT** objects to work effectively. Without **security**, any connected object, from refrigerators to manufacturing bots, can be hacked. Once hackers gain control, they can usurp the object's functionality and steal the user's digital data.

COURSE OBJECTIVE (S):

The objectives of this course are to:

1. Have a good working understanding of the best practices laid down by the IoT Security Foundation
2. Inculcate knowledge to be able to develop a security patching strategy and product update life-cycle.
3. Know how to research and assess IoT threats and risks as they arise.
4. Able to discuss the main threats and attacks on IoT products and services

COURSE OUTCOMES (COs)

After the completion of the course, the student will be able to:

CO#	Course Outcomes	POs	PSOs
CO1	Make use of IOT models and work effectively with security researchers on reported IoT security issues and concerns.	1 ,3, 8, 9 , 12	1
CO2	Recognize IoT security and vulnerability threats.	1 , 3, 5,9,12	1
CO3	Interpret how to secure an IoT environment	1 ,3,45, 9, 12	2
CO4	Interpret different IoT types of attacks.	1,4,5,9,12	1
CO5	Formulate Test Device Range-Latency and Capacity for IoT hardware	1,4,5,9,12	3
CO6	Design Trusted IoT Application Platforms	1,4,5,9,12	3

BLOOM'S LEVEL OF THE COURSE OUTCOMES

CO#	Bloom's Level					
	Remember (L1)	Understand (L2)	Apply (L3)	Analyze (L4)	Evaluate (L5)	Create (L6)
CO1			√			
CO2			√			
CO3		√	√	√		
CO4			√	√	√	
CO5						√
CO6						√

COURSE ARTICULATION MATRIX

CO#/ POs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	1	1	2				1	1			1	3		
CO2	3	2	3		2				1			1	3		
CO3	3	1	2	1	2				1			1		3	
CO4	3			2	2				1			1	3		
CO5	3			2	2				1			1	3		3
CO6	3			2	2				1			1	3		3

Note: 1-Low, 2-Medium, 3-High

COURSE CONTENT

THEORY:

UNIT – 1

IOT-SECURITY OVERVIEW

IoT Reference Model- Introduction -Functional View, **IoT Security Challenges**-Hardware Security Risks -Hardcoded/Default Passwords -Resource Constrained Computations -Legacy Assets Connections -Devices Physical Security, Software Security Risks -Software Vulnerabilities -Data Interception -Identification of Endpoints -Tamper Detection, **Lack of Industrial Standards.**

UNIT – 2

IOT- SECURITY & VULNERABILITY ISSUES

IoT Security Requirements -Data Confidentiality -Data Encryption -Data Authentication -Secured Access Control –**IoT-Vulnerabilities** – Secret-Key, Authentication/Authorization for Smart Devices -Constrained System Resources -Device Heterogeneity -Fixed Firmware.**IoT Attacks** -Side-channel Attacks -Reconnaissance -Spoofing -Sniffing -Neighbour -Discovery -Rogue Devices-Man-in-Middle

UNIT – 3

SECURED PROTOCOLS FOR IOT

Infrastructure-IPv6 -LowPAN , **Identification**-Electronic Product Code -uCode, **Transport**-Bluetooth -**LPWAN**, **Data** -MQTT -CoAP, **Multi-layer Frameworks**-Alljoyn,-IoTivity

UNIT – 4

SECURING INTERNET OF THINGS ENVIRONMENT

IoT Hardware -Test Device Range-Latency and Capacity -Manufacturability Test -Secure from Physical Attacks, **IoT Software -**Trusted IoT Application Platforms, -Secure Firmware Updating -Network Enforced Policy -Secure Analytics Visibility and Control

LEARNING RESOURCES:

4. https://www.postscapes.com/internet-of-things-protocols/
5. https://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_prot/index.html
6. https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html
7. https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/

JOURNALS/MAGAZINES:

1.https://ieeexplore.ieee.org/document/8600738/
2.https://ieeexplore.ieee.org/document/7005393/
3.https://scholar.google.com/scholar_lookup?title=A%20survey%20of%20secure%20middleware%20for%204.4.he%20Internet%20of%20Things&publication_year=2017&author=P.%20Fremantle&author=P.%20Scott
https://scholar.google.com/scholar_lookup?title=Internet%20of%20things%3A%20Vision%2C%20applications%20and%20research%20challenges&publication_year=2012&author=D.%20Miorandi&author=S.%20Sicari&author=F.%20De%20Pellegrini&author=I.%20Chlamtac

SWAYAM/NPTEL/MOOCs:

1. IOT Security: Mobility Security and Deception | Coursera
2. Welcome to Cybersecurity and the Internet of Things! | Coursera
3. Fundamentals of IoT Security-Udemy.

Self-Learning Exercises:

17. Explore different IOT security models
18. More exploration on Security challenges
19. Protocols for IOT Security
20. Explore applications of IOT

Course Title	Advanced topics in cyber security				**Course Type**		**Integrated**	
Course Code	M21TFS303	**Credits**	**3**		**Class**		**III Semester**	
Course Structure	TLP	Credits	Contact Hours	Work Load	Total Number of Classes Per Semester		Assessment in Weightage	
	Theory	4	4	4				
	Practice	-	-	-	Theory	Practical	CIE	SEE
	-	-	-	-				
	Total	**4**	**4**	**4**	**52**	**0**	**50**	**50**

COURSE OVERVIEW

Cybersecurity is security as it is applied to information technology. All information technology devices and facilities need to be secured against intrusion, unauthorized use, and vandalism. Additionally, the users of information technology should be protected from theft of assets, extortion, identity theft, loss of privacy and confidentiality of personal information, malicious mischief, damage to equipment, business process compromise, and the general activity of cybercriminals. The general public should be protected against acts of cyberterrorism, such as the compromise or loss of the electric power grid. Cybersecurity is a major endeavor of the IT industry. Although billions of dollars are spent annually on cybersecurity, no computer or network is immune from attacks or can be considered completely secure.

COURSE OBJECTIVE (S):

- To enable students to develop approaches that are in the frontier of cyber security engineering and research.
- To provide the student with knowledge about the state of the art in a plethora of cutting-edge cyber security topics.
- To provide the student with knowledge about how research is conducted in cyber security.
- To provide the student with knowledge about recent developments in network and application security via the utilization of newly established technologies.

COURSE OUTCOMES (COs)

After the completion of the course, the student will be able to:

CO#	Course Outcomes	POs	PSOs
CO1	Understand the fundamental pillars of cyber security research and evaluation. Must have knowledge on a broad spectrum of innovative technologies and on how they can be applied in the context of cyber security.	1,2,3,4,8,9,12	1
CO2	Identify research questions and challenges for a variety of topics in cyber security. Must be able to use various state of the art frameworks for analyzing network traffic, identifying adversaries, as well as for developing/deploying attacks.	1,2,3,5,9,12	1
CO3	Able to the ability to critically review, summarize and discuss scientific content in cyber security	1,2,3,4,8,9,12	2
CO4	Must be able to use various state of the art frameworks for analyzing network traffic, identifying adversaries, as well as for developing/deploying attacks	1,4,8,9,12	1

CO5	Carry out Computer Forensics Investigation	1,2,3,4,5	3
CO6	Hypothesize for Global Perspective on Cybercrime	1,2,3,4,5	3

BLOOM'S LEVEL OF THE COURSE OUTCOMES

CO#	Bloom's Level					
	Remember (L1)	Understand (L2)	Apply (L3)	Analyze (L4)	Evaluate (L5)	Create (L6)
CO1			√			
CO2			√			
CO3			√	√		
CO4			√	√		
CO5					√	√
CO6					√	√

COURSE ARTICULATION MATRIX

CO#/ POs	**PO1**	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**	**PSO1**	**PSO2**	**PSO3**
CO1	3	1	1	2				1	1			1	3		
CO2	3	2	3		2				1			1	3		
CO3	3	1	2	1	2				1			1		3	
CO4	3			2	2				1			1	3		
CO5	3	3	3	2	2										3
CO6	3	2	2	2	2										3

Note: 1-Low, 2-Medium, 3-High

COURSE CONTENT

THEORY:

UNIT – 1

Network Attacks ,Threat Landscape - Network Security: threats to watch , emerging threats, firewall .**Intrusion Detection And Prevention System:** IDPS - detection technologies, types of intrusion detection and prevention system (IDPS), security information and event management (SIEM), honeypot,

Network Infrastructure Security Best Practices: threats to the organization network infrastructure, best practices for network infrastructure security, critical security controls, physical security- information and communications technology: data center security – guidelines, environment security - information and communications technology

UNIT 2

addressing threats, baisc deployment questions, nstallation & configuration, securing the server platform, enforcing and maintaing security best practices, operations & maintenance, incident handling

web servers security, email security, database server security, dns servers security, web-application security versus perimeter security, attack surface, secure web application development- best practices, web application security testing, what do we need to secure?, security protocols

UNIT 3

windows security controls essential for home user, principle of least privilege(plp), autorun /autoplay, software restriction policy, browsers and security, mbsa (microsoft baseline security analyser), set up and configure windows firewall, physical security, basic guidelines for enabling security in your desktop, enabling security features in ms office, wireless network security: vulnerabilities, threats and countermeasures, wlan threats, attacks cause loss of integrity, attacks causing loss of availability, authentication attacks, attacks on encryption standards, home wireless threats, public wireless threats, malware analysis fundamentals, setting up malware analysis facility, static analysis, dynamic analysis, automatic analysis, malware collection process woth malware honeypots, memory analysis

Introduction to Cybercrime: Cybercrime: Definition and Origins of the Word, Cybercrime and Information Security, Who are Cybercriminals?, Classifications of Cybercrimes, Cybercrime: The Legal Perspectives, Cybercrimes: An Indian Perspective, Cybercrime and the Indian ITA 2000, A Global Perspective on Cybercrimes, Cybercrime Era: Survival Mantra for the Netizens. Cyberoffenses: How Criminals Plan Them: How Criminals Plan the Attacks, Social Engineering, Cyberstalking, Cybercafe and Cybercrimes, Botnets: The Fuel for Cybercrime, Attack Vector, Cloud Computing.

UNIT – 4

Understanding Computer Forensics: Introduction, Historical Background of Cyber forensics, Digital Forensics Science, The Need for Computer Forensics, Cyber forensics and Digital Evidence, Forensics Analysis of E-Mail, Digital Forensics Life Cycle, Chain of Custody Concept, Network Forensics, Approaching a Computer Forensics Investigation, Setting up a Computer Forensics Laboratory: Understanding the Requirements, Computer Forensics and Steganography, Relevance of the OSI 7 Layer Model to Computer Forensics, Forensics and Social Networking Sites: The Security/Privacy Threats, Computer Forensics from Compliance Perspective, Challenges in Computer Forensics, Special Tools and Techniques, Forensics Auditing, Antiforensics.

TEXT BOOKS:

12. https://www.cemca.org/ckfinder/userfiles/files/PG_Diploma_in_Cyber_Security/Course%20VIII_Advanced_Cyber_Security_Techniques.pdf
13. Sunit Belapure and Nina Godbole, Cyber Security: Understanding Cyber Crimes, Computer Forensics And Legal Perspectives, Wiley India Pvt Ltd, 2013
14. Surya Prakash Tripathi, Ritendra Goyal, Praveen Kumar Shukla, Introduction to information security and cyber laws, Dreamtech Press, 2015

REFERENCE BOOKS:

19. Thomas J. MowbrayA , Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions, John Wiley & Sons,
20. James Graham, Ryan Olson, Rick Howard, Cyber Security Essentials, CRC Press, 2010

JOURNALS/MAGAZINES

1) *cybersecurity.springeropen.com*
2) *academic.oup.com* › cybersecurity
3) https://www.techscience.com/journal/JCS
4) https://cyber.fiu.edu/security-journals/

SWAYAM/NPTEL/MOOCs:

1) https://www.mooc-list.com/tags/cybersecurity
2) https://www.coursera.org/specializations/cyber-security
3) https://www.cyberdegrees.org/resources/free-online-courses/

Self-Learning Exercises:

OPEN ELECTIVES….

Course Title	**Fundamentals of Cybersecurity**				**Course Type**		**Integrated**	
Course Code	M21CB302	**Credits**	**4**		**Class**		**I/II Semester**	
Course Structure	TLP	Credits	Contact Hours	Work Load	Total Number of Classes Per Semester		Assessment in Weightage	
	Theory	4	4	4				
	Practice	0	0	0	Theory	Practical	IA	SEE
	-	-	-	-				
	Total	**4**	**4**	**4**	**52**	**00**	**50**	**50**

COURSE OVERVIEW:

The fundamentals of cybersecurity course covers various concepts on providing security to networks, data, programs and other cyber infrastructure. The growing usage of internet by individuals and organizations is demanding for cyber security applications that protect cyber infrastructure and other resource to provides, therefore this course is very important and provides fundamental knowledge on cyber security.

COURSE OBJECTIVE (S):

The objectives of this course are to:

1. Explain the fundamentals of cyber security and their applications.
2. Inculcate knowledge of attacker techniques.
3. Describe integer and string vulnerabilities

4. Discuss the malicious code to steal information

COURSE OUTCOMES (COs)

After the completion of the course, the student will be able to:

CO#	Course Outcomes	POs	PSOs
CO1	Make use of fundamentals of cyber security to solve real world problems.	1 to 4, 8, 9 , 12	1
CO2	Develop solutions for defending various attacks in cyber security.	1 to 3, 5,9,12	1
CO3	Apply techniques to develop solutions to address various vulnerabilities	1 to 5, 9, 12	2
CO4	Create cyber security solutions to protect stealing information	1,4,5,9,12	1
CO5	Demonstrate Misdirection, Reconnaissance, and Disruption Methods	1,4,5,9,12	3
CO6	Summarize on stealing in formation and exploitation	1,4,5,9,12	3

BLOOM'S LEVEL OF THE COURSE OUTCOMES

CO#	Bloom's Level					
	Remember (L1)	Understand (L2)	Apply (L3)	Analyze (L4)	Evaluate (L5)	Create (L6)
CO1			√			
CO2			√			
CO3			√	√		
CO4						√
CO5					√	
CO6					√	

COURSE ARTICULATION MATRIX

CO#/	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	1	1	2				1	1			1	3		
CO2	3	2	3		2				1			1	3		

CO3	3	1	2	1	2				1			1		3	
CO4	3			2	2				1			1	3		
CO5	3			2	2				1			1			3
CO6	3			2	2				1			1			3

Note: 1-Low, 2-Medium, 3-High

Course Content:

Theory:

Contents
Unit1: **Cyber security Fundamentals: Network and security concepts**: Information assurance fundamentals,cryptography, encryption,public key encryption, domain name system, firewalls,virtualization, radio-frequency identification. **security principles**:-tokens, messaging, program execution.
Unit 2: **Attacker techniques and motivations:** Hackers cover tractks, tunneling techniques, fraud techniques, threat infrastructure.
Unit 3: **Exploitation: Techniques to gain foothold:** shell code, Integer vulnerabilities, stack overflow, string vulnerabilities, SQL Injection, malicious pdf files, race conditions, web tools, DoS conditions, bruteforce **and dictionary,** Misdirection, Reconnaissance, and Disruption Methods.
Unit 4: **Malicious code**: self replicating malicious code, evading detection and elevating privilages, rootkits, spyware, attacks against user accounts, token kidnapping, virtual machine detection, stealing in formation and exploitation.

Text Book:

1. James Graham et al, "Cyber security essentials", CRC press, 2010

Reference Books:

1. Thomos jhonson et al, "cyber security protecting critical infrastructure from cyber attack and warfare", springer, 2015.
2. Martti lehto, "Cyber security", springer, 2015

Journals/Magazines

1. Journal of cyber security
2. Springer journal of cyber security.
3. Elsevier computers and security

SWAYAM/NPTEL/MOOCs:

1. udacity – Introduction to cyber security
2. Coursera – cyber security

Self-Learning Exercises:

1. Python programming for cyber security
2. Ethical hacking and python

Course Title	**Ethical Hacking**				**Course Type**		**Soft Core**	
Course Code	M21TF3022	**Credits**	**3**		**Class**		**II Semester**	
Course Structure	TLP	Credits	Contact Hours	Work Load	Total Number of Classes Per Semester		Assessment in Weightage	
	Theory	4	4	4				
	Practice	0	0	0	Theory	Practical	CIE	SEE
	-	-	-	-				
	Total	**4**	**4**	**4**	**52**	**0**	**50**	**50**

COURSE OVERVIEW

Ethical hacking refers to the act of locating weaknesses and vulnerabilities of computer and information systems by duplicating the intent and actions of malicious hackers. Ethical hacking is also known as penetration testing, intrusion testing, or red teaming. An ethical hacker is a security professional who applies their hacking skills for defensive purposes on behalf of the owners of information systems. This course offers the insights about Casting the Establishment, Securing Permission, Wireless Hacking and Remote Control Insecurities.

COURSE OBJECTIVE (S):

The objectives of this course are to:

1. Learn aspects of security, importance of data gathering, foot printing and system hacking.
2. Learn tools and techniques to carry out a penetration testing.
3. Explain Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation.
4. Compare different types of hacking tools.

COURSE OUTCOMES (COs)

After the completion of the course, the student will be able to:

CO#	Course Outcomes	POs	PSOs
CO1	Explain aspects of security, importance of data gathering, foot printing and system hacking	1 to 4, 8, 9 , 12	1
CO2	Explain aspects of security, importance of data gathering, foot printing and system hacking	1 to 3, 5,9,12	1
CO3	Demonstrate how intruders escalate privileges.	1 to 5, 9, 12	2
CO4	Demonstrate how intruders escalate privileges..	1,4,5,9,12	1
CO5	Summarize Advanced Techniques Session Hijacking	1,4,5,9,12	3
CO6	Assess Web server hacking and web application hacking	1,4,5,9,12	3

BLOOM'S LEVEL OF THE COURSE OUTCOMES

CO#	Bloom's Level					
	Remember (L1)	Understand (L2)	Apply (L3)	Analyze (L4)	Evaluate (L5)	Create (L6)
CO1			√			
CO2			√			
CO3			√	√		
CO4					√	√
CO5				√	√	
CO6				√	√	

COURSE ARTICULATION MATRIX

CO#/ POs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	1	1	2				1	1			1	3		
CO2	3	2	3		2				1			1	2		
CO3	3	1	2	1	2				1			1		3	
CO4	3			2	2				1			1	3		
CO5	3			2	2				1			1			3

CO6	3			2	2				1			1			3

Note: 1-Low, 2-Medium, 3-High

COURSE CONTENT

THEORY:

UNIT – 1 **10hrs**

Casing the Establishment: What is foot printing, Internet Foot printing, Scanning, Enumeration, basic banner grabbing, Enumerating Common Network services. Case study: Network Security Monitoring.

UNIT – 2

Securing permission: Securing file and folder permission, Using the encrypting file system, Securing registry permissions. Securing service: Managing service permission, Default services in windows 2000 and windows XP. Unix: The Quest for Root, Remote Access vs Local access, Remote access, Local access, after hacking root.

UNIT – 3

Wireless Hacking: Wireless Foot printing, Wireless Scanning and Enumeration, Gaining Access, Tools that exploiting WEP Weakness, Denial of Services Attacks, Firewalls: Firewalls landscape, Firewall Identification-Scanning Through firewalls, packet Filtering, Application Proxy Vulnerabilities, Denial of Service Attacks, Motivation of Dos Attackers, Types of DoS attacks, Generic Dos Attacks, UNIX and Windows DoS.

UNIT – 4

Remote Control Insecurities, Discovering Remote Control Software, Connection, Weakness. VNC, Microsoft Terminal Server and Citrix ICA, Advanced Techniques Session Hijacking, Back Doors, Trojans, Cryptography, Subverting the systems Environment, Social Engineering, Web Hacking, Web server hacking web application hacking, Hacking the internet Use, Malicious Mobile code, SSL fraud, E-mail Hacking, IRC hacking, Global countermeasures to Internet User Hacking.

TEXT BOOKS:

1. Stuart McClure, Joel Scambray and Goerge Kurtz, Hacking Exposed 7: Network Security Secrets & Solutions, Tata Mc Graw Hill Publishers, 2010.

2. Bensmith, and Brian Komer, Microsoft Windows Security Resource Kit, Prentice Hall of India, 2010. **REFERENCE BOOKS:**

1. Stuart McClure, Joel Scambray and Goerge Kurtz, “Hacking Exposed Network Security Secrets & Solutions”, 5th Edition, Tata Mc Graw Hill Publishers, 2010.

2. Rafay Baloch, “A Beginners Guide to Ethical Hacking”.

3. Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, “Gray Hat Hacking The Ethical Hackers Handbook”, 3rd Edition, McGraw-Hill Osborne Media paperback (January 27, 2011)

JOURNALS/MAGAZINES

1. International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 4, Nov-Dec 2014

2. E. S. Raymond, The New Hacker's Dictionary, MIT Press, Cambridge, MA (1991).

3. S. Garfinkel, Database Nation, O'Reilly & Associates, Cambridge, MA (2000).

4.The first use of the term "ethical hackers" appears to have been in an interview with John Patrick of IBM by Gary Anthens that appeared in a June 1995 issue of Computer World

SWAYAM/NPTEL/MOOCs:

1. StationX – The Complete Ethical Hacking Course Bundle.
2. Udemy – Learn Ethical Hacking From Scratch.
3. Cybrary – The Art of Exploitation.
4. EH Academy – The Complete Cyber Security & Hacking Course.
5. Offensive Security – Metasploit Unleashed.
6. Coursera – Cryptography.

<table>
<tr><td>Course Title</td><td colspan="4">BLOCK CHAIN TECHNOLOGY</td><td colspan="2">Course Type</td><td colspan="2">Theory</td></tr>
<tr><td>Course Code</td><td>M21TF3023</td><td>Credits</td><td colspan="2">3</td><td colspan="2">Class</td><td colspan="2">I semester</td></tr>
<tr><td rowspan="5">Course Structure</td><td>TLP</td><td>Credits</td><td>Contact Hours</td><td>Work Load</td><td colspan="2" rowspan="2">13Hrs/ Semester</td><td colspan="2" rowspan="2">Assessment in Weightage</td></tr>
<tr><td>Theory</td><td>4</td><td>4</td><td>4</td></tr>
<tr><td>Practice</td><td>0</td><td>0</td><td>0</td><td rowspan="2">Theory</td><td rowspan="2">Practical</td><td rowspan="2">CIE</td><td rowspan="2">SEE</td></tr>
<tr><td>Tutorial</td><td>--</td><td>--</td><td>---</td></tr>
<tr><td>Total</td><td>4</td><td>4</td><td>4</td><td>52</td><td>0</td><td>50%</td><td>50%</td></tr>
</table>

COURSE OVERVIEW:

Course Description: Block chain is the distributed and decentralized database technology behind this crypto currency. This course explores the fundamentals of the public, transparent, secure, immutable and distributed database called block chain. Block chains can be used to record and transfer any digital asset not just currency. This course will introduce students to the workings and applications of this potentially disruptive technology. Its potential impact on financial services, government, banking, contracting and identity management.

COURSE OBJECTIVE

1. Understand the basic of Cryptography, Blockchain technology and tools

2. Demonstrate Ethereum principles and development cycle from Ethereum to bitcoin with necessary tools and techniques

3. Illustrate Wallets and client software and programming techniques with solidity and DApps

4. Analyse different Blockchain Platforms that can be used in real world applications.

COURSE OUTCOMES (COs)

After the completion of the course, the student will be able to:

CO#	Course Outcomes	POs	PSOs
CO1	Analyze various cryptography mechanisms and list out cryptography constructs for blockchain technology	1,2,3,5,6	1,2,3
CO2	Discuss various tools used for blockchain	1,2,3,5,6	1,2,3
CO3	Illustrate the concept of Ethereum for crypto currency and implementation aspects of DAO	1,2,3,5,6	1,2,3
CO4	Infer the concept of Wallets and client hardware and software for building a running client	1,2,3,5,6	1,2,3
CO5	Interpret various applications of Blockchain	1,2,3,5,6	1,2,3
CO6	Point out on Programming with solidity and DApps	1,2,3,5,6	3

BLOOM'S LEVEL OF THE COURSE OUTCOMES

CO#	Bloom's Level					
	Remember (L1)	Understand (L2)	Apply (L3)	Analyze (L4)	Evaluate (L5)	Create (L6)
CO1			√			
CO2	√	√				

CO3			√			
CO4		√	√			
CO5			√			

COURSE ARTICULATION MATRIX

CO#/ POs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	2	3	2		2	3							2	3	2
CO2	3	1	2		3	2							1	3	2
CO3	2	1	2		2	1							2	1	2
CO4	3	2	1		2	3							2	2	3
CO5	3	2	1		2	3							2	2	3
CO6	3	2	1		2	3									3

Note: 1-Low, 2-Medium, 3-High

COURSE CONTENT
THEORY

Contents
UNIT-1
Introduction to cryptography and Block chain: Introduction to cryptography-Symmetric and Public-key cryptography, Hash function, Digital Signatures-ECDSA, Memory Hard Algorithm,. **Introduction to Block chain:** Cryptographic constructs and block chain technology, Zero Knowledge Proof , Advantage over conventional distributed database, Block chain as Public Ledgers, networks, Types of Block chain.
UNIT-2
Ethereum: Crypto currency: History, Distributed Ledger, Bitcoin an overview, protocols - Mining strategy and rewards, bitcoin limitations, What Is Ethereum? Development from Bit coin to Ethereum, Ethereum vs Ether, Ethereum

netwoks, components of ethereum ecosystem, Ethereum Virtual Machine (EVM): Accounts, Transactions, Gas, Ether, Memory, Smart contracts, Truffle Design , Implementations of DAO, DAO and Intellectual Property.
UNIT-3
Wallets and client software: Nodes and miners, hardware and software requirements for building a running client, Wallets technology overview, wallet best practices. **Programming with solidity and DApps:** Data types, pre defined global variables and function, error handling, What is DApp, data storage, communication protocols, Basic DApp example: Auction DApp, Ethereum Name Service (ENS) history, specifications, and layers.
UNIT-4
Blockchain Applications: Internet of Things, Medical Record Management System, and Blockchain in Government and Block chain Security, Block chain Use Cases –Finance, Domain Name Service and future of Block chain.**Enterprise Blockchains and Applications:** Enterprise Blockchains: Hyperledger, R3 Corda, Quorum

SELF-LEARNING COMPONENT:

Distributed Ledger in Blockchain, Decentralized Applications.

TEXT BOOKS:

1. Joseph J. Bambara Paul R. Allen," Blockchain,A Practical Guide to Developing Business, Law, and Technology Solutions", McGraw-Hill Education Professional , Second edition, 2018
2. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfeder, Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press (July 19, 2016).
3. Melanie Swan "Blockchain: Blueprint for a New Economy", O'Reilly Media, Third edition, Aug 2015.
4. Andreas M. Antonopoulos, Gavin Wood "Mastering Ethereum", O'Reilly Media, Inc., November 2018
5. Joseph Holbrook "Architecting Enterprise Blockchain Solutions", Sybex, February 2020

REFERENCE BOOKS:

1. Mingjun Dai; Shengli Zhang; Hui Wang; Shi Jin "A Low Storage Room Requirement Framework for Distributed Ledger in Blockchain" Volume: 6, Pages: 22970 – 22975, Year: 2018.
2. Ruiguo Yu, Jianrong Wang, Tianyi Xu, Jie Gao Yongli An Gong Zhang, And Mei Yu "Authentication With Block-Chain Algorithm and Text Encryption Protocol in Calculationof Social Network ",Volume: 5,pp: 24944 – 24951, 09 November 2017.
3. Ashiq Anjum; Manu Sporny; Alan Sill " Blockchain Standards for Compliance and Trust" , Volume: 4, Issue: 4 ,Pages: 84 – 90,Year: 2017.
4. Morgen E. Peck; Samuel K. Moore "The blossoming of the blockchain" , Volume: 54, Issue: 10 Pages: 24 – 25, Year: 2017.
5. Inderscience Journal of blockchain and cryptocurrency.
6. Ledger Journal of Cryptocurrency and Blockchain Technology.